

NEWS BOX

DATENSCHUTZ



INHALTSVERZEICHNIS

- 2 Editorial
- 3 Kennzeichnung KI-generierter Werbeeinhalte
- 4 Kein Anspruch auf vollständige Kopie eines Compliance-Berichts
- 5 Praxisleitfaden zu KI-Systemen mit geringem Risiko
- 6 Auskunftsanspruch eines Kindes nach DS-GVO
- 7 Double-Opt-In-Nachweis anhand von IP-Adressen ist nicht ausreichend
- 8 GI fordert Reform für ethisches Hacking
- 9 Kopplungsverbot: Newsletter-Anmeldung für Kundenkonto
- 11 Impressum

AUSGABE

10/2026



Levent Ferik

EDITORIAL

Es hätte eine Zahl unter vielen sein können: 1,44 Millionen Dateien, knapp 5,8 Terabyte. Doch seit die Hackergruppe „Rhysida“ Anfang September ihre Beute aus dem Angriff auf zwei Berliner Senatsverwaltungen im Darknet veröffentlicht hat, ist daraus etwas sehr Konkretes geworden: Zugangsdaten, Personalakten, Verträge, Gehaltsdaten und eine KRITIS-Analyse der Berliner Wasserversorgung. Was Ende August als Erpressungsversuch begann, ist damit zu einem der gravierendsten bekannt gewordenen Cyber- und Datenvorfälle einer deutschen Landesverwaltung geworden. Bemerkenswert ist dabei weniger der technische Ablauf – ein kompromittierter Fernzugang, gefälschte Captcha-Abfragen, die klassische Rhysida-Handschrift – als das, was danach passierte. Berlin zahlte kein Lösegeld. Konsequenz – aber die „Rechnung“ kam prompt: Nach Ablauf des Ultimatums standen die Daten frei zugänglich im Netz. Für die Betroffenen ändert das wenig an der Ausgangslage: Sie haben nichts falsch gemacht und tragen trotzdem das Risiko von Identitätsdiebstahl,

Phishing mit echten internen Informationen und im schlimmsten Fall der Erpressung Einzelner mit ihren eigenen Daten.

Der Vorfall zeigt, wie schnell aus einem eigentlich „banalen“ Ransomware-Fall auch ein Vertrauensproblem für demokratische Prozesse werden kann, wenn hochsensible Verwaltungsdaten erst einmal öffentlich sind.

Für Datenschutzbeauftragte und Compliance-Verantwortliche liefert der Fall damit reichlich Diskussionsstoff, weit über Berlin hinaus: Wie belastbar sind die eigenen Meldeprozesse nach Art. 33/34 der Datenschutz-Grundverordnung (DS-GVO), wenn sich ein Angriff über Wochen entwickelt, statt an einem Tag aufzuschlagen? Wie kommuniziert man mit zehntausenden Betroffenen, deren Daten in einem einzigen Leak stecken? Und wie viel Redundanz und Segmentierung verträgt eine Verwaltung, deren digitale Dienste laut eigener Aussage weiterhin nur eingeschränkt verfügbar sind?



Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com



Kennzeichnung KI-generierter Werbeeinhalte

Die Wettbewerbszentrale hat einen Leitfaden zu den Kennzeichnungspflichten für KI-generierte Inhalte in der Werbung [↓](#) vorgelegt, der die seit dem 2. August 2026 geltenden Transparenzvorschriften der KI-Verordnung (Art. 50 KI-VO) mit dem lauterkeitsrechtlichen Rahmen des Gesetzes gegen den unlauteren Wettbewerb (UWG) verzahnt.

