NEWS BOX DATENSCHUTZ



INHALTSVERZEICHNIS

2 Editorial
3 Mehr als eine Checkliste: Wie das EDSA-Template die DSFA verändern könnte
4 Ransomware mit KI-Turbo: Warum nach dem Angriff die 72-Stunden-Frist läuft
5 Score, Algorithmus, Geschäftsgeheimnis: Der BGH muss das Auskunftsrecht ausloten
7 KI-Verordnung in der Praxis: Die neue Aufsicht und die Tücken des Bestands-schutzes
8 Wenn die KI mithört: Zwischen Datenschutz, Strafrecht und Betriebsvereinbarung
10 Impressum

SONDERAUSGABE

DAFTA



Andreas Jaspers

EDITORIAL

Liebe Leserinnen und Leser,

die Datenschutzfachtagung (DAFTA) findet zum Jubiläum in Zeiten großer Veränderungen durch künstliche Intelligenz (KI) statt. Dadurch ergeben sich neue Herausforderungen für Datenschutzverantwortliche in Betrieben und Behörden. KI-Systeme müssen beim Training und beim Output datenschutzkonform betrieben werden. Mit der Bundesnetzagentur gibt es zudem eine neue Aufsichtsbehörde für Digitalgesetze. Für das Training von KI-Systemen sieht ein Gesetzentwurf in Nordrhein-Westfalen die Einrichtung von KI-Reallaboren vor, in denen in Schutzräumen unter behördlicher Aufsicht KI-Systeme von den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) befreit werden. Diese neue Aufsichtsstruktur ist deshalb ein Thema der 50. DAFTA.
Ebenfalls auf der diesjährigen DAFTA werden Fragen zum betrieblichen Einsatz von KI – wie Best Practices beim KI-Einsatz im Arbeitsverhältnis, KI-Tools in der Datenschutzberatung oder die Protokollierung von Videokonferenzen – behandelt. Zudem werden aktuelle Fragen zum technisch-organisatorischen Datenschutz durch die Umsetzung der NIS-2-Richtlinie thematisiert.

Beim 45. RDV-Forum liegt ein Schwerpunkt auf dem Beschäftigungsdatenschutz. Behandelt werden u. a. die neuen EU-Regeln zur Lohngleichheit und Entgelttransparenz sowie neue Formen der Mitarbeiterüberwachung. Fragen der Datenschutzpraxis stehen im Vordergrund bei Themen wie der Datenschutz-Folgenabschätzung auf Grundlage des Templates des Europäischen Datenschutzausschusses (EDSA) oder der Änderung der Rolle von Datenschutzbeauftragten durch die KI-VO und den Data Act.
Auf der DAFTA und auf dem RDV-Forum 2026 wollen wir gemeinsam mit Gästen aus Wirtschaft, Aufsicht, Wissenschaft und Praxis diese aktuellen Fragen aufarbeiten und Lösungsmöglichkeiten aufzeigen.
Die **Jubiläums-DAFTA** und das **RDV-Forum** finden **hybrid** im **Marriott Hotel** in Köln statt. Wir würden uns freuen, Sie vom 11. bis 13. November 2026 in Köln oder online begrüßen zu dürfen.

Mit freundlichen Grüßen
Andreas Jaspers
Geschäftsführer Gesellschaft für Datenschutz und Datensicherheit (GDD)

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com



Foto: kaliel, Adobe Stock

Mehr als eine Checkliste: Wie das EDSA-Template die DSFA verändern könnte

Wann ist das Risiko einer Datenverarbeitung hoch? Welche Maßnahme senkt es? Und wann bleibt ein Restrisiko, das zur Konsultation der Aufsichtsbehörde zwingt? Das sind die Fragen, um die es bei einer DSFA geht. Ob KI bei der Beurteilung von Risiken helfen kann, wird derzeit unterschiedlich bewertet. Im Frühjahr kam Hilfe aus einer anderen Richtung, aus Brüssel. Der EDSA hat im März erstmals ein Template für die DSFA vorgelegt. Die Konsultation lief bis zum 9. Juni, die endgültige Fassung steht aus.

