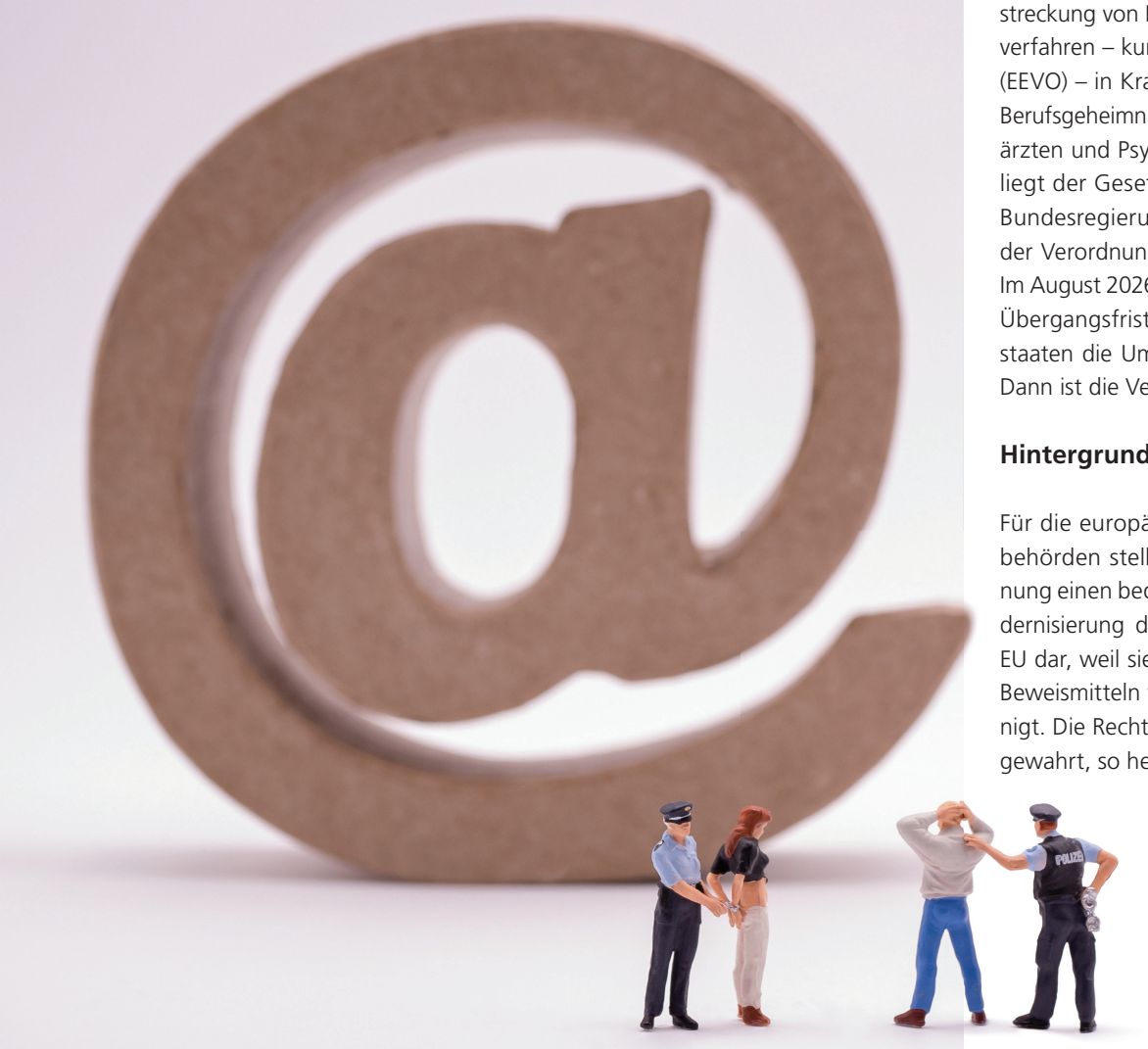
Verordnung von EU-Parlament und EU-Rat soll Strafverfolgung in Europa vereinfachen

E-Evidence ante portas

Kennen Sie die E-Evidence-Verordnung der EU? Wenn nicht, machen Sie sich schlau, denn sie kann auch Berufsgeheimnisträger wie Ärzte und Zahnärzte betreffen. Sie soll regeln, wie Strafverfolgungsbehörden in Europa schneller und einfacher an digitale Beweise kommen – zum Beispiel E-Mails, Chatverläufe oder gespeicherte Daten auf Servern. Ziel ist es, Straftaten besser aufzuklären, etwa bei Terrorismus oder Cyberkriminalität. Gleichzeitig gibt es Diskussionen über Datenschutz und die Rechte der Betroffenen.



