

## **Stellungnahme des Bundesverbandes Digitale Wirtschaft e.V. zum Verordnungsvorschlag über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM(2018) 225 final) sowie zum Richtlinien-vorschlag zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (COM(2018) 226 final)**

7. November 2019

### **Vorbemerkungen**

Der **Bundesverband Digitale Wirtschaft (BVDW) e.V.** ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld.

### **Kontakt:**

**Katharina Rieke**  
Referentin Digitalpolitik  
T: +49 30 206 218 617  
[rieke@bvdw.org](mailto:rieke@bvdw.org)

### **Einleitung**

Am 17. April 2018 hat die Europäische Kommission ihren Verordnungsvorschlag über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM(2018) 225 final) sowie einen Richtlinien-vorschlag zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (COM(2018) 226 final) vorgelegt. Der Europäische Rat hat bereits am 7. Dezember 2018 und am 8. März 2019 seine allgemeine Ausrichtung zur Verordnung sowie Richtlinie angenommen.

Obwohl das Europäische Parlament dieses Dossier in der letzten Legislaturperiode im federführenden Ausschuss für Bürgerliche Freiheit, Justiz und Inneres (LIBE) diskutiert hat, liegt noch kein Berichtsentwurf des Ausschusses vor. Zunächst wurden sogenannte „Working Documents“ verfasst, die verschiedenen Aspekte des Kommissionsvorschlags diskutieren.

Vor dem Hintergrund der Europawahl 2019 und der Wiederaufnahme der Arbeit des Europäischen Parlaments, möchte der BVDW die Gelegenheit nutzen und seine Sichtweise in die Verhandlungen miteinbringen.

### **1. Allgemeine Anmerkungen**

Es ist dem BVDW zu Beginn wichtig die E-Evidence Debatte in einen größeren Kontext einzuordnen.

Das grundlegende Ziel des E-Evidence Pakets besteht darin die Strafverfolgung in der digitalen Welt zu vereinfachen, zu verbessern und schneller zu gestalten. Dieses Ziel ist aus Sicht des BVDW zu begrüßen, da der technische Fortschritt Veränderungen,

auch in der Kommunikation, mit sich bringt die Möglichkeiten des Missbrauchs eröffnen. Eine Beschleunigung der grenzüberschreitenden Kooperation für elektronische Beweismittel ist somit unterstützenswert. Insbesondere da elektronische Beweismittel sich viel schneller verflüchtigen als herkömmliche Beweismittel. Dennoch ist der BVDW der Meinung, dass zunächst zu prüfen ist, ob dafür tatsächlich neue Regelungen notwendig sind, oder ob das bestehende europäische System der grenzüberschreitenden Strafverfolgung nicht ausreichend Mittel ermöglicht.

Man muss sich außerdem vor Augen führen, dass es in diesem Dossier um Grundrechte geht. Deswegen kann man nicht nur den einen Sicherheitsaspekt sehen, sondern muss beide Seiten der Debatte betrachten. Es geht hier um den Zugriff auf Daten und somit zusätzlich Gesichtspunkte des Datenschutzes und der Grundrechte der betroffenen Person. Auf der einen Seite diskutiert man die Stärkung des Rechts auf Privatsphäre durch die Datenschutzgrundverordnung und eine künftige ePrivacy Verordnung und will die Möglichkeiten der Datenverarbeitung radikal beschneiden. Auf der anderen Seite sollen Behörden eines Mitgliedstaates der Europäischen Union in Strafverfahren einen direkten und schnellen grenzüberschreitenden Zugriff auf personenbezogene Daten von Bürgerinnen und Bürgern eines anderen Mitgliedstaates bekommen, ohne dass dieser die Möglichkeit hat die Grundrechtskonformität zu prüfen. Der BVDW ist der Meinung, dass es der Europäischen Kommission nicht gelungen ist, einen adäquaten Interessensausgleich zu schaffen. Die in diesem Papier enthaltenen Änderungsvorschläge stehen somit unter der Prämisse der generellen Ablehnung des Kommissionsvorschlags.

Dieser allgemeine Hinweis ist vorab von großer Bedeutung, da seit geraumer Zeit nicht nur im Rahmen der E-Evidence Debatte die Zugriffsrechte des Staates gestärkt werden sollen, sondern auch in Deutschland unter anderem Staatstrojaner sowie ein Entschlüsselungszwang für Dienste wie Whatsapp diskutiert werden. Grundrechte, IT-Sicherheit und das Vertrauen der Menschen in die Technik dürfen aber dabei nicht aufs Spiel gesetzt werden.

## 2. Verordnung: Anforderungen an die Diensteanbieter (insbesondere Art. 2, 7, 9, 10)

### Vorschlag der Europäischen Kommission:

**Artikel 1(1):** (...) Diensteanbieter, der in der Union Dienstleistungen anbietet (...) unabhängig davon, wo sich die Daten befinden.