Deepfakes bei Bild, Ton und Video

Nach Art. 50 Abs. 4 KI-VO müssen Betreiber – definiert als jede Person oder Organisation, die ein KI-System beruflich nutzt, unabhängig von Unternehmensgröße – offenlegen, wenn erzeugte oder manipulierte Bild-, Ton- oder Videoinhalte als „Deepfake“ gemäß Art. 3 Nr. 60 KI-VO einzustufen sind. Entscheidend sind zwei kumulative Kriterien: Ähnlichkeit mit realen Personen, Objekten oder Orten sowie die Eignung, fälschlicherweise als echt zu erscheinen. Der Leitfaden empfiehlt, den Begriff „Ähnlichkeit“ weit auszulegen – realistisch wirkende, aber frei erfundene Motive genügen bereits, während offensichtlich unrealistische Darstellungen (Fabelwesen, surreale Kombinationen) ausgenommen bleiben. Die Täuschungseignung hängt maßgeblich vom Einzelfall ab, insbesondere von der Zielgruppe, der Technikaffinität, der Bildauflösung und dem

Kontext der Nutzung. Auch sogenannte AI-Models mit eigenen Social-Media-Profilen dürften danach regelmäßig kennzeichnungspflichtig sein. Bloße KI-gestützte Retuschen zur Fehlerbeseitigung (z. B. Rauschreduzierung) lösen dagegen keine Kennzeichnungspflicht aus.

Text, Chatbots und Avatare

Für Texte greift die Kennzeichnungspflicht nur eingeschränkt: Sie betrifft ausschließlich öffentlichkeitsrelevante Inhalte und entfällt bei menschlicher redaktioneller Kontrolle. Werbliche Texte dürften daher meist unbeeinträchtigt bleiben. Für Chatbots und KI-Avatare gilt hingegen nach Art. 50 Abs. 1 KI-VO eine strengere Vorgabe: Nutzer müssen zu Beginn der Interaktion klar informiert werden, dass sie mit einem KI-System und nicht mit einem Menschen kommunizieren, es sei denn, dies ist offensichtlich. Eine Kennzeichnung als lediglich „KI-unterstützt“ ist laut Leitfaden unzureichend, da sie über eine reine Mensch-KI-Interaktion hinwegtäuschen kann. Sämtliche Kennzeichnungen müssen gemäß Art. 50 Abs. 5 KI-VO klar, eindeutig, maschinenlesbar und barrierefrei gestaltet sein. Bei technikfernen Zielgruppen rät die Wettbewerbszentrale zu deutschsprachigen Hinweisen statt englischer Begriffe.

Haftung und AI-Washing

Der Leitfaden verweist auf eine wachsende Zahl von Gerichtsentscheidungen, die Unternehmen für fehlerhafte KI-Aussagen in die Haftung nehmen – wie etwa das Oberlandesgericht (OLG) Hamm im Fall eines Chatbots, der Ärzten falsche Facharzttitel zuschrieb. Als eigenständiges Problemfeld behandelt der Leitfaden zudem das „AI-Washing“: Die Bewerbung von Produkten als KI-basiert, obwohl keine entsprechende Technologie zum Einsatz kommt, stellt nach Auffassung der Wettbewerbszentrale eine irreführende Geschäftspraxis nach dem UWG dar und ist unabhängig von der KI-VO bereits nach geltendem Wettbewerbsrecht unzulässig.

Organisationen, die KI-generierte Werbemittel einsetzen, sollten im Zweifel eine Kennzeichnung vornehmen und dabei prüfen, ob die Sprache, die Platzierung und die Gestaltung der jeweiligen Zielgruppe tatsächlich verständlich sind – zumal viele Auslegungsfragen zur „Ähnlichkeit“ und Täuschungseignung nach eigener Einschätzung der Wettbewerbszentrale noch nicht gerichtlich geklärt sind.



Kein Anspruch auf vollständige Kopie eines Compliance-Berichts

Das Bundesarbeitsgericht hat mit Urteil vom 16.04.2026 (8 AZR 169/25) [🔗](#) klargestellt, dass sich das datenschutzrechtliche Auskunftsrecht nach Art. 15 Abs. 1 i. V. m. Abs. 3 S. 1 DS-GVO grundsätzlich nur auf die in einem Dokument enthaltenen personenbezogenen Daten bezieht und nicht auf das Dokument als Ganzes.

Sachverhalt

Eine leitende Angestellte war Gegenstand einer arbeitgeberseitig beauftragten Compliance-Untersuchung wegen des Vorwurfs eines einschüchternden Führungsverhaltens. Der daraus resultierende Abschlussbericht, in zwei Fassungen – mit und ohne ergänzende rechtliche Ausführungen und Mandantenhinweise –, enthielt neben Feststellungen zum Sachverhalt auch namentlich benannte Hinweisgeber sowie anwaltliche Wertungen zur Glaubhaftigkeit von Zeugenaussagen. Die Betroffene verlangte gestützt auf Art. 15 DS-GVO die vollständige Kopie beider Berichtsfassungen. Die Vorinstanz hatte ihr lediglich ein Einsichtsrecht in eine Fassung zugesprochen.

