COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 3/2025

Datenschutz im Wandel

Beim Einsatz von US-amerikanischen Cloud-Dienstleistern rücken Datenschutzfragen und die politische Großwetterlage immer stärker in den Fokus

Seite 6

Editorial

Liebe Leserin, lieber Leser,

die digitale Transformation schreitet weiter voran – und mit ihr wachsen die Anforderungen. Ob Künstliche Intelligenz, NIS-2 oder Digitale Souveränität: Es geht längst nicht mehr nur darum, Schritt zu halten. Es geht darum, die Weichen richtig zu stellen: verantwortungsvoll, praxisnah und mit einem klaren Ziel vor Augen.

In dieser Ausgabe unseres Magazins werfen wir genau diesen Blick nach vorn. Mit dem Schwerpunkt auf Künstlicher Intelligenz zeigen wir, wie Organisationen heute KI-Anwendungen gestalten können, ohne regulatorische oder ethische Risiken einzugehen. Warum dabei ein systematischer Umgang mit Trainingsdaten so entscheidend ist, erfahren Sie ebenfalls in diesem Heft.

Auch das Thema NIS-2 bleibt aktuell und dringlich. Unsere Beiträge helfen Ihnen dabei, zu erkennen, ob und wie Ihre Organisation betroffen ist, und welche Maßnahmen jetzt sinnvoll sind. Nicht als Bürokratiemonster, sondern als Teil einer souveränen, digitalen Infrastruktur.

Stichwort Souveränität: Gerade für den öffentlichen Sektor stellt sich die Frage, wie sich digitale Abhängigkeiten verringern lassen, ohne auf Innovation zu verzichten. Unser Artikel zur digitalen Selbstbestimmung zeigt: Es gibt Alternativen, aber sie erfordern klare Entscheidungen.

Und schließlich wird's persönlich: In dieser Ausgabe lernen Sie eine Persönlichkeit aus unserem Netzwerk kennen, die sich seit Jahren für verantwortungsvolle Innovation einsetzt. Denn auch das gehört für uns zur Zukunftsfähigkeit: Austausch, Haltung – und Menschen, die Dinge voranbringen.

Wir wünschen Ihnen anregende Impulse, neue Perspektiven und wie immer: konkrete Orientierung für Ihre Arbeit.

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*

Teamtage 2025: Ein Rückblick voller Qualität, KI und Kettenreaktionen

Was passiert, wenn Datenschutz, Informationssicherheit und Künstliche Intelligenz auf Teamspirit und Kreativität treffen? Genau das haben wir bei unseren Team-Tagen erlebt! Im Mittelpunkt stand das „Jahr der Qualität". Unser gemeinsames Commitment, Prozesse, Zusammenarbeit und Ergebnisse kontinuierlich zu verbessern. Neben aktuellen Entwicklungen im Datenschutz und in der Künstlichen Intelligenz haben wir uns auch mit der Frage beschäftigt: Wie sichern wir Qualität in einer zunehmend automatisierten Welt?
Abgerundet wurde das Ganze mit einer besonderen Teamaktion: Bei einer Impulsreaktion war nicht nur Geschick gefragt: Wir haben aus unterschiedlichsten Materialien eine Art „Murmelbahn" gebaut. Eine kreative Kettenreaktion, die zeigt, wie aus vielen Einzelteilen ein starkes Ganzes wird - ganz wie bei uns im Team.

„KI-Kompetenz": Was bedeutet das eigentlich?

Seit Februar 2025 verlangt die EU-KI-Verordnung den Aufbau von KI-Kompetenz in Organisationen. Es reicht nicht, nur technisch zu wissen, wie eine KI funktioniert. Man muss auch verstehen, wie sie Entscheidungen trifft, wie sie sich auf Menschen auswirkt und wo ethische oder rechtliche Probleme entstehen können. Erfahren Sie, was das konkret bedeutet, wen es betrifft und welche Maßnahmen nötig sind.

KLICK/SCAN

Warum der Mensch bei KI-Entscheidungen unverzichtbar bleibt

KI-Systeme können heute bereits erstaunliche Leistungen erbringen. Sie analysieren riesige Datenmengen in Sekunden, erkennen Muster, die dem Menschen verborgen bleiben oder treffen automatisierte Empfehlungen. Künstliche Intelligenz trifft blitzschnelle Entscheidungen – doch ohne menschliches Urteilsvermögen bleibt sie fehleranfällig. Lesen Sie, warum der Mensch im Entscheidungsprozess unverzichtbar ist und wie „Human in the Loop"-Konzepte Sicherheit, Vertrauen und Verantwortung gewährleisten.

KLICK/SCAN

„Dürfen Sie das sagen?" – Wo Schweigepflicht endet und das Datengeheimnis beginnt

Das Strafgesetzbuch (StGB) verbietet die unbefugte Weitergabe von Geheimnissen, die bestimmten Berufsgruppen im Rahmen ihrer beruflichen Tätigkeit anvertraut werden. Unser Blogbeitrag gibt einen Überblick über § 203 StGB, die Schweigepflicht von Berufsgeheimnisträgern und deren Bedeutung im Datenschutzrecht. Erfahren Sie, wie Ausnahmen und gesetzliche Vorgaben im Berufsalltag angewendet werden.

KLICK/SCAN

Warum viele Datentransfers ungewollt ins Drittland führen

Wer mit personenbezogenen Daten arbeitet, kommt heute kaum ohne internationalen Datentransfers aus. Doch wann liegt ein solcher eigentlich vor? Viele Unternehmen gehen fälschlich davon aus, keine Daten ins Drittland zu übermitteln. Erfahren Sie, warum das ein Irrtum sein kann und welche Pflichten sich daraus ergeben.

KLICK/SCAN

Zahl des Monats

90 %

90 % der europäischen Unternehmen sehen laut einer Bitkom-Studie digitale Souveränität als entscheidenden Wettbewerbsfaktor – aber weniger als ein Drittel fühlt sich darauf vorbereitet. Der Bedarf an unabhängigen, vertrauenswürdigen IT-Lösungen wächst – nicht nur politisch, sondern auch wirtschaftlich.

Veranstaltungen

Kostenlose Webinarreihe von voize und Althammer & Kill

KLICK/SCAN

Künstliche Intelligenz eröffnet enorme Möglichkeiten für die Pflege – von sprachgesteuerter Dokumentation bis hin zu intelligenter Unterstützung im Alltag. Doch viele Einrichtungen stellen sich ähnliche Fragen: Dürfen wir das einsetzen? Was gilt datenschutzrechtlich? Wird das zu kompliziert für unser Team?

In dieser Webinarreihe geben voize und die Datenschutzfachleute von Althammer & Kill konkrete Orientierung.

9. September 2025, 11–12 Uhr

KI & Datenschutz im Sozial- und Gesundheitswesen – wie beides zusammen funktioniert

Künstliche Intelligenz gilt als Zukunftstechnologie – auch in der Pflege. Gleichzeitig gelten hier besonders hohe Datenschutzanforderungen. Das führt häufig zu Unsicherheiten: Was darf man eigentlich? Was genau ist „KI" aus rechtlicher Sicht? Und wie kann man neue Technologien so gestalten und einsetzen, dass sie Vertrauen schaffen bei Trägern, Mitarbeitenden und Bewohnenden?

7. Oktober 2025, 10–11 Uhr

KI & digitale Souveränität im Sozial- und Gesundheitswesen: So ist es möglich.