Die Risikoabwägung nimmt das Formular zwar niemandem ab und es schreibt auch keine Methode fest. Es kann aber helfen, sie entscheidenden Fragen in der richtigen Reihenfolge zu stellen. Es gibt zudem vor, was am Ende dokumentiert sein muss. Sieben Abschnitte führen von der Beschreibung der Verarbeitung über Rechtsgrundlagen, Erforderlichkeit und Verhältnismäßigkeit zur Risikobewertung mit Maßnahmenplan, zum Rat des Datenschutzbeauftragten und zur Sicht der Betroffenen.

Der Digital-Omnibus will noch einen Schritt weiter gehen. Der Kommissionsvorschlag vom November 2025 fasst Art. 35 Abs. 4 bis 6 DS-GVO neu. Der EDSA soll der Kommission eine EU-weite Liste der Verarbeitungen vorschlagen, die eine DSFA verlangen, eine Liste derer, die keine verlangen, und eine gemeinsame Vorlage samt Methodik. Die Kommission nimmt sie per Durchführungsrechtsakt an. Die Listen der nationalen Aufsichtsbehörden, in Deutschland die Muss-Liste der DSK von 2018, gelten bis dahin weiter. EDSA und EDSB begrüßen die Harmonisierung, wollen Listen und Vorlage aber selbst verabschieden, statt der Kommission nur zuzuarbeiten. Die gemeinsame Methodik soll nach ihrer Vorstellung ein Rahmen mit Grundsätzen sein, keine starre Checkliste, damit Unternehmen ihre eingeführten Verfahren und Werkzeuge weiter nutzen können. Ob und wann das kommt, ist offen.

Wie die DSFA aktuell in der Aufsichtspraxis aussieht und was das Template dort bringt, weiß Andreas Sachs aus erster Hand. Er leitet das technische Referat des Bayerischen Landesamts für Datenschutzaufsicht. Am 11. November 2026 spricht er auf dem 45. RDV-Forum in Köln und online über „Datenschutz-Folgenabschätzung in der Praxis und das Template des EDSA“.

Datenschutz-Folgenabschätzung in der Praxis und das Template des EDSA

11. November 2026 I 16:00 Uhr

Referent: Andreas Sachs, Diplom-Informatiker, Leiter des technischen Referats sowie Vertreter des Präsidenten beim Bayerischen Landesamt für Datenschutzaufsicht, Ansbach

Jetzt mehr erfahren und anmelden: zum RDV-Forum



Foto: solom, Adobe Stock

Ransomware mit KI-Turbo: Warum nach dem Angriff die 72-Stunden-Frist läuft

Cyberkriminelle setzen KI ein, und sie werden damit schneller. Die spanische Datenschutzbehörde AEPD beschreibt in einem Blogbeitrag vom 28. September, wie KI-Agenten Cyberangriffe beschleunigen und Schwachstellen automatisiert ausnutzen. Zwar erzeugt ein Sprachmodell noch keine brauchbare Schadsoftware, aber Agentensysteme in der Hand eines erfahrenen Angreifers werden zum Multiplikator. Zwischen dem ersten Zugriff auf ein System und dem Abfluss der Daten vergehen Minuten statt Tagen. Und die KI greift nicht mehr eine einzelne Schwachstelle an, wie es Angreifer bisher taten. Sie durchleuchtet die gesamte Infrastruktur.

