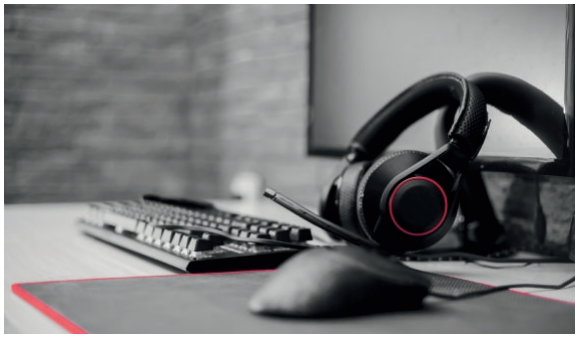
ADVANT Beiten

Datenschutz-Ticker

Februar 2025



+++ EU-KOMMISSION ZIEHT PLÄNE FÜR E-PRIVACY-VERORDNUNG UND KI-HAFTUNG ZURÜCK +++ EUGH: BUßGELDHÖHE RICHTET SICH NACH WELTWEITEM KONZERNUMSATZ +++ OLG SCHLESWIG: TRANSPORTVERSCHLÜSSELUNG BEI RECHNUNGSVERSAND PER E-MAIL UNZUREICHEND +++ ITALIEN: DATENSCHUTZBEHÖRDE BLOCKIERT DEEPSEEK +++ LEITLINIEN DER EU-KOMMISSION ZU VERBOTENEN KI-PRAKTIKEN +++

1. Gesetzesänderungen

+++ EU-KOMMISSION ZIEHT PLÄNE FÜR E-PRIVACY-VERORDNUNG UND KI-HAFTUNG ZURÜCK +++

In ihrem Arbeitsprogramm für das Jahr 2025 hat die EU-Kommission angekündigt, die Gesetzgebungsverfahren für zwei wichtige Vorhaben zu beenden. Zum einen geht es um die seit Jahren erwartete E-Privacy-Verordnung, mit der die Nutzung elektronischer Kommunikationsdienste innerhalb der EU neu geregelt werden sollte. Grund dafür sei die fehlende Einigung mit dem EU-Parlament und dass der Entwurf nicht mehr zeitgemäß sei. Zum anderen geht es um die AI Liability Directive, eine geplante Sonderregelung für die Haftung beim Einsatz und der Entwicklung von Künstlicher Intelligenz. Auch hier konnte sich die Kommission nicht mit dem Parlament einigen.

Zur Pressemitteilung der EU-Kommission (v. 12. Februar 2025)

Zum Arbeitsprogramm der EU-Kommission (v. 11. Februar 2025, Englisch)

2. Rechtsprechung

+++ EUGH: ERMESSEN DER BEHÖRDE BEI EXZESSIVEN ANTRÄGEN +++

Der Europäische Gerichtshof (EuGH) hat sich mit der Frage befasst, wann Anfragen von Verbrauchern an Datenschutzbehörden als exzessiv anzusehen sind und welche Maßnahmen die Behörden in solchen Fällen ergreifen können. Im zugrundeliegenden Fall hatte die österreichische Datenschutzbehörde die Bearbeitung einer Beschwerde eines Verbrauchers mit der Begründung abgelehnt, dass die Beschwerde exzessiv sei. Der Beschwerdeführer hatte innerhalb von 20 Monaten 77 ähnliche Beschwerden gegen verschiedene Verantwortliche eingereicht. Der EuGH entschied, dass Beschwerden nicht allein aufgrund ihrer Anzahl als exzessiv eingestuft werden können. Vielmehr müsse die Aufsichtsbehörde eine Missbrauchsabsicht des Antragstellers nachweisen. Bei exzessiven Anfragen kann die Behörde eine Gebühr verlangen oder sich weigern, tätig zu werden. Beides muss jedoch verhältnismäßig und gut begründet sein.

Zum Urteil des EuGH (v. 9. Januar 2025, C-416/23)

+++ EUGH: BUßGELDHÖHE RICHTET SICH NACH WELTWEITEM KONZERNUMSATZ +++

Der Europäische Gerichtshof (EuGH) hat entschieden, dass der Unternehmensbegriff, der für die Berechnung der Bußgeldobergrenze nach der DSGVO maßgeblich ist, kartellrechtlich zu verstehen ist. Dies bedeutet, dass bei der Verhängung einer Geldbuße der weltweite Gesamtumsatz eines Konzerns zu berücksichtigen ist. Für die Bestimmung der konkreten Höhe einer Geldbuße hat der EuGH einige zu berücksichtigende Kriterien formuliert, zu denen unter anderem die Art, die Schwere sowie die Dauer des Verstoßes, die Anzahl der von der Verarbeitung betroffenen Personen und das Ausmaß des entstandenen Schadens gehören. In jedem Fall, so betont der EuGH, muss die Geldbuße wirksam, verhältnismäßig und abschreckend sein.

