NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 4/2026

Levent Ferik

EDITORIAL

Im aktuellen Tätigkeitsbericht der BlnBDI ist nachzulesen, dass das Landgericht Berlin in einem Bußgeldverfahren gegen einen E-Commerce-Konzern eine Aussage getroffen hat, die über den Einzelfall hinausweist. Wer eine aufsichtsbehördliche Verwarnung erhält und den beanstandeten Zustand nicht abstellt, muss mit einem höheren Bußgeld rechnen. Die Rechtsgrundlage bilden Art. 83 Abs. 2 lit. e und lit. i Datenschutz-Grundverordnung (DS-GVO). Das ist keine Überraschung, sondern konsequente Rechtsanwendung.

In dem Sachverhalt geht es um einen „Klassiker“: Die BlnBDI hatte im Jahr 2022 einen Interessenkonflikt beim betrieblichen Datenschutzbeauftragten beanstandet. Die als DSB benannte Person war zugleich Geschäftsführer zweier konzernangehöriger Dienstleister, die Kundendaten des Unternehmens verarbeiteten. Die Behörde sprach eine Verwarnung aus und wies ausdrücklich auf die Rechtslage hin. Der Zustand blieb unverändert.

Das Gericht differenziert dabei sorgfältig. Den materiellen Verstoß bewertet es mangels besonderer Datenkategorien als gering; den Umstand des Ignorierens wertet es klar strafschärfend. Diese Unterscheidung ist sachgerecht. Sie belohnt Einsicht und Kooperationsbereitschaft, ohne Verstöße zu bagatellisieren.

Eine Verwarnung ist keine Einladung zur Risikoabwägung. Wer sie dokumentiert, intern eskaliert und abstellt, handelt richtig und darf auf Milde hoffen. Wer sie abheftet und abwartet, hat die höhere Strafe nicht nur in Kauf genommen, er hat sie sich verdient und liefert der Behörde den Beleg für systematische Mängel im Datenschutzmanagement gleich mit.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: magele-picture, Adobe Stock

Datenlöschung während laufendem Auskunftsverfahren unzulässig

Mit Gerichtsbescheid vom 21. Januar 2026 (Az. 29 K 7470/24) hat das Verwaltungsgericht Düsseldorf die Klage eines E-Mail-Marketing-Unternehmens gegen eine datenschutzrechtliche Verwarnung abgewiesen und damit eine praxisrelevante Klarstellung zum Verhältnis von Auskunftsanspruch und Löschpflicht nach DS-GVO getroffen.

Sachverhalt

Nachdem ein Betroffener im August 2022 eine unverlangte Werbe-E-Mail erhalten hatte, stellte er beim absendenden Unternehmen eine Auskunftsanfrage gemäß Art. 15 DS-GVO. Das Unternehmen übersandte zwar ein als „Datenschutzauskunft" bezeichnetes Dokument, bestätigte jedoch gleichzeitig die Löschung der Betroffenendaten – ohne dass ein Löschungsbegehren gestellt worden war. Die zuständige Aufsichtsbehörde erließ daraufhin eine Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO wegen rechtswidriger Datenverarbeitung.

Kernaussage des Gerichts

Das Gericht bestätigte die Verwarnung in vollem Umfang. Es stellte klar, dass die Erfüllung der Informationspflicht nach Art. 12 i. V. m. Art. 15 DS-GVO frühestens dann eintritt, wenn dem Antragsteller die begehrten Informationen vollständig und fristgerecht übermittelt wurden. Eine Löschung der Daten vor Abschluss des Auskunftsverfahrens ist damit rechtswidrig – unabhängig davon, ob der ursprüngliche Verarbeitungszweck (hier: E-Mail-Marketing) noch fortbesteht. Der Auskunftsanspruch selbst begründet einen eigenständigen Verarbeitungszweck, der die Datenspeicherung bis zur vollständigen Erfüllung rechtfertigt und gebietet. Darüber hinaus wies das Gericht darauf hin, dass das Vorgehen des Unternehmens auch die Überprüfung der Rechtmäßigkeit der ursprünglichen Datenerhebung faktisch vereitelt habe – ein Umstand, der nach Einschätzung des Gerichts auch die Verhängung eines Bußgelds gerechtfertigt hätte.

