COMPLIANCE konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 1/2026

NIS-2: Und jetzt?

Warum schnelles Handeln entscheidend ist

Seite 6

Editorial

Liebe Leserin, lieber Leser,

Künstliche Intelligenz ist in der Praxis angekommen. Beim 2. Norddeutschen KI-Forum in Hannover wurde deutlich: Die Frage lautet nicht mehr „Ob KI?“, sondern „Wie setzen wir sie verantwortbar um?“ Zwischen Innovationsdruck und regulatorischen Vorgaben braucht es Pragmatismus und klare Governance.

Gleichzeitig steigt der Handlungsdruck durch neue gesetzliche Anforderungen. Mit Inkrafttreten des deutschen NIS-2-Umsetzungsgesetzes gelten die erweiterten Pflichten verbindlich und ohne Übergangsfrist. Für viele Organisationen bedeutet das: Risikomanagement schärfen, Meldeprozesse strukturieren und Verantwortung auf Leitungsebene verankern.

Auch im Datenschutz werden die Spielregeln präziser. Das Bundesarbeitsgericht hat klargestellt, dass Betriebsvereinbarungen keine pauschale Rechtsgrundlage darstellen, sondern sich strikt an den Anforderungen der DSGVO messen lassen müssen.

Was heißt das für Sie? Regulierung ist kein Bremsklotz, sondern ein Rahmen. Wer ihn klug nutzt, schafft Resilienz, digitale Souveränität und echte Zukunftsfähigkeit.

Wir wünschen Ihnen eine anregende Lektüre und neue Impulse für Ihre Praxis.

Herzliche Grüße

Thomas Althammer & Niels Kill

Darüber wird gesprochen

KLICK/SCAN

Weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: *althammer-kill.de/news*

Rückblick: Anwendertreffen der Connext Communication GmbH in Paderborn

Zwei Tage intensiver Austausch, viele praxisnahe Gespräche und wertvolle Impulse: Beim Anwendertreffen der Connext Communication GmbH in Paderborn standen für uns vor allem Künstliche Intelligenz und NIS-2 im Mittelpunkt.

Gemeinsam mit Silvio Franke und Thomas Althammer haben wir mit zahlreichen Fach- und Führungskräften über konkrete Anwendungsfälle, regulatorische Anforderungen und sinnvolle Umsetzungsstrategien gesprochen. Besonders deutlich wurde: Der Bedarf an Orientierung an der Schnittstelle von IT, Sicherheit und Compliance wächst ebenso wie der Wunsch nach pragmatischen, rechtssicheren Lösungen mit echtem Mehrwert.

KDG Novelle 2026: Mehr Klarheit, wenig Umbruch.

KLICK/SCAN

Zum 1. März 2026 trat die novellierte Fassung des Kirchlichen Datenschutzgesetzes (KDG) in Kraft. Die Reform bringt spürbare Klarstellungen, aber nur begrenzten akuten Handlungsbedarf. Lesen Sie im Blogbeitrag, was Verantwortliche jetzt wissen sollten.

Von NIS-2 zu ISO 27001 und TISAX: Synergien im Sicherheits- und Datenschutzmanagement nutzen

Viele Organisationen verfügen bereits über ein Informationssicherheits- oder Datenschutzmanagement. NIS-2 kommt nun als weitere Regulierung durch die EU hinzu und wird durch das nationale Umsetzungsgesetz (NIS2UmsuCG) verbindlich. In diesem Artikel zeigen wir, wie sich ein NIS-2-konformes Risikomanagementsystem aufbauen lässt, wo sich die Anforderungen mit ISO 27001, TISAX und DSGVO überschneiden und wie Sie

KLICK/SCAN

Doppelarbeit vermeiden, indem Sie bestehende Strukturen gezielt weiterentwickeln.

Omnibus ohne Fahrplan: Die EU baut ihr Digitalrecht um

Die Kommission will Doppelregeln abbauen und Prozesse vereinheitlichen – inklusive Single-Entry-Point für Meldungen und möglichen

KLICK/SCAN

Anpassungen bei DSGVO und Cookies. Was bedeutet das konkret für Ihre Governance?

Bundesamt für Sicherheit in der Informationstechnik (BSI) klärt auf: Rettungsdienste von NIS-2 betroffen

Nachdem Rettungsdienste zuvor nicht betroffen sein sollten, stellt das BSI nun klar: Rettungsdienste fallen unter den Begriff der „Gesundheitsvorsorge“ und gelten damit als Gesundheitsdienstleister im Sinne des BSIG. Zur Begründung verweist das BSI unter anderem darauf, dass im Rettungsdienst regelmäßig Personal aus Gesundheitsberufen eingesetzt wird.

Neben ärztlichem Personal ist insbesondere der Beruf der Notfallsanitäter gemäß § 1 NotSanG als reglementierter Gesundheitsberuf im Sinne der Richtlinie 2005/36/EG einzuordnen. Die Tätigkeit dient der Beurteilung, dem Erhalt und der Wiederherstellung des Gesundheitszustandes und wird unmittelbar gegenüber Patientinnen und Patienten erbracht.

Zahl des Monats

443

So viele Datenschutzverletzungen wurden 2025 täglich im Schnitt in Europa gemeldet.

Datenschutz- und Sicherheitsverantwortliche in Europa erhielten im Jahr 2025 jeden Tag mehr als 443 Meldungen zu Datenpannen, ein bisheriger Höchststand seit Einführung der DSGVO. Diese Zahl zeigt den enormen Druck auf Reporting- und Responsestrukturen in Unternehmen. Gleichzeitig lagen die durchschnittlichen Kosten pro Fall bei etwa 4 Millionen Euro (inklusive regulatorischer Strafen).

Handlungsfähig im Ernstfall: NIS-2 Incident-Response

Wenn es ernst wird, zählt nicht nur die Technik, sondern auch, ob Sie innerhalb von 24 bzw. 72 Stunden eine saubere Meldung abgeben können. Dieser Artikel zeigt Ihnen, wann

KLICK/SCAN

ein Vorfall gemäß NIS-2 als „erheblich“ gilt, welche Meldewege in Deutschland gelten und wie Sie eine Incident-Response-Strategie entwickeln, die Sie im Ernstfall handlungsfähig hält.

Exchange SE: Digitale Souveränität durch eigene Kommunikationsinfrastruktur

Exchange SE ist weiterhin als On-Premise-Lösung verfügbar und damit ein konkreter Hebel für digitale Souveränität. Wer Mail, Kalender und Verzeichnisdienste unter eigener Kontrolle betreibt (auch im EU-Rechenzentrum), reduziert Abhän-

KLICK/SCAN

gigkeiten und stärkt Resilienz sowie Compliance. Der Beitrag zeigt, wann On-Premises oder hybride Modelle strategisch sinnvoll sind und welche Betriebsanforderungen dafür sitzen müssen.

Veranstaltungen

Norddeutsches KI-Forum

Einen Rückblick auf das spannende diesjährige KI-Forum finden Sie im Heft ab *Seite 12*. Dieses KI-Forum verpasst? Dann reservieren Sie sich gleich den Feburar 2027 in Ihrem Kalender und seien Sie beim nächsten Mal dabei, wenn sich alles um Innovationen und Anwendungen der Künstlichen Intelligenz dreht.

NIS-2: Und jetzt?

Was das neue Gesetz jetzt konkret für Ihr Unternehmen bedeutet und warum schnelles Handeln entscheidend ist.

von Maximilian Klose

Die EU-Richtlinie NIS-2 (2022/2555) schafft einen europaweiten einheitlichen Rechtsrahmen für Cybersicherheit in 18 für die Bevölkerung wichtigen Sektoren. Sie ersetzt die erste NIS-Richtlinie und fordert klarere Regeln, weitet Risikomanagementpflichten und Meldepflichten für Betreiber wichtiger Dienste aus und vertieft die bestehenden. Konkret müssen Mitgliedstaaten nationale IT-Sicherheitsstrategien vorlegen und eine Liste kritischer Infrastrukturen führen. Auch Gesundheitsdienstleister sind ausdrücklich erfasst – NIS-2 nennt das Gesundheitswesen neben Energie, Verkehr, Finanzen oder digitaler Infrastruktur als einen der anzuwendenden Bereiche.

Umsetzung in Deutschland

In Deutschland wurde die NIS-2-Richtlinie Ende 2025 per Gesetz in nationales Recht überführt. Der Bundestag verabschiedete das „Gesetz zur Umsetzung der NIS-2-Richtlinie", das am 6. Dezember 2025 im Bundesgesetzblatt in Kraft gesetzt wurde. Damit gilt NIS-2 erstmals verbindlich, ohne Übergangsfristen – sämtliche betroffenen Stellen müssen sofort handeln und die neuen Richtlinien einführen. Nach den Vorgaben des Gesetzes sind rund 30.000 Unternehmen in Deutschland betroffen. Das Spektrum reicht von Betreibern kritischer Infrastrukturen (KRITIS) bis zu neuen Kategorien „wichtiger Einrichtungen", wie zum Beispiel in der Energie-, Verkehrs- oder Gesundheitsversorgung.

Neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind nun weitere Behörden wie BBK und BNetzA für die Aufsicht zuständig. Verstöße gegen die Vorschriften können mit Bußgeldern zwischen 100.000 und 20 Millionen Euro geahndet werden.

- Gesetzeskraft: Veröffentlichung 5.12.2025, wirksam ab 6.12.2025.
- Betroffene Sektoren: Energie, Transport, Finanzwesen, IT, Gesundheit usw. – darunter künftig u. a. Krankenhäuser, Arztpraxen, Labore, Hersteller von Medizinprodukten.
- Neu: Neben KRITIS-Unternehmen auch besondere und wichtige Einrichtungen nach EU-Definition, vor allem große und mittelgroße Firmen in kritischen Branchen.
- Pflichten: Erweitertes Risikomanagement, Informationssicherheitsmanagement (z. B. ISO 27001), klare Meldewege bei Sicherheitsvorfällen (innerhalb Stunden/Tagen).
- Sanktionen: Bis zu 10 Mio. Euro (oder 2 % Jahresumsatz) Bußgeld bei Nichteinhaltung.

NIS-2 – Die wichtigsten Fakten

Inkrafttreten in Deutschland:
6. Dezember 2025

Betroffene Unternehmen:
ca. 30.000

Besonders betroffen:
Gesundheitswesen

Meldefristen:
24 Std. Erstmeldung bzw.72 Std. Detailmeldung
1 Monat Abschlussbericht

Bußgelder: bis 10 Mio. €
oder 2 % Jahresumsatz

Persönliche Haftung der Geschäftsleitung möglich

Fokus Gesundheitswesen

Gesundheit zählt zu den vorrangigen Sektoren, die ihre Sicherheitsbestimmungen anpassen müssen. Krankenhäuser, Großpraxen, Rettungsdienste, Labore, Pharmafirmen und Hersteller kritischer Medizintechnik fallen künftig unter NIS-2. Auch private Gesundheitsanbieter müssen IT- und Prozessschutz prüfen und nachweisen. Kritisch ist dies insbesondere für den Gesundheitssektor, weil Cyberangriffe auf Kliniken lebensbedrohliche Folgen haben können.

Die neue Regelung verlangt für das Gesundheitswesen den Nachweis geeigneter Schutzmaßnahmen: technische Maßnahmen wie Verschlüsselung und Zugangsschutz, regelmäßige Risikoanalysen, Notfallpläne sowie Meldung jedes schweren Vorfalls an die zuständige Behörde. Hiermit soll gewährleistet werden, dass z. B. bei Ransomware-Angriffen möglichst schnell reagiert wird und Versorgungsketten (OP-Systeme, Notfallversorgung) nicht zusammenbrechen. Insgesamt weitet sich die Resilienzpflicht stark aus:

Nach NIS-2 müssen auch mittlere Unternehmen im Gesundheitsbereich angemessene IT-Sicherheitsvorkehrungen in Anbetracht der neuen Regelungen treffen, genauso wie große Kliniken.

Anforderungen für Unternehmen nach NIS-2-Richtlinie und Umsetzungsgesetz

Die NIS-2-Richtlinie (zweite EU-Directive zu Netzwerk- und Informationssicherheit) und das deutsche NIS-2-Umsetzungsgesetz (in Kraft seit Dezember 2025) bringen umfassende neue Pflichten für rund 30.000 Unternehmen in Deutschland. Betroffen sind insbesondere mittelgroße und große Organisationen in kritischen Sektoren wie Gesundheit, Energie, Verkehr, digitale Infrastruktur, Finanzwesen u. a. Im Folgenden sind die wichtigsten Anforderungen aufgeführt, die NIS-2-betroffene Unternehmen nun genau umsetzen müssen, sowie deren Bezug zu einem ISMS nach ISO/IEC 27001:2022:

1. Registrierung beim BSI

Alle betroffenen Einrichtungen müssen sich innerhalb von drei Monaten nach Inkrafttreten der nationalen Regelung beim BSI registrieren. Dazu sind u. a. Angaben zu Unternehmensdaten, Ansprechpersonen (Kontaktstelle) und IP-Adressbereichen zu machen. Änderungen dieser Daten müssen regelmäßig aktualisiert werden. (Die Registrierungspflicht stellt sicher, dass Behörden wissen, welche Unternehmen unter NIS-2 fallen.)

2. Etablierung eines strukturierten Risikomanagements

Unternehmen müssen ein ganzheitliches Risikomanagement für die Informationssicherheit einführen, idealerweise durch Aufbau eines ISMS nach ISO/IEC 27001:2022. Alle IT-Systeme, Komponenten und Prozesse, die für die Dienste des Unternehmens genutzt werden (inkl. Büro-IT), fallen unter den Sicherheits-Geltungsbereich. Die Risiken sind systematisch zu analysieren und durch angemessene technische und organisatorische Maßnahmen nach dem Stand der Technik zu behandeln. Ein ISMS gemäß ISO 27001 hilft dabei erheblich, da viele NIS-2-Anforderungen bereits aus ISO 27001 bekannt sind.

3. Notfall- und Business-Continuity-Management

Unternehmen müssen Notfallmaßnahmen implementieren, um ihre Betriebsfähigkeit im Ernstfall aufrechtzuerhalten bzw. rasch wiederherzustellen. Dazu gehören ein systematisches Backup-Management, Notfallpläne und Krisenmanagementprozesse. Diese Vorgaben matchen mit ISO-Standards (z. B. Aspekte von ISO 27001 und ISO 22301 für Business Continuity) und verlangen, dass Unternehmen Pläne für Aufrechterhaltung und Wiederherstellung ihrer Dienste dokumentieren.

4. Sicherheit bei Entwicklung und Beschaffung

NIS-2 verlangt, Sicherheitsanforderungen bei der Beschaffung, Entwicklung und Wartung von IT-Systemen und -Komponenten zu berücksichtigen. Unternehmen müssen klare Sicherheitsvorgaben für neue Systeme definieren und durchsetzen (z. B. Secure Development Lifecycle, geprüftes Patch- und Änderungsmanagement). Die ISO 27001:2022 enthält hierfür einschlägige Controls (wie Secure System Engineering und Schwachstellenmanagement), was die Umsetzung erleichtert.

5. Sicherheit in der Lieferkette (Supply-Chain-Security)

Da viele Informationssicherheitsvorfälle über Dienstleister oder Zulieferer erfolgen, müssen Lieferanten und Dienstleister vertraglich auf hohe Sicherheitsstandards verpflichtet werden. Erfolgreiche Supply-Chain-Attacks haben immense Auswirkungen. Unternehmen sollen Sicherheitsrisiken entlang der gesamten Lieferkette adressieren (z. B. Mindestanforderungen an Dienstleister, Überprüfen von Drittparteien).

6. Identitäts- und Zugangsmanagement

Unternehmen müssen ein wirksames Identitäts- und Berechtigungsmanagement etablieren. Dazu gehören Zugriffskontrollen nach dem Need-to-know-Prinzip und zentrale Verwaltung der Berechtigungen. Technische Maßnahmen wie Multi-Faktor-Authentifizierung (MFA) und moderne Kryptografie sind verpflichtend, um den Zugang zu Systemen und die Kommunikation abzusichern. Die NIS-2 fordert den Einsatz von Verschlüsselung nach Stand der Technik in allen Kommunikationsverbindungen.

7. Management von Sicherheitsvorfällen (Incident Response) und Meldepflichten

Unternehmen müssen Konzepte zur Erkennung und Bewältigung von IT-Sicherheitsvorfällen einführen. Insbesondere erhebliche Sicherheitsvorfälle sind unverzüglich an das BSI zu melden (innerhalb 24 Stunden nach Feststellung). Innerhalb von 72 Stunden muss eine Folgemeldung mit Details und Bewertung erfolgen, sowie innerhalb eines Monats ein Abschlussbericht mit Ursachen und ergriffenen Maßnahmen. Zusätzlich kann das BSI Zwischenberichte verlangen und betroffene Behörden informieren. NIS-2 schreibt auch vor, dass ggfs. Kunden und die Öffentlichkeit informiert werden müssen, wenn sie von einem schweren Vorfall betroffen sein könnten. Eine effiziente Incident-Response-Struktur (inkl. 24/7 Meldekanal) muss somit eingerichtet werden. Diese Pflichten gehen über die bisherigen Anforderungen (BSIG §8b) hinaus, sind aber mit ISO-konformen Incident-Management-Prozessen gut zu integrieren.

8. Personelle Sicherheit und Awareness

Es müssen Maßnahmen zur personellen Sicherheit getroffen werden, z. B. Zuverlässigkeitsüberprüfungen für sicherheitsrelevante Stellen und Sensibilisierung der Mitarbeitenden. Regelmäßige Schulungen der Geschäftsführung und Mitarbeitenden sind erforderlich, um eine sicherheitsorientierte Kultur zu etablieren. NIS-2 betont, dass auch das Top-Management involviert und geschult sein muss. ISO 27001 verlangt ebenfalls Schulungs- und Awareness-Maßnahmen, sodass hier eine klare Deckungsgleichheit besteht.

9. Dokumentation und Nachweispflichten

Alle umgesetzten Sicherheitsmaßnahmen müssen umfassend dokumentiert sein. Betreiber kritischer Anlagen (KRITIS-Betreiber) sind verpflichtet, die Umsetzung ihrer Schutzmaßnahmen alle drei Jahre durch Audits/Zertifizierungen nachzuweisen und dem BSI Bericht zu erstatten. Andere betroffene Einrichtungen müssen zwar nicht regelmäßig auditieren, aber Maßnahmen dokumentieren und auf Verlangen des BSI ebenfalls Nachweise erbringen (das BSI kann Stichproben-Prüfungen anordnen). Unternehmen sollten sich also auf Prüfungen vorbereiten, z. B. durch interne Audits oder Zertifizierungen nach ISO 27001, um compliancegerecht die Wirksamkeit ihres ISMS zu belegen.

10. Staatliche Aufsicht und Sektorregelungen

Das BSI übernimmt die Aufsicht über die NIS-2-Umsetzung. Je nach Sektor können zusätzliche branchenspezifische Sicherheitsauflagen gelten (z. B. über das TKG für Telekommunikation oder EnWG für Energie). Unternehmen im Finanzsektor fallen parallel unter DORA (EU-Finanzsektor-Verordnung) statt NIS-2. Betroffene Unternehmen müssen die für sie einschlägigen Vorschriften kennen und erfüllen.

11. Sanktionen und persönliche Haftung

Die NIS-2-Regulierung sieht drastische Strafen bei Verstößen vor. Es drohen Bußgelder von bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Wert höher ist). Neu ist, dass auch Geschäftsleitung und verantwortliche Managerinnen und Manager persönlich haftbargemacht werden können, wenn sie Compliance-Pflichten verletzen.

NIS-2 ist somit eine Compliance-Vorgabe auf Management-Ebene, die Verantwortung der Führungskräfte ist explizit verankert. Unternehmen müssen diese Anforderungen sehr ernst nehmen, um rechtliche Risiken und Reputationsschäden zu vermeiden.

Sofortmaßnahmen für Unternehmen

- Registrierung beim BSI prüfen
- Gap-Analyse zur ISO 27001 durchführen
- Incident-Response-Prozess etablieren
- MFA flächendeckend einführen
- Lieferanten-Sicherheitsprüfung starten
- Notfall- und Backup-Konzept testen
- Geschäftsleitung schulen

Fazit

NIS-2 und das deutsche Umsetzungsgesetz schaffen einen verbindlich einzuhaltenden Rahmen für Cyber-Sicherheit in für die Bevölkerung wichtigen Sektoren wie dem Gesundheitssektor. Krankenhäuser und andere Anbieter müssen nun frühzeitig technisch nachrüsten und organisatorische Vorkehrungen treffen, um die neuen Vorgaben zu erfüllen. Die erweiterte Regulierung soll helfen, Risiken wie Cyberangriffe oder Systemausfälle in lebenswichtigen Bereichen deutlich zu senken.

Michaela Wilke – die Stimme, die Türen öffnet

Wenn Michaela Wilke morgens den Laptop aufklappt, ist sie schon „im Kontakt“. Headset auf, Posteingang prüfen, kurz sortieren und dann beginnt das, was sie an ihrem Job am meisten schätzt: echte Gespräche.

von Fabian Eggers

Michaela arbeitet seit 2012 im Vertrieb, kennt die Dynamik am Telefon, die kleinen Pausen, in denen man spürt, ob am anderen Ende gerade Interesse entsteht – oder Skepsis. Und sie weiß genau, wie man aus beidem etwas macht.

Vom Tierheim in den Vertrieb – und zwar mit voller Überzeugung

Ihr beruflicher Weg klingt zunächst wie ein überraschender Seitenwechsel: Ursprünglich ist Michaela gelernte Tierheim- und Pensionstierpflegerin. „Also was ganz anderes“, sagt sie selbst. Und doch passt der Schritt in den Vertrieb rückblickend erstaunlich gut: Wer mit Tieren arbeitet, braucht Geduld, Fingerspitzengefühl, Aufmerksamkeit und die Fähigkeit, Situationen schnell zu lesen. Eigenschaften, die auch im Vertrieb den Unterschied machen.

Heute bringt Michaela genau das in ihre Arbeit ein: Ruhe, Klarheit, eine gute Portion Humor und eine direkte, sympathische Art, die im Gespräch sofort ankommt.

Wie sie zu Althammer & Kill kam

Auf Althammer & Kill wurde Michaela über einen Kontakt aufmerksam, der vielen im Unternehmen bekannt ist: Mike Brust. Die beiden kennen sich seit mehreren Jahren. Als in unserem Vertrieb Verstärkung gesucht wurde, hat Mike sie angesprochen und dabei so überzeugend von uns gesprochen, dass Michaela nicht lange zögerte. „Deswegen bin ich heute hier“, sagt sie schlicht. Man merkt: Es war keine Bewerbung „ins Blaue“, sondern ein Schritt mit gutem Gefühl.

„Vertrieb heißt für mich: Spaß an Kommunikation“

Michaela beschreibt Vertrieb nicht als Druck oder stures Abschließen, sondern als etwas, das im Kern menschlich ist: Kommunikation, gemeinsames Arbeiten an Zielen und das Gefühl, etwas zu bewegen.

Dabei kennt sie auch ihre eigene Bühne sehr genau. Klassischer Ladenverkauf? Eher nicht. „Am Telefon kann man einfach auflegen, wenn man keine Lust hat“, sagt sie mit einem Lachen und trifft damit einen Punkt, der im Vertriebsalltag oft unterschätzt wird: Am Telefon zählt jede Sekunde. Wer dranbleibt, muss schnell Vertrauen aufbauen, klar sein und die andere Person trotzdem respektvoll „abholen“.

Ihre Aufgaben: dranbleiben, anbahnen, vorbereiten

Aktuell liegt Michaelas Schwerpunkt auf zwei Bereichen:
Kunden nachfassen – also Kontakt halten, Gesprächsfäden aufnehmen, anknüpfen, wenn das Timing passt. Neue Kunden akquirieren – inklusive Kaltakquise: anrufen, kurz vorstellen, Interesse wecken, erste Fragen beantworten und den nächsten Schritt organisieren.

Ein wichtiger Teil davon ist die Terminvorbereitung für den etablierten Vertrieb: Michaela pitcht das Unternehmen, klärt erste Eckpunkte, sammelt Informationen und sorgt dafür, dass im anschließenden Termin schon eine Basis da ist. Gerade in der Kaltakquise, sagt sie, müsse man „schon ein bisschen was wissen, damit das funktioniert“. Es geht also nicht ums „Durchklingeln“, sondern ums kluge Vorziehen: genug Kontext liefern, um Relevanz zu erzeugen ohne zu überfrachten.

Homeoffice, Teilzeit – und trotzdem mitten im Geschehen

Michaela arbeitet in Teilzeit und zu 100 % im Homeoffice. Ihr Arbeitsalltag ist klar strukturiert: Laptop auf, Headset auf, E-Mails checken und dann telefonieren, dokumentieren, nachhalten. Am Ende: Laptop zu.

Und ja, es gibt Rituale. Kaffee gehört dazu. „Junkie“, nennt sie sich augenzwinkernd. Zwei Tassen erlaubt sie sich offiziell – auch wenn sie „eigentlich gerne vier oder fünf“ trinken würde. Dazu permanent Tee, am liebsten Kamille. Kleine Details, die zeigen: Vertrieb ist Hochkonzentration und braucht genau die kleinen Anker, die den Tag stabil halten.

Was sie an ihrer Arbeit liebt: Menschen „aus der Reserve locken“

Am meisten Freude macht Michaela das Gespräch selbst. Weil es nie gleich läuft. Weil jeder Kontakt anders reagiert. Und weil es manchmal genau darum geht, einen Moment zu finden, in dem aus „eigentlich keine Zeit“ plötzlich ein echtes Gespräch wird. Sie beschreibt das sehr treffend: Niemand hat Lust auf einen Anruf, bei dem am Ende das Portemonnaie aufgeht. Alle wissen das. Aber trotzdem kann man eine Ebene finden, auf der man sich versteht und sogar gemeinsam lacht. „Den Menschen abholen am anderen Ende des Headsets“ – das ist für Michaela der Kern ihres Jobs.

Erfolg ist mehr als eine Zahl

Natürlich gibt es Ziele. Und natürlich gehören Zahlen zum Vertrieb. Aber Michaela misst Erfolg nicht nur daran, ob ein Auftrag zustande kommt. Ein Tag ist für sie auch dann erfolgreich, wenn ein Gespräch richtig gut war. Wenn der Kunde zum Beispiel sagt: „Normalerweise gehe ich nie ran… aber mit Ihnen war das richtig schön.“

„Genau so öffnen sich Türen. Und genau so beginnt Zusammenarbeit.“

Selbst ein klares „Wir kommen nicht zusammen“ kann für sie ein gutes Ergebnis sein; wenn es respektvoll, offen und angenehm war. Denn daraus entsteht oft etwas, das man im CRM nicht sofort ablesen kann: Vertrauen. Und Vertrauen wirkt nach. Gerade in unseren Themenfeldern, wo Entscheidungen selten „mal eben“ fallen.

Blick nach vorn: Diese Themen prägen 2026

Für 2026 sieht Michaela zwei Schwerpunkte, die in Unternehmen weiter stark an Bedeutung gewinnen werden:

Künstliche Intelligenz (KI):
Viele Unternehmen sind aktuell noch in der Orientierungsphase: Welches Tool ist sinnvoll? Wie wird es eingesetzt? Sobald Klarheit entsteht, steigt der Bedarf an Unterstützung, besonders bei der Implementierung und bei der Frage, was dabei zu beachten ist. Michaela nennt hier auch das Thema Schatten-KI: Wenn Tools genutzt werden, ohne dass Prozesse, Datenschutz oder Sicherheitsanforderungen sauber geregelt sind. Genau dort sieht sie Althammer & Kill als starken Partner.

Informationssicherheit und NIS-2:
Mit der NIS-2-Richtlinie ist das Thema Informationssicherheit für viele Organisationen nicht mehr optional, sondern Pflicht und Priorität. Michaela rechnet mit spürbar steigender Nachfrage.

Kurz gefragt: Was man über Michaela wissen sollte

Basis: Berlin, Vertriebserfahrung seit 2012

Stärke: Gesprächsführung, Timing, verbindliche Kommunikation

Arbeitsmodus: Teilzeit, 100 % Homeoffice, strukturiert und konsequent

Lieblingsmoment: Wenn aus Skepsis ein gutes Gespräch wird – inklusive Lachen

Blick in die Zukunft: KI (inkl. Schatten-KI) und Informationssicherheit/NIS-2

Michaela Wilke ist die Art Kollegin, die man am liebsten zuerst anrufen lässt: weil sie zuhört, schnell versteht, sauber sortiert und weil sie es schafft, dass man am Ende des Gesprächs denkt: „Okay, das war jetzt wirklich nett.“

Zwischen Pragmatismus und Überregulierung

Das von Althammer & Kill mit der HSVN initiierte 2. Norddeutsche KI-Forum in Hannover stand ganz im Zeichen der Frage, wie sich KI unter engen rechtlichen und organisatorischen Grenzen pragmatisch in Wirtschaft, Verwaltung und kommunale Praxis integrieren lässt.

von Thomas Althammer

Die Expertinnen und Experten diskutierten mit den Teilnehmenden aus Unternehmen, Kommunen, Organisationen und Wissenschaft entlang konkreter Use Cases statt abstrakter Zukunftsszenarien: Wie kann die Sozialwirtschaft/Energiebranche/Pflege KI sorgfältig einführen und nutzen? „Mit Augenmaß!“ sagt Thomas Althammer, Geschäftsführer des Beratungsunternehmens Althammer & Kill.

Volles Haus, klare Schwerpunkte

Das KI-Forum knüpfte an die Premiere 2025 an und wurde erneut von der Kommunalen Hochschule für Verwaltung in Niedersachsen (HSVN) und Althammer & Kill organisiert, unterstützt von kommunalen Spitzenverbänden und weiteren Partnern. Mit über 220 Teilnehmenden war die Veranstaltung ausgebucht, was den Handlungsdruck

Dr. Tina Klüwer

hinsichtlich Künstlicher Intelligenz (KI) in der Fläche unterstrich. Die Mischung aus Entscheidern, IT-Verantwortlichen und Führungskräften aus Wirtschaft, Verwaltung und Wissenschaft sorgte für eine Atmosphäre mit spürbarem Gestaltungswillen: Diskussionen drehten sich um konkrete Projekte, Governance-Fragen und Skalierung, nicht um KI-Grundsatzdebatten.

Zentral war die Beobachtung: KI ist für die Organisationen kein Zukunftsthema mehr, sondern wandert in Umsetzungsprojekte – etwa in Antragsbearbeitung, Wissensmanagement oder Plattformen für den öffentlichen Nahverkehr. „Dass trotz der Komplexität der Technologie sowie den hohen regulatorischen Anforderungen bereits viele Projekte in der Pilotphase sind, zeigt uns, dass KI in Verwaltung und Privatwirtschaft angekommen ist.“, sagte Thomas Althammer. Parallel wächst der Druck durch Digitalisierungsprojekte wie Registermodernisierung, XÖV-Standards und NIS-2-Vorgaben, die sowohl zusätzliche Pflichten als auch neue Einsatzfelder für KI schaffen. Damit verschiebt sich die Frage von „Ob KI?“ hin zu „Wie verantwortbar, mit welchen Partnern und auf welcher Infrastruktur?“.

Zwischen Überregulierung und Umsetzungswillen

Die Eröffnungs-Keynote von Dr. Tina Klüwer zeichnete das Spannungsfeld scharf nach: Europa verfügt über exzellente Forschung, starke Ingenieurtradition „Made in Germany“ und eine gewachsene Innovationslandschaft, hinkt aber bei den Zukunftstechnologien hinter den USA und China her. Sichtbar werde das unter anderem daran, dass die zehn wichtigsten Tech-Unternehmen der Welt fast ausschließlich aus den USA stammen und Deutschland im Innovationsindex 2025 erstmals nicht mehr in den TOP 10 vertreten war (Platz 11). Gleichzeitig fehlen in Deutschland und der EU aus ihrer Sicht gezielte Zukunftsinnovationen – ein Problem, das durch mangelnde Bildungsinvestitionen verschärft wird; bei den Pro-Kopf-Ausgaben für Bildung liegt Deutschland als drittgrößte Volkswirtschaft im globalen Vergleich auf dem schwachen 56. Platz.

Klüwer leitete daraus konkrete Forderungen ab:
- Stärkere Forschungsanreize, etwa durch bessere finanzielle Rückflüsse aus Lizenzvergaben an Lehrstühle.
- Verbindlicher Austausch zwischen Forschung und Wirtschaft, um Transfer zu erzwingen.
- Ausbau von Startup-Ökosystemen und leichterer Zugang zu Wagniskapital.
- Überarbeitung regulatorischer Rahmenbedingungen sowie mehr Investitionen in Bildung, um langfristig Innovationsfähigkeit zu sichern.

Norddeutsches KI-Forum

Noch zugespitzter formulierte es IT-Fachanwalt Joerg Heidrich, der den europäischen AI Act als defacto „KI-Verhinderungsgesetz“ bezeichnete. Er argumentierte, dass die Normierung mit ihren Pflichten viele Organisationen faktisch von der Eigenentwicklung oder produktiven Nutzung leistungsfähiger KI-Systeme ausschließe – insbesondere, wenn sie als Hochrisiko-Systeme gelten.

Als Beispiel nannte Heidrich den HR-Bereich. Dort rutsche nahezu jede KI-Unterstützung – von der Bewerbervorauswahl über Aufgabenzuteilung bis zu Beförderungs-

Podiumsdiskussion: Hat Deutschland das Zeug zur KI-Nation?

entscheidungen – in die Hochrisiko-Kategorie. Damit wird die Abwägung „KI-Entscheidung vs. menschliche Entscheidung“ nicht nur zur ethischen, sondern auch zur haftungsrechtlichen Frage. Unternehmen und Verwaltungen können dem aus seiner Sicht nur begegnen, indem sie eine klare Risikoklassifizierungen vornehmen, ein Compliance-Management speziell für KI aufbauen, eine hohe Datenqualität sicherstellen, oder konsequent menschliche Aufsicht etablieren und Einsätze möglichst außerhalb der Hochrisiko-Zone gestalten.

Praxisbeispiele: Vom LLM Vertragsmanagement bis zu Verwaltungsagenten

Zu den „Praxis-Workshops“ gehörten dabei unter anderem Beispiele der Landeshauptstadt Hannover, die zeigten, wie KI in bestehenden Fachanwendungen verankert werden kann.

Anne Vogler und Simon Pauka vom Institut für integrierte Produktion Hannover (IPH) zeigten KI-Potenziale für KMU am Beispiel eines dokumentenzentrierten Wissensmanagements. Ziel war, Verträge und Dokumente zentral, intuitiv und über ein Open-Source-Sprachmodell zugänglich zu machen. Dazu setzten sie auf den RAG-Ansatz (Retrieval-Augmented-Generation).

Dr. Laurine Oldenburg und Benjamin Klein von GovConnect präsentierten ein Praxisbeispiel aus der Verwaltung, das deutlich machte, wie breit der Einsatz von KI-Agenten gedacht werden kann. Die vorgestellte Plattform umfasst unter anderem:

- eine Agentenbibliothek für Sachbearbeitung sowie Bürgerinnen und Bürger,

In den großzügigen Pausen steht das Netzwerken im Fokus.

Thomas Althammer und Prof. Dr. Tim Brockmann begrüßen zum Abendprogramm.

- Analyse und Reporting-Funktionen für Kommune, Land und Partner,
- Rollen und Rechtemanagement, Integrations- und Konnektorkonzepte zu Fachverfahren,
- spezialisierte KI-Module und kombinierte Nutzung von Datenbanken und Large Language Models (LLMs).

Mit derzeit 39 Pilotprojekten – davon 27 in Kommunen – adressiert die Plattform typische Anwendungsfälle wie die Erstellung und das Auffinden von Inhalten, Bürgerkommunikation und Prozessabwicklung. Oldenburg betonte, dass der Erfolg nicht nur von der Technologie, sondern auch vom Change-Management abhängt: „Verwaltungen müssen die Veränderung aktiv gestalten, Mitarbeitende mitnehmen und den Mehrwert der Lösungen sichtbar machen, damit Akzeptanz und Kompetenz wachsen.“

Mensch im Mittelpunkt: Human in the Loop und sichere Nutzung

Monika Frech vom Hasso-Plattner-Institut für Digital Engineering rückte die Rolle des Menschen im KI-Einsatz in den Mittelpunkt. Wenn KI-Einführung in Organisationen gelingen soll, darf die Handlungsmacht auf der Metaebene nicht von Menschen auf Maschinen verschoben werden. Effizienz sei nicht automatisch Wert, Geschwindigkeit nicht zwingend Qualität, Automatisierung nicht per se Fortschritt. Entscheidend sei die Frage: Welches konkrete Problem löst die KI und wo ist ihr Einsatz sinnvoll? Frech zeigte, wie Design Thinking – Verstehen, Beobachten, Ideen finden, Prototyp testen und iterieren – helfen kann, den Einsatz von KI entlang echter Nutzerbedürfnisse zu gestalten. Human in the Loop bedeutet aus ihrer Sicht, die Verteilung von Entscheidung und Verantwortung zwischen Mensch und Maschine bewusst zu regeln: Wer darf was entscheiden, wer kontrolliert wen, wann greift welche Eskalation? Ihr Bild „KI ist ein richtiger Hammer. Wenn Sie aber nicht wissen, welchen Nagel Sie damit einschlagen wollen, dann schlagen Sie erstmal nur um sich“ brachte diesen Pragmatismus eindrücklich auf den Punkt.

Die sicherheitsrelevante Perspektive beleuchtete Petra Alef vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Sie unterschied Risiken bei ordnungsgemäßer Nutzung, Missbrauch sowie Angriffen von außen und ging beispielsweise auf KI-Agenten ein, die planen, delegieren, komplexe Aufgaben ausführen, Werkzeuge nutzen und auf externe Datenquellen zugreifen.

Durch ihren breiten Zugriff – etwa auf Endgeräte, E-Mails oder Cloud-Ressourcen – können sie bei unzureichender Absicherung zum Einfallstor werden. Anwendungen wie CloudBot/MoltBot, die Mails versenden, Skills nachladen und auf Serverkomponenten zugreifen können, verdeutlichen die mögliche Angriffsdynamik.

Gegenmaßnahmen umfassen vor allem sorgfältige Auswahl und Kuratierung der Trainingsdaten, Filterung von Ein- und Ausgabedaten sowie das Prinzip der Datensparsamkeit bei Berechtigungen und Zugriffen.

Im Prompting-Block zeigten Thomas Althammer und Joerg Heidrich, wie generative KI als Output-Beschleuniger und Qualitätsverstärker fungieren kann – vorausgesetzt, sie wird bewusst konfiguriert. Neben Beispielen für Lieblingsprompts und -tools gab es jede Menge praktische Hinweise:

- In den Einstellungen die Option zur Nutzung von Daten zur Modellverbesserung deaktivieren
- Halluzinationen durch Verifizierung von Fakten und Zitaten begegnen
- Präzise Prompts statt vager Anweisungen formulieren
- Ergebnisse durch zweite Modelle oder alternative Tools gegenprüfen lassen
- Der KI explizit sagen, was sie nicht tun soll (Negativ Instruktionen)

Fazit: Mit Augenmaß agieren

Über alle Beiträge hinweg zeichnete das KI-Forum ein deutliches Bild: Der Widerspruch zwischen europäischem Regulierungsanspruch und wirtschaftlicher und kommunaler Praxis ist real, aber er muss nicht lähmen.

Unternehmen und Kommunen warten nicht auf perfekte Rahmenbedingungen, sondern wählen gezielt Anwendungsfelder mit konkretem Nutzen – von Wohngeldanträgen über Bürger-und Kundenkommunikation bis hin zu Wissensmanagement und Nahverkehr – und legen parallel die strukturellen Grundlagen für rechtssichere Skalierung.

KI-Forum 2026 – das Veranstaltungs-Team

Führungskräfte und Verantwortliche setzen sich mit dem Umgang mit KI auseinander, um Chancen und Risiken der Technologie bestmöglich auszubalancieren. Sie müssen einen ausgewogenen Ansatz finden, um an Innovation und Fortschritt zu partizipieren, ohne die ethischen Grundsätze und die Verantwortung für ihre Zielgruppen aus den Augen zu verlieren.

Die Kombination aus Pragmatismus und Kooperation bringt dabei die Digitalisierung voran. Die Regulierung mag schwerfällig sein; die Praxis in den Unternehmen ist es nicht. Damit wird das Norddeutsche KI-Forum zum Labor dafür, wie Deutschland trotz komplexer Rahmenbedingungen mit KI tatsächlich vorankommen kann. &

Save the date

Dieses KI-Forum verpasst? Dann merken Sie sich gleich den **Februar 2027** vor und seien Sie beim nächsten Mal dabei, wenn sich alles um Innovationen und Anwendungen der Künstlichen Intelligenz dreht.

Betriebsvereinbarung unter Druck

Warum der EuGH die Spielregeln für Datenschutz im Beschäftigungskontext neu justiert und Unternehmen jetzt genauer hinsehen sollten

von Winona Wenning

Das Bundesarbeitsgericht (BAG) konkretisiert nach Vorlage an den EuGH die Anforderungen an Betriebsvereinbarungen als datenschutzrechtliche Rechtsgrundlage. Für Unternehmen bedeutet das: mehr Präzision, mehr Dokumentation und vielleicht auch weniger Spielraum. Das Bundesarbeitsgericht hat mit Urteil vom 08.05.2025 (8 AZR 209/21) eine für die Praxis relevante Entscheidung getroffen – mit europäischer Unterstützung. Ursprung war die geplante Einführung einer cloudbasierten HR-Software namens „Workday" – schon im Testbetrieb übermittelte man sensible Daten deutscher Beschäftigter an andere Konzernteile, auch in die USA.

Weil er damit die Grenzen der zugehörigen Betriebsvereinbarung mehrfach als überschritten ansieht, klagt ein Mitarbeiter auf Schadensersatz. Am Ende spricht das Gericht dem Mitarbeiter 200€ zu. Doch die Relevanz der Entscheidung liegt nicht im Betrag, sondern in der dogmatischen Klärung, welche die Richter aus Erfurt anstrebten:

Wann kann eine Betriebsvereinbarung überhaupt eine tragfähige datenschutzrechtliche Rechtsgrundlage sein?

Zum Fall

Zur Einführung der neuen HR-Software hatte man eine Betriebsvereinbarung als Rechtsgrundlage geschlossen, welche aber zunächst nur die Testphase regelte. Zu den angeblichen Testzwecken wurden auch Datenkategorien von deutschen Beschäftigten, welche in der Vereinbarung gar nicht benannt waren, bereits innerhalb des Konzerns in Drittländer übermittelt. Der Mitarbeiter klagte auf Ersatz der durch Kontrollverlust erlittenen Schäden, verursacht durch Nichteinhaltung der DSGVO, gemäß Art. 82 Abs. 1 DSGVO.

Mit seiner Klage scheiterte er zunächst vor dem Arbeitsgericht in Ulm und bei der Berufung vor dem Landesarbeitsgericht. Das BAG lies den Fall dann zur Revision zu. Statt der angestrebten 3000€ sprach man ihm am Ende nur 200€ Schadensersatz zu. Klar wird dennoch:

Die gefasste Betriebsvereinbarung regelte den Testbetrieb der neuen HR-Software. Erlaubt war die Übertragung bestimmter Daten (Name, Eintrittsdatum, Arbeitsort etc.). Durch die Verarbeitung zusätzlicher sensibler Daten (u.a. Gehalt, private Anschrift, Steuer-ID) und die erst für den Produktivbetrieb notwendige Drittlandsübermittlung wurden die Grenzen der Betriebsvereinbarung überschritten. Fanden also diese Verarbeitungen ohne Rechtsgrundlage statt?

Ja. Das BAG stellt fest:

- Die Verarbeitung der zusätzlichen Datenkategorien und die im Test nicht notwendige USA-Übermittlung waren durch die Betriebsvereinbarung nicht gedeckt. Mit der Überschreitung scheidet Art. 88 Abs. 1 DSGVO iVm der Betriebsvereinbarung als Rechtsgrundlage aus.
- Die generelle Begründung durch § 26 Abs. 1 BDSG iVm Art. 88 Abs. 1 DSGVO ist nicht zulässig, da § 26 Abs. 1 BDSG nicht spezifisch genug ist.
- Zu Testzwecken können Echtdaten notwendig sein, wenn sog. „Dummy-Daten" dazu tatsächlich nicht ausreichen. Werden bestimmte Datenkategorien nicht in die Betriebsvereinbarung aufgenommen, sind diese wohl auch nicht erforderlich. Das berechtigte Interesse des Arbeitsgebers Art. 6 Abs. 1 lit. f DSGVO scheidet auch aus.

Zur Frage, ob die konkrete Betriebsvereinbarung die Anforderungen der DSGVO erfüllte, äußerte sich das BAG nicht, denn der Kläger schränkte sein Begehren im Prozess insoweit ein. Zur abstrakten Klärung der Frage auf europäische Ebene kam es durch die Vorlage an den EuGH (C-65/23) dennoch.

Rechtliche Grundlage: Wo liegt der Knackpunkt?

Jede Verarbeitung von personenbezogenen Daten erfordert gem. Art. 6 bzw. Art. 9 DSGVO eine Rechtsgrundlage. Für den Beschäftigungskontext ermöglicht Art. 88 DSGVO dem nationalen Gesetzgeber die Schaffung von nationalen Spezialregeln unter besonderen Voraussetzungen durch Gesetze oder Kollektivvereinbarungen. So erlaubt § 26 Abs. 4 BDSG es, die Verarbeitung personenbezogener Daten der Beschäftigten auch auf Grundlage einer Kollektivvereinbarung durchzuführen. Also sind Datenverarbeitungen, welche eine Betriebs- oder Dienstvereinbarung vorsieht, immer erlaubt – oder?

Daraus ergaben sich die folgenden Leitfragen:

1. Müssen Kollektivvereinbarungen gem. Art. 88 DSGVO als Rechtsgrundlage stets auch alle sonstigen DSGVO-Vorgaben wie Art. 5, Art. 6, Art. 9 DSGVO einhalten?
2. Falls ja: Steht den Parteien einer Kollektivvereinbarung bei der Beurteilung der Erforderlichkeit der Verarbeitung im Sinne der genannten Normen ein Spielraum zu, welcher durch Gerichte nur eingeschränkt überprüfbar ist?
3. Falls ja: Worauf darf in diesem Fall die gerichtliche Kontrolle beschränkt werden?

Was sagt der EuGH?

Der EuGH weist in seiner Entscheidung darauf hin, dass Art. 88 DSGVO die Voraussetzungen schafft, unter denen in den Mitgliedsstaaten spezifischere Vorschriften zur Verarbeitung von Beschäftigtendaten gelten dürfen – auch in Form der Betriebsvereinbarung. Diese sollen neben allen konkreten Anforderungen der Öffnungsklausel auch nicht das Schutzniveau der DSGVO unterschreiten und nicht gegen Ziele und Inhalt der DSGVO verstoßen. So soll, auch wenn per Betriebsvereinbarung eine Rechtsgrundlage für Datenverarbeitung geschaffen wird, besonders das in Art. 5, 6 und 9 DSGVO normierte Kriterium der Erforderlichkeit einer Verarbeitung für die beabsichtigten Zwecke eingehalten werden.

Zentrale Vorgabe sollen die Grundprinzipien der Verordnung in Art. 5 sowie die Betroffenenrechte aus Kapitel 3 der DSGVO sein. Auch dazu müssen geeignete und besondere Maßnahmen zum Schutz der Rechte und Freiheiten der Beschäftigten vorgesehen werden.

Hinsichtlich Frage 2 bestätigt der EuGH, dass den Parteien einer Kollektivvereinbarung zwar grundsätzlich Beurteilungsspielraum hinsichtlich der Erforderlichkeit zusteht. Diese Beurteilung soll dennoch uneingeschränkt der gerichtlichen Kontrolle unterliegen.

Mit anderen Worten: Eine Betriebsvereinbarung ist kein „datenschutzrechtlicher Freifahrtschein". Öffnungsklausel heißt nicht Öffnung nach unten, denn nationale Vorschriften wie auch Betriebsvereinbarungen bewegen sich innerhalb der Systematik der DSGVO und ihrer Grundprinzipien. Sie konkretisieren für besondere Situationen, sie ersetzen aber nicht die Verordnung.

Erkenntnisse für die Praxis

Die Entscheidung ist „nur“ eine Präzisierung, aber eine mit deutlicher Wirkung. Betriebsvereinbarungen waren oft ein einfaches Instrument, um komplexe HR- oder IT-Systeme datenschutzrechtlich zu „rahmen“. Jetzt ist klar: Dieses Instrument bleibt zulässig, aber nur bei ausreichend hoher Regelungsqualität.

1. Anforderungen an Betriebsvereinbarungen als Rechtsgrundlage

Betriebsvereinbarungen müssen präzise formuliert werden, dabei sind

- exakte Beschreibung der Verarbeitungszwecke,
- Dokumentation der Erforderlichkeit, ggf. unter Abwägung von Alternativen,
- abschließende Benennung der Datenkategorien und der betroffenen Personengruppen,
- Regelung von Zugriffsrechten und Rollen sowie Löschung,
- dokumentierte technische und organisatorische Maßnahmen und
- Sicherstellung der transparenten Information der Betroffenen, insbesondere zu Übermittlungen

zentrale Punkte. Unklare und pauschale Formulierungen bergen das Risiko nicht die Anforderungen an eine Rechtsgrundlage zu erfüllen. Wer hier bereits genau dokumentiert, schafft den ersten Nachweis, dass das Schutzniveau der DSGVO nicht unterstritten wird. Auch im Verzeichnis von Verarbeitungstätigkeiten sollte nicht lediglich „Betriebsvereinbarung“ als Rechtsgrundlage stehen. Art. 8 Abs. 1 DSGVO ist in Verbindung mit der konkreten Vereinbarung zu nennen. Alternativ kann ggf. § 26 Abs. 4 BDSG als Ausgangspunkt herangezogen werden.

Kernaussagen der Entscheidung BAG 08.05.2025 – 8 AZR 209/21

- Schadensersatz nach Art. 82 DSGVO bei Überschreitung der Betriebsvereinbarung hinsichtlich Datenkategorien und Verarbeitungsformen möglich
- Nutzung von Echtdaten zu Testzwecken kann zulässig sein – wenn tatsächlich erforderlich
- Betriebsvereinbarungen als Rechtsgrundlage müssen ausreichend spezifisch ausgestaltet sein
- § 26 Abs. 1 BDSG genügt nicht als spezifischere Vorschrift i.S.d. Art. 88 Abs. 1 DSGVO

2. Bedeutung von § 26 Abs. 1 BDSG

Der EuGH hat erneut klargestellt, dass § 26 Abs. 1 BDSG nicht automatisch als spezifischere Vorschrift im Sinne von Art. 88 DSGVO genügt. Beim BAG folgert man, dass die fragliche Norm nicht mehr über Art. 88 DSGVO zur Anwendung kommt. Eine Anwendung über andere Mechanismen der DSGVO sei weiterhin denkbar, beispielweise als nationale Vorschrift im Sinne des Art. 6 Abs. 3 DSGVO.

Praktisch bedarf es also einer Einzelfallprüfung dort, wo man sich bisher auf § 26 Abs. 1 BDSG berief, ob die Vorschrift dort bestand hat. Eine schematische Berufung auf § 26 BDSG reicht nicht.

3. Unzureichende Betriebsvereinbarungen?

Unzureichende Betriebsvereinbarungen können unter Umständen im Rahmen von Art. 6 Abs. 1 lit. f DSGVO berücksichtigt werden. Dann muss jedoch eine saubere und dokumentierte Interessenabwägung erfolgen – inklusive Berücksichtigung ggf. notwendiger Schutzmaßnahmen, um die Betroffenen zu schützen.

4. DSG-EKD und KDG

Auch Dienstvereinbarungen von Organisationen, welche dem kirchlichen Datenschutzrecht unterfallen, können eine Kollektivvereinbarung gem. Art. 88 DSGVO darstellen. Die jeweiligen Normen zur Verarbeitung im Beschäftigungsverhältnis (§ 49 Abs. 1 DSG-EKD, § 53 Abs. 1 KDG) entsprechen inhaltlich dem § 26 Abs. 1 BDSG, sodass die obigen Voraussetzungen wohl übertragbar sind.

Fazit

Die Entscheidung stärkt nicht nur die Rechte von Beschäftigten, sie erhöht auch die Anforderungen an die Dokumentation und sowie die Zusammenarbeit zwischen HR, IT, Datenschutz und dem Betriebsrat. Im Unternehmen bedeutet das: Betriebsvereinbarungen sind weiterhin ein starkes Instrument – aber nur, wenn sie DSGVO-technisch sauber konstruiert sind. &

Althammer & Kill Akademie

KLICK/SCAN

Mehr Informationen, weitere Termine und Anmeldemöglichkeiten finden Sie unter: *althammer-kill.de/akademie*

31. März 2026 – kostenloses Webinar

Die „hohe Kunst“ der Datenschutz-Folgenabschätzung

Ein neues System soll eingeführt, oder Daten anders verarbeitet werden? Das zieht datenschutzrechtlich Handlungsbedarf nach sich. Die Datenschutz-Folgenabschätzung (kurz: DSFA) ist eines der wichtigsten Elemente der Datenschutz-Grundverordnung. Sie soll den Schutz von personenbezogenen Daten betroffener Personen sicherstellen. Denn wer Daten anderer Personen verarbeitet, muss dadurch entstehende Risiken immer im Blick behalten.

1. April // 29. April // 19. Mai 2026 – Online-Seminar

NIS-2-Management-Pflichtschulung

Die NIS-2-Richtlinie bringt weitreichende Veränderungen für Unternehmen im Bereich der Cybersicherheit mit sich. Diese Schulung richtet sich gezielt an Geschäftsleitungen und Führungskräfte und vermittelt praxisnah, wie Sie Ihre Organisation wirksam und gesetzeskonform aufstellen. Anhand konkreter Fallbeispiele und bewährter Vorgehensweisen zeigen wir, wie sich Cybersicherheit systematisch in bestehende Unternehmensprozesse integrieren lässt. So entwickeln Sie nicht nur eine tragfähige Sicherheitsstrategie, sondern erfüllen auch die gesetzlichen Anforderungen effizient und nachhaltig.

15. April 2026 – kostenloses Webinar

EU-KI-Verordnung: Das gilt seit 02. Februar 2025

Tauchen Sie ein in die Welt der EU-KI-Verordnung! In diesem kostenlosen Webinar erfahren Sie, welche neuen Regelungen auf Unternehmen und KI-Nutzer zukommen. Wir beleuchten die wichtigsten Aspekte der Verordnung, von der Begrifflichkeit der KI bis zur Einstufung von KI-Systemen, und zeigen auf, wie Sie sich optimal vorbereiten können.

29. April 2026 – kostenloses Webinar

Souverän reagieren auf IT-Notfälle und Datenschutzpannen

Angesichts der aktuellen Cyber-Bedrohungen lautet die Frage nicht, ob es in Ihrer Organisation zu einer Datenpanne kommt, sondern nur, wann es passiert. Wer dann falsch reagiert, riskiert massive Schäden – vom Verdienstausfall über Vertrauensverlust bis zu Bußgeldern. Vollkommen unvorbereitet in diese Situation zu stolpern, ist fahrlässig.

12.–13. Mai 2026 – Online-Seminar

Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Auch wenn keine Datenschutzbeauftragten bestellt werden müssen, sind Datenschutzgesetze und -regelungen einzuhalten und umzusetzen. Hier kommt der Datenschutzkoordinator bzw. die Datenschutzkoordinatorin, als fachliche Unterstützung der Unternehmensleitung und Mitarbeitenden ins Spiel. Sie haben einen internen oder externen Datenschutzbeauftragten? Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

Haben Sie Fragen?

Ihre Ansprechpartnerin für alle Themen rund um die Althammer & Kill-Akademie:

Nina Hoffmann
veranstaltung@althammer-kill.de
Tel. +49 511 330603-0

Was passiert, wenn's passiert: Datenpannen bewältigen

Angesichts der aktuellen Cyber-Bedrohungslage lautet die Frage nicht, ob es in Ihrer Organisation zu einer Datenpanne kommen wird, sondern nur, wann es so weit ist. Wer dann ein paar minimale Vorbereitungen getroffen hat, gewinnt seine Handlungsfähigkeit schnell zurück.

von Johannes Endres

Wenn es passiert, ist es zu spät für Grundsatzdiskussionen: Ein Sicherheitsvorfall, ein technischer Ausfall oder eine Datenschutzpanne verlangt sofortiges, strukturiertes Handeln. Gerade Organisationen mit sensiblen Daten – etwa im Gesundheits- und Sozialwesen – stehen dann unter enormem Druck: Betrieb sichern, Schäden begrenzen, Vertrauen erhalten und rechtliche Pflichten einhalten. Entscheidend ist dabei nicht, ob ein Vorfall eintritt, sondern wie souverän die Organisation reagiert.

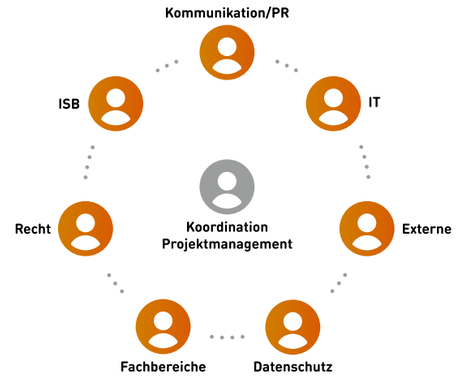
Den Notfall erkennen: „Human Firewall" greift

Die erste Hürde ist nicht die Lösung, sondern das Erkennen des Problems. Denn spektakuläre Cyber-Angriffe stehen zwar im Fokus der Aufmerksamkeit, doch andere Vorfälle kommen viel häufiger vor.

Um den Blick auf die realen Problemfälle zu weiten, sollte man die drei Sicherheitsanforderungen für Daten beachten:

- Die Vertraulichkeit ist verletzt, wenn jemand Daten zu sehen bekommt, die ihn nichts angehen. Solche Vorfälle entstehen zum Beispiel durch eine E-Mail an falsche Empfänger, Personalakten in einem unverschlossenen Büro oder den Passwort-Verlust durch Phishing.
- Die Verfügbarkeit ist verletzt, wenn benötigte Daten nicht zur Verfügung stehen. Das kann durch einen Verschlüsselungs-Trojaner passieren, aber viel häufiger durch Verschusselung eines Passworts oder den Ausfall eines Cloud-Systems.
- Die Integrität ist verletzt, wenn Daten verfälscht wurden. Das kann beispielsweise absichtlich durch einen verärgerten Mitarbeitenden passieren oder versehentlich durch eine Änderung in der falschen Datei.

Technische Warnsysteme können viele der Risiko-Szenarien nicht erkennen. Umso wichtiger ist deshalb die „Human Firewall": gut geschulte Mitarbeitende. Sie müssen sich über Auffälligkeiten wundern und sie melden – ohne Umwege und ohne Unsicherheit. Dafür braucht es einen klar definierten und allgemein bekannten Meldeweg.



Krisen brauchen Rollen – keine Helden.

Mindestens genauso wichtig ist eine positive Fehlerkultur. Wer aus Scham oder Angst schweigt („Ich habe da auf einen Link geklickt…"), verzögert die folgenden Schritte. Und Zeit ist in Notfällen der größte Gegner.

Krisenbehandlung aufsetzen: Klare Aufgabenverteilung

Sobald ein Vorfall bekannt ist, muss die Organisation umschalten: weg vom Tagesbetrieb, hin zur Krisensteuerung. Best Practice ist ein Notfall- bzw. Krisenteam mit klarer Leitung – idealerweise durch eine Projektmanagement-Rolle, die koordiniert und Entscheidungen strukturiert vorbereitet. Denn die Bewältigung einer Datenpanne ist ein Projekt.

Das Projektmanagement sollte nicht in der IT angesiedelt werden, denn die Techniker sind in dieser Phase mit der

Eindämmung und Analyse ausgelastet und sollten nicht zusätzlich „nebenbei“ die Gesamtkoordination übernehmen müssen.

In das Krisenteam gehören neben dem Projektmanagement und einer Verbindung zur IT auf jeden Fall Datenschutz- und Informationssicherheits-Expertise sowie zwingend Kommunikation/PR. Ziel ist eine abgestimmte Vorgehensweise mit klaren Verantwortlichkeiten.

Schaden begrenzen: isolieren, sperren, dokumentieren

Die ersten Maßnahmen der IT-Abteilung müssen vor allem die Ausbreitung des Schadens verhindern. Dazu gehört, betroffene Systeme sofort zu sperren – nötigenfalls durch Änderung der Passwörter. Verbindungen müssen gekappt und kompromittierte Endgeräte müssen unverzüglich in Quarantäne gestellt werden. Von Anfang an sollte das Krisen-Team ein genaues Protokoll führen. Beobachtungen, Entscheidungen und Maßnahmen müssen jeweils mit Zeitstempel sowie den Beteiligten dokumentiert werden.
Das hilft nicht nur bei der Nachbereitung, sondern ist auch für Nachweise gegenüber Aufsichtsbehörden, Versicherungen oder Vertragspartnern essenziell.

„Ein Vorfall ist kein IT-Problem – sondern ein Projekt mit IT-Anteil.“

Minimale Vorbereitungen

- Awareness bei Mitarbeitenden schaffen („Human firewall“)
- Meldewege einrichten und bekannt machen
- Rollen und Verantwortlichkeiten für ein Krisen-Team vorab festlegen
- Krisen-Projektmanagement benennen und schulen
- Notfall-Kommunikations-Kanal etablieren
- Meldepflichten und Kontakt-Informationen erfassen

Nutzende informieren: klare Ansagen, alternative Arbeitsweisen

Parallel zur technischen Eindämmung braucht es sofortige, wirksame interne Kommunikation. Mitarbeitende müssen wissen, was sie tun und lassen sollen. Eine klare, kurze Anweisung wie „Bitte loggen Sie sich in System XY nicht mehr ein“ ist besser als allgemeine Warnungen und ausschweifende Erklärungen des technischen Hintergrunds.

In diese Nachricht gehört auch eine klare Anweisung zur Außenkommunikation. Denn die muss zentralisiert, abgestimmt und kontrolliert ablaufen. So lässt sich der Reputationsschaden begrenzen und das Vertrauen externer Partner erhalten. Die Mitarbeitenden brauchen dazu drei klare Anweisungen: eine Sprachregelung wie „Wir erleben gerade einen Cyberangriff“, das Verbot darüber hinaus mit Externen über die Situation zu reden und die Kontaktdaten der Stelle, an die sie alle externen Anfragen leiten sollen.

Damit diese Information zu den Mitarbeitenden gelangen kann, muss vorher (jetzt!) ein Notfall-Kommunikationskanal geplant werden. Denn wenn der Vorfall beispielsweise Microsoft 365 betrifft, stehen Mail und Teams nicht mehr zur Verfügung. Je nach Organisation eignen sich Chat-Gruppen in einem anderen Messenger, persönliche Information mit einem Gang durch alle Büros oder auch vorab vereinbarte Telefonketten. Und der Betrieb muss weitergehen. Für unverzichtbare Kernprozesse braucht es alternative Arbeitsweisen. In der Praxis heißt das oft wieder auf Papier und Stift zurückzugreifen, z. B. in der Pflegedokumentation. Wer dafür keinen Plan hat, verliert in der Krise doppelt: durch IT-Ausfall und durch organisatorisches Chaos.

Auf private Endgeräte und schnell aktivierbare kostenlose Cloud-Dienste sollte man nur nach genauer Prüfung zurückzugreifen. Denn wer sich in der Hektik für unsichere Systeme entscheidet, produziert gleich den nächsten Sicherheitsvorfall.

Folgeschäden verhindern: Kommunikation und Meldepflichten steuern

Viele Schäden entstehen nicht durch den Vorfall selbst, sondern durch falsches Verhalten danach.

Wirkung	Schaden
Reputationsverlust	Einbußen bei Engagement und Spenden
Datenschutzverletzung	Bußgeld, Schadensersatz
Betriebsunterbrechung	Keine Leistungserbringung
(Cyber-)Versicherung	Leistungskürzung
Vertragsverletzungen	Schadensersatz, Konventionalstrafen, Auftragsverlust

Neben der schon erwähnten Außenkommunikation sind hier die Mitteilungspflichten zentral. Datenschutzrechtlich gilt bei meldepflichtigen Datenschutzverletzungen eine Frist von 72 Stunden ab Kenntnis. Das heißt, die Uhr tickt, sobald man erkennt, dass eine Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität personenbezogener Daten wahrscheinlich ist.

Je nach Vertragslage müssen auch Geschäftspartner oder die Cyber-Versicherung schnell vom Vorfall erfahren. Hinzu kommen je nach Branche noch weitere Meldestellen und Aufsichtsbehörden. In der Praxis ist das alles nur zu schaffen, wenn Zuständigkeiten und Abläufe vorbereitet sind.

Nacharbeiten: wiederherstellen, lernen, besser werden

Nach der akuten Krisenbewältigung beginnen die Nacharbeiten mit der Wiederherstellung der digitalen Infrastruktur. An dieser Stelle lohnt es sich, einen systematischen Plan aufzustellen. Der sollte sicherstellen, dass die für Kernprozesse dringlichsten System zuerst wieder laufen. Zudem kann dies der richtige Moment für strategische IT-Investitionen sein, etwas veraltete Systeme durch neue zu ersetzen.

Mindestens so wichtig ist eine strukturierte Nachanalyse: Was war die Ursache? Wo waren Schwachstellen? Was hat in der Krisenbewältigung funktioniert und was nicht? Dabei darf der Fokus ausschließlich auf Ursachen und Abhilfe liegen; Schuldzuweisung sind schädlich. Denn eine positive Fehlerkultur ist auch hier der Schlüssel, um Wiederholungen zu verhindern.

Fazit

Vorbereitung ist die beste Schadensbegrenzung. Notfälle lassen sich nicht vollständig verhindern, aber sie lassen sich beherrschen. Wer einige minimale Vorbereitungen trifft, kann verhindern, dass eine Krise sich zur Katastrophe auswächst. Doch für Organisationen, die von ihrer digitalen Infrastruktur abhängig sind, genügt das noch nicht. Sie sollten ein vollständiges Notfallmanagement aufsetzen, das beispielsweise vorab geplante und getestete Ersatz-Systeme für Kernprozesse umfasst. &

Impressum

Redaktion/V. i. S. d. P.:
Fabian Eggers,
Thomas Althammer

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Schutzgebühr Print-Ausgabe: 5,– €

Gestaltung:
Designbüro Winternheimer, *winternheimer.net*

Fotos Mini-Figuren:
Katja Borchhardt, *miniansichten.de*

Anschrift:
Althammer & Kill GmbH & Co. KG
Roscherstraße 7 · 30161 Hannover
Tel. +49 511 330603-0
althammer-kill.de

ALTHAMMER & KILL

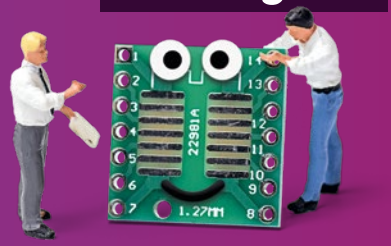
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

Wir sind Digitalisierungskenner, Datenversteher und Vorwärtsdenker –
Ihr Experte für Datenschutz, Informationssicherheit, Künstliche Intelligenz und Compliance.
Unsere 45 Mitarbeitenden bringen Digitalisierung und Datenschutz bundesweit in Einklang.

Datenschutz

Informations-sicherheit

Künstliche Intelligenz



Compliance

althammer-kill.de

KLICK/SCAN