



Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Referentenentwurf des
Bundesministeriums für Justiz und Verbraucherschutz

**Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544
und zur Durchführung der Verordnung (EU) 2023/1543
über die grenzüberschreitende Sicherung und Herausgabe
elektronischer Beweismittel im Strafverfahren
innerhalb der Europäischen Union**

Berlin, 01.08.2025
Abt. II/ jg-kj-mh

I. - Vorbemerkung

Die Gewerkschaft der Polizei (GdP) mit über 207.000 Mitgliedern größte Polizeigewerkschaft hierzulande bedankt sich für die Gelegenheit zur Stellungnahme zum vorliegenden Referentenentwurf zur Umsetzung des europäischen E-Evidence Gesetzgebungspakets.

Die Vorschriften zur grenzüberschreitenden Sicherung und Herausgabe elektronischer Beweismittel fallen in eine Zeit, in der die Europäische Union ihre Bemühungen verstärkt, den digitalen Raum sicherheitsrechtlich zu ordnen. Das sogenannte E-Evidence-Paket stellt dabei einen ersten, wichtigen Baustein in einer Reihe legislativer Maßnahmen dar, mit denen die EU auf bestehende Herausforderungen im Bereich der digitalen Strafverfolgung reagiert. Diese Entwicklung ist eingebettet in die umfassendere sicherheitspolitische Strategie der EU-Kommission, die unter dem Titel „ProtectEU“ darauf abzielt, den Schutz der inneren Sicherheit in einer zunehmend digitalisierten Welt zu stärken. Die Vereinfachung des Zugriffs auf elektronische Beweismittel ist dabei ein zentrales Anliegen und Ausdruck der Erkenntnis, dass effektive Strafverfolgung ohne zeitgerechte und grenzüberschreitend verfügbare digitale Informationen nicht mehr möglich ist.

In diesem Zusammenhang ist jedoch auch festzustellen, dass nach wie vor **bestehende datenschutzrechtliche Hürden** zu einer faktischen Blockade digitaler Ermittlungsarbeit führen. Diese strukturellen Hemmnisse wirken sich auch bei grenzüberschreitenden Ermittlungen aus und laufen dem Ziel des E-Evidence-Pakets, eine effektivere europäische Strafverfolgung im digitalen Raum zu ermöglichen, faktisch entgegen. Die GdP fordert daher insgesamt **eine kritische Überprüfung datenschutzrechtlicher Vorgaben** vorzunehmen, die in der Praxis Ermittlungsbehörden bei der Bekämpfung schwerster Kriminalität unverhältnismäßig einschränken.

II. - Bedeutung des E-Evidence-Pakets im europäischen Sicherheitskontext

Die GdP begrüßt daher, dass zusammen mit der Strategie „ProtectEU“ und dem „Fahrplan zum Zugang zu Daten bei der Strafverfolgung“ auch ein europäischer sicherheitspolitischer Rahmen geschaffen wird, in dem die praktische Umsetzbarkeit des E-Evidence-Instruments ausdrücklich unterstützt wird – etwa durch die geplante Verbesserung sicherer Kommunikationswege, einheitlicher Austauschformate und erweiterter Zugriffsmöglichkeiten für Ermittlungsbehörden. Allerdings sind Mitgliedsstaaten bei der Implementierung des E-Evidence Pakets wie auch bei zukünftigen europäischen Instrumenten auf kraftvolle finanzielle sowie personelle Unterstützung durch die EU angewiesen, um bei der Komplexität und Summe der neuen europäischen Initiativen möglichen Vertragsverletzungsverfahren entgegenzuwirken. Ebenso weist die GdP darauf hin, dass viele zentrale Maßnahmen - wie der Ausbau interoperabler IT-Systeme oder die Vereinheitlichung von Verfahrenswegen - konsequent, gesamteuropäisch und unterstützt auch durch finanzielle Mittel der EU umgesetzt werden müssen, damit die neuen europäischen Instrumente wie die Herausgabe- und Sicherungsanordnungen auch unter Alltagsbedingungen zuverlässig und grenzüberschreitend funktionieren. Dazu gehört auch, dass diese Instrumente durch interoperable Schnittstellen mit Europol und bestehenden EU-Systemen (z. B. SIENA, QU-EST+) verbunden werden.