Digitale Souveränität bedeutet: Technik selbstbestimmt nutzen, Daten unter Kontrolle behalten und unabhängig handeln. Besonders wenn Künstliche Intelligenz im Spiel ist. In der Pflege geht es hierbei um mehr als nur eine IT-Frage: Es geht um Vertrauen, Transparenz und Alltagstauglichkeit.

Datenschutz im Wandel: US-Politik und US-Cloud-Dienstleister

Angesichts der dynamischen Rechtslage und politischen Unsicherheiten ist ein proaktiver Umgang mit Daten in der Cloud unerlässlich. Wie können Risiken minimiert und die Software-Souveränität gestärkt werden?

Von David Armbrust

In einer zunehmend vernetzten Welt sind Cloud-Dienste für viele Unternehmen unverzichtbar geworden. Sie bieten Flexibilität, Skalierbarkeit und oft auch Kostenvorteile. Doch gerade beim Einsatz von US-amerikanischen Cloud-Dienstleistern rücken Datenschutzfragen und die politische Großwetterlage immer stärker in den Fokus. Die aktuelle US(-Trump)-Regierung und ihre potenziellen Auswirkungen auf internationale Datenflüsse werfen neue Fragen auf, die Unternehmen nicht ignorieren dürfen.

Das Damoklesschwert des CLOUD Act und die EU-Datenhoheit

Der US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) erlaubt es US-Behörden auf Daten zuzugreifen, die von US-Unternehmen – auch wenn sie außerhalb der USA gespeichert sind – kontrolliert werden, sofern es eine „verhältnismäßige" Begründung zur Einsicht in die Daten gibt. Die Problematik des CLOUD Act verschärft sich im Kontext des Konzepts der EU-Datenhoheit (EU Data Boundary). Die EU-Datenhoheit ist ein Bestreben sicherzustellen, dass die Daten europäischer Bürger und Unternehmen innerhalb der EU verbleiben und ausschließlich europäischem Recht unterliegen. Dies steht in direktem Konflikt mit den weitreichenden Befugnissen des CLOUD Act.

Dies stellt eine grundlegende Herausforderung für europäische Unternehmen dar, die sich auf die Speicherung ihrer Daten in der EU verlassen, um DSGVO-Konformität zu gewährleisten. Der CLOUD Act ist eine ständige Bedrohung, da er die räumliche Trennung der Daten untergräbt und US-Zugriffsrechte über europäisches Recht stellen könnte.

US(-Trump)-Politik und der Angemessenheitsbeschluss: Ein heikles Gleichgewicht

Derzeit bildet der Angemessenheitsbeschluss der EU-Kommission für den Datentransfer in die USA (Trans-Atlantic Data Privacy Framework) die Grundlage für den rechtssicheren Datenaustausch zwischen der EU und den USA. Dieses Abkommen ermöglicht den USA ein angemessenes Datenschutzniveau ohne zusätzliche Schutzmaßnahmen von europäischer Seite und soll die jahrelange Unsicherheit nach dem Scheitern von Safe Harbor und Privacy Shield beenden.

Doch die erneute Präsidentschaft von Donald Trump könnte dieses mühsam erreichte Gleichgewicht empfindlich stören. Trumps „America First"-Politik und sein Hang zu unilateralen Entscheidungen führen dazu, dass die USA erneut Maßnahmen ergreifen, die das Vertrauen in den aktuellen Angemessenheitsbeschluss untergraben.

Was die US(-Trump)-Politik so kritisch macht

Schon in seiner ersten Amtszeit zeigte Donald Trump eine Tendenz, nationale Sicherheitsmechanismen über individuelle Datenschutzrechte zu stellen und die Befugnisse von US-Geheimdiensten zu stärken. Die erneute Amtszeit verstärkt diese Haltung weiter, was zu einer aggressiveren Durchsetzung von Datenanfragen führen könnte, ohne Rücksicht auf die in Europa geltenden Prinzipien der Verhältnismäßigkeit und Notwendigkeit. Dies untergräbt die im Angemessenheitsbeschluss vorgesehenen Garantien eines effektiven Rechtsschutzes.

Der aktuelle Angemessenheitsbeschluss wurde speziell geschaffen, um auf die Bedenken des Europäischen Gerichtshofes (EuGH) hinsichtlich des US-Überwachungsrechts einzugehen, unter anderem durch die Einrichtung eines Privacy and Civil Liberties Oversight Board (PCLOB).

Die Trump-Regierung stellt die Unabhängigkeit und Effektivität solcher Schutzmechanismen durch politische Einflussnahme oder die Benennung kritischer Personen in Frage. Dies zeigt sich schon allein dadurch, dass Trump das aus fünf Beamten bestehende DPRC durch Druck und Einflussnahme auf zwei Personen verkleinert hat.

Die Trump-Regierung könnte außerdem den Druck auf US-Unternehmen erhöhen, Daten an US-Behörden herauszugeben, möglicherweise ohne Rücksicht auf europäische Datenschutzinteressen. Dies könnte die eingebauten Schutzmechanismen, die den Zugriff auf das Notwendige beschränken sollen, ad absurdum führen.

Zudem ist zu beachten, dass Trump bereits in seiner ersten Amtszeit wiederholt internationale Abkommen in Frage gestellt, aufgekündigt oder neu verhandelt hatte. Dies schloss auch Handelsabkommen und multilaterale Abkommen ein. Die Gefahr bestand nun auch für den Angemessenheitsbeschluss.

In einer seiner ersten Executive Orders beschloss Trump, dass alle nationalen Sicherheitsentscheidungen der Biden-Regierung (einschließlich relevanter Entscheidungen, auf denen der Angemessenheitsbeschluss fußt) innerhalb von 45 Tagen überprüft und möglicherweise verworfen werden sollten. Eine Abwertung der Bedeutung des Abkommens von US-Seite hätte die Legitimität aus europäischer Sicht drastisch reduziert.

Zuletzt führt genau diese unberechenbare und undurchsichtige Art der Trump-Politik zu einer massiven Rechtsunsicherheit. Bereits kleine politische Aussagen oder die Andeutung von Gesetzesänderungen könnten ausreichen, um die Rechtmäßigkeit des Datentransfers in Frage zu stellen. Unternehmen werden in eine Ungewissheit getrieben, ob ihre Datenübertragung dauerhaft rechtssicher ist.

Die Reaktion der Europäischen Kommission und die Gefahr eines „Schrems-III"-Urteils

Angesichts der genannten Risiken könnte die Europäische Kommission gezwungen sein, den Angemessenheitsbeschluss zu überprüfen und im schlimmsten Fall zu kippen. Die Kommission ist verpflichtet, kontinuierlich zu bewerten, ob das Datenschutzniveau im Drittland USA weiterhin den EU-Standards entspricht. Sollten die Handlungen oder politischen Ausrichtungen der Trump-Regierung die im Beschluss zugesicherten Schutzgarantien – insbesondere im Hinblick auf den Zugriff von US-Geheimdiensten – als unzureichend erscheinen lassen, hätte die Kommission keine andere Wahl, als den Beschluss zurückzuziehen.

Dies würde die Tür für ein weiteres „Schrems"-Urteil weit öffnen. Max Schrems und seine Organisation NOYB haben bereits die Vorgängerabkommen (Safe Harbor und Privacy Shield) erfolgreich vor dem Europäischen Gerichtshof (EuGH) angefochten, da dieser die Zugriffsrechte der US-Geheimdienste ohne ausreichenden Rechtsschutz für EU-Bürger als nicht DSGVO-konform einstufte. Eine weiterhin aggressive Einstellung der US-Regierung in Datenschutzfragen würde die Argumente für eine erneute Anfechtung stärken und die Wahrscheinlichkeit erhöhen, dass auch der aktuelle Angemessenheitsbeschluss durch den EuGH für ungültig erklärt wird.