Laut **Artikel 2 (3)** des Kommissionsvorschlags sollen Kommunikationsdienste, soziale Medien, Online-Marktplätze, andere Hosting-Dienste Anbieter, Cloud-Dienste und Domain-Registrierungsstellen von den neuen E-Evidence Regelungen betroffen sein.

### **Artikel 2(4): „der/die in der Union Dienstleistungen anbietet/anbieten“**

- a) der/die juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt/versetzen, die unter Nummer 3 genannten Dienste in Anspruch zu nehmen, und
- b) eine wesentliche Verbindung zu dem/den unter Buchstabe a genannten Mitgliedstaat(en) hat/haben;

Art. 2 (6) definiert „elektronische Beweismittel“ als Beweismittel, die **zum Zeitpunkt des Erhalts** eines Zertifikats über eine Herausgabe- oder Sicherungsanordnung in elektronischer Form von einem Diensteanbieter oder in seinem Auftrag gespeichert werden und aus gespeicherten **Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten** bestehen.“

Art. 2 (12) definiert den „**Anordnungsstaat**“ als den Mitgliedstaat, in dem die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung erlassen wird.

Art. 2 (13) definiert den „**Vollstreckungsstaat**“ als den Mitgliedstaat, in dem der Adressat der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung ansässig oder niedergelassen ist und an den die Europäische Herausgabeanordnung und das Zertifikat über eine Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung und das Zertifikat über eine Europäische Sicherungsanordnung zur Vollstreckung übermittelt werden

Die betroffenen Diensteanbieter können **direkt** vom Anordnungsstaat mit einer Herausgabeanordnung (EPOC) oder einer Sicherungsanordnung (EPOC-PR) kontaktiert werden und müssen die angefragten Daten innerhalb von spätestens 10 Tagen liefern. Im Notfall sogar innerhalb von 6 Stunden. Im Fall einer Sicherungsanordnung muss die Sicherung der Daten für 60 Tage gewährleistet werden.

Gibt es für den Diensteanbieter Gründe warum er die Daten gar nicht oder nicht fristgerecht liefern kann, muss er dies dem Anordnungsstaat mitteilen. **Nur wenn der Diensteanbieter der Meinung ist, dass die Anordnung gegen die Charta der Grundrechte verstößt oder offensichtlich missbräuchlich ist, soll der Vollstreckungsstaat informiert werden.**

Anordnungen für Transaktions- und Inhaltsdaten können nur für Straftaten erlassen werden, die im Anordnungsstaat mit einer Freiheitsstrafe **im Höchstmaß von drei Jahren** geahndet werden.

## Forderungen des BVDW

### **Notifizierungsverfahren**

Aus Sicht des BVDW sind im vorgeschlagenen System der Europäischen Kommission nicht genügend Sicherheitsvorkehrungen getroffen worden. Der Europäische Rat hat dies bereits zu einem gewissen Grad mit seinem neuen **Artikel 7a** verbessert.

Der BVDW ist der Meinung, dass die Einführung eines **Notifizierungsverfahrens** unbedingt notwendig ist. Allerdings nicht nur für Inhaltsdaten, wie vom Europäischen Rat vorgeschlagen, sondern in allen Fällen und für alle Daten, die in den Anwendungsbereich der Gesetzgebung fallen. Der Anordnungsstaat sollte das Zertifikat eines EPOC und eines EPOC-PR gleichzeitig an den Vollstreckungsstaat übermitteln müssen.

Es darf nicht die alleinige Aufgabe des Diensteanbieters sein, die rechtliche Einschätzung der **Grundrechtskonformität** einer Herausgabe- oder Sicherungsanordnung

durchzuführen und zu entscheiden, ob die Anordnung missbräuchlich ist oder nicht. Diese **Prüfpflicht muss weiterhin dem Staat obliegen**.

Darüber hinaus muss sichergestellt werden, dass auch das strafrechtliche System des Vollstreckungsstaates in Betracht gezogen wird. Die Genehmigung der Anordnungen erfolgt im Anordnungsstaat, aber auch die Bemessung der Höchststrafe geht nur vom Strafrecht des Anordnungsstaates aus. Hier weicht die E-Evidence Verordnung eindeutig vom Grundsatz der doppelten Strafbarkeit ab. Dies bedeutet, dass die Herausgabe der Daten nicht davon abhängig ist, ob die Tat in dem Land, in dem die Daten angefordert werden, auch strafbar ist. Es bedarf eines lückenlosen und sicheren Systems, das auch das strafrechtliche System des Vollstreckungsstaates mitberücksichtigt. Hier sollte das Verhältnis zu der seit 2014 bestehenden Europäischen Ermittlungsanordnung in Strafsachen geprüft werden. Insbesondere, die in Artikel 11 der Richtlinie gelisteten Gründe für die Versagung der Anerkennung oder der Vollstreckung der Ermittlungsanordnung.