Die GdP fordert in diesem Zusammenhang eine deutliche personelle und finanzielle Stärkung der europäischen Sicherheitsagenturen, insbesondere von Europol, Eurojust und CEPOL. Die

erfolgreiche Umsetzung des E-Evidence-Instruments setzt voraus, dass diese Agenturen ihre koordinierenden, analysierenden und unterstützenden Funktionen wirksam erfüllen können. Insbesondere Europol muss in die Lage versetzt werden, als operatives Analysezentrum und technischer Dienstleister für die Mitgliedstaaten zu agieren – etwa durch den Ausbau seiner Innovation Lab-Infrastruktur, eine stärkere Einbindung in Interoperabilitätsprojekte sowie durch gezielte Investitionen in hochqualifiziertes Fachpersonal.

Die im Rahmen der Polizeichef-Erklärung vom April 2025 formulierten Vorschläge zur Weiterentwicklung Eurocols weisen hier den richtigen Weg und sollten durch die EU-Kommission prioritär aufgegriffen werden. In ihrer gemeinsamen Erklärung zur zukünftigen Entwicklung Eurocols unterstreichen die Polizeichefs der EU die Notwendigkeit, Interoperabilität, Informationsaustausch und Datenverarbeitung im Rahmen der europäischen Sicherheitsarchitektur zu stärken und Europol als zentralen Informations-Hub auszubauen. Diese Ziele müssen durch gezielte Finanzierung, Ausweitung der IT-Infrastruktur sowie eine europäische Polizeicloud unterstützt werden, um grenzüberschreitende Ermittlungen wirksam zu ermöglichen.

Das E-Evidence-Paket stellt in diesem Zusammenhang einen wichtigen und begrüßenswerten ersten Schritt dar: Die Möglichkeit, digitale Beweismittel durch Sicherungsanordnungen einzufrieren und in einem zweiten Schritt gezielt anzufordern, verbessert die Effizienz grenzüberschreitender Ermittlungen und sichert digitale Spuren, bevor sie gelöscht werden können.

Klar ist aber auch: Die Sicherung und Herausgabe elektronischer Beweismittel setzen deren Verfügbarkeit voraus. Deshalb hält die GdP an ihrer langjährigen Forderung fest, dass eine verpflichtende, anlasslose Vorratsdatenspeicherung erforderlich bleibt, um schwerste Straftaten effektiv bekämpfen zu können. Die nun geschaffenen Instrumente helfen nur dort weiter, wo Daten tatsächlich noch vorhanden sind, eine zielgerichtete und rechtstaatlich abgesicherte Vorratsdatenspeicherung ist daher aus Sicht der GdP unverzichtbar für eine vollständige und zukunfts feste Strafverfolgung im digitalen Raum. Vor diesem Hintergrund verweist die GdP auch auf die Bestrebungen der Europäischen Kommission, im Rahmen des „Fahrplans zum Zugang zu Daten bei der Strafverfolgung“ ein harmonisiertes EU-weites Regelwerk zur Mindestspeicherung spezifischer Datenkategorien zu schaffen. Nur durch eine europäische Lösung kann der derzeitigen Fragmentierung nationaler Regelungen begegnet und ein funktionierender, grenzüberschreitender Zugriff auf digitale Beweise gewährleistet werden. Die GdP unterstützt daher ausdrücklich die Entwicklung eines unionsweit kohärenten Rechtsrahmens zur Mindestdatenspeicherung, wie er auch im Kontext der Strategie „ProtectEU“ als sicherheitspolitisches Kernanliegen formuliert wurde.

Darüber hinaus weist die GdP mit Nachdruck darauf hin, dass die erfolgreiche Umsetzung europäischer Sicherheitsvorhaben nicht allein von rechtlichen oder technischen Maßnahmen abhängt, sondern maßgeblich auch von den Bedingungen, unter denen die Einsatzkräfte arbeiten. Der stetig steigende Koordinations-, Dokumentations- und IT-Aufwand bei grenzüberschreitenden Ermittlungen belastet bereits heute viele Polizeibeschäftigte. Die GdP fordert deshalb, im Zuge der europäischen Sicherheitsarchitektur gezielt Maßnahmen zur Verbesserung der Arbeitssituation zu ergreifen – etwa durch Entlastung bei administrativen Prozessen, die Harmonisierung von Arbeitszeit- und Einsatzregelungen sowie die Förderung europäischer Austauschformate (z. B. Erasmus+). Eine angemessene personelle Ausstattung und moderne Arbeits-

umgebungen müssen integraler Bestandteil aller neuen europäischen Sicherheitsinitiativen sein. Nur wenn die polizeilichen Beschäftigten europaweit unter guten und fairen Bedingungen arbeiten können, lassen sich die ambitionierten europäischen Sicherheitsziele auch tatsächlich verwirklichen.