Die Bedeutung einer Exit-Strategie

Gerade weil die politische und rechtliche Lage so dynamisch ist, ist eine wohlüberlegte Exit-Strategie beim Einsatz von Cloud-Dienstleistern, insbesondere solchen aus den USA, unerlässlich. Eine Exit-Strategie beschreibt den Plan, wie Daten und Anwendungen im Falle eines Anbieterwechsels oder einer Kündigung des Dienstes sicher und ohne Unterbrechung migriert werden können.

Dazu gehören folgende Aspekte:

- **Datenportabilität** stellt sicher, dass Daten in einem offenen und portablen Format vorliegen, das einfach zu exportieren und in ein anderes System zu importieren ist.
- **Vertragliche Regelungen** und Vertragsbedingungen bezüglich der Datenherausgabe und etwaiger Kosten für den Export von Daten und klare SLAs (Service Level Agreements) sind hier entscheidend.
- **Evaluierung** im Vorfeld, welche alternativen Lösungen es gibt und ob diese technologisch mit Ihren aktuellen Systemen kompatibel sind.
- Regelmäßige, unabhängige **Backups der Cloud-Daten** durchführen und diese auch auf Vollständigkeit und Richtigkeit testen zu lassen.
- Idealerweise sollte die Exit-Strategie in regelmäßigen Abständen getestet werden, um sicherzustellen, dass sie im Ernstfall reibungslos funktioniert.

Software-Souveränität: Mehr als nur ein Schlagwort

Angesichts der Herausforderungen gewinnt das Konzept der Software-Souveränität massiv an Bedeutung. Es geht dabei nicht nur um den physischen Speicherort der Daten, sondern auch um die Kontrolle über die Drittanbieter, die diese Daten verarbeiten. Werden Anwendungen von US-Anbietern genutzt, besteht immer ein gewisses Abhängigkeitsverhältnis. Im schlimmsten Fall könnten essenzielle Dienste von einem Tag auf den anderen eingeschränkt oder gesperrt werden, was gravierende Auswirkungen auf die Geschäftsprozesse hätte.

Software-Souveränität bedeutet, dass Unternehmen die Kontrolle über ihre IT-Infrastruktur, ihre Anwendungen und damit auch über ihre Daten behalten. Dies kann durch den Einsatz von Open-Source-Software, die Entwicklung eigener Lösungen oder die Nutzung von Cloud-Diensten europäischer Anbieter, die klar definierte Datenschutzstandards erfüllen und keinem US-Zugriffsrecht unterliegen, erreicht werden. Ziel ist es, die Abhängigkeit von einzelnen Anbietern zu minimieren und die Fähigkeit zu wahren, kritische Systeme auch in Krisenzeiten zu betreiben.

Fazit und Ausblick

Der Einsatz von US-Cloud-Dienstleistern bleibt ein Balanceakt zwischen Komfort und Risiko. Während die Vorteile der Cloud unbestreitbar sind, müssen Unternehmen die potenziellen Fallstricke des CLOUD Act im Konflikt mit der EU-Datenhoheit und die Unsicherheiten, die eine sich ändernde politische Landschaft – insbesondere durch die derzeitige Trump-Regierung – für den Angemessenheitsbeschluss mit sich bringt, ernst nehmen. Es ist keine Zeit zu Zögern; proaktives Handeln ist nun gefragt. Investitionen in datenschutzkonforme europäische Alternativen und die Stärkung der eigenen digitalen Resilienz zahlen sich langfristig aus und sichern die Handlungsfähigkeit des Unternehmens, selbst wenn der Wind sich dreht. &

Konkrete Handlungsempfehlungen:

- Überprüfen Sie alle bestehenden Datenschutz-Folgenabschätzungen, die US-Cloud-Dienstleister betreffen. Analysieren Sie die aktuellen Risiken unter Berücksichtigung der jüngsten Entwicklungen beim CLOUD Act und der potenziellen Unsicherheiten des Trans-Atlantic Data Privacy Frameworks. Passen Sie die Risikobewertung entsprechend an und dokumentieren Sie die Gründe für die Neubewertung sorgfältig.
- Wo eine Übertragung von Daten in die USA nicht gänzlich vermieden werden kann, sollten die TOMs verstärkt werden. Dazu gehören:
  - Starke Verschlüsselung: Implementieren Sie eine Ende-zu-Ende-Verschlüsselung, bei der der Schlüssel ausschließlich in Ihrer Kontrolle liegt (Bring Your Own Key – BYOK). So können selbst US-Behörden im Falle eines Zugriffs keine Klartextdaten einsehen.
  - Pseudonymisierung und Anonymisierung: Wenn möglich, pseudonymisieren oder anonymisieren Sie Daten, bevor sie in die Cloud übertragen werden. Dies reduziert das Risiko für die betroffenen Personen erheblich.
  - Datenminimierung: Sammeln und verarbeiten Sie nur die Daten, die unbedingt notwendig sind. Weniger Daten bedeuten ein geringeres Risiko.
  - Regelmäßige Audits und Kontrollen: Überprüfen Sie regelmäßig die Einhaltung der vereinbarten Sicherheitsmaßnahmen durch den Cloud-Dienstleister und führen Sie gegebenenfalls eigene Audits durch.
- Prüfen Sie aktiv europäische Cloud-Anbieter, die vergleichbare Dienste anbieten und deren Datenverarbeitung ausschließlich europäischem Recht unterliegt. Der Umstieg auf einen europäischen Anbieter kann langfristig die rechtliche Sicherheit und Ihre Software-Souveränität deutlich erhöhen.
- Sensibilisieren Sie Ihre Mitarbeitenden für die Risiken des Datentransfers in die USA und schulen Sie sie in der korrekten Anwendung der umgesetzten TOMs

Gerhard Müller – Brückenbauer zwischen IT, Sozialwirtschaft und gesellschaftlicher Verantwortung

Es gibt Menschen, die mit ihrer Laufbahn nicht nur beeindruckende Stationen verbinden, sondern auch konsequent daran arbeiten, Strukturen zu verändern und anderen auf diesem Weg zu helfen. Gerhard Müller ist einer von ihnen.

Von Fabian Eggers

Er ist Informatiker, Netzwerker, Sozialunternehmer, Community-Manager und ein Mensch, dem es um mehr geht als bloße Effizienz. Ihn treibt an, wie Technik dem Menschen dienen kann.

Heute arbeitet Müller als Community Manager im Caritas-Netzwerk IT e.V., bringt seine IT-Expertise in die Sozialwirtschaft ein und engagiert sich zugleich ehrenamtlich in der Wirtschaft, unter anderem als Vorsitzender des Fachausschusses Digitalisierung bei der IHK für München und Oberbayern. Seine Motivation? Brücken bauen. Zwischen Welten, die sich oft fremd bleiben – Wirtschaft und Wohlfahrt, Technik und Menschlichkeit, Vision und Realität.

Vom IT-Unternehmer zur gesellschaftlichen Verantwortung

Gerhard Müllers Karriere begann klassisch mit einem Informatikstudium an der TU München. Doch schnell wurde ihm klar: Er wollte nicht nur in Strukturen arbeiten, sondern sie selbst mitgestalten. Nach einem kurzen Intermezzo in einem Beratungsunternehmen gründete er gemeinsam mit elf Mitstreitern das IT-Beratungsunternehmen TNG Technology Consulting. Über 20 Jahre lang entwickelte er das Unternehmen als Partner und Geschäftsführer mit – auf über 500 Mitarbeitende. Das Unternehmen wuchs jährlich um 20 bis 30 Prozent, doch irgendwann war für Müller klar: Es musste eine neue Phase kommen.