Seit 2023 ist die Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren – kurz E-Evidence-Verordnung (EEVO) – in Kraft, relativ unbemerkt von Berufsgeheimnisträgern wie Ärzten, Zahnärzten und Psychotherapeuten. Seit Juni liegt der Gesetzentwurf der deutschen Bundesregierung zur Implementierung der Verordnung in nationales Recht vor. Im August 2026 verstreicht die dreijährige Übergangsfrist der EEVO, um Mitgliedstaaten die Umsetzung zu ermöglichen. Dann ist die Verordnung verbindlich.

Hintergrund

Für die europäischen Strafverfolgungsbehörden stellt die E-Evidence-Verordnung einen bedeutenden Schritt zur Modernisierung der Strafverfolgung in der EU dar, weil sie den Zugang zu digitalen Beweismitteln vereinfacht und beschleunigt. Die Rechte der Betroffenen blieben gewahrt, so heißt es.

Strafverfolgungsbehörden können direkt bei Dienstanbietern in anderen EU-Mitgliedstaaten Informationen anfordern, ohne dass eine Mitwirkung der Justizbehörden des ersuchten Staates erforderlich ist. Dies betrifft alle Arten elektronischer Beweismittel, einschließlich Teilnehmer-, Verkehrs- und Inhaltsdaten.

Die mit der Verordnung verbundene Europäische Herausgabeanordnung ermöglicht es, digitale Beweismittel direkt von Anbietern anzufordern. Die Anbieter sind verpflichtet, die angeforderten Daten innerhalb von zehn Tagen bereitzustellen, in Notfällen sogar innerhalb von acht Stunden. Zusätzlich soll die Europäische Sicherungsanordnung sicherstellen, dass Daten zunächst gespeichert werden können, um eine spätere Herausgabe zu ermöglichen.

Die Inhalte der Verordnung muten wie eine Passage aus Orwells 1984 an. Strafverfolgungsbehörden aus anderen EU-Mitgliedstaaten können Anbieter elektronischer Dienste direkt zur Herausgabe von Daten verpflichten – ohne vorherige Zustimmung oder Information der nationalen Justizbehörden. Auch Daten aus elektronischen Patientenakten (ePA), Praxisverwaltungssystemen oder Cloud-Diensten könnten betroffen sein. Hochsensible Patientendaten, die unter die ärztliche Schweigepflicht fallen, sollen ausländischen Ermittlungsbehörden preisgegeben werden können?

Nationales Recht am Beispiel Deutschlands

Die Bundesregierung will im Gesetzentwurf vom Juni 2025 die EU-Verordnung rechtssicher in deutsches Recht umsetzen und einen Ausgleich zwischen effektiver Strafverfolgung und dem Schutz der Grundrechte schaffen. Gleichzeitig soll der Umgang mit Daten von Ärzten, Anwälten und anderen Berufsgeheimnisträgern sensibel behandelt werden. Der Entwurf sieht vor, dass solche Daten nur unter strengen Bedingungen herausgegeben werden dürfen – etwa nur durch deutsche Behörden, wenn die betroffene Person in Deutschland lebt. Des Weiteren soll die Möglichkeit bestehen, dass bei einer Herausgabeanordnung eines ausländischen Staates, die deutsche Behörde informiert werden muss. Deutsche Behörden können laut Gesetzentwurf die Herausgabe dann verweigern, wenn z. B. Datenschutzrechte verletzt werden oder die Anordnung gegen deutsches Recht verstößt.

Betrifft das auch Zahnärzte?

