NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

2 Editorial
3 BSI veröffentlicht Handreichung zur NIS-2-Geschäftsleitungsschulung
5 Leitfaden für Penetrationstests von LLMs
6 Praxistipps zur Beendigung einer Auftragsverarbeitung
7 Rechtslage bei Verteidigungsfällen – Relevanz für Arbeitgeber
9 Datenschutzkonzepte für Digitalisierungsvorhaben
10 Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortlichkeit
12 Impressum

AUSGABE
11/2025

Levent Ferik

EDITORIAL

Künstliche Intelligenz (KI) hält Einzug in die Ministerien:
In Albanien ist mit Diella eine virtuelle „Ministerin“ im Amt, die Korruption bekämpfen soll. In Deutschland sorgt der Weimatar – ein digitaler Minister-Avatar – für Schlagzeilen. Innovation ja, aber der Datenschutz darf hier kein Randthema sein. Sobald KI in staatlichen Entscheidungsprozessen eingesetzt wird, stehen zentrale Prinzipien der Datenschutz-Grundverordnung **(DS-GVO)** auf dem Prüfstand:

- **Transparenz (Art. 5 Abs. 1 lit. a DS-GVO):** Bürger/innen müssen wissen, *ob* und *wie* KI an behördlichen Entscheidungen beteiligt ist.
- **Rechtmäßigkeit der Verarbeitung (Art. 6 DS-GVO):** Eine klare gesetzliche Grundlage ist zwingend – insbesondere, wenn sensible Daten in KI-Modelle einfließen.
- **Betroffenenrechte (Art. 12 ff. DS-GVO):** Auskunft, Berichtigung, Widerspruch und Löschung müssen auch bei KI-gestützten Prozessen uneingeschränkt gelten.
- **Automatisierte Entscheidungen (Art. 22 DS-GVO):** Niemand darf ausschließlich auf Grundlage automatisierter Prozesse betroffen werden – auch nicht durch eine „digitale Ministerin“.
- **Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO):** Behörden müssen belegen können, dass KI-gestützte Verfahren datenschutzkonform gestaltet sind.

Gerade im öffentlichen Bereich gilt: Staatliche Entscheidungen bedürfen demokratischer Legitimation, rechtlicher Kontrolle und menschlicher Verantwortung. KI kann Prozesse unterstützen, aber sie darf **nicht** an die Stelle von Verantwortlichkeit treten.
Wenn es gelingt, Innovation und Datenschutz gemeinsam zu denken, kann KI im öffentlichen Sektor mehr sein als nur ein Experiment, nämlich ein Schritt zu einer verantwortungsvollen digitalen Verwaltung.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: VectographyStudio, Adobe Stock

BSI veröffentlicht Handreichung zur NIS-2-Geschäftsleitungsschulung

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** hat eine neue Handreichung zur Geschäftsleitungsschulung im Rahmen der Umsetzung der NIS-2-Richtlinie veröffentlicht. Die Publikation richtet sich an Führungsebenen von Unternehmen und Einrichtungen, die künftig als „wichtige" oder „besonders wichtige Einrichtungen" unter die NIS-2-Regulierung fallen. Ziel ist es, Geschäftsleitungen auf ihre neuen Pflichten im Bereich Cybersicherheit und Risikomanagement vorzubereiten.

Ziel und Bedeutung der Schulungspflicht

Mit der Umsetzung der NIS-2-Richtlinie in deutsches Recht wird Cybersicherheit (nun noch deutlicher) zur **Leitungsverantwortung**. Geschäftsleitungen müssen künftig sicherstellen, dass geeignete technische, organisatorische und personelle Maßnahmen implementiert und regelmäßig überprüft werden. Die BSI-Handreichung dient als Orientierungshilfe, um entsprechende Schulungen zu planen und umzusetzen.

Das Ziel besteht darin, Führungskräfte für Risiken, Haftung und Compliance-Anforderungen zu sensibilisieren und ihre Rolle bei der strategischen Steuerung der Informationssicherheit zu stärken.

