

# NEWS BOX

DATENSCHUTZ



## INHALTSVERZEICHNIS

- 2 Editorial
- 3 Inkasso und Datenschutz
- 4 Urheberrechtsschutz für KI-assistierte Werke
- 5 Personalakten sind nicht Teil des Bewerbungsverfahrens
- 6 „Recht auf Löschen“ in der Praxis – erhebliche Umsetzungsdefizite europaweit
- 7 Novelliertes Kirchliches Datenschutzgesetz (KDG) in Kraft getreten
- 8 Datenschutzkonforme Anwesenheitsübersicht im Zeiterfassungssystem
- 9 Mieterselbstauskunft: Datenschutzaufsicht zieht klare Grenzen
- 10 Biometrischer Abgleich mit Bildern aus dem Internet: Bundestag-Gutachten sieht KI-VO-Verstoß
- 12 Impressum

AUSGABE

# 5/2026



Levent Ferik

## EDITORIAL

SPD und CDU haben sich für ein Social-Media-Verbot unter 14 Jahren ausgesprochen. Der Impuls ist verständlich, die Lösung aber zu kurz gedacht. Verbote verlagern Risiken nur – Kinder weichen auf andere Plattformen aus, melden Probleme seltener und erwerben weniger Medienkompetenz.

Der Verbraucherzentrale Bundesverband (vzbv) benennt in seinem Positionspapier vom März 2026 das eigentliche Problem präzise: Nicht der Internetzugang an sich schadet, sondern das Design der Plattformen. Autoplay, Endlos-Scrollen, engagement-optimierte Algorithmen und personalisierte Werbung auf Basis umfassender Profilbildung – das sind die strukturellen Risiken. Ein Mindestalter ändert daran nichts. Der vzbv fordert stattdessen sichere Grundeinstellungen als verbindlichen Default für alle Konten: private Profile, deaktivierte Standortfreigabe, eingeschränkte Kontaktoptionen, keine personalisierte Werbung und standardmäßig deaktivierte In-Game-Käufe.

Aus Datenschutzsicht kommt ein weiterer Punkt hinzu: Eine flächendeckende Altersverifikationspflicht als Zugangshürde erzwingt die Erhebung personenbezogener Daten aller Nutzerinnen und Nutzer – unverhältnismäßig und kontraproduktiv. Überzeugender ist der Ansatz des vzbv, eine Altersverifikation nur dort einzusetzen, wo Volljährige bewusst restriktive Einstellungen aufheben wollen, und das strikt datenminimiert, etwa über die EUDI-Wallet. Ein wirksamer Jugendschutz im digitalen Raum ist aufwendiger als ein Verbot, denn er erfordert klare technische Vorgaben, die konsequente Durchsetzung und Aufsicht. Der vzbv-Ansatz zeigt, dass das regulatorisch möglich ist. Gut, dass dieser Vorschlag jetzt auf dem Tisch liegt.



---

**Sagen Sie uns Ihre Meinung**  
[kundenservice@datakontext.com](mailto:kundenservice@datakontext.com)

# Inkasso und Datenschutz

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat einen praxisorientierten FAQ-Katalog zu datenschutzrechtlichen Fragen im Inkassowesen [veröffentlicht](#). Das Dokument enthält auch für Datenschutzbeauftragte bei Unternehmen mit Inkasso-Bezug relevante Klarstellungen.



Foto: studio v-zwoelf, Adobe Stock

## Datenweitergabe und Rechtsgrundlagen

Inkassodienstleister erhalten Schuldnerdaten vom ursprünglichen Gläubiger. Eine gesonderte Einwilligung der betroffenen Person ist nicht erforderlich; Rechtsgrundlage ist Art. 6 Abs. 1 lit. b bzw. lit. f Datenschutz-Grundverordnung (DS-GVO). Die Einschaltung von Adressdienstleistern zur Ermittlung aktueller Anschriften ist ebenfalls auf Art. 6 Abs. 1 lit. f DS-GVO gestützt zulässig. Bonitätsabfragen bei der SCHUFA sind erlaubt, wenn ein berechtigtes wirtschaftliches Interesse besteht. Meldungen offener Forderungen an Wirtschaftsauskunfteien sind unter den Voraussetzungen des § 31 Abs. 2 Bundesdatenschutzgesetz (BDSG) möglich.