Entscheidung des Gerichts

Das Bundesarbeitsgericht (BAG) bestätigte unter Bezugnahme auf die einschlägige Rechtsprechung des Europäischen Gerichtshofs (EuGH), u. a. „FT“, „Österreichische Datenschutzbehörde“, dass Art. 15 Abs. 3 DS-GVO lediglich eine Modalität der Anspruchsausübung nach Art. 15 Abs. 1 DS-GVO regelt und untrennbar mit diesem verbunden ist. Die Kopie muss zwar sämtliche personenbezogenen Daten vollständig und in verständlicher Form wiedergeben; ein eigenständiger Anspruch auf das Dokument als solches besteht jedoch nicht. Nur wenn die Kontextualisierung zur Verständlichkeit der Daten unerlässlich ist, kann sich der Anspruch ausnahmsweise auf Auszüge oder ganze Dokumente erstrecken.

Zwar enthielt der Bericht, bezogen auf das Führungsverhalten der Klägerin, personenbezogene Daten im weiten Sinne von Art. 4 Nr. 1 DS-GVO, der nach ständiger Rechtsprechung des EuGH auch subjektive Bewertungen und Stellungnahmen erfasst. Die zusätzlich enthaltenen rein rechtlichen Ausführungen und Mandantenhinweise stellte das Gericht jedoch nicht als Informationen „über“ die betroffene Person dar, sondern lediglich als Ausdruck der rechtlichen Einschätzung des Verantwortlichen. Da die Klägerin diese Bestandteile nicht zur Ausübung ihrer Betroffenenrechte (Berichtigung, Löschung, Einschränkung) benötigte, bestand kein Anspruch auf eine (auch nur teilgeschwärzte) Gesamtkopie. Ergänzend verneinte der Senat auch einen entsprechenden Anspruch aus § 83 Abs. 1 Betriebsverfassungsgesetz (BetrVG) bzw. § 26 Abs. 2 Sprecherausschussgesetz (SprAuG), da das dortige Einsichtsrecht in die Personalakte ebenfalls nicht auf eine vollständige Kopie sämtlicher Unterlagen gerichtet ist.

Verantwortliche können Auskunftsansprüche nach Art. 15 DS-GVO zu internen Untersuchungsberichten auf die darin enthaltenen personenbezogenen Daten begrenzen und rein rechtliche Bewertungen, Prozessstrategien oder Mandantenhinweise regelmäßig ausklammern, sofern deren Kenntnis zur Verständlichkeit der übrigen Daten nicht erforderlich ist.



Praxisleitfaden zu KI-Systemen mit geringem Risiko

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) hat im Juli 2026 einen praxisorientierten Leitfaden zum datenschutzkonformen und digital-souveränen Einsatz Künstlicher Intelligenz vorgelegt. Adressiert werden explizit Verantwortliche in kleineren Verwaltungen sowie in kleinen und mittleren Unternehmen (KMU), die KI-Systeme mit begrenztem oder minimalem Risiko im Sinne der KI-VO einsetzen – etwa interne Chatbots oder Tools zur Textzusammenfassung. Damit schließt der LfDI bewusst eine Lücke zu bestehenden Orientierungshilfen, die sich überwiegend auf komplexere Hochrisikosysteme konzentrieren.

Weiter auf DataAgenda lesen [↗](#)

Eine Jubiläumsbühne für den Datenschutz.

**Hybrid:
Online &
in Köln**

50. DAFTA

12.-13. November 2026

45. RDV-Forum

11. November 2026

Künstliche Intelligenz – Werkzeug oder Partner? Herausforderungen für den Datenschutz!