Bedeutung für die Praxis

Verantwortliche sollten sicherstellen, dass interne Prozesse eine voreilige Datenlöschung bei laufenden Betroffenenanfragen ausschließen. Eingehende Auskunftsersuchen sind konsequent zu dokumentieren, und Löschvorgänge dürfen erst nach vollständiger, nachweisbarer Erfüllung der Auskunftspflicht erfolgen. Das Urteil unterstreicht zudem die Bedeutung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO.

Foto: Thanaporn, Adobe Stock

Kennzeichnungspflichten für KI-generierte Inhalte

Die Wettbewerbszentrale hat im Februar 2026 einen Leitfaden veröffentlicht, der Unternehmen Orientierung bei der wettbewerbsrechts- und KI-verordnungskonformen Nutzung KI-generierter Inhalte geben soll. Im Fokus stehen Kennzeichnungspflichten nach Art. 50 KI-Verordnung der EU (KI-VO) 2024/1689, die ab dem 2. August 2026 vollumfänglich gelten.

Deepfakes und KI-Bilder

Betreiber – also alle Unternehmen und Selbstständigen, die KI-Systeme beruflich einsetzen – sind verpflichtet, Bild-, Ton- oder Videoinhalte zu kennzeichnen, die als Deepfake im Sinne des Art. 3 Nr. 60 KI-VO einzustufen sind. Entscheidend ist dabei nicht allein die abstrakte Ähnlichkeit mit realen Personen oder Objekten, sondern auch, ob der Inhalt geeignet ist, beim Betrachter fälschlicherweise einen wahren Eindruck zu erwecken. Die Wettbewerbszentrale empfiehlt, im Zweifel zu kennzeichnen, insbesondere bei realistisch wirkenden Personendarstellungen in Werbemitteln. Auch KI-generierte „AI Models", die eigene Social-Media-Auftritte betreiben, fallen nach aktueller Einschätzung unter diese Pflicht.

KI-Texte und redaktionelle Kontrolle

Für KI-generierte Texte gilt eine Kennzeichnungspflicht nur bei öffentlichkeitsrelevanten Inhalten – und auch dort entfällt sie, wenn eine natürliche oder juristische Person die redaktionelle Verantwortung übernimmt. Werbetexte sind daher in der Regel nicht kennzeichnungspflichtig, sofern geschulte Mitarbeitende die Endkontrolle ausüben. Die Kennzeichnung muss in jedem Fall klar, verständlich und barrierefreiheitskonform erfolgen. Ein optisch wahrnehmbarer Hinweis vor dem Text gilt als ausreichend.

Chatbots, KI-Avatare und AI Washing

Beim Einsatz von Chatbots und KI-Avataren ist zu Beginn jeder Interaktion transparent zu machen, dass keine menschliche Kommunikation stattfindet. Ein Hinweis wie „KI-unterstützt" genügt dabei nicht, da er keine eindeutige Abgrenzung zur menschlichen Bearbeitung ermöglicht. Zusätzlich warnt die Wettbewerbszentrale vor sogenanntem „AI Washing": Wer Produkte fälschlicherweise als KI-basiert bewirbt, verstößt gegen das UWG-Verbot irreführender Werbung – unabhängig von der KI-VO. Der Grundsatz lautet: Wer KI verspricht, muss KI liefern.

Foto: Design Stock, Adobe Stock

EuGH: Banken haften auch ohne Verurteilung ihrer Organmitglieder

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 29. Januar 2026 (C-291/24) entschieden, dass die EU-Geldwäscherichtlinie einer nationalen Regelung entgegensteht, die Sanktionen gegen juristische Personen von der förmlichen Feststellung der Schuld natürlicher Personen abhängig macht. Das Urteil stärkt die Durchsetzbarkeit von Compliance-Anforderungen im Finanzsektor.

Weiter auf DataAgenda lesen

Foto: Bartek, Adobe Stock

Kündigung wegen mangelhafter Bearbeitung einer Whistleblower-Meldung

Das Arbeitsgericht Offenbach hat mit Urteil vom 25. November 2025 (Az. 1 Ca 136/25) in einem arbeitsrechtlich bedeutsamen Fall entschieden: Die außerordentliche fristlose Kündigung eines General Counsel eines Konzerns war unwirksam, die hilfsweise ordentliche Kündigung hingegen sozial gerechtfertigt.