Die meisten Ransomware-Angriffe richten sich nach dem BKA gegen Unternehmen. Nach einer Bitkom-Umfrage vom September war fast jedes zweite Unternehmen im vergangenen Jahr betroffen, jedes fünfte betroffene hat schon einmal Lösegeld gezahlt.
Nach einer Lösegeldforderung werden die meisten Unternehmen wohl zunächst entscheiden, ob sie zahlen. Die Forderung setzt aber zugleich eine datenschutzrechtliche Frist in Gang. Nach Art. 33 DS-GVO meldet der Verantwortliche eine Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt wurde. Bekannt ist die Verletzung nach den Leitlinien 9/2022 des EDSA zur Meldung von Datenschutzverletzungen (2023), sobald der Verantwortliche nach der Forderung sein System geprüft und den Angriff bestätigt hat.
Ein typischer Ransomware-Angriff trifft zwei der drei Schutzziele, nach denen der EDSA Datenschutzverletzungen einteilt. Die

Verschlüsselung nimmt dem Verantwortlichen den Zugriff auf die Daten, das ist eine Verletzung der Verfügbarkeit. Die Kopie in den Händen der Angreifer ist eine Verletzung der Vertraulichkeit, die auch eine Lösegeldzahlung nicht wiederherstellt. Denn ob die Täter die Kopie danach löschen, lässt sich nicht prüfen. Ob ein Unternehmen überhaupt zahlen darf, ist rechtlich nicht eindeutig geklärt. Die DS-GVO gibt darauf keine Antwort. Die Frage führt aus dem Datenschutzrecht hinaus ins Straf- und Sanktionsrecht.
Dort setzt Forum 4 der 50. DAFTA an. Am 12. November 2026 spricht Jan Spittka (Clyde & Co) in Köln und online über „Rechtliche Aspekte bei Lösegeldforderungen nach Cyberangriffen". Er erörtert, ob und wann Unternehmen zahlen dürfen, welche straf- und sanktionsrechtlichen Risiken drohen und wann Aufsichtsbehörden und Betroffene einzubinden sind.

Rechtliche Aspekte bei Lösegeldforderungen nach Cyberangriffen

12. November 2026 I 14:50 Uhr, FORUM 4

Referent: Jan Spittka, Rechtsanwalt | Partner, Clyde & Co., Düsseldorf

Leitung: Prof. Dr. Michael Meier, Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn, Leiter der Abteilung Cyber Security, Fraunhofer FKIE; GDD-Vorstand, Bonn

Jetzt mehr erfahren und anmelden: Zur DAFTA



Foto: Dilok, Adobe Stock

Score, Algorithmus, Geschäftsgeheimnis: Der BGH muss das Auskunftsrecht ausloten

Schufa-Score, Auskunftsrecht und Geschäftsgeheimnis beschäftigen am 21. Oktober den BGH. Der I. Zivilsenat verkündet dann seine Entscheidung in mehreren Parallelverfahren gegen die Schufa. Die Klägerinnen und Kläger hatten 2023 Auskunft über ihre gespeicherten Daten und Scorewerte erhalten. Sie halten das Scoring-Verfahren für intransparent und verlangen mehr Informationen darüber, wie ihr Score berechnet wird.

Gestützt wird der Anspruch auf Art. 15 Abs. 1 lit. h DS-GVO. Bei automatisierter Entscheidungsfindung einschließlich Profiling schuldet der Verantwortliche danach aussagekräftige Informationen über die involvierte Logik. Die Vorinstanz, das OLG Dresden, versteht den Anspruch weit. Die Schufa wurde verurteilt, die Gewichtung der Kriterien zueinander mitzuteilen, außerdem die Aussagekraft des konkreten Werts. Die grobe Einstufung einzelner Datenarten genügte dem OLG nicht.
Die Obergrenze zieht das OLG bei Angaben, mit denen sich der Score mathematisch nachrechnen ließe. Das Auskunftsrecht solle der betroffenen Person nur ermöglichen, ihren Score auf Fehler und Plausibilität zu prüfen. Dafür genüge eine Information, die auch ein Laie versteht.
Umstritten ist vor allem, wie genau die Gewichtung offenzulegen ist. Gregor Thüsing und Lorenz Fander halten eine grobe Gewichtung für ausreichend, also die Angabe, welche Faktoren das Ergebnis wesentlich und welche es weniger wesentlich beeinflusst haben. Die Gewichtung der Faktoren zueinander sei nicht geschuldet, weil sie im Ergebnis das Berechnungsverfahren offenlegen würde (RDV 2026, 136).
Vom Umfang des Anspruchs zu trennen ist die Frage, wann der Verantwortliche eine geschuldete Auskunft wegen eines Geschäftsgeheimnisses verweigern darf. Den Rahmen dafür hat der EuGH 2025 in der Sache Dun & Bradstreet gesetzt.