Aus Sicht des BVDW ist es zudem grundlegend wichtig, dass die Behörde des Vollstreckungsstaates sofort die Möglichkeit hat, die Validität der Anordnung zu prüfen. Bisher müssen Bedenken des Vollstreckungsstaates vom Anordnungsstaat nur in Betracht gezogen werden. Es bedarf hier einer klaren Verbindlichkeit.

Zur Sicherung der Presse- und Rundfunkfreiheit bedarf es zudem in der geplanten E-Evidence Verordnung zwingend fest verankerter und klar umrissener Ausnahmen für Journalistinnen und Journalisten. Der aktuelle Entwurf lässt journalistische Grundprinzipien wie das Redaktionsgeheimnis und den Informantenschutz vollkommen außer Betracht und ist in dieser Form ein nicht hinnehmbarer Eingriff in die Arbeit von Presse und Rundfunk.

### **Fristen**

Des Weiteren sind die Fristen von 10 Tagen und 6 Stunden zu kurz angelegt. Diensteanbieter sind in einem so kurzen Zeitrahmen kaum in der Lage eine adäquate Prüfung der Anordnungen durchzuführen. Es stellt sich zudem die Frage, wie die Diensteanbieter gewährleisten sollen, dass 24 Stunden am Tag und 7 Tage die Woche Mitarbeiter zur Verfügung stehen, die mögliche Anordnungen bearbeiten und im Notfall innerhalb von 6 Stunden reagieren können. Dies wäre eine sehr große Belastung. Der BVDW ist daher der Meinung, dass man diese Fristen flexibler und individueller gestalten sollte. Insbesondere sollte man hier auch die Situation von Klein- und mittelständischen Unternehmen beachten und ihnen mehr Flexibilität ermöglichen.

### **Rechtsbehelfe**

Der BVDW sieht zudem den Bereich der Rechtsbehelfe des Artikel 15ff kritisch. Sowohl die Diensteanbieter, als auch die betroffenen Personen, dessen Daten angefordert werden, müssen sich mit dem Justizsystem des Anordnungsstaates auseinandersetzen. Es sind die dortigen Gerichte, die über die Zulässigkeit der Anordnung entscheiden. Für Diensteanbieter und auch Nutzer ist dies nachteilig, da ihnen die Rechtsordnung meist fremd ist. Bisher wird keine Möglichkeit vorgesehen die Legitimität der Anordnung im Vollstreckungsstaat anzufechten.

### **Sicherheit der Daten**

Das Thema Datensicherheit muss darüber hinaus auch weiter diskutiert werden. Die Daten, die zu übermitteln sind, müssen auf eine sichere Art und Weise geteilt werden.

Zudem muss gewährleistet werden, dass der Anordnungsstaat die Daten ausschließlich im Rahmen des Strafverfahrens verwendet, für das die Anordnung ausgestellt wurde. Hierfür müssen die richtigen technischen Voraussetzungen geschaffen werden, die einen solchen Transfer sicher ermöglichen. Diese Standards sind bisher nicht in die vorgeschlagene Gesetzgebung eingearbeitet und vorgesehen.

### **Internationaler Kontext**

Abschließend möchte der BVDW auch darauf hinweisen, dass es als überaus befremdlich einzustufen ist, dass die Europäische Kommission im Juni 2019 bereits ein Verhandlungsmandat für Gespräche mit den USA zu einem E-Evidence Abkommen erhalten hat, bevor man sich überhaupt innereuropäisch auf die Ausgestaltung dieser Gesetzgebung geeinigt hat.

### **3. Richtlinie: Bereitstellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren:**

Neben der E-Evidence Verordnung wurde von der Europäischen Kommission zusätzlich eine Richtlinie im Paket vorgeschlagen. Diese regelt die Bereitstellung von gesetzlichen Vertretern der Diensteanbieter in der Union zwecks Entgegennahme, Befolgung und Durchsetzung von Beschlüssen und Anordnungen. Da die Verordnung den Anwendungsbereich sehr weit fasst, müssen laut Richtlinie auch Diensteanbieter aus nicht-Mitgliedstaaten, die Dienstleistungen in der EU erbringen, einen Vertreter in einem Mitgliedstaat für die Zwecke der Verordnung benennen. Die Diensteanbieter sind frei darin zu entscheiden in welchem Mitgliedstaat sie dies tun und ob sie einen oder mehrere benennen möchten.

Generell ist auch diese Richtlinie und ihr allgemeines Ziel zu befürworten, allerdings möchte der BVDW darauf hinweisen, dass in dieser Richtlinie nicht mehr von „elektronischen“ Beweismitteln die Rede ist, sondern nur von „Beweismitteln“. Es stellt sich somit die Frage, ob es Sinn und Zweck dieser Richtlinie ist, Vertreter zu benennen, die auch Ansprechpartner bei der Anfrage anderer Beweismittel sein sollen. Hier bedarf es aus BVDW Sicht einer Klarstellung, dass es weiterhin nur um elektronische Beweismittel geht und kein ganzheitlich neues europäisches strafrechtliches System angestrebt wird.