Sachverhalt

Im Oktober 2023 ging beim Konzern eine Whistleblower-Meldung über mutmaßlich rechtswidrige Praktiken bei der Hauslos-Gewinnung in einer Tochtergesellschaft ein. Der Kläger – als Group General Counsel Mitglied des Group Management Committee und fachlicher Vorgesetzter des Compliance Officers – war Teil des internen Untersuchungsteams. Die Untersuchung wies erhebliche Mängel auf: Die Konzernrevision wurde entgegen der internen Verfahrensordnung nicht eingebunden, der Abschlussbericht lag erst elf Monate später vor, und die Kommunikation gegenüber dem Hinweisgeber sowie gegenüber den Abschlussprüfern fiel verharmlosend aus. Die rechtswidrigen Praktiken wurden erst im März 2025 vollständig abgestellt.

Kernaussagen des Gerichts

Die fristlose Kündigung scheiterte teilweise an der nicht gewährten Zwei-Wochen-Frist des § 626 Abs. 2 Bürgerliches Gesetzbuch (BGB): Mehrere Kündigungsvorwürfe waren dem Unternehmen bereits seit Dezember 2024 bekannt, sodass die Frist insoweit abgelaufen war. Im Übrigen beurteilte das Gericht das Fehlverhalten als Schlechtleistung, die typischerweise keine außerordentliche Kündigung rechtfertigt.
Die ordentliche Kündigung hingegen erwies sich als wirksam. Das Gericht stellte fest, dass aus der herausgehobenen Funktion des General Counsel – unabhängig von einer ausdrücklichen Vertragsregelung – besondere Überwachungs-, Kontroll- und Schadensabwehrpflichten erwachsen. Diese hatte der Kläger über mehr als ein Jahr schuldhaft verletzt, indem er Verfahrensverstöße des Compliance Officers unkommentiert ließ und die Geschäftsführung nicht über Missstände informierte. Eine Abmahnung war entbehrlich, da dem Kläger angesichts seiner exponierten Stellung klar sein musste, dass derartige Pflichtverletzungen nicht toleriert würden.
Einen Anspruch auf Weiterbeschäftigung bis zum Ablauf der Kündigungsfrist verneinte das Gericht ebenfalls – die besondere Vertrauensposition des General Counsel stand einer Weiterbeschäftigung entgegen.

Foto: Anna Lurye, Adobe Stock

Altersverifikation und Algorithmen-Regulierung für sichere soziale Medien

Die SPD-Bundestagsfraktion hat Mitte Februar 2026 ein Impulspapier zum Schutz von Kindern und Jugendlichen in sozialen Medien vorgelegt. Es skizziert ein gestuftes Regulierungsmodell, das den Jugendschutz mit datenschutzrechtlichen Anforderungen verknüpft und dabei zentral auf die europäische EUDI-Wallet setzt.

Altersgestufte Zugangsregelung

Das Papier schlägt ein dreistufiges Modell vor: Für Kinder unter 14 Jahren soll die Nutzung sozialer Medien vollständig untersagt werden; Plattformen werden zur technischen Durchsetzung verpflichtet. Jugendliche zwischen 14 und 16 Jahren sollen ausschließlich auf algorithmusfreie Jugendversionen zugreifen dürfen – ohne personalisierte Feeds, Endlos-Scrollen, Push-Benachrichtigungen oder Gamifizierung. Der Zugang erfolgt nur nach Verifikation durch die Erziehungsberechtigten via EUDI-Wallet. Ab 16 Jahren sollen algorithmische Empfehlungssysteme standardmäßig deaktiviert sein (Opt-in-Modell).

Datenschutzkonforme Altersverifikation

Ein zentrales Anliegen des Papiers ist die DS-GVO-konforme Ausgestaltung der Altersverifikation. Die EUDI-Wallet soll lediglich die Zugehörigkeit zu einer Altersgruppe bestätigen, ohne die Identität der nutzenden Person offenzulegen. Anonymität und Pseudonymität sollen so gewahrt bleiben, während Bot-Netzwerke und koordinierte Fake-Accounts eingedämmt werden. Die Autoren betonen, dass bestehende nationale Jugendschutzlösungen bei der europäischen Weiterentwicklung berücksichtigt werden müssen.

Durchsetzung und KI-Transparenz

Für Verstöße gegen Plattformvorgaben fordert das Papier ein abgestuftes Sanktionsinstrumentarium bis hin zu temporären Netzsperren als Ultima Ratio. Ergänzend wird auf die Kennzeichnungspflichten der KI-Verordnung verwiesen. Diese dürften im Rahmen laufender Vereinfachungsinitiativen nicht abgeschwächt werden. Sollte bis Sommer 2026 keine europäische Einigung erkennbar sein, behalten sich die Unterzeichner ausdrücklich nationalstaatliche Regelungen vor.