## E-Mail, Löschung und Auskunft

Für den E-Mail-Versand von Inkassodaten genügt im Regelfall eine qualifizierte Transportverschlüsselung; Ende-zu-Ende-Verschlüsselung ist nicht generell erforderlich. Löschanträge nach Art. 17 DS-GVO können rechtmäßig abgelehnt werden, solange ein Vorgang in Bearbeitung ist oder handels- und steuerrechtliche Aufbewahrungsfristen nach § 257 Handelsgesetzbuch (HGB) bzw. § 147 Abgabenordnung (AO) von bis zu acht Jahren laufen. In diesen Fällen erfolgt statt Löschung eine Einschränkung der Verarbeitung mit strikter Zugangsbeschränkung. Auskunftsanträge nach Art. 15 DS-GVO sind wie bei jedem anderen Verantwortlichen möglich; bei begründeten Identitätszweifeln darf der Inkassodienstleister eine zusätzliche Verifikation verlangen.



## Urheberrechtsschutz für KI-assistierte Werke

Das Landgericht Frankfurt am Main hat mit Urteil vom 17. Dezember 2025 (Az. 2-06 O 401/25) [↗](#) eine einstweilige Verfügung bestätigt, die einer Musikerin und ihrem Digitalvertrieb die weitere Verbreitung und Bewerbung eines Liedtextes untersagt. Die Entscheidung ist urheberrechtlich bedeutsam, weil sie grundlegende Fragen zur Schutzfähigkeit von Werken klärt, an deren Entstehung KI-Systeme beteiligt waren.

### Sachverhalt

Die Klägerin behauptete, den Liedtext im April 2025 eigenständig ohne den Einsatz von künstlicher Intelligenz (KI) verfasst zu haben. Lediglich in einem späteren Schritt sei das KI-System SunoAI zur Musikproduktion genutzt worden. Eine bekannte Künstlerin übernahm Teile des Textes in ihr eigenes Lied, das über Streaming-Plattformen veröffentlicht und über soziale Medien beworben wurde. Die Beklagte, ein Digitalvertrieb, berief sich darauf, ihr sei die Rechtfreiheit des Liedes vertraglich zugesichert worden.

### Kernaussagen des Gerichts

Die Kammer entwickelte eine abgestufte Darlegungslast: Grundsätzlich muss die Urheberin die Schutzfähigkeit eines Werks darlegen und glaubhaft machen. Bringt die Gegenseite jedoch konkrete Anhaltspunkte für einen KI-generierten Output vor – wie hier ein Musikgutachten –, muss die Urheberin ihrerseits detailliert den Schaffensprozess erläutern und darlegen, welche Gestaltungselemente auf menschlicher Schöpfung beruhen. Im Eilverfahren genügt hierfür eine eidesstattliche Versicherung.

Den Einwand, der Sachverhalt eigne sich wegen der erforderlichen Sachverständigenbegutachtung nicht für ein Eilverfahren, wies das Gericht ausdrücklich zurück: Eine solche Argumentation würde urheberrechtlichen Eilrechtsschutz faktisch aushöhlen und widerspräche sowohl Art. 19 Abs. 4 Grundgesetz (GG) als auch Art. 9 der EU-Enforcement-Richtlinie.

Inhaltlich stellte das Gericht fest, dass der menschlich verfasste Originaltext – trotz späterer KI-Überarbeitung – urheberrechtlich schutzfähig bleibt. Entscheidend ist, dass sich der Schutzbereich des Originaltextes auf KI-bearbeitete Fassungen erstreckt, solange die prägenden, schöpferischen Elemente des Originals erkennbar bleiben. Das Vertriebsverschulden der Beklagten ist für den Unterlassungsanspruch irrelevant.

### Einordnung

Das Urteil liefert erstmals eine praktische Handreichung für den Umgang mit KI-assistierten Werkschöpfungen im Urheberrecht: Schutzfähig ist der menschliche Beitrag, auch wenn KI nachgelagert eingesetzt wurde – vorausgesetzt, die individuelle Schöpfung bleibt im Ergebnis erkennbar. Die Entscheidung ist noch nicht rechtskräftig.