- Geschäftsgeheimnisse sind geschützt, dürfen aber nicht dazu führen, dass jede Auskunft verweigert wird. Auskunftsrecht und Geheimnisschutz sind im Einzelfall abzuwägen.
- Nach Möglichkeit ist die Auskunft so zu erteilen, dass die Geheimnisse gewahrt bleiben.

Hält der Verantwortliche Informationen für geschützt, hat er sie der Aufsichtsbehörde oder dem Gericht zu übermitteln, die den Umfang der Auskunft bestimmen.
Das OLG Dresden hat im SCHUFA-Fall den Algorithmus und die Daten der Vergleichsgruppen zu den geschützten Geschäftsgeheimnissen gezählt, ohne eine solche Abwägung vorzunehmen.
Drei Wochen nach der Verkündung beim BGH, am 11. November 2026, spricht Dr. Manuel Klar auf dem 45. RDV-Forum in Köln und online über „Die Zurückweisung datenschutzrechtlicher Auskunftsansprüche aus Gründen der Geheimhaltung“.

Die Zurückweisung datenschutzrechtlicher Auskunftsansprüche aus Gründen der Geheimhaltung

11. November 2026 I 14:45 Uhr

Referent: Dr. Manuel Klar, Rechtsanwalt für Datenschutzrecht, Gleiss Lutz, München | Lehrbeauftragter für Datenschutzrecht an der Universität Regensburg

Jetzt mehr erfahren und anmelden: zum RDV-Forum

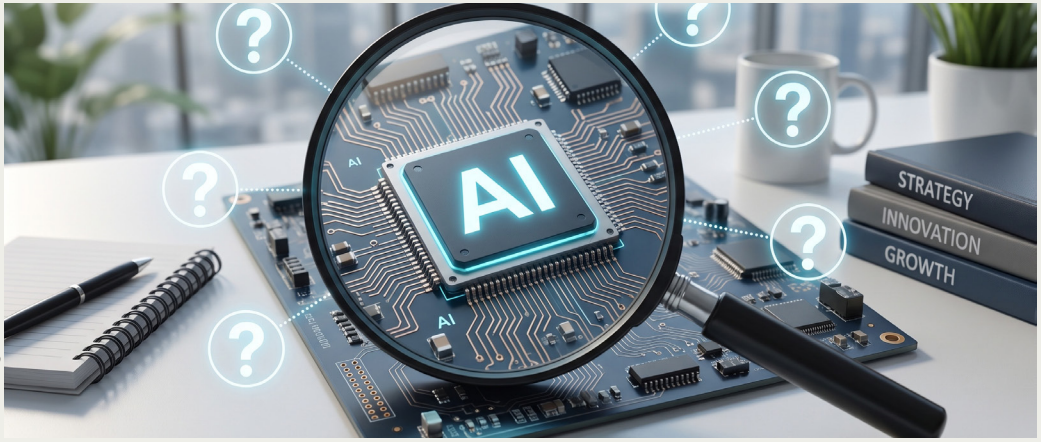


Foto: AADigitalArts, Adobe Stock

KI-Verordnung in der Praxis: Die neue Aufsicht und die Tücken des Bestandsschutzes

Seit Ende Juli ist die Bundesnetzagentur zentrale Marktüberwachungsbehörde für die KI-Verordnung. Seit August nimmt sie über ein Online-Formular Beschwerden wegen Verstößen an. Ihr KI-Service-Desk bietet mit dem KI-Compliance Kompass eine erste, unverbindliche Einschätzung, ob und wie weit die KI-VO ein System erfasst.