Jetzt anmelden: www.dafta.de

Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT



Auskunftsanspruch eines Kindes nach DS-GVO

Das Verwaltungsgericht Berlin hat mit Urteil vom 30.06.2026 (Az. 42 K 41/25) [↗](#) entschieden, dass ein sorgeberechtigter, getrennt lebender Elternteil ohne Zustimmung des anderen Elternteils keine Übersendung der kindbezogenen Entwicklungsdokumentation einer Kindertagesstätte im Wege des Auskunftsanspruchs nach Art. 15 DS-GVO verlangen kann.

Sachverhalt

Der Kläger, der gemeinsam mit der von ihm getrennt lebenden Kindesmutter das Sorgerecht für den gemeinsamen minderjährigen Sohn hat, hatte bei der Leitung einer Kindertagesstätte Auskunft über die zu seinem Sohn gespeicherten personenbezogenen Daten verlangt (konkret die Übersendung der Entwicklungsdokumentationen). Die Einrichtung verweigerte dies mangels Zustimmung der Kindesmutter. Die daraufhin

vom Kläger angerufene Berliner Beauftragte für Datenschutz und Informationsfreiheit stellte in ihrer Abschlussnachricht keinen Verstoß gegen die DS-GVO fest und verwies auf die familienrechtliche Klärungsbefähigung der Vertretungsfrage. Der Kläger klagte auf Neubescheidung seiner Beschwerde.

Entscheidung des Gerichts

Das Gericht bestätigte zunächst den Prüfungsmaßstab für aufsichtsbehördliche Beschwerdebescheide: Nach Art. 57 Abs. 1 lit. f DS-GVO i. V. m. Art. 77 DS-GVO muss die Behörde den Sachverhalt in angemessenem Umfang aufklären. Ob ein Verstoß gegen die DS-GVO vorliegt, unterliegt voller gerichtlicher Kontrolle, während der Behörde beim aufsichtlichen Einschreiten selbst (Art. 58 Abs. 2 DS-GVO) ein nur eingeschränkt überprüfbarer Ermessensspielraum zusteht – unter Verweis auf die einschlägige EuGH-Rechtsprechung zur zweistufigen Prüfung.

In der Sache bestätigte das Gericht, dass die betroffene Person im Sinne des Art. 15 DS-GVO der Sohn ist und der Kläger nur mit wirksamer Vertretungsmacht als dessen Vertreter handeln konnte. Diese fehlte hier: Nach § 1687 Abs. 1 S. 1 Bürgerliches Gesetzbuch (BGB) ist bei getrennt lebenden, gemeinsam sorgeberechtigten Eltern für Angelegenheiten von erheblicher Bedeutung für das Kind das gegenseitige Einvernehmen erforderlich. Das Gericht ordnete das Auskunftsverlangen als eine solche erheblich bedeutsame Angelegenheit ein, da die Entwicklungsdokumentation als fachliche Grundlage für gemeinsam zu treffende Bildungsentscheidungen, etwa zur Wahl der Bildungseinrichtung, diene. Öffentliche und private Stellen, die mit Auskunftersuchen einzelner sorgeberechtigter Elternteile für gemeinsame Kinder konfrontiert sind, sollten prüfen, ob das Auskunftsbegehren eine für das Kind erheblich bedeutsame Angelegenheit betrifft. Ist dies der Fall, ist grundsätzlich das Einvernehmen beider Elternteile erforderlich, bevor Auskunft nach Art. 15 DS-GVO erteilt werden kann.



Double-Opt-In-Nachweis anhand von IP-Adressen ist nicht ausreichend

Das Verwaltungsgericht Düsseldorf hat mit Urteil vom 27.07.2026 (Az. 29 K 9714/24) [↗](#) die Anforderungen an den Einwilligungsnachweis nach Art. 7 Abs. 1 DS-GVO konkretisiert und die Klage eines Onlinemarketing-Unternehmens gegen eine datenschutzrechtliche Verwarnung abgewiesen.

Sachverhalt

Ein Beschwerdeführer hatte sich mehrfach, zuletzt im Jahr 2024, bei der zuständigen Aufsichtsbehörde gemeldet, weil er unerwünschte Werbe-E-Mails von der klagenden Gesellschaft erhielt, ohne jemals eine Einwilligung dazu erteilt zu haben. Zum Nachweis der behaupteten Einwilligung legte die Klägerin lediglich die E-Mail-Adresse, eine IP-Adresse

nebst Zeitstempel sowie eine Double-Opt-In-IP-Adresse nebst Zeitstempel vor. Die eigentliche Bestätigungs-E-Mail konnte sie nicht vorlegen, obwohl ihr eigenes, der Behörde gegenüber beschriebenes, Verfahren gerade die Speicherung solcher Bestätigungs-E-Mails vorsah. Die Aufsichtsbehörde sprach daraufhin eine Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO aus.