## Personalakten sind nicht Teil des Bewerbungsverfahrens

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat sich im Tätigkeitsbericht 2024 [↗](#) grundsätzlich gegen die Praxis ausgesprochen, im öffentlichen Dienst von Bewerbenden die Einwilligung zur Personalakteneinsicht zu verlangen, und entsprechende Änderungen bei der Senatsverwaltung für Finanzen (SenFin) angeregt.

Weiter auf DataAgenda lesen [↗](#)



Bild: NDABCREATIVITY - stock.adobe.com

- ✓ Praxisnah & zertifiziert
- ✓ Mehr Sicherheit im Arbeitsalltag
- ✓ Sofort umsetzbares Know-how

auch als  
Inhouse-  
Schulung  
buchbar

## Ausbildung zum/zur Datenschutzkoordinator/in

Datenschutzkompetenz gezielt aufbauen

16.-17.06.2025 | Köln

Referent: Thomas Mühtlein

Jetzt anmelden: [www.datakontext.com](http://www.datakontext.com)

# „Recht auf Löschen“ in der Praxis - erhebliche Umsetzungsdefizite europaweit



Foto: TravelCinemaStudio, Adobe Stock

Der Europäische Datenschutzausschuss (EDSA) [↗](#) hat seinen Abschlussbericht zur vierten Runde des Coordinated Enforcement Framework (CEF) veröffentlicht. Thema des CEF 2025 war die Umsetzung des Rechts auf Löschung nach Art. 17 DS-GVO. 32 europäische Aufsichtsbehörden beteiligten sich; 764 Verantwortliche – darunter 60 in Deutschland [↘](#) – antworteten auf einen einheitlichen Fragebogen. Das allgemeine Compliance-Niveau wird als „durchschnittlich“ bewertet.

## Wiederkehrende Problemfelder

Sieben Hauptprobleme wurden identifiziert. Im Vordergrund stehen fehlende klare interne Regelungen zu Zeitpunkt und Modalitäten der Löschung, fehlende Schulungen sowie Rechtsunsicherheiten bei Ausnahmetatbeständen, Aufbewahrungsfristen, der Löschung in Back-up-Systemen und den Anforderungen an die Anonymisierung. Zur Anonymisierung als Löschersatz formuliert der Bericht besondere Kritik: Einige Verantwortliche ersetzten die Löschung durch Anonymisierungsmaßnahmen, ohne hinreichende Garantien für deren Irreversibilität zu bieten.

## Folgemaßnahmen und Ausblick

Einige Aufsichtsbehörden haben formelle Untersuchungen eingeleitet oder planen weiterführende Maßnahmen. Der deutsche Annex [↘](#) enthält nationale Best Practices. Das CEF 2026 wird sich auf die Transparenz- und Informationspflichten nach Art. 12–14 DS-GVO konzentrieren. Für Datenschutzbeauftragte empfiehlt sich ein internes Audit zu Art. 17 DS-GVO mit Schwerpunkt auf Back-up-Löschprozessen, Anonymisierungsstandards, Ausnahmeprüfung und Schulungsdokumentation.



# Novelliertes Kirchliches Datenschutzgesetz (KDG) in Kraft getreten

**A**m 1. März 2026 sind das novellierte Gesetz über den kirchlichen Datenschutz (KDG) und seine Durchführungsverordnung (KDG-DVO) in Kraft [↗](#) getreten. Es handelt sich dabei um die erste große Reform seit der Einführung der europäischen DS-GVO. Der Verband der Diözesen Deutschlands (VDD) hatte die Neufassung im November 2025 beschlossen. Um wirksam zu werden, musste sie von den einzelnen Diözesanbischöfen für ihr jeweiliges Bistum in Kraft gesetzt werden.

## Geltungsbereich und Einordnung

Das KDG gilt auf Grundlage des in Art. 91 DS-GVO verankerten Selbstbestimmungsrechts der Kirchen für alle deutschen (Erz-)Diözesen, Kirchengemeinden, Caritas-Verbände, Krankenhäuser, Pflegeeinrichtungen und sonstigen kirchlichen Rechtsträger. Das KDG rückt mit der Reform näher an die Systematik der DS-GVO heran, ohne das verfassungsrechtlich abgesicherte kirchliche Selbstbestimmungsrecht aufzugeben.