Foto: Sina Ettmer, Adobe Stock

FAQ-Katalog zum KI-Einsatz in Steuerkanzleien

Die Bundessteuerberaterkammer (BStBK) hat jüngst einen umfangreichen FAQ-Katalog zum Einsatz künstlicher Intelligenz im steuerberatenden Berufsstand ⭳ veröffentlicht. Das Dokument adressiert praxisrelevante Fragen aus den Bereichen Datenschutz, Berufsrecht, Tool-Governance und Qualitätssicherung – und ist damit auch für Datenschutzbeauftragte in Kanzleien von unmittelbarer Relevanz.

Datenschutz und Berufsgeheimnis als zentrale Leitplanken

Der Katalog stellt klar: Mandantendaten dürfen grundsätzlich nicht in öffentlich zugängliche KI-Dienste wie ChatGPT eingegeben werden, sofern keine ausreichende vertragliche Absicherung besteht. Die berufsrechtliche Verschwiegenheitspflicht nach § 57 Steuerberatungsgesetz (StBerG) und § 203 Strafgesetzbuch (StGB) gilt technologieneutral – also auch beim Einsatz von künstlicher Intelligenz (KI). Sollen mandatsbezogene Daten verarbeitet werden, sind entweder eine Anonymisierung oder der Abschluss eines Auftragsverarbeitungsvertrags sowie einer Verschwiegenheitsvereinbarung nach § 62a StBerG erforderlich. EU-basierte Anbieter sind ausdrücklich zu bevorzugen; bei Drittstaatenanbietern – insbesondere außerhalb der EU – gelten erhöhte Anforderungen.

DS-GVO-Compliance und Datenschutz-Folgenabschätzung

Sobald KI-Systeme personenbezogene Daten verarbeiten, greifen vollumfänglich die DS-GVO-Grundsätze: Rechtsgrundlage, Datenminimierung, Zweckbindung, Löschkonzepte und Drittstaatentransfers müssen geprüft und dokumentiert sein. Die Aufsichtsbehörden verlangen nach Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung, wenn der KI-Einsatz voraussichtlich hohe Risiken für Betroffenenrechte birgt. In diesem Fall entsteht auch für kleinere Kanzleien die Pflicht zur Bestellung eines Datenschutzbeauftragten.

KI-Kompetenz als Betreiberpflicht

Kanzleien, die KI eigenverantwortlich einsetzen, gelten als Betreiber im Sinne von Art. 3 Nr. 4 KI-VO und sind nach Art. 4 KI-VO verpflichtet, für ausreichende KI-Kompetenz ihres Personals zu sorgen. Eine gesetzliche Pflicht zur Nutzung von KI oder zur Bestellung eines KI-Beauftragten besteht nicht – die Bundessteuerberaterkammer empfiehlt jedoch ausdrücklich, einen internen Ansprechpartner zu benennen sowie ein KI-Verzeichnis als Compliance-Werkzeug einzuführen. Fachliche Endverantwortung verbleibt stets beim Berufsträger; KI-Ergebnisse sind grundsätzlich kritisch zu prüfen und dürfen nicht ungeprüft übernommen werden.

Foto: Wolfilser, Adobe Stock

Aufbewahrung von Steuerunterlagen unter Beachtung des Datenschutzrechts

Die Bundessteuerberaterkammer (BStBK) hat Anfang des Jahres 2026 ihren FAQ-Katalog zur digitalen Aufbewahrung ⇩ aktualisiert. Das Dokument behandelt handels- und steuerrechtliche Aufbewahrungspflichten nach Handelsgesetzbuch (HGB), Abgabenordnung (AO) sowie den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) und greift dabei an mehreren Stellen datenschutzrechtlich relevante Fragestellungen auf.

Aufbewahrungsfristen und Grundprinzipien

Die Aufbewahrungsfristen betragen zehn Jahre für Jahresabschlüsse und Handelsbücher, acht Jahre für Buchungsbelege und Rechnungen (ab 2025) sowie sechs Jahre für sonstige Unterlagen. Die BStBK empfiehlt aus Gründen der Rechtssicherheit – insbesondere im Hinblick auf steuerstrafrechtliche Exkulpationsmöglichkeiten und Fördermittelrecht – eine einheitliche Frist von mindestens zehn Jahren anzuwenden. Anlauf- und Ablaufhemmungen nach §§ 170, 171 Abgabenordnung (AO) können die Fristen erheblich verlängern.