Entscheidung des Gerichts

Das Gericht bestätigte die Rechtmäßigkeit der Verwarnung in vollem Umfang. Zentral ist die Beweislastregel des Art. 7 Abs. 1 DS-GVO: Beruft sich der Verantwortliche auf eine Einwilligung als Rechtsgrundlage, muss er deren Erteilung nachweisen können. Gelingt dieser Nachweis nicht, gilt die Einwilligung als nicht bzw. nicht wirksam erteilt – mit denselben Rechtsfolgen wie bei einer tatsächlich fehlenden Einwilligung.

In der Sache stellte das Gericht klar, dass IP-Adressen für einen solchen Nachweis strukturell ungeeignet sind. Da eine IP-Adresse einem Gerät und nicht einer bestimmten Person zugeordnet ist und zwischen E-Mail-Adresse und IP-Adresse kein notwendiger Zusammenhang besteht, lassen sich daraus weder die Identität des Einwilligenden noch der Inhalt der übermittelten Erklärung ableiten. Dies gelte nach Auffassung des Gerichts gleichermaßen für die beim Double-Opt-In-Verfahren erfasste zweite (Bestätigungs-)IP-Adresse.

Für einen tragfähigen Einwilligungsnachweis reicht die bloße Protokollierung von IP-Adressen und Zeitstempeln nicht aus. Erforderlich ist regelmäßig die tatsächliche Speicherung und Vorlagefähigkeit der Bestätigungserklärung selbst. Unternehmen sollten zudem sicherstellen, dass ihre dokumentierten Double-Opt-In-Prozesse in der betrieblichen Praxis auch tatsächlich eingehalten werden, da Abweichungen – wie hier das Nichtvorhalten der Bestätigungs-E-Mail – zulasten des Verantwortlichen gewertet werden.



GI fordert Reform für ethisches Hacking

Die Gesellschaft für Informatik e. V. (GI) hat gemeinsam mit LOAD e. V. – Verein für liberale Netzpolitik, der AG KRITIS sowie Fachexpert*innen ein Whitepaper [📄](#) vorgelegt, das eine grundlegende Reform der §§ 202a–c des Strafgesetzbuches (StGB) fordert. Grundlage hierfür sind drei Workshops und mehrere Expertengespräche im Mai/Juni 2026 zum Thema „Responsible Disclosure“.

Das Kernproblem

Nach geltendem Recht macht sich strafbar, wer unbefugt auf gesicherte Daten zugreift – und zwar unabhängig von der Motivation. Wer eine Schwachstelle entdeckt und meldet, belastet sich damit faktisch selbst. Besonders der stark kritisierte § 202c StGB kriminalisiert bereits die Herstellung und Verbreitung sogenannter „Hacker*innen-Tools“, was auch legitime Sicherheitsforschung (etwa Pen-Tests, Reverse

Engineering oder Dekompilieren) erschwert. Als Präzedenzfall dient der Fall „Modern Solutions“: Ein IT-Experte wurde verurteilt, obwohl er eine E-Commerce-Sicherheitslücke im Sinne des Kundenschutzes aufgedeckt hatte. Das Bundesverfassungsgericht bestätigte im Jahr 2024 die Verurteilung.

Die Rechtsunsicherheit betrifft mehrere Rechtsgebiete gleichzeitig: neben dem Strafrecht auch das Abhörverbot nach § 5 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), § 42 Abs. 2 Bundesdatenschutzgesetz (BDSG), das Geschäftsgeheimnisgesetz (§ 5 GeschGehG) sowie urheberrechtliche Vorschriften zum Dekompilieren (§§ 69d, e Urheberrechtsgesetz (UrhG)). Auch datenschutzrechtlich bleibt unklar, wie sich Art. 32 DS-GVO (der Verantwortliche ist zur Überprüfung seiner technisch-organisatorischen Maßnahmen verpflichtet) mit dem strafrechtlichen Risiko für externe Tester*innen verträgt.