## Wesentliche inhaltliche Neuerungen

Ein zentraler Schwerpunkt betrifft die Aufarbeitung von Missbrauch: Das neue KDG stellt ausdrücklich klar, dass die Aufarbeitung sexualisierter Gewalt ein überragendes kirchliches Interesse darstellt und datenschutzrechtlich privilegiert wird. Damit erhalten die meisten Diözesen, die bereits Spezialgesetze zur Aktennutzung erlassen haben, eine konsistente Grundlage im übergeordneten Gesetz.

Im digitalen Bereich schafft die Reform mehrere neue Rechtsgrundlagen: Die Übertragung von Gottesdiensten und anderen kirchlichen Veranstaltungen wird in einem eigenen Paragraphen geregelt. Streaming ist grundsätzlich zulässig, sofern Betroffene vorab informiert werden, schutzwürdige Interessen – insbesondere von Minderjährigen – beachtet werden und bei Gottesdiensten die Möglichkeit eingeräumt wird, nicht im Bild in einer Aufzeichnung zu erscheinen. Ein neuer § 18 KDG-DVO schafft einen eigenen Rechtsrahmen für Cloud-Dienste, löst bisherige Rechtsunsicherheiten ab und fordert klare Risikobewertungen sowie Exit-Strategien für Anbieter. Weitere strukturelle Anpassungen: Die Pflicht zur Bestellung eines Datenschutzbeauftragten greift künftig erst ab 20 Mitarbeitenden statt wie bisher ab 10. Einwilligungen bedürfen nicht mehr zwingend einer Unterschrift auf Papier. Ehrenamtliche werden datenschutzrechtlich Beschäftigten gleichgestellt. Mehrere Änderungen schützen zudem die Integrität von Kirchenbüchern und kirchlichen Urkunden, darunter eine ausdrückliche Ausnahme vom Löschrecht für Taufregister.

## Handlungsbedarf

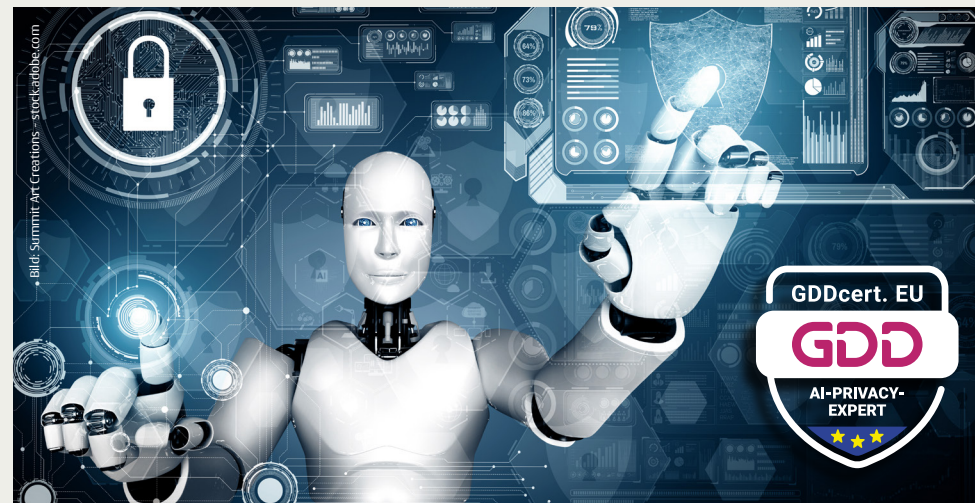
Die Reform ist insbesondere für Krankenhäuser, Pflegeeinrichtungen, Bildungsträger, kirchliche Verwaltungen und deren Dienstleister relevant. Prioritär zu prüfen sind die Anpassung interner Datenschutzdokumentationen, die Überprüfung von Verträgen mit IT- und Cloud-Dienstleistern auf Konformität mit den neuen Standards sowie die Schulung der Mitarbeitenden zu den geänderten Regelungen. Mit der katholischen Reform ist der Konsolidierungsprozess des kirchlichen Datenschutzes in Deutschland abgeschlossen. Die evangelische Kirche hatte ihr Datenschutzgesetz (DSG-EKD) bereits im Mai 2025 in Kraft gesetzt.



## Datenschutzkonforme Anwesenheitsübersicht im Zeiterfassungssystem

**E**in Fallbeispiel aus dem sächsischen Tätigkeitsbericht Datenschutz 2025 zeigt, wie die flächendeckende Freischaltung einer „Anwesenheitsübersicht“ in einem elektronischen Zeiterfassungssystem gegen den Grundsatz der Datenminimierung verstoßen kann – und welche Konsequenzen drohen, wenn Verantwortliche die datenschutzrechtliche Erforderlichkeit nicht hinreichend begründen können.