Diese Einschätzung hängt vor allem an einer Frage: Ist das System ein Hochrisiko-KI-System? Noch bleibt Zeit für die Antwort. Der Digitale Omnibus verschiebt die Pflichten für Hochrisiko-KI nach Anhang III auf den 2. Dezember 2027. Wer sein System vor dem Stichtag einführt, genießt nach Art. 111 Abs. 2 KI-VO zudem Bestandsschutz.

Aber der Bestandsschutz trägt nur, solange das System in seiner Konzeption nicht erheblich verändert wird, und KI-Systeme werden selten so belassen, wie sie eingeführt wurden. Mit der nächsten erheblichen Änderung gelten die Pflichten dann für das gesamte System. Nachträglich erfüllen lassen sie sich kaum: Datenqualität, technische Dokumentation und menschliche Aufsicht müssen von Anfang an in die Konzeption eingeplant sein.

Die Wertungen der KI-VO gelten zudem über ihre unmittelbare Anwendbarkeit hinaus schon heute. Die Einstufung als Hochrisiko-KI ist ein starkes Indiz dafür, dass eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO nötig ist. Die Anwendungsfälle des Anhangs III sind zugleich die Fälle, in denen die Grenze zur automatisierten Einzelentscheidung nach Art. 22 DS-GVO zu prüfen ist. Zudem könnten die Anforderungen der KI-VO schon vor ihrem Geltungsbeginn den Sorgfaltsmaßstab konkretisieren, an dem sich Verkehrspflichten nach § 823 BGB bemessen.

Der Maßstab zur Einordnung steht in Art. 6 KI-VO. Im vielen Betrieben ist vor allem Abs. 2 relevant: Ein System ist hochriskant, wenn seine Zweckbestimmung einen Anwendungsfall des Anhangs III erfasst. Im Beschäftigungsbereich, wenn das System

- Bewerbungen sichtet und Bewerber bewertet,
- über Beförderungen oder Kündigungen mitentscheidet,
- Aufgaben nach Verhalten oder Merkmalen zuweist oder
- Leistung und Verhalten von Beschäftigten beobachtet und bewertet.

Die 50. DAFTA und das 45. RDV-Forum greifen diese Fragen aus mehreren Perspektiven auf: Andrea Sanders-Winter erläutert die neue Aufsicht für Digitalgesetze durch die Bundesnetzagentur, Kai Zenner ordnet den aktuellen Stand des Digitalen Omnibus ein und Prof. Dr. Rolf Schwartmann zeigt, wie die EU-Leitlinien die Einstufung als Hochrisiko-KI in der Praxis steuern. Ergänzend widmet sich ein Forum den Grenzen von KI im Arbeitsverhältnis.

High-Risk oder nicht? Die EU-Leitlinien zur Klassifizierung von KI-Systemen

11. November 2026 I 14:00 Uhr
Referent: Prof. Dr. Rolf Schwartmann, Leiter der Kölner Forschungsstelle Medienrecht, Technische Hochschule Köln; Vorstandsvorsitzender der GDD e.V., Bonn

Sachstand Datenomnibus und Datenschutzbeauftragt

12. November 2026 I 9:15 Uhr
Referent: Kai Zenner, Digitalreferent im Europäischen Parlament, Brüssel

Neue Aufsicht für Digitalgesetze durch die Bundesnetzagentur

12. November 2026 I 9:35 Uhr
Referentin: Andrea Sanders-Winter, Leiterin der Abteilung Digitales bei der Bundesnetzagentur, Bonn

KI im Arbeitsverhältnis

12. November 2026 I 16:45 Uhr, Forum 5
Referenten: Dr. Ruben Plum-Schneider, Persönlicher Referent der BfDI, Bonn; Dr. Johannes Dilling, Dilling Rechtsanwälte, Köln
Leitung: Prof. Dr. Gregor Thüsing, LL.M. (Harvard), Institut für Arbeitsrecht und Recht der sozialen Sicherheit der Universität Bonn; GDD-Vorstand, Bonn

Jetzt mehr erfahren und anmelden: Zur DAFTA



Foto: Akash Tholiya, Adobe Stock

Wenn die KI mithört: Zwischen Datenschutz, Strafrecht und Betriebsvereinbarung

Die Hamburger Senatskanzlei hat KI-Protokolle für Besprechungen erprobt. Wer Kamera und Mikrofon einschaltet, sollte damit in die Transkription einwilligen. Nach dem Hamburgischen Datenschutzbeauftragten lässt sich das datenschutzrechtlich „kaum als freiwillige Einwilligung“ deuten, wenn die Alternative Schweigen oder der Chat ist (Tätigkeitsbericht 2025). Für den großflächigen Einsatz stehe die Einwilligung „auf tönernen Füßen“. Er rät zu einer Dienstvereinbarung.

Die Senatskanzlei hatte eingewandt, die Protokollierung sei keine Aufzeichnung, weil nichts in wiedergabefähiger Form gespeichert werde. Datenschutzrechtlich ist die Umwandlung von Sprache in Text aber eine Verarbeitung personenbezogener Daten, auch ohne gespeicherte Audiodatei. Strafrechtlich ist das Argument hingegen tatsächlich entscheidend.
§ 201 StGB stellt die Aufnahme des nichtöffentlich gesprochenen Wortes unter Strafe. Die unmittelbare und ausschließliche Umsetzung in Text ist keine solche Aufnahme, solange das Gesprochene nicht dauerhaft gespeichert und nicht wieder hörbar gemacht werden kann. Nach wohl herrschender Ansicht geht die Pufferspeicherung marktüblicher Tools aber über die flüchtige Verarbeitung hinaus und ist daher tatbestandlich erfasst. Gelöst werden könnte den Fall aber über das Merkmal „unbefugt". Was datenschutzrechtlich erlaubt ist, soll strafrechtlich nicht verboten sein. Ansonsten bliebe nur die Einwilligung.
Zudem braucht die Verarbeitung eine Rechtsgrundlage nach Art. 6 DS-GVO. Eine wirksame datenschutzrechtliche Einwilligung scheitert im Beschäftigungsverhältnis aber oft an der Freiwilligkeit. Das Gesamtkonzept, das Georg Karl Bittorf mit anderen in den GDD-Erfa-Kreisen entwickelt hat, setzt für Beschäftigte deshalb auf eine Betriebsvereinbarung, für leitende Angestellte auf eine Richtlinie. Die Einwilligung bleibt Externen vorbehalten. Zu beachten ist, dass die Betriebsvereinbarung das Schutzniveau der DS-GVO nach dem EuGH nicht absenken darf. Wer transkribiert, muss daher begründen, warum ein Ergebnisprotokoll nicht genügt.
Strenger wäre der Maßstab, wenn die Stimme als besondere Kategorie zählte. Unter Art. 9 DS-GVO fällt die Stimme aber nur, wenn sie der eindeutigen Identifizierung dient. Das ist nach überwiegender Ansicht bei der Transkription nicht der Fall. Eine Grenze ist erst erreicht, wenn das System Stimmprofile speichert und Personen meetingübergreifend wiederkennt. Das Konzept rät dennoch zu einer Sprechertrennung nur über Metadaten wie dem Login.
Übrigens: Reines Transkribieren macht ein Tool nicht zur Hochrisiko-KI. Wie sich KI-gestützte Protokolle risikobewusst im Betrieb einführen lassen, stellt Georg Karl Bittorf in Forum 1 der 50. DAFTA vor. Wer tiefer einsteigen möchte, ist am 12. November 2026 in Köln oder online dabei.

Videokonferenzen mit KI protokollieren

12. November 2026 I 13:30 Uhr, FORUM 1

Referent: Georg Karl Bittorf, Konzern-Datenschutzbeauftragter beim Bezirksverband Westliches Westfalen der Arbeiterwohlfahrt, Dortmund; Leiter GDD-Erfa-Kreise Dortmund und Essen

Leitung: Bettina Herman, atarax Unternehmensgruppe, Herzogen-aurach; GDD-Vorstand, Bonn

Jetzt mehr erfahren und anmelden: Zur DAFTA

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