Digitaler Jahresabschluss und elektronische Signatur

Jahresabschlüsse, die originär elektronisch aufgestellt und qualifiziert elektronisch signiert wurden, sind als Original digital aufzubewahren. In Papierform erstellte Abschlüsse hingegen müssen weiterhin im Original in Papierform verbleiben – ein ersetzendes Scannen ist hier unzulässig. Sonstige Unterlagen können GoBD-konform digitalisiert und elektronisch aufbewahrt werden. Die eIDAS-Verordnung unterscheidet dabei drei Signaturarten mit unterschiedlicher Beweiskraft; die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift rechtlich gleichgestellt.

DS-GVO-Schnittstellen: Löschfristen, Schwärzen und Drittlandtransfers

Der FAQ-Katalog widmet einen eigenen Abschnitt den datenschutzrechtlichen Anforderungen im Aufbewahrungskontext. Das Speicherbegrenzungsgebot nach Art. 5 Abs. 1 lit. e DS-GVO steht in einem Spannungsverhältnis zu gesetzlichen Aufbewahrungspflichten, die als Rechtsgrundlage nach Art. 6 Abs. 1 lit. c DS-GVO dienen. Vor Löschvorgängen ist stets eine organisatorische Freigabe einzuholen; automatisierte Löschungen nach Fristablauf sind ohne vorherige Prüfung unzulässig. Bei Betriebsprüfungen sind Datenzugriffe inhaltlich und zeitlich zu begrenzen; nicht prüfungsrelevante personenbezogene Daten sind durch geeignete Zugriffsbeschränkungen oder digitales Schwärzen zu schützen. Für die Auslagerung an Drittlandsanbieter gelten die Anforderungen aus Kapitel 5 DS-GVO sowie die Folgen der Schrems-II-Entscheidung des EuGH – eine Einzelfallprüfung des Schutzniveaus bleibt zwingend erforderlich.

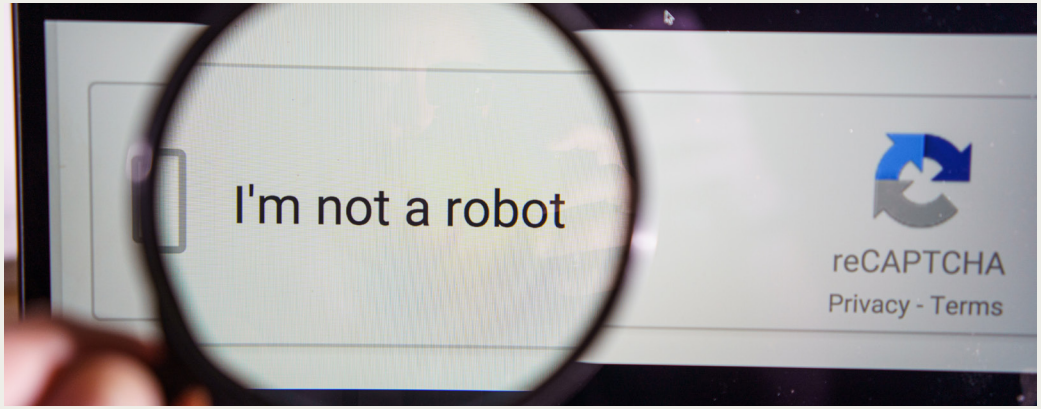

Foto: Rokas, Adobe Stock

Google ändert datenschutzrechtliche Rolle bei reCAPTCHA

Ab dem 2. April 2026 wechselt Google bei seinem Bot-Schutzdienst reCAPTCHA von der Rolle des Verantwortlichen (Data Controller) in die des Auftragsverarbeiters (Data Processor). Dies hat unmittelbare Konsequenzen für alle Websitebetreiber, die reCAPTCHA einsetzen: Sie werden künftig selbst zum datenschutzrechtlichen Verantwortlichen im Sinne der DS-GVO. Darüber hat Google die relevanten Nutzerkreise sowohl per E-Mail als auch über einen entsprechenden Blogbeitrag informiert.

Was sich ändert

Die Datenverarbeitung durch reCAPTCHA wird ab April 2026 nicht mehr unter Googles allgemeiner Datenschutzerklärung und Nutzungsbedingungen erfolgen, sondern auf Grundlage des Google Cloud Data Processing Addendum. Die bisherigen Verweise auf Googles Datenschutzrichtlinie im reCAPTCHA-Badge werden von Google selbst entfernt. Websitebetreiber, die diese Verweise zusätzlich eigenständig in ihre Datenschutzdokumentationen oder Webseiten integriert haben, werden aufgefordert, diese ebenfalls zu entfernen.