Inhalte und Struktur der Handreichung

Das BSI benennt zentrale Themenfelder, die in Schulungen abgedeckt werden sollten:

- **Regulatorischer Rahmen:** Überblick über die NIS-2-Richtlinie, ihre nationale Umsetzung und rechtliche Pflichten – etwa Registrierung, Meldepflichten und Aufsichtsbefugnisse
- **Risikomanagement:** Einführung in die Identifikation, Bewertung und Steuerung von Sicherheitsrisiken sowie Anforderungen an Sicherheitskonzepte
- **Meldeprozesse:** Vorgaben für Erst-, Detail- und Schlussmeldungen bei Sicherheitsvorfällen und Aufbau interner Meldeprozesse
- **Lieferketten- und Dienstleistermanagement:** Bewertung externer Risiken und vertragliche Absicherung von Cyber- und Compliance-Anforderungen
- **Praxisorientierung:** Der Einsatz von Simulationen und Fallstudien wird empfohlen, um Entscheidungsverantwortliche praxisnah zu schulen.

Adressaten und Umsetzung

Die Adressaten sind die Mitglieder der Geschäftsleitung sowie gegebenenfalls weitere leitende Personen mit Entscheidungs- oder Kontrollbefugnissen. Das BSI empfiehlt regelmäßige Schulungen – mindestens jährlich oder bei relevanten regulatorischen Änderungen. Diese können intern oder durch externe Fachstellen durchgeführt werden.
Mit der neuen Handreichung unterstützt das BSI Unternehmen dabei, ihre **Führungsverantwortung im Bereich Cybersicherheit systematisch wahrzunehmen**. Die Schulung der Geschäftsleitung gilt als wesentlicher Baustein einer wirksamen NIS-2-Compliance und trägt dazu bei, Cybersicherheits- und Datenschutzanforderungen künftig noch enger zu verzahnen.

Foto: vejaa, Adobe Stock

Der Erwerb gebrauchter oder „refurbished“ IT-Geräte wirft nicht nur technische, sondern auch datenschutzrechtliche Fragen auf. Besonders heikel wird es, wenn auf einem erworbenen Notebook noch personenbezogene Daten des Vorbesitzers vorzufinden sind. Doch wer trägt in diesem Fall die Verantwortung nach der DS-GVO?

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die Stelle, die über die **Zwecke und Mittel der Verarbeitung** entscheidet.

- Der bloße Erwerber eines Geräts, auf dem noch Daten vorhanden sind, hat diese Daten **nicht selbst erhoben** und verfolgt zunächst auch **keinen eigenen Zweck** mit deren Verarbeitung.
- Eine Verantwortlichkeit i. S. d. DS-GVO wird deshalb **nicht automatisch allein durch den Besitz** der Daten begründet.
- Der eigentliche Datenschutzverstoß liegt bei dem Händler oder Vorbesitzer, der seiner Pflicht zur ordnungsgemäßen Datenlöschung nicht nachgekommen ist.

Weiter auf DataAgenda lesen

Shabbir - stock.adobe.com

Risiken minimieren und Compliance sicherstellen!

Datenschutz-Folgenabschätzung

Bewertung - Planung - Umsetzung und Einbindung in ein Datenschutz-Managementsystem

1. Dezember 2025 I online
Referentin: Katsiaryna Hashko

Schwerpunktthemen:

- ✓ Kriterien zur Begründung einer Datenschutz-Folgenabschätzung
- ✓ Organisieren und Priorisieren der Arbeitsschritte
- ✓ Dokumentationspflichten
- ✓ Praktische Umsetzung einer Datenschutz-Folgenabschätzung
- ✓ Checklisten und Erfassungsbögen

Jetzt anmelden: www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Taposh Barmon, Adobe Stock

Leitfaden für Penetrationstests von LLMs

Die Allianz für Cyber-Sicherheit hat einen Leitfaden veröffentlicht, der sich mit Penetrationstests für Large Language Models (LLMs) befasst. Ziel ist es, klassische Prüfmethoden aus dem Bereich der IT-Sicherheit auf die spezifischen Eigenschaften und Risiken von LLMs zu übertragen. Für Datenschutz- und Compliance-Verantwortliche ist das Dokument besonders interessant, da Schwachstellen in KI-Systemen unmittelbare Auswirkungen auf die Vertraulichkeit und Integrität personenbezogener Daten haben können.