Er verkaufte seine Anteile. Aber nicht, um sich zur Ruhe zu setzen, sondern um sich ganz dem Thema „lebenslanges Lernen“ und gesellschaftlichem Engagement zu widmen. „Ich wollte etwas Sinnstiftendes tun“, sagt Müller. Das führte ihn über Umwege zur Sozialwirtschaft. Als Interimsgeschäftsführer der Organisation „mitunsleben GmbH“ lernte er die Herausforderungen der Branche aus nächster Nähe kennen – inklusive der schmerzhaften Erfahrung, die Insolvenz anmelden zu müssen. Eine Phase, die ihn nicht entmutigte, sondern ihm deutlich machte, wie dringend Veränderungen nötig sind.

IT trifft Menschlichkeit: Die Arbeit im Caritas-Netzwerk

Seit 2022 bringt Müller seine Expertise in das Caritas-Netzwerk IT e. V. ein. Die Organisation agiert bundesweit als Vernetzer, Impulsgeber und Unterstützer von rund 150 Mitgliedsorganisationen mit über 100.000 Mitarbeitenden. Und das bei gerade einmal 1,75 Stellen im operativen Geschäft. „Unsere Ressourcen sind knapp, aber wir schaffen viel, weil wir ein gemeinsames Ziel haben“, erklärt Müller. Dieses Ziel: IT & Digitalisierung nicht nur technisch zu denken, sondern im Sinne der Menschen.

Dabei ist Digitalisierung für Müller kein Selbstzweck. „Ohne IT-Sicherheit gibt es keine sinnvolle Digitalisierung. Und ohne Digitalisierung keine realistische Antwort auf den demografischen Wandel.“ Besonders in der Sozialwirtschaft müsse man jetzt handeln, um in Zukunft überhaupt noch handlungsfähig zu sein. Für Gerhard Müller ist dabei klar: Es braucht zentralere Strukturen, professionelle IT-Dienstleister und eine grundlegende Veränderung im Selbstverständnis vieler Organisationen.

Sozialwirtschaft denkt zu klein? Müller fordert neue Strukturen

Ein zentrales Problem sieht er in der kleinteiligen Struktur der Wohlfahrt. Über 6.000 Caritas-Träger – 90 Prozent davon mit weniger als 50 Mitarbeitenden – kämpfen mit denselben Problemen, aber oft ohne Synergien zu nutzen. „Wir müssen weg vom Silodenken“, fordert Müller. Seine Vision: zentralisierte Serviceeinheiten, etwa auf Bundeslandebene, die Themen wie IT-Betrieb, Cybersicherheit, Lohnbuchhaltung oder Mobilität bündeln. Organisationen wie Flixbus oder Jochen Schweizer nennt er als Beispiele: „Die kümmern sich um Prozesse, sodass sich ihre Partner ganz auf ihre Kernkompetenzen konzentrieren können. Warum sollte das in der Sozialwirtschaft nicht gehen?“

Das bedeute nicht das Ende von Subsidiarität – im Gegenteil. Für Müller ist Subsidiarität richtig verstanden: Verantwortung dort belassen, wo sie sinnvoll ist, aber dort abgeben, wo es andere besser können.

„Die Herausforderungen der Zukunft können wir nur gemeinsam lösen. Und dabei geht es nicht um Ego oder Macht, sondern um Wirkung – für die Menschen.“

KI als Kulturtechnik: Chancen und Widersprüche

Künstliche Intelligenz ist für Müller kein Schreckgespenst, sondern eine riesige Chance. „Nach Lesen, Schreiben und Rechnen ist KI die vierte Kulturtechnik“, sagt er. Doch er sieht auch: Die Digitalisierung überrollt eine Branche, die dafür strukturell und personell kaum gewappnet ist. „Unsere Klienten nutzen längst KI – bei psychologischen Fragen, Gesundheitsthemen oder Familienproblemen. Und wir in der freien Wohlfahrt haben noch nicht einmal angefangen, uns wirklich damit zu beschäftigen.“

Dabei sieht Müller die ethische Verantwortung ganz klar auf Seiten der Träger. „Wenn wir mit Technik Menschen helfen können, dann ist es unsere Verpflichtung, das auch zu tun.“ Der technologische Fortschritt sei mit christlichen Werten keinesfalls unvereinbar. Er sei vielmehr eine Einladung, Nächstenliebe neu zu denken.

Zusammenarbeit mit Althammer & Kill: Expertise, die ankommt

Die Verbindung zu Althammer & Kill entstand während seiner Zeit bei „mitunsleben GmbH“. Heute sieht Müller in dem Unternehmen einen wichtigen Partner für die Sozialwirtschaft – nicht nur durch professionelle Datenschutzberatung, sondern durch ganzheitliche Unterstützung. Besonders hebt er die menschliche Zugänglichkeit von Thomas Althammer hervor: „Ein echter Trusted Advisor – so jemanden fragt man gerne wieder.“ Ob bei Konferenzen, Papers zur KI-Nutzung oder praxisnahen Angeboten wie Hinweisgeberschutzlösungen – für Gerhard Müller ist Althammer & Kill „Hilfe, die ankommt“. Der langfristige Aufbau von Vertrauen und die Unterstützung bei der strukturellen Weiterentwicklung der freien Wohlfahrt sind für ihn zentrale Stärken der Zusammenarbeit.

Fazit: „Win-Win für die Gesellschaft“

Gerhard Müller ist vieles: Techniker, Stratege, Visionär, Macher. Doch vor allem ist er jemand, der Menschen zusammenbringt – über Sektorengrenzen hinweg. Er kennt die Sprache der Wirtschaft genauso wie die Nöte der Sozialwirtschaft. Und er nutzt seine Energie, um beide Welten miteinander zu verbinden. Denn für ihn ist klar: „Die Herausforderungen der Zukunft können wir nur gemeinsam lösen. Und dabei geht es nicht um Ego oder Macht, sondern um Wirkung – für die Menschen.“

Althammer & Kill Akademie

KLICK/SCAN

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

3. September 2025 // 12. November 2025
kostenloses Webinar

Der datenschutzkonforme Internetauftritt

Eine Website muss nicht nur ansprechend, nutzerfreundlich und professionell sein, auch die Datenschutzkonformität gehört zu einem seriösen Internetauftritt dazu. Was früher als „nice to have" galt, ist heute ein klares Muss: Von Cookies und Drittdiensten über die transparente Gestaltung der Datenschutzerklärung und des Einwilligungsmanagements muss die Frage geklärt werden: Wie erfülle ich die datenschutzrechtlichen Vorgaben, schütze die Daten meiner Nutzerinnen und Nutzer und komme so Sanktionen durch die Aufsichtsbehörde zuvor?

17. September 2025 // 26. November 2025
kostenloses Webinar

NIS-2: Was bedeutet die Richtlinie für mein Unternehmen?

Fallen Sie unter NIS-2? Ihnen werden Methoden gezeigt, mit denen Sie prüfen können, ob Sie unter die Richtlinie fallen und ein Informationssicherheitsmanagement gemäß der Anforderungen der NIS-2-Richtlinie in ihrer Organisation bzw. in Ihrem Unternehmen implementieren müssen.