III. - Zum Vorhaben

Aus Sicht der GdP ist das Vorhaben zu begrüßen. Mit der Umsetzung der Verordnung (EU) 2023/1543 und der Richtlinie (EU) 2023/1544 wird ein überfälliger Schritt vollzogen, um die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel innerhalb der Europäischen Union zu vereinfachen und effizienter zu gestalten.

Die Fallzahlen im Bereich der Internetkriminalität steigen im Zuge der weltweiten Digitalisierung auch innerhalb Europas seit Jahren kontinuierlich an. Bereits im Jahr 2018 wies der Europäische Rat darauf hin, dass in rund 85 % aller strafrechtlichen Ermittlungen digitale Beweismittel eine Rolle spielen. Heute sind elektronische Daten faktisch in nahezu jeder Strafverfolgung unverzichtbar. Zugleich handelt es sich bei diesen Delikten häufig um grenzüberschreitende Sachverhalte. Nach Angaben des Europäischen Rates sind in über 50 % aller Ermittlungsverfahren Rechtshilfeersuchen erforderlich, um elektronische Beweise zu sichern. In der Praxis erweisen sich diese Verfahren jedoch oftmals als zeitaufwendig, kompliziert und ineffektiv. Trotz einzelner Ermittlungserfolge kommt es gerade bei komplexen und transnational organisierten Tätern häufig nicht zur Anklage, weil die notwendigen Rechtshilfeprozesse scheitern oder sich zu lange hinziehen. Zahlreiche Verfahren müssen deshalb eingestellt werden, obwohl substantielle Verdachtsmomente vorliegen. Daher kann die Bedeutung eines zeitgemäßen und praktikablen Zugriffs auf digitale Beweismittel aus Sicht der Strafverfolgungsbehörden nicht hoch genug eingeschätzt werden.

Die Einführung direkter Herausgabe- und Sicherungsanordnungen gegenüber Diensteanbietern in anderen Mitgliedstaaten stellt eine Entlastung der Ermittlungsbehörden dar. Die bislang bestehenden, häufig langwierigen und bürokratisch aufwendigen Rechtshilfeverfahren werden damit in vielen Fällen entbehrlich sein. Auch die mit dem Entwurf vorgesehene klare Zuständigkeitsverteilung auf nationaler Ebene sowie die geplanten technischen und organisatorischen Rahmenbedingungen, insbesondere die Einführung standardisierter Verfahren und Fristen, sind grundsätzlich geeignet, die polizeiliche und staatsanwaltschaftliche Praxis rechtssicher und anwenderfreundlich zu gestalten.

Positiv hervorzuheben ist, dass Diensteanbieter ausdrücklich in die Pflicht genommen werden, etwa durch die verbindliche Benennung eines in der EU ansässigen Empfangsbevollmächtigten für Zustellungen im Rahmen des EBewMG. Dadurch wird eine zuverlässige und rechtssichere Zusammenarbeit mit den Ermittlungsbehörden gewährleistet. Ebenso zu begrüßen ist die Möglichkeit der Verhängung empfindlicher Bußgelder bei Verstößen gegen Pflichten nach dem EBewMG. Dies schafft einen wirksamen Anreiz zur Einhaltung der Vorgaben und stärkt die praktische Umsetzbarkeit des Gesetzes.

Problematisch sehen wir jedoch die nach wie vor ungelöste Situation im Verhältnis zu Drittstaaten, insbesondere zu den Vereinigten Staaten. Nach US-Recht ist es Diensteanbietern grund-

sätzlich verboten, bestimmte Daten, insbesondere Inhaltsdaten, an ausländische Strafverfolgungsbehörden herauszugeben, wenn sie auf Servern in den USA gespeichert sind. Gleichzeitig verpflichtet die E-Evidence-Verordnung genau diese Anbieter zur Herausgabe, wenn sie ihre Dienste in der EU anbieten. Dieser Rechtskonflikt bringt Diensteanbieter in eine Zwangslage, birgt erhebliche Rechtsunsicherheit und gefährdet letztlich die Funktionsfähigkeit des gesamten Verordnungssystems – zumal ein Großteil relevanter Daten von US-Unternehmen verwaltet wird. Die in der Verordnung vorgesehene Möglichkeit, gerichtliche Entscheidungen bei Konflikten einzuholen, bietet hier keine praxistaugliche Lösung, da sie mit erheblichem Zeit- und Rechtsrisiko verbunden ist. Weitere Verhandlungen über ein bilaterales Abkommen zwischen der EU und den USA sind daher zwingend erforderlich. Die Bundesregierung muss sich auf europäischer Ebene nachdrücklich für ein ausgewogenes und rechtssicheres Abkommen einsetzen, um dem dahinterstehenden Strafverfolgungsinteresse gerecht zu werden.