Daten aus elektronischen Patientenakten (ePA), Praxisverwaltungssystemen oder Cloud-Diensten könnten betroffen sein, auch wenn die Verordnung gegenüber dem ursprünglichen Kommissionsentwurf einen „effektiven Schutz für Daten von Berufsgeheimnisträgern vor dem Zugriff staatlicher Ermittlungsbehörden gewährt". Bundeszahnärztekammer und Bundes-KZV haben sich in einer Stellungnahme an die Bundesregierung skeptisch geäußert: „Dieses Schutzniveau muss jedoch auch auf nationaler Ebene umfassend und unmissverständlich gewährleistet werden." Es geht um nichts Geringeres als hochsensible Patientendaten, die unter die ärztliche Schweigepflicht fallen und nun vor dem Zugriff ausländischer Ermittlungsbehörden geschützt werden müssen.

Arztgeheimnis gefährdet?

Bundesärztekammer (BÄK) und die Bundeszahnärztekammer (BZÄK) befürchten, die Verordnung werde nationale Schutzvorschriften wie das Beschlagnahmeverbot (§ 97 StPO) unterlaufen, da sie derzeit keine automatischen Ausnahmen für Berufsgeheimnisträger vorsieht – und die betroffenen Personen oder Institutionen (z. B. Arztpraxen) müssen nicht zwingend informiert werden, wenn ihre Daten herausgegeben werden. Das erschwert die Wahrung der Rechte der Betroffenen.

Es fehlt eine klare und umfassende Definition, welche Daten unter das Berufsgeheimnis fallen und wie diese geschützt werden sollen. BZÄK und auf europäischer Ebene der Council of European Dentists (CED) fordern seit Jahren Nachbesserungen. Auf Initiative der Bundeszahnärztekammer hatte der Council of European Dentists (CED) den EU-Gesetzgeber frühzeitig aufgefordert, das Arzt- und Berufsgeheimnisses zu wahren und entsprechende Ausnahmen in der geplanten Verordnung zu verankern: Schutz der ePA und anderer sensibler Speicherorte durch explizite Regelungen sowie die Einführung eines automatischen Beschlagnahmeverbots für vertrauliche Daten. Immerhin konnte ein Teilerfolg erzielt werden, wie beschrieben.

Rechtliche Maßnahmen

Um das Arztgeheimnis vor Zugriffen, wie sie in der E-Evidence-Verordnung vorgesehen sind zu schützen, sind sowohl rechtliche als auch technische und organisatorische Maßnahmen erforderlich. Rechtlich muss die Bundesregierung aktiv werden, um auf nationaler Ebene zu verhindern, dass Daten von Geheimnisträgern ohne richterliche Kontrolle herausgegeben werden. Auch das Beschlagnahmeverbot nach § 97 StPO müsste entsprechend ausgeweitet werden, um elektronische Daten aus Cloud-Diensten und digitalen Patientenakten zu schützen. Last, but not least müssten betroffene Personen und Institutionen über jede Datenanforderung informiert werden, um rechtliche Schritte (Widerspruch) einleiten zu können. Vor jeder Herausgabe sensibler Daten sollte eine unabhängige richterliche Prüfung erfolgen – natürlich auch bei grenzüberschreitenden Anfragen.

Daten technisch schützen

Die technischen und organisatorischen Schutzmaßnahmen reichen von der Ende-zu-Ende-Verschlüsselung sensibler Daten über das Gebot, die Datenspeicherung auf nationalen Servern laufen zu lassen bis hin zur Zugriffsprotokollierung, um Missbrauch dokumentieren zu können und letztlich zählt auch die Sensibilisie-

rung von Geheimnisträgern zum Schutz der Daten.

Verlust von Betroffenenrechten

Die Datenschutzkonferenz (DSK), also das Gremium der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern, äußert sich kritisch zur E-Evidence-Verordnung der EU. Ihre Hauptbedenken betreffen den Schutz personenbezogener Daten und die rechtsstaatliche Kontrolle bei grenzüberschreitenden Ermittlungen. In ihrer Stellungnahme vom 12. April 2024 zählt sie vier Kernpunkte ihrer Kritik an der EEVO auf: fehlende richterliche Kontrolle, Gefahr für die Grundrechte, Datenschutzstandards variieren in den EU-Staaten, Transparenz und Kontrolle fehlen, sprich Regeln zur Nachvollziehbarkeit der Datenanforderungen.