18. September 2025 – Online-Seminar

KI-Grundlagenseminar

Das Grundlagenseminar für Künstliche Intelligenz (KI) bietet Mitarbeitenden die Möglichkeit, ein grundlegendes Verständnis für eine der wichtigsten Technologien unserer Zeit zu entwickeln. Das Seminar vermittelt, wie KI funktioniert, welche Anwendungsbereiche existieren und welche Chancen als auch Risiken damit verbunden sind.

23. September 2025 // 4. November 2025
Online-Seminar

NIS-2-Management-Pflichtschulung: Cybersicherheit strategisch führen – Pflichten nach § 38 BSIG gemäß NIS2UmsuCG erfüllen

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.

24.–25. September 2025 // 2.–3. Dezember 2025
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.

1. Oktober 2025 // 17.12.2025
kostenloses Webinar

Die EU-KI-Verordnung (EU-KI-VO) – Was Sie ab dem 02. Februar 2025 wissen müssen!

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.

8. Oktober 2025 – kostenloses Webinar

Klare Leitplanken für KI – Ihre Roadmap zur erfolgreichen Richtlinie

Erfahren Sie, wie Sie eine fundierte KI-Richtlinie entwickeln, die Chancen neuer Technologien nutzt und zugleich Risiken für Datenschutz, Transparenz und Ethik minimiert. In dieser Session zeigen wir praxisnah, welche Bausteine eine gute Richtlinie enthalten sollte und wie Sie diese an die Anforderungen Ihrer Organisation anpassen. So schaffen Sie klare Leitplanken für den verantwortungsvollen Einsatz von KI.

15. Oktober 2025 – 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.

22. Oktober 2025 // 10. Dezember
kostenloses Webinar

Datenschutz-Folgenabschätzung – eine Einführung in die „hohe Kunst" des Datenschutzes

Das Webinar vermittelt eine Einführung in die Datenschutz-Folgenabschätzung (DSFA) als zentrales Instrument der DSGVO, um Risiken bei der Verarbeitung personenbezogener Daten zu erkennen und zu minimieren. Dabei wird gezeigt, dass die sogenannte „hohe Kunst" des Datenschutzes praxisnah und einfacher umzusetzen ist, als häufig angenommen. Nach dem Webinar wissen die Teilnehmenden, wie eine DSFA aufgebaut ist und in welchen Situationen sie in ihrer Organisation notwendig wird.

5. November 2025 – kostenloses Webinar

Wie arbeite ich datenschutzkonform mit KI?

Künstliche Intelligenz prägt zunehmend unseren Alltag und bringt neben vielen Chancen auch Herausforderungen für den Schutz der Privatsphäre mit sich. Um die Technologie verantwortungsvoll nutzen zu können, sind ein grundlegendes Verständnis ihrer Funktionsweise sowie klare Datenschutzrichtlinien entscheidend. Die Teilnehmenden erwerben praxisnahes Wissen, um KI sicher einzusetzen und persönliche Daten wirksam zu schützen.

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

Der DRK-Landesverband Hessen e.V. im erfolgreichen NIS-2-Assessment

Der DRK-Landesverband Hessen e. V. entschied sich für ein NIS-2-Assessment, um die Einhaltung gesetzlicher Vorgaben sicherzustellen, die eigenen Sicherheitsmaßnahmen zu verbessern und als Vorbild für die 35 angeschlossenen Kreisverbände zu dienen.

Von Christian Pinnecke

Der DRK-Landesverband Hessen e. V. mit Sitz in Wiesbaden ist einer von 19 Landesverbänden des Deutschen Roten Kreuzes und gliedert sich in 35 Kreisverbände sowie 394 Ortsvereine. Er bildet das zentrale organisatorische Bindeglied zwischen den Kreisverbänden und den Bundesstrukturen. Seine Aufgaben umfassen:

- Katastrophenschutz & Krisenhilfe: Bereitstellung von Notunterkünften, Verpflegung und Unterstützung bei Krisen und Großschadenslagen.
- Rettungsdienst & Notfallvorsorge: Organisation von professionellen Rettungsdiensten und medizinischer Notfallversorgung.
- Pflege & soziale Arbeit: Unterstützung älterer und hilfsbedürftiger Menschen durch mobile Pflegedienste und Betreuungsangebote.
- Bildung & Schulungen: Ausbildung in Erster Hilfe, Katastrophenschutz und sozialen Berufen.
- Humanitäre Hilfe weltweit: Bereitstellung von Katastrophenhilfe und langfristigen Entwicklungsprojekten in Krisengebieten.
- Ein wesentlicher Bestandteil der Arbeit des Landesverbands ist die Sicherstellung einer funktionierenden digitalen Infrastruktur, insbesondere für die kritischen Dienstleistungen wie den Katastrophenschutz.

Ausgangssituation: Warum ein NIS-2 Assessment?

Mit der neuen NIS-2-Richtlinie wird der Kreis der verpflichteten Unternehmen und Organisationen erheblich erweitert. Besonders Betreiber von Kritischen Infrastrukturen (KRITIS) stehen vor der Herausforderung, ihre IT-Sicherheit an die gestiegenen Anforderungen anzupassen. Für den DRK-Landesverband Hessen e. V. war frühzeitig klar, dass er von der Richtlinie betroffen sein könnte. Vor allem das Katastrophenschutzlager in Fritzlar, das weltweit in Krisensituationen Unterstützung leistet, könnte in den Geltungsbereich von NIS-2 fallen.

Neben der reinen rechtlichen Einordnung verfolgte der Landesverband weitere Ziele:

- Erhöhung der Cybersicherheit und Identifikation von Verbesserungsmöglichkeiten.
- Schaffung eines einheitlichen Standards für die 35 Kreisverbände.
- Sicherung der Einsatzfähigkeit für den Katastrophenschutz.
- Schärfung der Argumentationsgrundlage für Budget- und Ressourcenentscheidungen.

Norbert Gerlach, Fachverantwortlicher für Digitalisierung beim DRK-Landesverband Hessen e. V., erläutert: „Innerhalb der IT war uns klar, dass wir unter NIS-2 fallen. Mit dem Assessment wollten wir diese Einschätzung von externer Seite bestätigen lassen."

Das Assessment: Ablauf und Zusammenarbeit

Das NIS-2-Assessment wurde als strukturiertes Standardprodukt durchgeführt und in mehreren Schritten umgesetzt:

1. Vorbereitung & Analyse

- Prüfung der rechtlichen Vorgaben und Einordnung des DRK-Landesverbands in den NIS-2-Rahmen
- Analyse der bestehenden IT- und Sicherheitsmaßnahmen
- Untersuchung der kritischen Dienstleistungen mit Fokus auf das Katastrophenlager in Fritzlar

2. Durchführung

- Durchführung von strukturierten Interviews mit Verantwortlichen
- Prüfung relevater Sicherheits- und Compliance-Dokumente
- Bewertung der bestehenden technischen und organisatorischen Maßnahmen

3. Auswertung und Ergebnisse

- Dokumentation der rechtlichen Einordnung: Nur der Standort Fritzlar fällt unter NIS-2
- Identifikation von Verbesserungspotenzial bei den Sicherheitsmaßnahmen
- Bereitstellung einer detaillierten Präsentation der Ergebnisse für die Führungsebene

„Wir haben die Website des Kunden analysiert, um die angebotenen Dienstleistungen zu verstehen, und die

„Innerhalb der IT war uns klar, dass wir unter NIS-2 fallen. Mit dem Assessment wollten wir diese Einschätzung von externer Seite bestätigen lassen."

Norbert Gerlach, Fachverantwortlicher für Digitalisierung beim DRK-Landesverband Hessen e. V.

1	2	3
Herausforderung und Ziel	**Lösung**	**Nutzen**
Sicherstellung der NIS-2 Compliance	Durchführung eines strukturierten NIS-2 Assessments	klare Bestätigung der gesetzlichen Einordnung
Stärkung der IT-Sicherheitsmaßnahmen	Analyse der rechtlichen Rahmenbedingungen	verbesserte Argumentationsgrundlagen für Entscheidungen
Orientierung für 35 Kreisverbände	Identifikation relevanter KRITIS-Dienstleistungen	eine gestärkte Sicherheitsstrategie

rechtlichen Vorgaben geprüft, da der Kunde bereits Betreiber Kritischer Infrastruktur ist. Ein besonderer Schwerpunkt wurde auf die KRITIS-Dienstleistungen gelegt." erklärt Christian Pinnecke, Berater für Informations- und IT-Sicherheit bei Althammer & Kill.

„Wir empfehlen unseren Kreisverbänden die Nutzung des Assessments, damit sie Klarheit in Richtung NIS-2 bekommen."

Norbert Gerlach, Fachverantwortlicher für Digitalisierung beim DRK-Landesverband Hessen e. V.

Empfehlung für andere Organisationen

Aufgrund der positiven Erfahrung empfiehlt der DRK-Landesverband Hessen e.V. das Assessment auch seinen angeschlossenen, aber rechtlich unabhängigen Kreisverbänden. Warum?

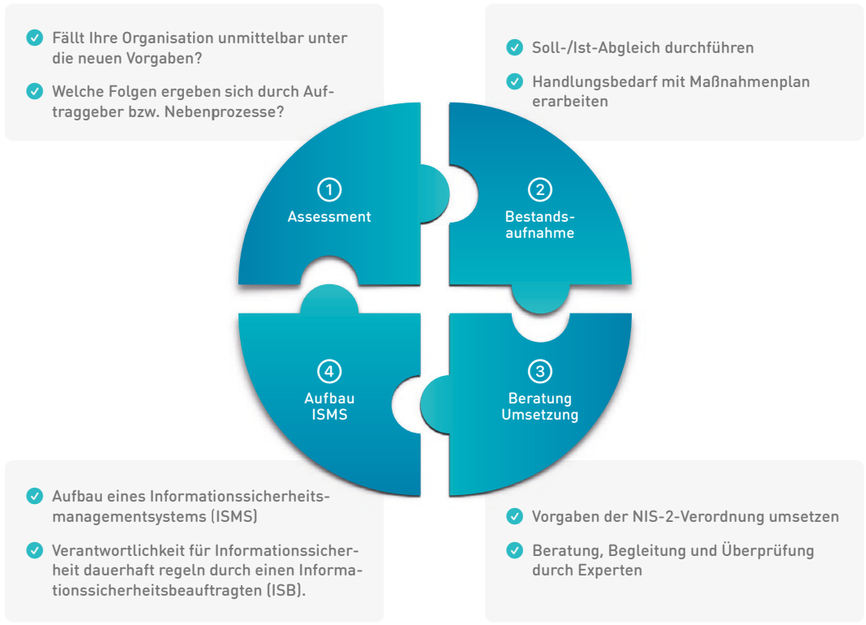
- Klärung der individuellen Betroffenheit von NIS-2
- Identifikation von Handlungsfeldern zur Verbesserung der Cybersicherheit
- Mehr Transparenz für strategische Entscheidungen

Fazit und Zukunftsausblick

Das NIS-2-Assessment beim DRK-Landesverband Hessen e. V. hat gezeigt, wie wichtig eine strukturierte und professionelle Herangehensweise an regulatorische Anforderungen ist. Die externe Bewertung bestätigte nicht nur die bisherigen Einschätzungen, sondern lieferte auch eine fundierte Grundlage für strategische Entscheidungen im Bereich IT-Sicherheit.

Besonders wertvoll war die gewonnene Klarheit über die eigene Betroffenheit: Während der Landesverband als Ganzes nicht unter die NIS-2-Richtlinie fällt, ist der Standort Fritzlar als kritische Infrastruktur einzustufen. Diese Erkenntnis ermöglicht eine gezielte Fokussierung der Sicherheitsmaßnahmen an der richtigen Stelle. Darüber hinaus hat das Assessment dazu beigetragen, Sicherheitsbewusstsein auf Führungsebene zu stärken und eine überzeugende Argumentationsgrundlage für Investitionen in die IT-Sicherheit zu schaffen. Durch die Empfehlung an die angeschlossenen Kreisverbände zeigt sich der DRK-Landesverband Hessen e. V. als Vorreiter in Sachen IT-Sicherheit und Compliance. Mit Blick auf die Zukunft wird der Landesverband weiterhin auf Transparenz, Sicherheitsbewusstsein und Prävention setzen, um für kommende Herausforderungen in der digitalen Welt bestens vorbereitet zu sein.

Die erfolgreiche Umsetzung eines NIS-2-Assessments beim DRK-Landesverband Hessen e. V. folgt einem strukturierten Prozess, der insgesamt vier zentrale Bausteine enthält: Assessment, Bestandsaufnahme, Beratung & Umsetzung sowie der Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Diese Bausteine bilden die Grundlage, um die Anforderungen der NIS-2-Richtlinie effizient und nachhaltig umzusetzen. Sie stellen sicher, dass alle relevanten rechtlichen und sicherheitsrelevanten Aspekte berücksichtigt werden und ermöglichen eine gezielte Verbesserung der IT-Sicherheit.



Digitale Souveränität in Gefahr? Die DSFA zu Microsoft 365 braucht ein Update!

Warum Unternehmen ihre bestehende Datenschutz-Folgenabschätzung (DSFA) zu Microsoft 365 dringend überprüfen sollten und was die Integration von KI, neue Use Cases und geopolitische Entwicklungen damit zu tun haben.

Von Levin Rühmann und Fabian Brandenburger

Viele Unternehmen haben bereits vor einiger Zeit eine Datenschutz-Folgenabschätzung (DSFA) im Zusammenhang mit dem Einsatz von Microsoft 365 (M365) durchgeführt, häufig jedoch auf Basis von Rahmenbedingungen, die sich inzwischen grundlegend verändert haben. Der Einsatz von M365 entwickelt sich kontinuierlich weiter: neue Funktionen, veränderte Formen der Zusammenarbeit sowie neue datenschutzrechtliche Risiken machen eine erneute Bewertung erforderlich.

Warum ein Update jetzt nötig ist

Neue Funktionen = neue Risiken: Mit der Integration von Microsoft Co-Pilot in nahezu alle M365-Anwendungen (z. B. Teams, Word, Excel, Outlook) verändern sich die datenschutzrechtlichen Rahmenbedingungen grundlegend. Auch ohne Co-Pilot-Enterprise-Lizenz ist die Funktion über persönliche M365-Konten grundsätzlich nutzbar – mit potenziellen Risiken für die Verarbeitung personenbezogener Daten.

Durch neue Funktionen in M365 entstehen neue Risiken, welche im Rahmen einer Datenschutz-Folgenabschätzung betrachtet werden müssen. In diesem Zusammenhang sind wirksame technische und organisatorische Maßnahmen entscheidend, um die neu entstanden Risiken zu minimieren. Besonders kritisch: Co-Pilot kann auf im Tenant veröffentlichte Inhalte zugreifen. Das kollidiert mit dem datenschutzrechtlichen Grundsatz des „Need to know". Daten dürfen nur den Personen zugänglich sein, die sie zur Aufgabenerfüllung benötigen. Ein fehlendes Rollen- und Berechtigungskonzept kann dazu führen, dass sensible Informationen intern ungewollt offengelegt werden.

Zudem ist zu prüfen, welche Daten verarbeitet, übertragen oder potenziell zur Verbesserung von KI-Modellen genutzt werden. Ohne klare Rechtsgrundlage, etwa bei personenbezogenen Daten in Dokumenten, ist die Nutzung unzulässig.

Organisatorische Maßnahmen wie ein Datenklassifizierungskonzept sind zwingend erforderlich. Auch rechtliche Fragestellungen zum KI-Einsatz nach der EU-KI-VO insgesamt (z. B. Verantwortlichkeit, Transparenz, Zweckbindung) müssen bewertet werden. Neue Funktionen bringen immer auch neue Datenschutzpflichten mit sich. Microsoft Co-Pilot ist hier nur ein aktuelles Beispiel.

Risiken:
- Automatisierte Verarbeitung personenbezogener Daten ohne Rechtsgrundlage
- Unberechtigte Zugriffsmöglichkeiten auf team- oder abteilungsübergreifende Inhalte
- Fehlende zentrale Deaktivierungsoption auf Systemebene

Geopolitik und Rechtslage: Trump, CLOUD-Act, ChatGPT & Co.

Die Rückkehr von Donald Trump in das Weiße Haus sowie jüngste Entwicklungen im Bereich der US-Politik verdeutlichen erneut die Bedeutung digitaler Souveränität für europäische Unternehmen und Behörden. Besonders sichtbar wurde dies im Fall der Kontosperrung von Karim Khan, dem Chefankläger des Internationalen Strafgerichtshofs, durch Microsoft auf Anordnung US-amerikanischer Behörden. Dieses Ereignis macht die politische Einflussnahme der USA auf globale Cloud-Dienste und die potenzielle Gefährdung der Unabhängigkeit europäischer Institutionen deutlich.

Relevante Entwicklungen:
- Fall Karim Khan (2025): Der Fall Karim Khan und die Sperrung seines Microsoft-Kontos wirft Fragen der digitalen Souveränität auf. Microsoft hat das Konto des IStGH-Chefanklägers aufgrund von US-Sanktionen gegen den Gerichtshof gesperrt, was zu Kritik an der Abhängigkeit internationaler Institutionen von US-Anbietern führte. Dies ist ein Beispiel direkter politscher Einflussnahme.
- OpenAI-Urteil (USA, 13. Mai 2025): Speicherung und Auswertung von Chatverläufen bei Nutzung von ChatGPT Free, Pro oder Plus wird durch zuständiges Gericht angeordnet, d.h. OpenAI darf keine Verlaufsdaten mehr löschen. Nutzer haben kaum Kontrolle über die Verwendung ihrer Daten.
- CLOUD Act: US-Unternehmen müssen US-Behörden Zugriff auf alle verwalteten Daten gewähren, egal wo die Daten physisch gespeichert sind, d. h. weltweit, was den Einfluss US-amerikanischer Politik auf globale Cloud-Dienste manifestiert.
- Gefahr für DSGVO-Konformität und digitale Souveränität: Die Kombination aus US-Recht und den technischen Gegebenheiten vieler Cloud-Dienste gefährdet den Schutz personenbezogener Daten und die Selbstbestimmung europäischer Nutzerinnen und Mutzer.

Diese Entwicklungen unterstreichen die dringende Notwendigkeit für europäische Unternehmen und Institutionen, ihre digitale Souveränität zu stärken etwa durch den verstärkten Einsatz europäischer Cloud-Angebote, technische Kontrollmechanismen und klare vertragliche Datenschutzvereinbarungen.

„Die Datenschutz-Folgenabschätzung ist gemäß Art. 35 DSGVO regelmäßig zu überprüfen und bei Änderungen der Verarbeitung fortzuschreiben.“

Jetzt handeln: Das sollte geprüft werden

Angesichts der sich dynamisch ändernden technischen und rechtlichen Rahmenbedingungen müssen Unternehmen ihre Risiken im Umgang mit Cloud-Diensten und KI-Funktionen neu bewerten. Dabei ist es entscheidend, genau zu analysieren, welche Geschäftsprozesse in die Cloud ausgelagert werden und welche Abhängigkeiten daraus entstehen können.

Eine fundierte Risiko- und Business-Impact-Analyse sowie Exitstrategien sind unverzichtbar, um die Kontrolle über Daten und Abläufe zu bewahren.

Technische Konfigurationen von Microsoft 365 und weiteren Cloud-Diensten:
- Rollen- und Berechtigungskonzepte auf Aktualität und Angemessenheit prüfen
- Sichtbarkeit und Zugriffsrechte für veröffentlichte Dokumente evaluieren
- Aktivierung und Konfiguration von KI-Funktionen wie Copilot kritisch hinterfragen
- Nutzung weiterer Cloud-Apps und neuer Funktionalitäten in den Blick nehmen und auf Datenschutzrisiken prüfen

Interne Prozesse und Governance:
- Klare Nutzungsrichtlinien für Cloud- und KI-Dienste im Unternehmen etablieren und regelmäßig anpassen
- Mitarbeitende umfassend über Zugriffsrechte und Funktionsweisen der eingesetzten Anwendungen und Systeme informieren und schulen
- Entscheidungsprozesse zum Einsatz neuer Funktionen und Dienste transparent gestalten und dokumentieren
- Regelmäßige Audits und Kontrollen der technischen Konfigurationen durchführen
- Geschäftsprozesse systematisch erfassen und Abhängigkeiten durch Cloud-, KI- und weitere IT-Dienste identifizieren
- Risiko- und Business-Impact-Analysen für kritische Prozesse erstellen und regelmäßig aktualisieren
- Exit- und Notfallstrategien entwickeln und dokumentieren, um bei Störungen schnell reagieren zu können

Ergebnis: DSFA-Update statt Neuanfang

Die bereits durchgeführte Datenschutz-Folgenabschätzung kann in vielen Fällen als solide Basis dienen. Sie muss jedoch aktualisiert und erweitert werden, um neue Risiken, veränderte Anwendungsfälle und technische Weiterentwicklungen zu berücksichtigen. Nur so bleibt die Bewertung realistisch und die Datenschutzstrategie wirksam.

Blick nach vorne: Digitale Souveränität als Ziel

Immer mehr Unternehmen hierzulande setzen sich mit den Risiken wachsender Abhängigkeiten auseinander, sowohl bei Cloud-Diensten als auch im Bereich von KI-Anwendungen. Insbesondere bei der Nutzung leistungsstarker KI-Modelle internationaler Anbieter entstehen neue Herausforderungen in Bezug auf Datenschutz, Datenhoheit und regulatorische Kontrolle.

Vor diesem Hintergrund gewinnen souveräne Cloud-Infrastrukturen und alternative Plattformen zunehmend an Bedeutung. Sie versprechen mehr Kontrolle über Daten, Prozesse und eingesetzte Technologien, insbesondere bei sensiblen und geschäftskritischen Anwendungen. Auch etablierte Technologiekonzerne entwickeln derzeit Angebote, die sich an europäischen Datenschutzanforderungen orientieren und lokale Datenhaltung

Stichwort
Datenschutzfolgenabschätzung

Ziel:
Risiken für die Rechte und Freiheiten Betroffener frühzeitig erkennen und wirksam minimieren.

Pflicht:
Bei besonders risikoreichen Verarbeitungen (Art. 35 DSGVO).