Empfehlungen der GI

Zentrale Forderung ist die Einführung einer Schädigungsabsicht als zusätzliches Tatbestandsmerkmal in den §§ 202a–b StGB, sodass die Beweislast auf die Herstellerseite verlagert wird. Zudem solle eine unzureichende Sicherung (z. B. unverschlüsselte Passwörter) nicht als „besondere Sicherung“ im Sinne des § 202a StGB gelten. § 202c StGB solle nicht die Werkzeuge, sondern nur deren missbräuchliche Verwendung sanktionieren. Als Vorbilder werden Polen, Portugal und Belgien genannt, die ethisches Hacking unter bestimmten Voraussetzungen bereits straffrei stellen.

Ausdrücklich abgelehnt werden dagegen ein Hacker*innen-Register sowie eine Pflicht zur De-Anonymisierung Meldender, da beides zeitkritische Meldungen verzögern und das Risiko von Repressionen erhöhen würde. Die GI verweist zudem auf den ab September 2026 greifenden Cyber Resilience Act, dessen verpflichtende Meldewege um freiwillige Meldemöglichkeiten für externe Forschende ergänzt werden sollten.



Kopplungsverbot: Newsletter-Anmeldung für Kundenkonto

Das Oberlandesgericht (OLG) München hat mit Urteil vom 23.04.2026 (Az. 29 U 599/24 e [↗](#)) entschieden, dass Onlinehändler die Registrierung eines Kundenkontos nicht an die gleichzeitige Einwilligung zum Newsletter-Bezug koppeln dürfen, wenn den Nutzern dabei keine echte Wahlmöglichkeit verbleibt. Geklagt hatte ein Verbraucherschutzverband gegen einen Shoppingclub-Betreiber, dessen Bestätigungs-E-Mail zur Kontoregistrierung zugleich als Double-Opt-In für den Newsletter fungierte. Eine gesonderte Ablehnungsoption fehlte. Den Kunden blieb nur der nachträgliche Widerruf.

Verstoß gegen das Koppelungsverbot

Das Gericht stützte seine Entscheidung auf Art. 7 Abs. 4 DS-GVO. Eine Einwilligung gilt danach nicht als freiwillig, wenn die betroffene Person faktisch keine andere Wahl hat, als der Datenverarbeitung zuzustimmen, um eine Leistung in Anspruch nehmen zu können. Unter Bezugnahme auf die Rechtsprechung des EuGH (u. a. im Verfahren „Orange România“) stellte der Senat klar, dass eine „ungebührliche Beeinträchtigung“ der Willensfreiheit bereits dann vorliegt, wenn die Verweigerung der Einwilligung nicht ebenso schnell und einfach zum gewünschten Ergebnis führt wie deren Erteilung. Da die beklagte Vertragspartei keine gleichwertige Alternative – etwa einen Gastzugang – anbot, war die vertragscharakteristische Leistung (Lieferung reduzierter Markenartikel) auch objektiv ohne Newsletter-Zusendung erfüllbar. Die Kopplung ging damit über das zur Vertragserfüllung Erforderliche hinaus.

Einordnung als Marktverhaltensregelung

Bemerkenswert ist die zweite Kernaussage des Urteils: Das OLG München bestätigt unter Verweis auf die Entscheidung des Bundesgerichtshofs (BGH) „Arzneimittelbestelldaten II“, dass Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11 und Art. 7 Abs. 4 DS-GVO zugleich Marktverhaltensregelungen im Sinne des § 3a UWG darstellen. Ein Verstoß gegen die DS-GVO-Einwilligungsanforderungen kann somit unmittelbar lauterkeitsrechtliche Unterlassungsansprüche begründen – auch losgelöst von einem Verfahren nach dem Unterlassungsklagengesetz (UKlaG).

Verantwortliche sollten Double-Opt-In-Prozesse dahingehend prüfen, ob eine echte Ablehnungsmöglichkeit gleichwertig zur Zustimmung angeboten wird, und Gastzugänge als datenschutzkonforme Alternative in Betracht ziehen.



DATA AGENDA
PODCAST

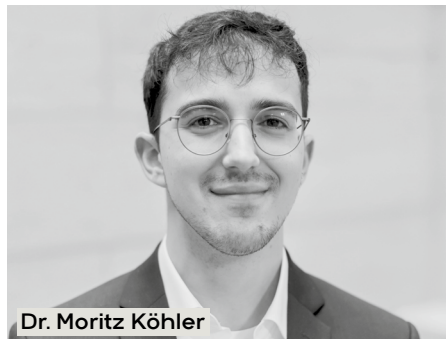


(Quelle: TH Köln/Schmügel)

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

Folge #97

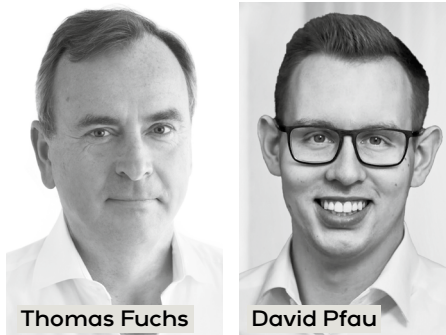
Künstliche Intelligenz in
Justiz und Verwaltung
zwischen Unterstützung
und Ersetzung



Dr. Moritz Köhler

Folge #98

Privacy by smart Design –
Smarte Brillen in schönen
Farben



Thomas Fuchs

David Pfau

DataAgenda Podcast Folge 97: Künstliche Intelligenz in Justiz und Verwaltung zwischen Unterstützung und Ersetzung

Der Einsatz Künstlicher Intelligenz (KI) durch Gerichte in der Rechtsprechung muss gleich mehrere rechtliche Hürden überwinden. Sie ergeben sich vordringlich aus dem Grundgesetz, das nur den menschlichen Richter kennt. Er darf sich aber unterstützen lassen. Wo die Grenze zur Ersetzung überschritten ist, besprechen ich mit Dr. Moritz Köhler, Experte für richterliche Verantwortung und Künstliche Intelligenz. Auch in der Verwaltung darf der Staat sich von KI nur helfen lassen. Insgesamt sind dabei Blicke in die DSGVO und die KI-VO unverzichtbar, wenn es um Entscheidungen geht, die von oder mit Hilfe von KI getroffen werden. Unter der Überschrift Staatsmodernisierung sollen mit KI Verwaltungsverfahren optimiert werden. Auch darum geht es im Podcast.

Zum Podcast bitte [hier](#)  klicken.

DataAgenda Podcast Folge 98: Privacy by smart Design – Smarte Brillen in schönen Farben

Smarte Brillen sind auf dem Vormarsch und viele Argumente pro und contra sind ausgetauscht. Ein DataAgenda-Datenschutz-Podcast kommt natürlich nicht ohne eine Diskussion der Probleme der DS-GVO und des TDDDG aus. Sie gehen von der Reichweite der Haushaltsausnahme, über Fragen der Zulässigkeit und der Betroffenenrechte bis hin zur Zulässigkeit des Produkts nach dem TDDDG, denn natürlich muss für Brillen, in denen Kameras und Mikrophone versteckt sind, auch ein Verbot diskutiert werden. Wenn man aber Technik nicht verhindern will, sondern Produkte regulieren muss, kommt es vor allem auf die Produktgestaltung an. Darüber, wie man smarte Brillen so kenntlich machen kann, dass man sie in ihrer Funktion erkennt und über weitere Fragen geht es im Gespräch mit Thomas Fuchs, dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und David Pfau, dem Geschäftsführer von conneri. Zum Podcast bitte [hier](#)  klicken.

Weitere Folgen unter DataAgenda.de/podcast 

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



Datenschutz- Awareness nachhaltig stärken

Interaktive E-Learning-Kurse mit echter
Moderation statt KI-Stimme

Unsere E-Learning-Kurse:

- ✓ Von GDD-Expert/innen entwickelt
- ✓ TV-Studio-Qualität mit professioneller Moderation
- ✓ vollanimierte Lerneinheiten, Study Buddy, Micro-Learning
- ✓ Barrierefrei nach BFGG
- ✓ Full-Service: Onboarding inklusive

Jetzt kostenfrei testen: www.datakontext.com/elearning

UNIVADO

 DATAKONTEXT