Zum Urteil des EuGH (v. 13. Februar 2025, C-383/23)

+++ OLG SCHLESWIG: TRANSPORTVERSCHLÜSSELUNG BEI RECHNUNGSVERSAND PER E-MAIL UNZUREICHEND +++

Das Oberlandesgericht (OLG) Schleswig hat festgestellt, dass Unternehmen Rechnungen im B2C-Bereich, die per E-Mail versendet werden, Ende-zu-Ende verschlüsseln müssen, da eine reine Transportverschlüsselung nach der DSGVO nicht ausreicht. Ein Unternehmen hatte einem Kunden eine Rechnung per E-Mail zugesandt. Unbekannte Dritte manipulierten die Rechnung und gaben eine andere Bankverbindung an, an die der Kunde den Rechnungsbetrag von EUR 15.000 überwies. Da sich der Kunde weigerte, die Rechnung (nochmals) zu begleichen, klagte das Unternehmen. Nach Ansicht des OLG hat die Zahlung an die Betrüger zwar nicht zur Erfüllung der Forderung geführt. Dem Kunden stehe aber in Höhe der Forderung ein Schadensersatzanspruch nach der DSGVO zu, den er dem Anspruch entgegenhalten könne. Das Unternehmen hätte zwingend eine Ende-zu-Ende-Verschlüsselung einsetzen müssen, um Manipulationen zu verhindern.

Zum Urteil des OLG Schleswig (v. 18. Dezember 2024, 12 U 9/24)

+++ BGH: EUR 500 SCHADENSERSATZ WEGEN UNBERECHTIGTEN SCHUFA-EINTRAGS +++

Der Bundesgerichtshof (BGH) hat geurteilt, dass wegen eines unberechtigten SCHUFA-Eintrags ein Schadensersatzanspruch in Höhe von EUR 500 angemessen ist. Im Rahmen eines Telekommunikationsvertrages hatte das Unternehmen einen unberechtigten SCHUFA-Eintrag vorgenommen. Hiergegen wehrte sich die Kundin und verlangte wegen eines Datenschutzverstoßes immateriellen Schadensersatz in Höhe von EUR 6.000. Aufgrund des Eintrags sei ihr z. B. ein Kredit verweigert worden. Das OLG Koblenz sprach der Betroffenen jedoch lediglich eine Summe von EUR 500 zu. Der BGH weist die Revision zurück und bestätigt, dass der zugesprochene immaterielle Schadensersatz im vorliegenden Fall angemessen und verhältnismäßig sei. Ein höherer Betrag komme nicht in Betracht, da die Betroffene keinen konkreten materiellen Schaden dargelegt habe. Zudem habe der Schadensersatz nach der DSGVO nur eine Ausgleichsfunktion und keinen Genugtuungs- oder generalpräventiven Charakter.

Zum Urteil des BGH (v. 28. Januar 2025, VI ZR 183/22)

3. Behördliche Maßnahmen

+++ ITALIEN: DATENSCHUTZBEHÖRDE BLOCKIERT DEEPSEEK +++

Die italienische Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP) hat die Nutzung von DeepSeek in Italien verboten und eine Untersuchung eingeleitet. Die GPDP hatte die beiden chinesischen Betreiber des KI-basierten Chatbots aufgefordert, Informationen über die Rechtmäßigkeit und den Umfang der Verarbeitung personenbezogener Daten vorzulegen. Die Antwort von DeepSeek beschränkte sich darauf, dass die Software nicht in Italien angeboten werde und die DSGVO daher nicht anwendbar sei. Die Behörde war anderer Ansicht, da zumindest die webbasierte Version für italienische Nutzer zugänglich war und genutzt wurde. Aufgrund diverser Datenschutzverstöße und mangelnder Kooperation mit der Behörde untersagte die GPDP DeepSeek mit sofortiger Wirkung die Verarbeitung personenbezogener Daten italienischer Nutzer. Gleichzeitig leitete die Behörde eine Untersuchung gegen DeepSeek ein.