Weiter auf DataAgenda lesen [↗](#)



## Werden Sie zertifizierter KI-Datenschutz-Experte GDDcert. EU

15.-18.06.2026 | online

**Sichern Sie sich jetzt Ihren Platz!**

- KI-Projekte datenschutzkonform und rechtssicher umsetzen lernen
- Mit der Zertifizierung GDDcert. EU den Karrierevorteil sichern
- Praxisnahes Know-how direkt von erfahrenen GDD-Experten nutzen

Jetzt anmelden: [www.datakontext.com/KI-Experte](http://www.datakontext.com/KI-Experte)



## Mieterselbstauskunft: Datenschutzaufsicht zieht klare Grenzen

**E**in aktueller Fall (Ziffer 2.2.) aus dem Tätigkeitsbericht 2025 der Sächsischen Datenschutzaufsichtsbehörde [↓](#) verdeutlicht, dass Mieterselbstauskünfte in der Praxis nach wie vor häufig datenschutzrechtlich unzulässige Abfragen enthalten – und dass Aufsichtsbehörden auch ohne festgestellten Verstoß im Einzelfall tätig werden können.

### Der Fall

Ein Mietinteressent erhielt von einem Wohnungsmakler bereits vor der Wohnungsbesichtigung eine umfangreiche Selbstauskunft, die u. a. Staatsangehörigkeit, Familienstand und die geschäftliche Telefonnummer abfragte. Da der Betroffene das Formular aufgrund seiner datenschutzrechtlichen Bedenken nicht ausfüllte, lag zwar noch kein

vollendeter Verstoß vor. Die Aufsichtsbehörde sah jedoch hinreichende Anhaltspunkte dafür, dass der Makler gleichartig gegenüber anderen Mietinteressenten verfährt, und nahm dies zum Anlass für eine förmliche Beanstandung.

### Dreistufiges Prüfungsmodell

Die Behörde legte ein praxisnahes Stufenmodell zugrunde, das die zulässigen Verarbeitungsgrundlagen und den jeweiligen Datenkatalog klar differenziert:

- **Vor der Besichtigung** ist die Datenerhebung auf Name, Wohnanschrift und Kontaktdaten beschränkt (Art. 6 Abs. 1 lit. f DS-GVO). Angaben zur Staatsangehörigkeit oder zum Familienstand sind in diesem Stadium unzulässig.
- **Nach Bekundung eines konkreten Anmietinteresses** greift Art. 6 Abs. 1 lit. B DS-GVO (vorvertragliche Maßnahmen). Zulässig sind nun Daten zur Beurteilung der Zahlungsfähigkeit – nicht jedoch Einkommensangaben weiterer Haushaltsmitglieder oder Kontaktdaten vorheriger Vermieter.
- **Erst nach der Auswahlentscheidung** dürfen Nachweise (Einkommensnachweise, Personalausweis, Mietschuldenfreiheitsbescheinigung) verlangt werden. Dabei sind nicht relevante Angaben – etwa Religionszugehörigkeit oder Geburtsort – vom Bewerber zu schwärzen. Hierauf ist ausdrücklich hinzuweisen.

### Konsequenzen und Orientierungshilfe

Der Makler wurde verpflichtet, den Inhalt der Selbstauskunft anzupassen, deren Einsatz vor Besichtigungsterminen zu unterlassen und alle unzulässig erhobenen, noch gespeicherten Daten unverzüglich zu löschen (Art. 17 Abs. 1 lit. d DS-GVO).

Die Datenschutzkonferenz hat zu diesem Themenbereich eine Orientierungshilfe [↓](#) veröffentlicht, die als strukturierte Prüfgrundlage für Verantwortliche und deren Berater dienen kann.

# Biometrischer Abgleich mit Bildern aus dem Internet: Bundestag-Gutachten sieht KI-VO-Verstoß



Foto: Alexander, Adobe Stock

**E**in gemeinsames Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages vom Januar 2026 kommt zu einem klaren Ergebnis: Ein automatisierter biometrischer Abgleich von Gesichtsbildern mit öffentlich zugänglichen Internetdaten ist technisch ohne den Aufbau einer Datenbank nicht praktikabel – und ein solcher Datenbankaufbau wäre mit Art. 5 Abs. 1 lit. e KI-Verordnung (KI-VO) unvereinbar.