Handlungsbedarf für Verantwortliche

Datenschutzbeauftragte und Websitebetreiber sollten prüfen, ob und wo Verweise auf Googles Datenschutzerklärung im Zusammenhang mit reCAPTCHA bestehen – etwa in Cookie-Hinweisen, Datenschutzerklärungen oder im Quellcode. Diese Verweise sind nach dem 2. April 2026 inhaltlich nicht mehr zutreffend. Darüber hinaus empfiehlt sich die Prüfung, ob ein Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO mit Google abzuschließen bzw. zu aktualisieren ist.

Kritische Einordnung aus der Community

In der Diskussion zum Blogbeitrag weisen Datenschutzpraktiker auf eine strukturelle Spannung hin: Obwohl Websitebetreiber formal die Rolle des Verantwortlichen übernehmen, bleiben Zweck und Mittel der Verarbeitung durch Google weitgehend vorgegeben. Die Frage, inwieweit eine echte Weisungsbefugnis gegenüber Google im Rahmen des standardisierten Vertragswerks besteht, bleibt offen. Google hat angekündigt, die zugehörige Dokumentation vor dem 2. April 2026 zu aktualisieren.

(Möglicherweise) rechtswidrige Dashcam-Aufnahme als Beweismittel zugelassen

Das Landgericht Frankenthal (Pfalz) hat mit Urteil vom 7. Juli 2025 (Az. 5 O 4/25) entschieden, dass Videoaufnahmen einer in einem geparkten Fahrzeug verbauten Rundum-Kamera in einem Zivilverfahren als Beweismittel verwertet werden dürfen – auch wenn ein Datenschutzverstoß nicht ausgeschlossen werden kann.

Foto: RoClickMag, Adobe Stock

Sachverhalt

Ein Tesla-Fahrer parkte sein Fahrzeug am Straßenrand und öffnete die hintere Fahrertür, um sein Kind aus dem Auto zu holen. Ein vorbeifahrender Opel kollidierte mit der geöffneten Tür und verursachte einen Schaden von über 8.000 Euro. Der Opel-Fahrer bestritt die Schuld und behauptete, die Tür sei für ihn unvermittelt geöffnet worden. Die Bordkamera des Tesla hatte den gesamten Vorgang aufgezeichnet.

Entscheidung des Gerichts

Die Kammer ließ die Videoaufnahme als Beweismittel zu und verurteilte den Opel-Fahrer sowie dessen Versicherung zur Zahlung von 70 Prozent des entstandenen Schadens. Das Video belegte, dass die Tür bereits deutlich geöffnet war, bevor der Opel die Stelle passierte, und der Unfall damit vermeidbar gewesen wäre. Den Tesla-Fahrer trifft ein Mitverschulden von 30 Prozent, da er die Tür über einen längeren Zeitraum weit geöffnet stehen ließ.

Datenschutzrechtliche Einordnung

Besonders relevant ist die datenschutzrechtliche Abwägung des Gerichts: Ein etwaiger Datenschutzverstoß führe nicht automatisch zu einem Verwertungsverbot. Videoaufnahmen seien jedenfalls dann prozessual verwertbar, wenn sie lediglich neutrale Verkehrsvorgänge dokumentieren und das Beweisinteresse des Geschädigten das Datenschutzrecht des Unfallgegners überwiegt. Diese Interessenabwägung fiel hier zugunsten des Tesla-Fahrers aus. Das Urteil ist noch nicht rechtskräftig; Berufung wurde zum Pfälzischen Oberlandesgericht Zweibrücken eingelegt.

DATA AGENDA PODCAST

Der **Experten-Talk** mit
Prof. Dr. Schwartmann

(Quelle: TH Köln/Schmülgen)

Folge #87

Reformbedarf bei der DSGVO: Eine Parallelspur für den Digitalomnibus

Dr. Stefan Brink

Folge #88

NIS-2: Regulierung als Chance oder Bürokratie-monster?

Dr. Judith Nink

Folge #89

KI Omnibus
Update März 2026

Kai Zenner

Folge #90

KI Omnibus Update März 2026 reloaded: Reallabore Spezial

Andreas Jaspers, Prof. Dr. Tobias Keber, Prof. Dr. Dr. Felix Sahm, Dr. Dominik Roderburg, Kai Zenner





Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Stefan Waldeisen
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter