# NEWS BOX DATENSCHUTZ

## INHALTSVERZEICHNIS




AUSGABE 8/2024

RDV

DATAKONTEXT

Levent Ferik

# EDITORIAL

Ist es ein „gutes Zeichen“, wenn Microsoft Klage gegen den Europäischen Datenschutzbeauftragten (EDSB) beim Gericht der Europäischen Union einreicht und dabei von der EU-Kommission unterstützt wird? Oder zeigt dies, dass das Phänomen „Vendor Lock-in“ auch die EU-Kommission betrifft? Grund für das Zerwürfnis sind die hohen Anforderungen an den datenschutzkonformen Einsatz von Microsoft 365 und die Frage, ob der EDSB mit seinen Maßnahmen gegen den Grundsatz der Verhältnismäßigkeit verstoßen hat. Der EDSB hatte im März 2024 mutmaßliche Datenschutzverstöße bei der Nutzung von Microsoft 365 durch die EU-Kommission öffentlich gemacht und zahlreiche Maßnahmen angeordnet.
Auch eine andere europäische Institution, die UEFA, machte kürzlich in datenschutzrechtlicher Hinsicht von sich reden. Für das sogenannte „Crowd Management“ bei der EURO 2024 hatte die UEFA eine Ticket-App entwickelt, die anonymisierte Standortdaten an Behörden wie die Polizei sendete. Diese Datenerfassung wurde jedoch weder im Google Play Store noch im Apple App Store explizit erwähnt, was gegen die Transparenzanforderungen der Datenschutz-Grundverordnung (DS-GVO) verstößt.
Neben der UEFA haben auch andere Verantwortliche negative Datenschutz-Karmapunkte gesammelt: Kommunikationsdaten von über 14.000 Insassinnen aus 20 Gefängnissen und forensischen Kliniken standen nach Angaben der IT-Sicherheitsexpertin und Aktivistin Lilith Wittmann frei zugänglich im Internet.

Elon Musk plant eine neue Funktion für Tesla-Fahrzeuge, bei der die Autopilot-Funktion deaktiviert wird, wenn „unsachgemäße Nutzung“ festgestellt wird. Datenschutzbedenken sind hier noch unklar, da Tesla-Fahrer erfahrungsgemäß wohlwollend auf solche Entwicklungen reagieren.
Meta geriet ebenfalls in die Kritik, weil es plante, öffentliche Nutzerdaten von Facebook, Instagram und Threads zur Schulung von KI-Assistenten zu verwenden. Nach heftiger Kritik wurde dieses Vorhaben vorerst verschoben.
Die Pornoindustrie gilt als Innovationstreiber in der Technologiebranche, besonders bei KI/AI. Das Berliner „Cybrothel“ bietet Kunden die Möglichkeit, Sex-Dolls mit generativer KI zu buchen und stundenweise Zimmer und Dienste zu reservieren.
Ein weiteres kontroverses Projekt ist „prison of the future – Cognify“. Die Idee dahinter ist, Täter nicht für Jahre einzusperren, sondern sie innerhalb weniger Minuten mit künstlichen Erinnerungen zu rehabilitieren.
Die Gesellschaft wird künftig verstärkt technologische Entwicklungen gegen ethische Bedenken abwägen müssen.

Ihr
Levent Ferik

**Sagen Sie uns Ihre Meinung**
**kundenservice@datakontext.com**

# Standardisierte Prüfung von Messengern

**Der Europäische Datenschutzausschuss (EDSA) hatte bereits auf Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) die Umsetzung des Auskunftsrechts durch die für die Verarbeitung Verantwortlichen nach Art. 15 DS-GVO als Thema für seine dritte koordinierte Durchsetzungsmaßnahme im Jahr 2024 ausgewählt.**

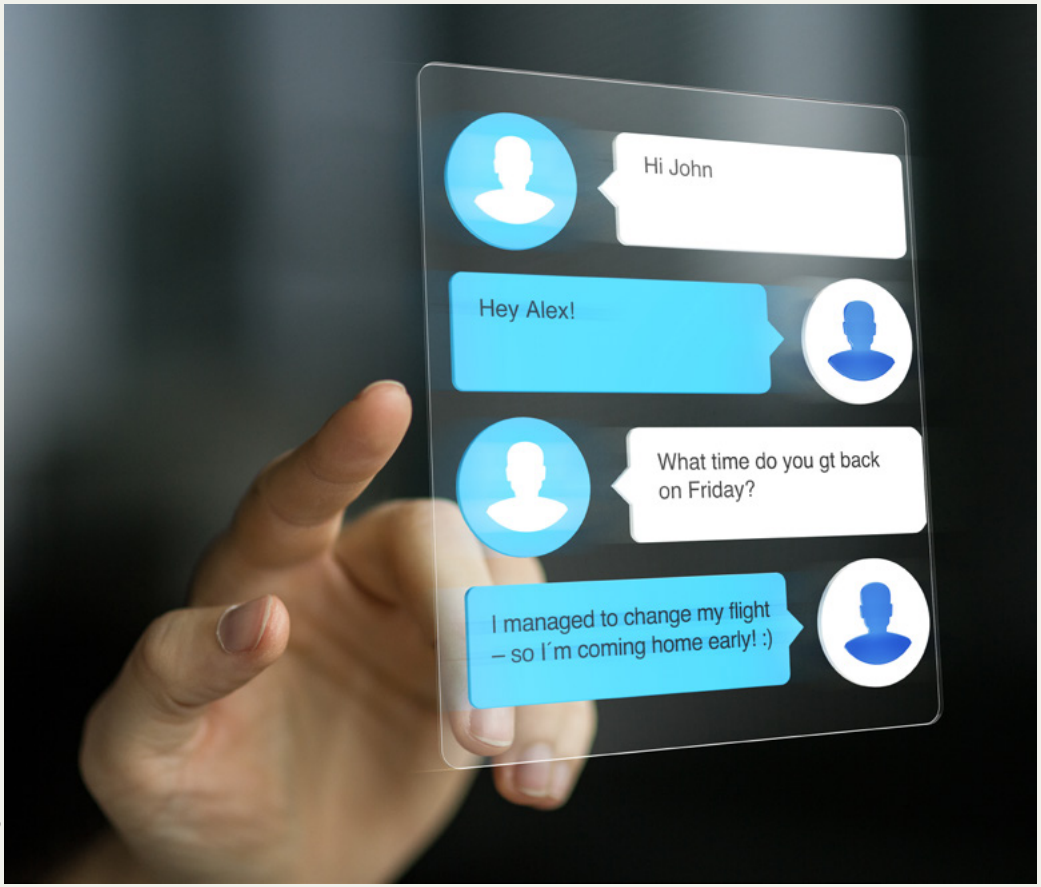


Foto: vegefox.com, Adobe Stock

Die koordinierten Maßnahmen erfolgen auf Basis des Beschlusses des EDSA vom Oktober 2020, einen koordinierten Durchsetzungsrahmen (Coordinated Enforcement Framework – CEF) einzurichten. Eine weitere Schlüsselmaßnahme im Rahmen der Strategie zur Verbesserung der Rechtsdurchsetzung stellt der im EDSA eingerichtete Expertenpool (**S**upport **P**ool of **E**xperts, SPE) dar.
In genau diesem Rahmen hat der BfDI ein weiteres eigenes Projekt initiiert und mit Beteiligung eines Experten aus dem SPE durchgeführt. Dabei wurde ein standardisierter Prüfkatalog zur Überprüfung der Nutzeroberfläche von Messenger-Diensten entwickelt (Standardised Messenger Audit – Frontend), der nun als Arbeitsgrundlage für die Kontrolle von Messenger-Diensten eingesetzt werden kann.
Das Projekt liefert einen Testkatalog mit obligatorischen, empfohlenen und optionalen Anforderungen, die ein GDPR-konformes Messenger-Frontend erfüllen muss. Der Katalog kann Datenschutzbehörden bei ihrer Arbeit unterstützen, aber auch Unternehmen, die ihre Produkte überprüfen und verbessern möchten.

Die beiden Dokumente können hier abgerufen werden:
1. Standardised messenger audit – Frontend requirements
2. Standardised messenger audit – Audit methodology


Foto: WoGi, Adobe Stock

# Auskunftsrecht vs. anwaltliche Verschwiegenheitspflicht

**Das Missbrauchspotenzial des Art. 15 DS-GVO ist recht hoch, und viele Fragestellungen im Zusammenhang mit dem Auskunftsrecht scheinen nach wie vor auch einer gewissen Dynamik innerhalb der Rechtsprechung unterworfen zu sein.**

Eine in der Praxis oftmals anzutreffende Frage scheint zu sein, ob das Auskunftsrecht genutzt werden kann, um im Rahmen einer juristischen Auseinandersetzung, nützliche Informationen über die eigene Person vom gegnerischen Anwalt zu erhalten.

In einem von der Sächsischen Datenschutzbeauftragten (LfD Sachsen) beschriebenen Fall forderte eine in einen Rechtsstreit verwickelte Person vom gegnerischen Rechtsanwalt Auskunft gemäß Art. 15 DS-GVO und forderte die Löschung seiner personenbezogenen Daten. Der Rechtsanwalt reagierte nicht darauf, woraufhin der Bürger Klage bei der LfD Sachsen einreichte.

Nach Prüfung der Rechtslage entschied die LfD wie folgt:

- Der Bürger hat grundsätzlich keinen Anspruch auf Auskunft oder Löschung gegenüber einem gegnerischen Rechtsanwalt.
- Diese Einschränkung des Auskunftsrechts ergibt sich aus Art. 23 Abs. 1 lit. g DS-GVO i. V. m. § 29 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG).
- Demnach ist das Auskunftsrecht ausgeschlossen, wenn durch die Auskunft Informationen preisgegeben würden, die nach einer Rechtsvorschrift geheim gehalten werden müssen, insbesondere solche, die der berufsrechtlichen Verschwiegenheitspflicht unterliegen.
- Diese umfasst grundsätzlich alle Informationen, die einem Rechtsanwalt im Rahmen seiner Berufsausübung bekannt werden (§ 43a Abs. 2 Bundesrechtsanwaltsordnung [BRAO]).
- Ausnahmen gelten nur für offenkundige Tatsachen oder solche, die keiner Geheimhaltung bedürfen, was jedoch selten der Fall ist.
- Auch die Tatsache, dass personenbezogene Daten bekannt sind, kann im Rahmen eines Mandatsverhältnisses relevant sein und unterliegt der Geheimhaltungspflicht, da der Rechtsanwalt andernfalls seine Berufspflichten verletzen würde.

## Fazit:

In einem solchen Fall greift die generelle Regel des § 29 Abs. 1 Satz 2 BDSG, wonach der Auskunftsanspruch keine Informationen umfasst, die der berufsrechtlichen Verschwiegenheitspflicht unterliegen, also alles, was Rechtsanwälten im Rahmen ihrer Berufsausübung bekannt wird (§ 43a Abs. 2 Satz 2 BRAO).


Foto: STOATPHOTO, Adobe Stock

# 4,3 Millionen Euro Bußgeld: Überschießende Datenübermittlung an externen Auditor

**Bei Prüfungen durch externe Auditoren müssen Unternehmen häufig große Mengen interner Daten – einschließlich personenbezogener Daten von Beschäftigten oder Kunden – weitergeben.**

In einem Fall in Niedersachsen hatte ein Unternehmen zwar datenschutzrechtliche Maßnahmen umgesetzt, dennoch stellte die niedersächsische Datenschutzaufsicht einige Mängel fest und verhängte deshalb ein Bußgeld und sprach Verwarnungen aus (vgl. 29. Tätigkeitsbericht 2023, Abschnitt G.3.5 ).

Weiter auf DataAgenda lesen

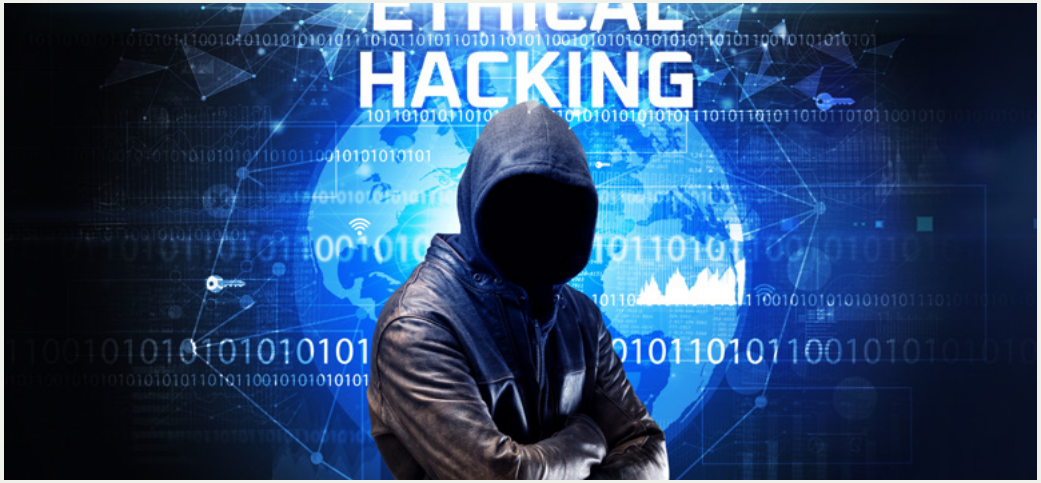


Foto: ra2 studio, Adobe Stock

# Ländervergleich: Wann beginnt „strafbares Hacking“?

**Verantwortliche im Bereich der IT-Sicherheit, der Informationssicherheit oder auch des Datenschutzes können mit dem Thema Hacking nicht nur im Zusammenhang mit böswilligen Angriffen auf die Systeme der verantwortlichen Stelle in Berührung kommen. „Angreifer“ oder Eindringlinge können durchaus auch „hehre Absichten“ haben oder genau zu diesem Zweck vom Verantwortlichen beauftragt worden sein.**

Ein sogenannter White-Hat-Hacker ist beispielsweise ein Angreifer, der in Systeme eindringt, dabei jedoch keinen Schaden verursacht. Im Gegenteil, er handelt im Interesse des betroffenen Unternehmens. White-Hat-Hacker führen oft im Rahmen einer Auftragsverarbeitung Penetrationstests durch und arbeiten völlig legal sowie in Absprache mit den Unternehmen, die sie testen.
Ein Grey-Hat-Hacker ist eine Unterkategorie des White-Hat-Hackers. Während White-Hat-Hacker meist beauftragt werden und sich strikt an die gesetzlichen Rahmenbedingungen halten, bewegen sich Grey-Hat-Hacker – wie der Name schon sagt – in einer rechtlichen Grauzone. Sie greifen Systeme an, um Sicherheitslücken aufzudecken, ohne dazu unbedingt autorisiert zu sein.
Unter anderen mit diesem Graubereich beschäftigt sich eine Ausarbeitung des Wissenschaftlichen Dienstes des Bundestags, unter dem Titel: Die Strafbarkeit des „Hackings“ – Rechtslage im internationalen Vergleich.
Auftragsgemäß untersucht diese Ausarbeitung die aktuellen strafrechtlichen Rechtsnormen im Bereich des „Hacking“. Dabei wird insbesondere auf die bestehenden Regelungen in Deutschland sowie auf die aktuelle Rechtslage in ausgewählten Mitgliedstaaten eingegangen. Zudem wird die Problematik bzw. der Umgang mit der „gewollten“ Aufdeckung von Sicherheitslücken dargestellt.
Damit können die oben genannten Funktionen aus den Bereichen IT-Sicherheit, Informationssicherheit, Datenschutz, aber ggf. auch Auftragsverarbeiter, die für Verantwortliche Penetrationstests etc. durchführen, die Ausarbeitung dazu nutzen, um die kritischen Grenzbereiche zwischen legalem Hacking und strafbarem Handeln auszuloten und sich einen länderübergreifenden Überblick über das Thema zu verschaffen.

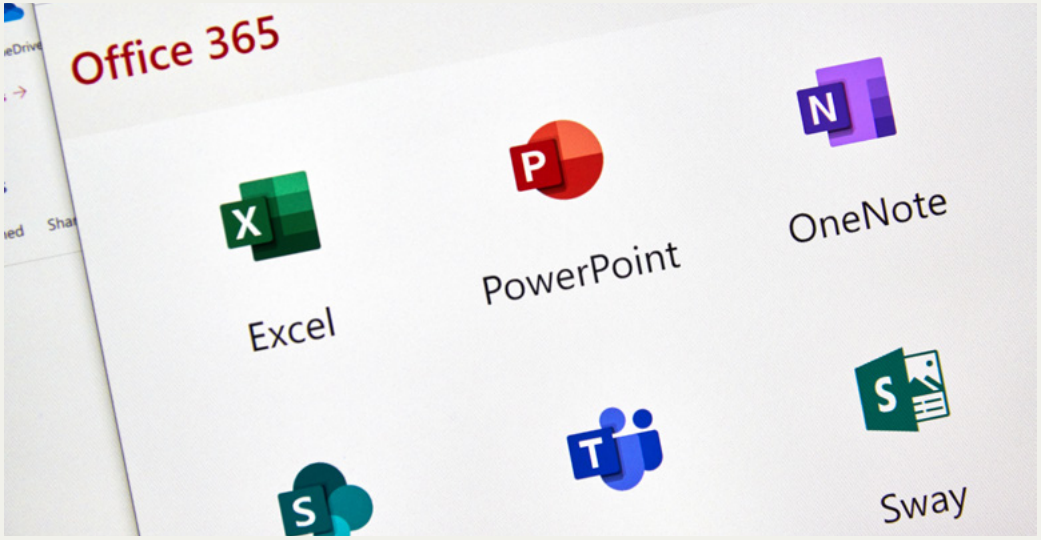


Foto: dennizn, Adobe Stock

# DSFA: Leitfaden für MS 365

**Microsoft vertritt die Auffassung, dass es in Microsoft Office 365 nichts gibt, was notwendigerweise die Erstellung einer Datenschutz-Folgenabschätzung (DSFA/DPIA) durch einen Datenverantwortlichen erfordern würde. Die etwaige Notwendigkeit, eine DSFA durchzuführen, hinge davon ab, wie der Verantwortliche Office 365 bereitstellt, konfiguriert und verwendet.**

Mit anderen Worten: In dem Zustand, in dem Microsoft MS 365 zur Nutzung bereitstellt, geht von den Anwendungen kein derartiges Risiko aus, welches eine Risikoabschätzung nach Art. 35 DS-GVO auslösen würde. Erst der Verantwortliche schafft durch die Art und Weise sowie die Zwecke, für die er die Software verwendet, ein Risiko, welches gegebenenfalls im Rahmen einer DSFA zu betrachten ist. Unabhängig davon, ob man diese Auffassung für überzeugend hält, können interessierte Verantwortliche auf den Seiten von Microsoft einen neuen Leitfaden abrufen, wie eine DSFA für MS 365 durchgeführt werden könnte.

Teil 1 des bereitgestellten Dokuments bietet den Verantwortlichen Informationen zu Office 365, die ihm als Datenverantwortlicher bei der Entscheidung helfen sollen, ob eine DSFA erforderlich ist. Sollte dies der Fall sein, findet der Verantwortliche in den Teilen 2 und 3 weitere Informationen von Microsoft, die ihn bei der Erstellung einer DSFA unterstützen sollen.

Teil 2 enthält allgemeine Antworten, die für alle Office-365-Dienste relevant sind, sowie die notwendigen Elemente einer DSFA. In Teil 3 werden produktspezifische Informationen bereitgestellt, die auf die wichtigsten Informationsbedürfnisse der Kunden abgestimmt sind, um ihre eigene DSFA zu erstellen. Zudem enthält Teil 3 ein beispielhaftes DSFA-Dokument, das heruntergeladen und angepasst werden kann, um die Erstellung einer DSFA zu erleichtern.

Office 365 umfasst Anwendungen und Dienste wie Exchange Online, SharePoint, OneDrive für Arbeit und Schule, Viva Engage und Microsoft Teams. Eine umfassendere Liste der über Office 365 verfügbaren Dienste finden Interessierte in den Tabellen 1 und 2 des Office 365-Leitfadens – Anträge betroffener Personen.

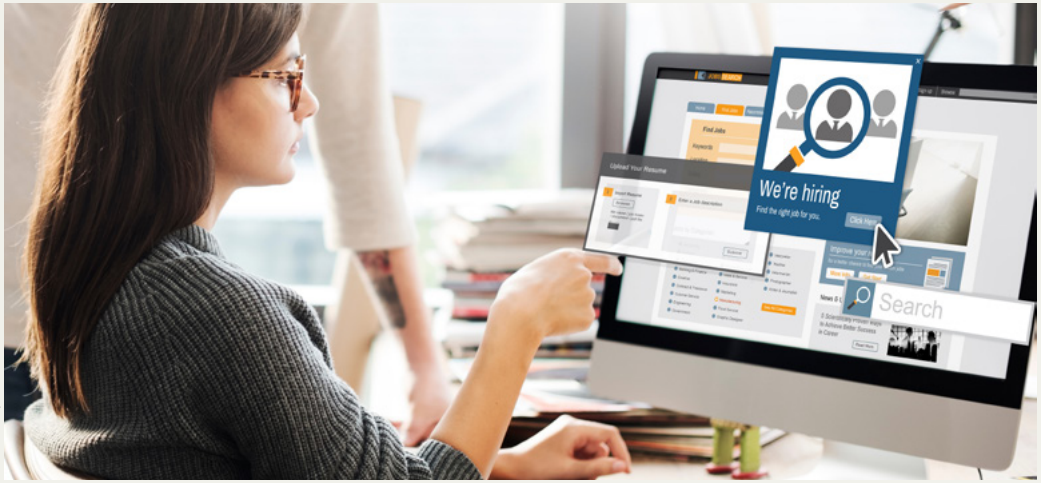


Foto: Rawpixel.com, Adobe Stock

# Anspruch des Betriebsrats auf Bewerbungsunterlagen in Papierform?

**In vielen Organisationen wird das gesamte Recruiting über sogenannte Bewerbermanagementsysteme abgewickelt (bspw. SAP SuccessFactors Recruiting).**

Zu den zahlreichen Vorteilen solcher Systeme gehört sicherlich, dass allen am Bewerbungsprozess beteiligten Personengruppen durch entsprechende Rollen- und Zugriffsberechtigungen zweckgebundene Einsichtsrechte erhalten und der Prozess von Anfang bis Ende medienbruchfrei gestaltet werden kann.

Weiter auf DataAgenda lesen

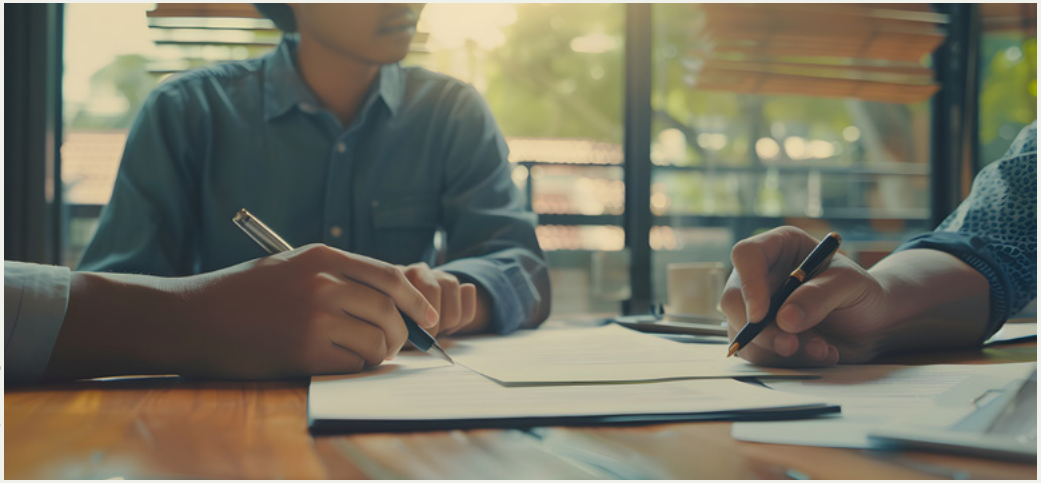

Foto: Ziyan Yang, Adobe Stock

# Neue Orientierungshilfe zum Thema „Gemeinsame Verantwortlichkeit“

**Bislang gab es nur wenige Veröffentlichungen seitens der Aufsichtsbehörden, die sich mit dem Thema der gemeinsam Verantwortlichen beschäftigen, obwohl die Rechtsfigur der „Gemeinsamen Verantwortlichkeit“ und die damit verbundene Frage, wie eine solche vertragliche Vereinbarung zwischen den beteiligten Verantwortlichen tatsächlich auszugestalten ist, seit Bekanntwerden des Art. 26 DS-GVO bei vielen Verantwortlichen große Fragezeichen aufgeworfen hat.**

Nach langer Zeit hat nun der Bayerische Landesbeauftragte für den Datenschutz hat eine Orientierungshilfe Gemeinsame Verantwortlichkeit veröffentlicht. Die neue Orientierungshilfe stellt die gemeinsame Verantwortlichkeit im Licht der Rechtsprechung insbesondere des Europäischen Gerichtshofs vor und gibt Handlungsempfehlungen für die bayerischen öffentlichen Stellen, von denen natürlich auch Verantwortliche außerhalb Bayerns profitieren können.
Nach Auffassung des BayLfD ist die Rechtsfigur der gemeinsamen Verantwortlichkeit weitaus häufiger anzutreffen, als gemeinhin angenommen wird. Die Orientierungshilfe möchte daher helfen, mögliche „Berührungsängste“ abzubauen, die gegebenenfalls daraus erwachsen, dass die gemeinsame Verantwortlichkeit den Anwendern immer noch weniger „vertraut“ erscheint als die seit jeher bekannte Auftrags(daten)verarbeitung.
Das Kurzpapier Nr. 16 „Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO“ der Datenschutzkonferenz unternahm als eine der ersten aufsichtsbehördlichen Veröffentlichungen zum Thema den Versuch, den Begriff und die mit dem Thema zusammenhängenden Abgrenzungsfragen aufzuarbeiten.
Die noch bestehenden Unsicherheiten rund um diese Rechtsfigur hat der LfDI BW versucht auszuräumen und ein Vertragsmuster für die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO zur Verfügung gestellt. Dieses Muster wurde auf Grundlage gemeinsamer Überlegungen mit einer Reihe von Unternehmen und öffentlichen Stellen entwickelt.
Erwähnenswert ist in diesem Zusammenhang auch die GDD-Praxishilfe XV: „Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO“. Mit dieser Veröffentlichung hat die GDD ihren Beitrag zur Beseitigung der bestehenden Verunsicherung geleistet und den Datenschutzpraktikern in Unternehmen und Behörden, die die Vorgaben aus Art. 26 DS-GVO umzusetzen bzw. deren Einhaltung zu überwachen haben, eine praxisbezogene Hilfestellung an die Hand gegeben. Abgerundet wurde die Praxishilfe durch eine Musterchecklist zum Joint Controllership.


## Data Agenda Podcast Folge 57: KI-Kompetenz Pflichten und Chancen für Unternehmen

Am 12. Juli 2024 wird die KI-Verordnung im Amtsblatt der EU veröffentlicht und am 1. August 2024 in Kraft treten. Was ist ein KI-System und was bedeutet es, dass es autonom agiert? Warum kann KI nicht denken und trotzdem sinnvoll in menschlicher Sprache antworten und Fragen stellen? Welche Nutzung von KI-Systemen ist gefahrlos möglich? Wo muss man aufpassen? Was bedeutet „prompten“ und wie geht das? Wie setzt man sich mit KI-Ergebnissen auseinander? Wie behält man als Mensch die Kontrolle über das Werkzeug KI? Was bedeutet der Einsatz von KI-Systemen im Unternehmen? Wo kann die Technologie helfen, wo nicht? Nach Ablauf einer Übergangsphase am 1. Februar 2025 müssen Betreiber und Anbieter von KI-Systemen sowie deren Beschäftigte diese Fragen kompetent beantworten können.
Wie das gelingen kann, ist Thema des Podcasts mit **Paula Cipierre**, Director of Data Ethics & Innovation bei ada Learning.

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

Bild: Alwie99d - stock.adobe.com