Vorläufiges Fazit

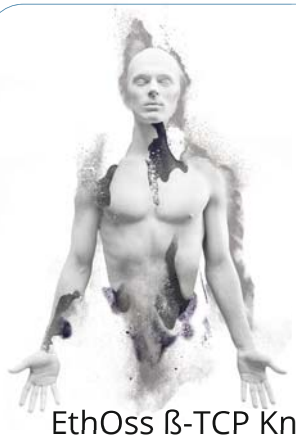
Seit dem ursprünglichen Kommissionsentwurf der E-Evidence-Verordnung gab es mehrere Änderungen und Konkretisierungen, die insbesondere die praktische Umsetzung und den Datenschutz betreffen. Beim direkten Zugriff auf Daten sind die sensiblen Daten ausgenommen, bei denen weiterhin eine Prüfung durch die Behörden des Empfängerstaats erforderlich ist.

Ab dem 18. August 2026 sind Telekommunikationsdienste und Internetprovider, aber auch alle Cloud-Servicebetreiber, Onlineshops, Portale, Foren oder sonstige für Nutzer zugängliche elektronische Dienste verpflichtet, auf Anordnung von Strafverfolgungsbehörden aus allen EU-Mitgliedsländern bestimmte Daten ihrer Nutzer herauszugeben oder vorübergehend zu speichern. Es drohen Bußgelder bei Missachtung.

AWU

Quellen: Deutsche Datenschutzkonferenz, IHK, bfdi.bund.de, EUR-lex

Ihre Top 6 Produkte Oralchirurgie



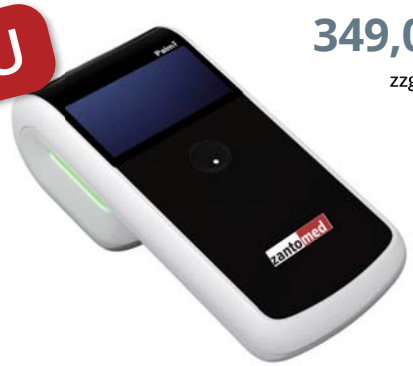
ab 349,00 €
zzgl. MwSt.

Menge	Nachlass
3-5	3% Nachlass
6-9	6% Nachlass
Ab 10 aufwärts	10% Nachlass

EthOss ß-TCP Knochenregeneration

Die besondere Formel aus 65% ß-TCP und 35% Kalziumsulfat ermöglicht die Steuerung der Viskosität von pastös bis fest und erlaubt ein Arbeiten ohne Kollagenmembran.

NEU



349,00 €
zzgl. MwSt.

Vitamin D Sofort-Test Gerät

Point-of-Care-Diagnostikgerät misst innerhalb von weniger als 15 Minuten den Gesamt-25-OHVitamin-D Spiegel; liefert in Verbindung mit einem speziellen Immunoassay-Analysator direkt am Behandlungsstuhl präzise, schnelle und zuverlässige Ergebnisse.

NEU

ab 149,00 €
zzgl. MwSt.

Root-Ex Wurzelentferner Set

Diese innovativen Harpunenstecker ermöglichen die minimalinvasive Entfernung von abgebrochenen Wurzelspitzen und Zahnfragmenten ohne operativen Eingriff.

NEU

339,00 €
zzgl. MwSt.

Vitamin D Praxis-Sofort-Test (25 Stk.)

Unsere Vitamin-D Praxis-Sofort-Tests ermöglichen eine präzise Messung des Vitamin-D-Spiegels im Blut, insbesondere des 25-Hydroxyvitamin-D (25-OH-VD), welches den besten Indikator für den Vitamin-D-Status im Körper darstellt.

Aktionspreis
ab 75,75 €
zzgl. MwSt.

Safescraper® gebogen

Safescraper® gerade

Safescraper®

Die intraorale Gewinnung von kortikalen Knochenspänen gelingt mittels dem originalen Safescraper®-Twist sicher, einfach und schnell.

NEU

139,95 €
zzgl. MwSt.

Labrida BioClean Chitosan Bürste (5 Stk.)

Oszillierende Spezialbürste für die effiziente aber schonende Periimplantitisbehandlung auf Titan und Keramikoberflächen an Implantaten

Zantomed GmbH
Ackerstraße 1 · 47269 Duisburg
info@zantomed.de · www.zantomed.de

Tel.: +49 (203) 60 799 8 0
Fax: +49 (203) 60 799 8 70
info@zantomed.de

Preise zzgl. MwSt. Irrtümer und Änderungen vorbehalten.

zantomed
www.zantomed.de