Schwerpunkte des Leitfadens

Der Leitfaden orientiert sich am etablierten Vorgehen für Penetrationstests, adaptiert dieses jedoch auf die besonderen Angriffspunkte von LLMs. Behandelt werden unter anderem Prompt-Injektionen, also gezielte Manipulationen durch Eingaben, die zu ungewollten oder vertraulichen Ausgaben führen können. Auch Szenarien wie adversariale Angriffe, Modellvergiftung oder der Zugriff auf interne Datenstrukturen werden berücksichtigt. Ein weiterer Fokus liegt auf der Sicherheit von Schnittstellen und APIs, die häufig zentrale Einfallstore darstellen.
Neben technischen Angriffsszenarien geht es auch um organisatorische Rahmenbedingungen. So wird empfohlen, Penetrationstests klar zu dokumentieren, Ergebnisse nachvollziehbar zu bewerten und die Nachbereitung in bestehende Sicherheits- und Compliance-Prozesse einzubetten.

Bedeutung für den Datenschutz

Aus datenschutzrechtlicher Sicht hebt der Leitfaden hervor, dass nur notwendige Daten in LLM-Systeme eingespeist werden sollten. Insbesondere sensible Informationen dürfen nicht unkontrolliert verarbeitet oder durch Tests offengelegt werden. Betreiber sollten daher strikte Zugriffskontrollen etablieren und eine klare Trennung zwischen Test- und Produktionsumgebungen vorsehen. Ebenso wichtig sind vertragliche Regelungen mit externen Prüfern, die Geheimhaltung, Löschpflichten und den Umgang mit Testdaten verbindlich festlegen.
Der Leitfaden verdeutlicht, dass Penetrationstests für LLMs ein wichtiges Instrument sind, um Risiken frühzeitig zu erkennen und Datenschutzverletzungen zu vermeiden. Verantwortliche sollten die Ergebnisse solcher Tests systematisch in bestehende Sicherheitsstrategien einbinden und gegebenenfalls Datenschutz-Folgenabschätzungen aktualisieren.

Foto: Song_about_summer, Adobe Stock

Praxistipps zur Beendigung einer Auftragsverarbeitung

Das GDD-Kurzpapier 3 bietet praxisorientierte Empfehlungen zur datenschutzkonformen Beendigung von Auftragsverarbeitungsverhältnissen gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO. Es richtet sich an Datenschutzbeauftragte und Verantwortliche, die ihre Pflichten im Zusammenhang mit der Beendigung von Auftragsverarbeitungen verstehen und umsetzen möchten.

Pflichten des Auftragsverarbeiters

Gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO ist der Auftragsverarbeiter verpflichtet, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und alle vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Diese Verpflichtung basiert auf den Grundsätzen der Datenminimierung und Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. c und e DS-GVO. Eine Ausnahme von dieser Löschpflicht besteht nur, wenn eine gesetzliche Aufbewahrungspflicht, beispielsweise aus steuerrechtlichen Gründen, besteht.

Pflichten des Verantwortlichen / Haftung bei nicht erfolgter Löschung

Obwohl Art. 28 Abs. 3 S. 2 lit. g DS-GVO keine direkten Pflichten für den Verantwortlichen festlegt, ergibt sich aus Art. 28 Abs. 1 DS-GVO die Verantwortung des Verantwortlichen, nur mit Auftragsverarbeitern zusammenzuarbeiten, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt. Darüber hinaus verpflichtet Art. 28 Abs. 3 S. 2 lit. h DS-GVO den Verantwortlichen, sicherzustellen, dass der Auftragsverarbeiter ihm alle erforderlichen Informationen zur Verfügung stellt, um die Einhaltung der Pflichten aus der DS-GVO nachzuweisen und Überprüfungen zu ermöglichen. Dies umfasst auch die Überprüfung der ordnungsgemäßen Löschung personenbezogener Daten nach Beendigung der Verarbeitung. Kommt der Auftragsverarbeiter seiner Löschpflicht nicht nach, kann der Verantwortliche haftbar gemacht werden, wenn der Auftraggeber seiner Überwachungspflicht nicht ausreichend nachgekommen ist. Es wird empfohlen, klare vertragliche Regelungen zur Löschung der Daten und zur Nachweispflicht des Auftragsverarbeiters zu treffen.