Zur Pressemitteilung der GPDP (v. 30. Januar 2025, Englisch)

Zum Beschluss der GPDP (v. 30. Januar 2025, Englisch)

+++ DEUTSCHE DATENSCHUTZBEHÖRDEN LEITEN PRÜFVERFAHREN GEGEN DEEPSEEK EIN +++

Neben der italienischen Datenschutzbehörde (siehe oben) haben auch mehrere deutsche Datenschutzaufsichtsbehörden koordinierte Prüfverfahren gegen die Anbieter des KI-Chatbots DeepSeek eingeleitet. In den Verfahren soll zunächst geklärt werden, ob die beiden hinter DeepSeek stehenden chinesischen Unternehmen einen Vertreter in der EU benannt haben. Nach der DSGVO muss jeder Verantwortliche, der Dienstleistungen für Personen in der EU erbringt, aber selbst nicht in der EU niedergelassen ist, einen Vertreter in der EU benennen. Dieser Verantwortliche dient als Anlaufstelle für Datenschutzbehörden und betroffene Personen in allen datenschutzrechtlichen Fragen. Ein Verstoß gegen diese Verpflichtung kann mit einem Bußgeld geahndet werden.

Zur Pressemitteilung der hessischen Datenschutzbehörde (v. 20. Februar 2025)

+++ SPANIEN: BUßGELD VON EUR 4 MIO. GEGEN GENERALI WEGEN DATENPANNE +++

Die spanische Datenschutzbehörde Agencia Española de Protección de Datos (AEPD) hat gegen den Versicherungskonzern Generali España ein Bußgeld in Höhe von EUR 4 Mio. verhängt, nachdem unbefugte Dritte Zugriff auf Daten von ehemaligen und aktuellen Kunden nehmen konnten. Aufgrund des Cyberangriffs wurden von den Tätern ca. 25.000 Datensätze verkauft, die u.a. Ausweiskopien und IBAN-Nummern von Kunden enthielten. Die AEPD begründete das Bußgeld mit unzureichenden technischen und organisatorischen Maßnahmen, einem Verstoß gegen Privacy by Design sowie einer unterlassenen, aber aufgrund der umfangreichen Datenverarbeitung im IT-System erforderlichen Datenschutz-Folgenabschätzung.

Zum Bußgeldbescheid der AEPD (v. 27. Januar 2025, Spanisch)

Zur Meldung auf GDPRhub (v. 27. Januar 2025, Englisch)

4. Stellungnahmen

+++ LEITLINIEN DER EU-KOMMISSION ZU VERBOTENEN KI-PRAKTIKEN +++

Die EU-Kommission hat Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz (KI) im Sinne der KI-Verordnung veröffentlicht. Die KI-Verordnung teilt KI-Systeme in verschiedene Risikokategorien ein, darunter verbotene Systeme, Hochrisikosysteme und Systeme, die Transparenzpflichten unterliegen. Die Leitlinien befassen sich mit verbotenen KI-Praktiken, die aufgrund ihres Risikopotenzials als inakzeptabel gelten, z. B. schädliche Manipulation, Social Scoring und Emotionserkennung, und enthalten rechtliche Erläuterungen und praktische Beispiele, die den Beteiligten helfen sollen, die Anforderungen der KI-Verordnung zu verstehen und einzuhalten. Damit soll eine einheitliche Anwendung der KI-Verordnung in der gesamten EU gewährleistet werden. Allerdings weist die EU-Kommission selbst darauf hin, dass die Leitlinien nicht verbindlich sind und die maßgebliche Auslegung dem EuGH vorbehalten bleibt.

Zur Pressemitteilung der EU-Kommission und den Leitlinien (v. 4. Februar 2025)

+++ EDSA VERABSCHIEDET ERKLÄRUNG ZUR ALTERSSICHERUNG +++

Der Europäische Datenschutzausschuss (EDSA) hat eine Erklärung zur Alterssicherung beschlossen. In der Erklärung listet der EDSA zehn Grundsätze für die rechtmäßige Verarbeitung personenbezogener Daten bei der Bestimmung des Alters oder der Altersspanne einer Person auf. Ziel ist es, ein kohärentes europäisches Vorgehen bei der Alterssicherung zu gewährleisten, um Minderjährige zu schützen und gleichzeitig die Grundsätze des Datenschutzes zu wahren. So betont der EDSA beispielsweise, dass der Altersnachweis nicht zu unnötigen Datenschutzrisiken für natürliche Personen führen und nicht zur Identifizierung, Lokalisierung, Profilerstellung oder Nachverfolgung von Personen über die Altersverifikation hinaus verwendet werden darf. Unternehmen müssen sich an eine strikte Zweckbindung und Datensparsamkeit halten. In vielen Fällen stellt die Altersverifikation ein hohes Risiko für die Rechte und Freiheiten der Betroffenen dar, so dass eine Datenschutz-Folgenabschätzung erforderlich ist.