## Anlass: Geplante Erweiterung polizeilicher Befugnisse

Hintergrund sind Referentenentwürfe des Bundesinnenministeriums, die Sicherheitsbehörden den nachträglichen biometrischen Abgleich mit Internetdaten ermöglichen sollen – ein Vorhaben, das im aktuellen Koalitionsvertrag verankert ist. Die Prüfung beschränkt sich auf die KI-VO; datenschutz- und grundrechtliche Aspekte bleiben dabei ausdrücklich ausgeklammert.

## Technisch ohne Datenbank nicht realisierbar

Das Gutachten legt ein weites Datenbankverständnis zugrunde: Auch temporäre Speicher und Indexstrukturen, die für eine effiziente Suche zwingend erforderlich sind, gelten als Datenbanken. Alle untersuchten Alternativansätze – Live-Suche, Focused Crawling, API-Zugriffe – erweisen sich als nicht praktikabel oder qualitativ unzureichend. Theoretische Umgehungsszenarien über Vektorrepräsentationen oder Modellgewichte verlagern die Datenbankfunktion lediglich auf andere Systemebenen, heben sie aber nicht auf.

## Rechtlich: Verbot nach Art. 5 KI-VO

Da jede operative Umsetzung zwingend einen Datenbankaufbau erfordert, läuft das geplante System nach Einschätzung der Gutachter auf eine nach Art. 5 Abs. 1 lit. e KI-VO verbotene Praxis hinaus. Die Ausnahme für nationale Sicherheit nach Art. 2 Abs. 3 KI-VO greift für Polizeibehörden im Regelfall nicht. Das Gutachten dürfte die laufenden Ressortabstimmungen damit erheblich beeinflussen.

# DA

DATA AGENDA  
PODCAST



(Quelle: TH Köln/Schmüngen)

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

Folge #**91**

KI-Kompetenz und  
KI-Kompetenzen



Céleste Spahić

Folge #**92**

KI-Omnibus  
Update Mai 2026



Kai Zenner


## Data Agenda Podcast Folge 91: KI-Kompetenz und KI-Kompetenzen

KI ist ein Werkzeug, welches vielfältig eingesetzt wird. Das erfordert Verständnis für die neue Technik und Kompetenz für den Einsatz. Allerdings kann KI auch Kompetenzen in Menschen entfalten und gezielt eingesetzt werden, um sich seiner selbst bewusster zu werden. Wie das gehen kann, erklärt die Buchautorin Céleste Spahić im DataAgenda Datenschutz Podcast.

Zum Podcast bitte [hier](#)  klicken.

## Data Agenda Podcast Folge 92: Update KI-Omnibus Mai 2026

Die KI-Verordnung soll mit Wirkung ab August 2026 geändert werden. Entsprechend laufen die Verhandlungen zwischen dem EU-Parlament, den EU-Mitgliedstaaten und der EU-Kommission auf Hochtouren. Eigentlich sollten sie bereits am 28. April 2026 abgeschlossen sein. Doch eine Einigung konnte nicht erzielt werden. Kai Zenner, Büroleiter des Europaabgeordneten Axel Voss (EVP), berichtet aus dem Maschinenraum der Verhandlungen über das Scheitern im April und skizziert die möglichen weiteren Wege für das Schicksal der Änderungen an der KI-Verordnung. Eine Entscheidung darüber soll am 11. Mai fallen.

Zum Podcast bitte [hier](#)  klicken.

Weitere Folgen unter [DataAgenda.de/podcast](https://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](http://www.datakontext.com/newsletter)

# So entwickeln Sie ein rechtskonformes Löschkonzept

Praxisratgeber inklusive Leitfaden, Checkliste, Muster und Vorlagen

## Löschen nach DS-GVO in der Praxis

Sascha Kremer  
2. überarbeitete Auflage 2024  
136 Seiten/DIN A 4  
ISBN: 978-3-89577-951-0  
**99,99 €**  
inkl. E-Book & Umsetzungshilfen



Bestellen Sie direkt unter:  
[www.datakontext.com/loeschkonzepte](http://www.datakontext.com/loeschkonzepte)

DATAKONTEXT