Weiter auf DataAgenda lesen

Foto: Comofoto, Adobe Stock

Rechtslage bei Verteidigungsfällen – Relevanz für Arbeitgeber

Die Bundesvereinigung der Deutschen Arbeitgeber (BDA) hat ein Positionspapier zu den arbeits- und sicherheitsrechtlichen Rahmenbedingungen im Spannungs- und Verteidigungsfall veröffentlicht. Vor dem Hintergrund der aktuellen geopolitischen Lage wird deutlich, dass auch Unternehmen einen Beitrag zur Landes- und Bündnisverteidigung leisten müssen. Auch für Datenschutz- und Compliance-Verantwortliche ist das Papier relevant, da es nicht nur Eingriffe in Arbeitsverhältnisse beschreibt, sondern auch erweiterte Meldepflichten und die Verarbeitung personenbezogener Daten vorsieht.

Arbeitsrechtliche Regelungen im Frieden

Im Friedenszustand können Beschäftigte freiwilligen Wehrdienst leisten, Reservistenpflichten nachkommen oder sich im Katastrophen- und Zivilschutz engagieren. Arbeitgeber müssen in diesen Fällen teils Freistellungen gewähren, wobei Erstattungsansprüche gegenüber dem Gemeinwesen bestehen können. Bereits jetzt unterliegen Unternehmen mit kritischer Infrastruktur (KRITIS), digitalen Diensten oder besonderem öffentlichen Interesse erhöhten IT-Sicherheitsanforderungen. Sicherheitsvorfälle sind zu melden, und Systeme müssen nach dem Stand der Technik geschützt werden.

Eingriffe im Spannungs- oder Verteidigungsfall

Mit der Ausrufung eines Spannungs- oder Verteidigungsfalls greifen weitergehende Regelungen. Die Wehrpflicht wird aktiviert, Reservisten und Wehrpflichtige können einberufen werden. Während der Dienstzeit ruht das Arbeitsverhältnis, und es besteht ein besonderer Kündigungsschutz. Durch Unabkömmlichstellungen oder Zurückstellungen können bestimmte Arbeitnehmer von der Dienstpflicht freigestellt werden, wenn sie für den Betrieb unverzichtbar sind. Darüber hinaus kann das Gesetz zur Sicherstellung von Arbeitsleistungen für Zwecke der Verteidigung einschließlich des Schutzes der Zivilbevölkerung (Arbeitssicherstellungsgesetz – ASG) die Zuweisung von Arbeitskräften vorschreiben und die Arbeitgeberwahl einschränken. Auch im Zivilschutz haben Beschäftigte Anspruch auf Freistellung mit Fortzahlung des Entgelts, teilweise mit Erstattungsansprüchen für Arbeitgeber.

Reformvorhaben und Datenschutzaspekte

Geplant sind umfassende Änderungen, darunter das Wehrdienst-Modernisierungsgesetz (WDModG) mit Anpassungen beim Arbeitsplatzschutz und im ASG sowie Reformen zur Vereinfachung der Ersatzkraftbereitstellung. Auf der Ebene der Cybersicherheit sollen die Umsetzung der NIS2-Richtlinie und das KRITIS-Dachgesetz zu erweiterten Meldepflichten und höheren Bußgeldrahmen führen. Besonders relevant für Datenschutzverantwortliche ist die geplante Übermittlung personenbezogener Daten aus Melderegistern und Jobcentern an die Bundesagentur für Arbeit, um im Verteidigungsfall Arbeitskräfte gezielt erfassen und zuweisen zu können.

14. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

26.–27. Januar 2026 | Garmisch Partenkirchen

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

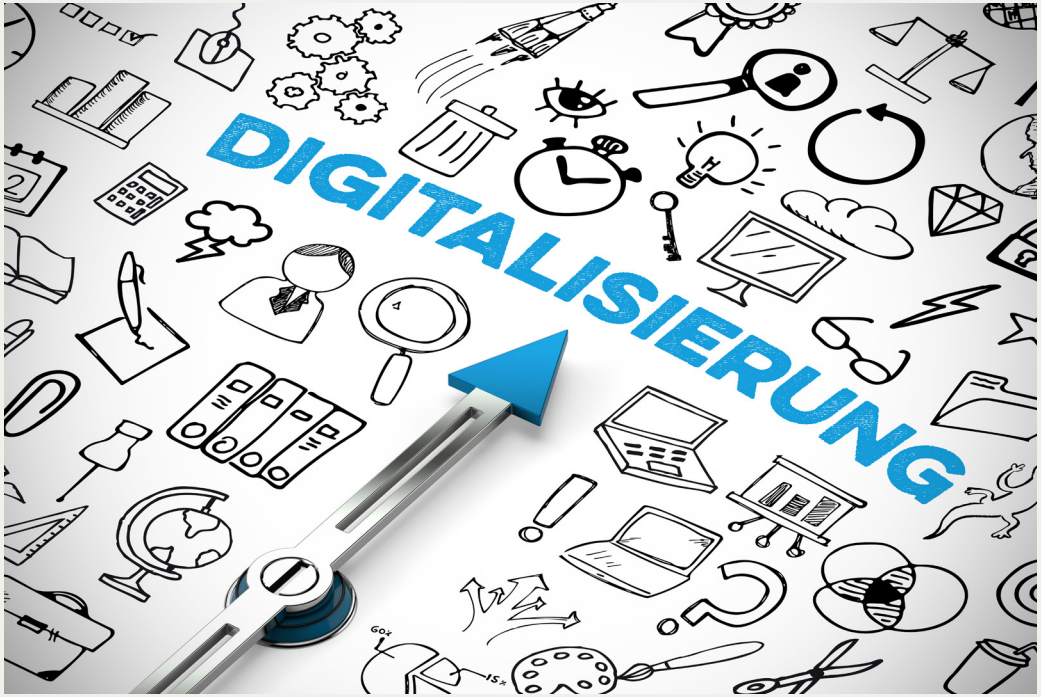

Foto: Robert Kneschke, Adobe Stock

Datenschutzkonzepte für Digitalisierungsvorhaben

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) im Rahmen seiner sog. Allgemeinen Kurz-Informationen (AKI) einige Empfehlungen für die Erstellung von Datenschutzkonzepten im Rahmen von Digitalisierungsvorhaben ⇩ veröffentlicht. Selbstverständlich können auch Verantwortliche außerhalb Bayerns von den Empfehlungen profitieren, wen sie digitale Projekte planen und dabei datenschutzrechtliche Anforderungen systematisch umsetzen möchten.

Bedeutung und Nutzen

Der BayLfD hebt hervor, dass ein **Datenschutzkonzept** ein zentrales Instrument ist, um Projekte von der Planung bis zur Umsetzung datenschutzkonform zu gestalten. Es dient insbesondere dazu,

- Verarbeitungsvorgänge transparent zu dokumentieren,
- Verantwortlichkeiten klar zu regeln,
- Risiken frühzeitig zu erkennen,
- erforderliche Nachweise wie **Datenschutz-Folgenabschätzungen (DSFA)** oder technische und organisatorische Maßnahmen vorzubereiten.

Damit unterstützt ein Datenschutzkonzept auch die **Rechenschaftspflicht** nach Art. 5 Abs. 2 DS-GVO und erleichtert die Bewertung datenschutzkonformer Projekte durch andere Stakeholder.

Vorgehensweise

Der BayLfD empfiehlt ein **iteratives Vorgehen**: Das Konzept wächst parallel zum Projekt. Zentrale Schritte sind:
die Erfassung und Beschreibung der Verarbeitungsvorgänge, inkl. Datenkategorien und Löschfristen;
die Klärung der datenschutzrechtlichen Rollen (Verantwortlicher, Auftragsverarbeiter);
die Festlegung von Zweck und Rechtsgrundlage jeder Verarbeitung;
die Risikoanalyse und die Prüfung der Notwendigkeit einer DSFA;
die Abstimmung mit der Informationssicherheit;
die Implementierung geeigneter **technischer und organisatorischer Maßnahmen**;
der Abschluss, die Qualitätssicherung und die Integration in das Datenschutzmanagementsystem.
Ein Datenschutzkonzept ist zwar nicht ausdrücklich gesetzlich vorgeschrieben, in der Praxis hat es sich aber als praxisnahes Instrument bewährt. Es ermöglicht Verantwortlichen Datenschutzanforderungen frühzeitig zu berücksichtigen und Rechenschaftspflichten effizient zu erfüllen.