Zur Pressemitteilung des EDSA (v. 12. Februar 2025)

Zur Erklärung des EDSA (v. 11. Februar 2025, Englisch)

DIGITAL COMPLIANCE - WAS UNTERNEHMEN JETZT WISSEN MÜSSEN

Die digitale Transformation bringt Chancen, aber auch neue regulatorische Herausforderungen mit sich.

Unternehmen stehen vor einer wachsenden Zahl an Vorschriften, die sicherstellen sollen, dass digitale Produkte, Dienstleistungen und Prozesse rechtlich konform und sicher sind.

Digital Compliance umfasst eine Vielzahl von Regelungen, die Unternehmen betreffen – von **Datenrecht** über **Künstliche Intelligenz (KI)** bis hin zu **Cybersicherheit** und **Plattformregulierung**. Neue Verordnungen wie die **KI-Verordnung**, **DORA** (Digital Operational Resilience Act), **CRA** (Cyber Resilience Act) oder **NIS2** (Network and Information Security Directive) haben erhebliche Auswirkungen auf die Geschäftspraxis in vielen Branchen.

Wir helfen Ihnen, den Überblick zu behalten: Über den nachfolgenden Link finden Sie die wichtigsten Informationen zu den aktuellen und kommenden regulatorischen Anforderungen – verständlich erklärt und praxisnah aufbereitet.

Bleiben Sie compliant und gestalten Sie die digitale Zukunft sicher und nachhaltig.

Digital Compliance in Europa 2025

Ihre Ansprechpartner

Für Rückfragen sprechen Sie den ADVANT Beiten Anwalt Ihres Vertrauens an oder wenden Sie sich direkt an das ADVANT Beiten Datenschutz-Team:

Büro Frankfurt
Mainzer Landstrasse 36 | 60325 Frankfurt am Main

Dr. Andreas Lober

+49 69 756095-582
vCard

Susanne Klein, LL.M.

+49 69 756095-582
vCard

Lennart Kriebel

+49 69 756095-582
vCard

Fabian Eckstein, LL.M.

+49 69 756095-582
vCard

Jason Komninos, LL.M.

+49 69 756095-582
vCard

Mirjam Kaiser

+49 69 756095-582
vCard

Büro Düsseldorf
Cecilienallee 7 | 40474 Düsseldorf

Mathias Zimmer-Goertz

+49 211 518989-144
vCard

Christian Frederik Döpke, LL.M.
+49 211 518989-144
vCard

Büro München
Ganghoferstrasse 33 | 80339 München

Katharina Mayerbacher

+89 35065-1363
vCard

Dr. Birgit Münchbach

+89 35065-1312
vCard

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH ist Mitglied von ADVANT, einer Vereinigung unabhängiger Anwaltskanzleien. Jede Mitgliedskanzlei ist eine separate und eigenständige Rechtspersönlichkeit, die nur für ihr eigenes Handeln und Unterlassen haftet. Dieser Datenschutz-Ticker wurde in Zusammenarbeit mit den ADVANT Partnerkanzleien Nctm und Altana erstellt.

REDAKTION (verantwortlich)
Dr. Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

BB-Datenschutz-Ticker@advant-beiten.com
www.advant-beiten.com

Hinweis: Zur besseren Lesbarkeit verzichten wir auf die Verwendung männlicher und weiblicher Sprachformen. Wir verwenden das generische Maskulinum, womit alle Geschlechter gleichermaßen gemeint sind.

Zur Newsletter Anmeldung

E-Mail weiterleiten

Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie künftig keine Informationen erhalten möchten, können Sie sich jederzeit abmelden.

© Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH
Alle Rechte vorbehalten 2025

Impressum

ADVANT Beiten
Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, 80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811
Weitere Informationen (Impressumsangaben) unter:
https://www.advant-beiten.com/de/impressum

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH ist Mitglied von ADVANT, einer Vereinigung unabhängiger Anwaltskanzleien. Jede Mitgliedskanzlei ist eine separate und eigenständige Rechtspersönlichkeit, die nur für ihr eigenes Handeln und Unterlassen haftet.