Foto: Ummeya, Adobe Stock

Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortlichkeit

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat ein neues Kurzpapier veröffentlicht, das sich mit der praktischen Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortlichkeit nach der Datenschutz-Grundverordnung (DS-GVO) befasst. Ziel ist es, Verantwortlichen eine Orientierung zu geben, wie sie Dienstleister und Kooperationspartner rechtlich korrekt einordnen können.

Zentrales Kriterium für die Einordnung als Auftragsverarbeitung ist die Weisungsgebundenheit des Dienstleisters. Bestimmt die verantwortliche Stelle allein über den Zweck und die wesentlichen Mittel der Verarbeitung und ist der Dienstleister an diese Vorgaben gebunden, spricht dies eindeutig für ein Verhältnis nach Art. 28 DS-GVO. Ein entsprechender Vertrag allein reicht allerdings nicht aus; entscheidend ist die tatsächliche Ausgestaltung der Zusammenarbeit. Typisch für Auftragsverarbeiter ist, dass sie lediglich als „verlängerter Arm" der verantwortlichen Stelle handeln, keine eigenen Entscheidungsbefugnisse besitzen und kein eigenes Interesse an den Verarbeitungsergebnissen haben.

Demgegenüber liegt eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO vor, wenn zwei oder mehr Parteien gemeinsam über Zweck und wesentliche Mittel der Verarbeitung bestimmen. Maßgeblich ist nicht die vertragliche Bezeichnung, sondern der funktionale Einfluss auf die Datenverarbeitung. Dabei müssen die Beteiligten nicht gleichrangig sein oder denselben Umfang an Kontrolle ausüben. Entscheidend ist, dass die wesentlichen Entscheidungen – etwa über die Erhebung, Auswahl, Nutzung oder Speicherdauer von Daten – tatsächlich von mehreren Stellen getragen werden. Die GDD betont, dass eine bloße Abstimmung in Randfragen hierfür nicht ausreicht.

Das Papier macht deutlich, dass die Abgrenzung stets einzelfallbezogen erfolgen muss. Während bei klarer Weisungsgebundenheit regelmäßig von einer Auftragsverarbeitung auszugehen ist, erfordert die Annahme gemeinsamer Verantwortlichkeit eine sorgfältige Prüfung, ob die Beteiligten tatsächlich gemeinsam über die Kernelemente der Verarbeitung entscheiden. Die dargestellten Indikatoren sollen Verantwortliche dabei unterstützen, eine rechtssichere Einordnung vorzunehmen, ersetzen jedoch nicht die detaillierte Analyse des konkreten Verarbeitungsszenarios.

Data Agenda Podcast Folge 77: KI in der Justiz

Eine moderne Justiz muss mit moderner Technik ausgestattet sein, wenn die Richter ihre wichtige Aufgabe für den Rechtsstaat erfüllen sollen. In der Anwaltschaft ist eine Unterstützung durch KI auf dem Vormarsch. Welche Möglichkeiten und Einsatzfelder gibt es in für Bots in der Justiz? Roboterrichter darf es nicht geben. Aber dürfen Richter sich helfen lassen? Wo legen die Möglichkeiten und welche Grenzen ziehen KI-Verordnung und Richterrecht? Wie steht es um die KI-Kompetenz an den Gerichten.

Isabelle Biallaß, Richterin am Oberlandesgericht Hamm, Mitglied im Vorstand des EDV-Gerichtstags e.V., Lehrbeauftragte an der TH Köln und Autorin zahlreicher Beiträge zum Einsatz Künstlicher Intelligenz in der Justiz, unter anderem im juris PraxisKommentar Elektronischer Rechtsverkehr gewährt Einblicke in den Maschinenraum der KI in der Justiz.

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:
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

KI-Kompetenz aufbauen und nachweisen

70 Minuten Video-Learning mit 3 GDD-Experten

- ✓ Art. 4 der KI-VO einfach erfüllen!
- ✓ Abschlusstest & Zertifikat zur Dokumentation
- ✓ Flexibel abrufbar – ideal für alle Beschäftigten
- ✓ Inklusive 20-seitigem Merkblatt für nachhaltige Wissensvermittlung
- ✓ Von den GDD-Experten Prof. Dr. Rolf Schwartmann, Kristin Benedikt, RA Andreas Jaspers

Jetzt bestellen: www.datakontext.com/Video-KI-Kompetenz

DATAKONTEXT