Beispiel:
Einsatz von Microsoft 365 mit Verarbeitung sensibler Daten, Einführung weiterer Apps oder Anwendungen, KI-Funktionen und globalem Zugriff mittelts Co-Pilot.

ermöglichen. Ob diese Lösungen ihren Versprechen in der Praxis gerecht werden, bleibt jedoch abzuwarten und muss kritisch begleitet werden.

Ziel dieser Entwicklungen ist es, digitale Unabhängigkeit und technologische Selbstbestimmung zu stärken – als strategische Grundlage für sichere, datenschutzkonforme und zukunftsfähige Digitalisierung.

Fazit: Keine Zeit für Stillstand

Technologie, Regulierung und Abhängigkeiten entwickeln sich dynamisch, insbesondere im Kontext von Cloud- und KI-Anwendungen. Wer seine Datenschutz-Folgenabschätzung nicht regelmäßig aktualisiert, riskiert, zentrale technische und organisatorische Entwicklungen zu übersehen. Das kann zu rechtlichen Unsicherheiten und Kontrollverlust führen. Das gilt insbesondere auch für Plattformen wie Microsoft 365, deren kontinuierliche Erweiterung neue Abhängigkeiten schafft und eine erneute Bewertung der Risiken erforderlich macht, inklusive der Entwicklung realistischer Exit-Strategien

Handlungsimpuls

Die DSFA sollte mindestens einmal jährlich überprüft und bei funktionalen, technischen oder organisatorischen Änderungen angepasst werden. Nur so bleibt sie ein wirksames Instrument für Datenschutz, Compliance und digitale Souveränität. &

Regulierte Intelligenz: KI mit Verantwortung

Ab August 2025 gelten neue, zusätzliche Regeln für KI mit allgemeinem Verwendungszweck. Unternehmen müssen jetzt handeln, um compliant und zukunftssicher zu bleiben.

Von Fabian Brandenburger

Künstliche Intelligenz (KI) ist längst keine Zukunftsmusik mehr – sie ist in vielen Branchen zum festen Bestandteil geworden. Besonders sogenannte General Purpose AI (GPAI), also KI-Modelle mit breitem Einsatzspektrum, revolutionieren Geschäftsprozesse, Kundeninteraktionen und Produktinnovationen. Doch mit wachsender Bedeutung steigt auch die Verantwortung. Um Risiken zu minimieren und Vertrauen zu schaffen, setzt die EU erstmals einen umfassenden Rechtsrahmen für KI-Modelle mit allgemeinem Verwendungszweck (mit systemischem Risiko): Diese zusätzlichen Regelungen der KI-Verordnung (KI-VO) treten ab dem 2. August 2025 verbindlich in Kraft und stellen Anbieter, Betreiber und Einkäufer von KI mit allgemeinem Verwendungszweck vor neue Herausforderungen und Chancen.

Die zwei Gesichter der General Purpose AI (GPAI)

KI-Modelle mit allgemeinem Verwendungszweck (GPAI) sind flexibel und können in unterschiedlichsten Szenarien eingesetzt werden. Man kann sie mit einem Schweizer Taschenmesser vergleichen: Vielseitig, nützlich und anpassbar.

Gleichzeitig gibt es KI-Modelle, die aufgrund ihrer Funktionsweise und Auswirkungen als potenziell riskanter eingestuft werden: KI-Modelle mit allgemeinem Verwendungszweck mit systemischen Risiken (GPAI+). Diese Modelle sind eher mit einem Schweizer Taschenmesser mit Dietrichfunktion zu vergleichen, d. h. vielseitig, nützlich, anpassbar, aber ein leistungsfähiges Werkzeug, das missbrauchsanfällig ist und daher strenger kontrolliert werden muss.

Beispiele für GPAI:
- Sprachmodelle wie GPT-4 oder Metas LLaMA, die natürlichsprachliche Aufgaben erledigen: vom Textgenerieren bis zur Übersetzung
- Bildgeneratoren wie Stable Diffusion, die fotorealistische oder künstlerische Bilder erzeugen
- Multimodale Systeme wie Google Gemini, die Text, Bild und andere Datenformen verknüpfen können

Diese Technologien bieten enorme Vorteile gegenüber bisherigen Modellen wie etwa Automatisierung, verbesserte Entscheidungsfindung und gesteigerte Effizienz. Gleichzeitig bergen sie höhere Risiken hinsichtlich Fehlinformationen, Diskriminierung, Sicherheitslücken oder Manipulation.

„Wer KI strategisch nutzt, muss regulatorisch vorbereitet sein. Das ist kein Widerspruch, sondern der nächste logische Schritt."

Neue Regelungen ab dem 02.08.2025 im Überblick

Die EU-KI-Verordnung definiert klare Rahmenbedingungen, um den verantwortungsvollen Umgang mit KI sicherzustellen:

1 Transparenz und technische Dokumentation (Art. 50 u. Kapitel V KI-VO)

Anbieter müssen nachvollziehbar offenlegen, wie ihre KI-Modelle trainiert wurden, auf welchen Daten sie basieren und welche potenziellen Risiken bestehen. Gleichzeitig sind Betreiber von KI-Systemen verpflichtet, Nutzende umfassend über die Funktion und den Einsatz der KI zu informieren. Diese Transparenz ist essenziell, um Vertrauen bei Kundeninnen und Kunden sowie Regulierungsbehörden aufzubauen und die Nachvollziehbarkeit von Entscheidungen zu gewährleisten.

Die in Artikel 50 der KI-VO verankerte Kennzeichnungspflicht für KI-generierte Inhalte soll dazu dienen die Transparenz zu gewährleisten und Risiken wie Desinformation oder Täuschungen durch Deepfakes zu minimieren. Für Unternehmen bedeutet das: Sie müssen sicherstellen, dass erkennbar ist, wenn Inhalte nicht von Menschen, sondern von KI-Systemen erzeugt wurden.

2 Governance auf EU- und nationaler Ebene (Kapitel VII KI-VO)

Die Regulierung erfolgt durch ein mehrstufiges Kontrollsystem: Nationale Aufsichtsbehörden überwachen die Einhaltung der Vorschriften vor Ort, während das Europäische Gremium für Künstliche Intelligenz (sog. KI-Gremium) nach Art. 65 KI-VO die Koordination und Harmonisierung übernimmt. Unternehmen müssen daher ihre internen Prozesse anpassen, um sowohl nationalen als auch europäischen Anforderungen gerecht zu werden.

3 Notifizierende Behörden und notifizierte Stellen (Kapitel III, Abschnitt 4 KI-VO)

Diese Institutionen sind verantwortlich für die Klassifizierung von GPAI-Modellen und die Bewertung ihrer systemischen Risiken. Vor der Markteinführung neuer KI-Produkte wird eine Prüfung und Zulassung notwendig, um den sicheren Einsatz zu gewährleisten – die sogenannte Konformitätsbewertung.

4 Vertraulichkeit (Artikel 78 KI-VO)

Geschäftsgeheimnisse und sensible Informationen der Anbieter sind geschützt, doch die EU fordert gleichzeitig eine Mindestoffenlegung, insbesondere bei Modellen mit hohem Missbrauchspotenzial (GPAI+). So soll eine Balance zwischen Innovation und Sicherheit gefunden werden, ohne dass KI-Systeme als undurchsichtige Blackboxes agieren.

Gut zu wissen

Relevante Definitionen

KI-Modelle mit allg. Verwendungszweck (Art. 3 Nr. 63 KI-VO):
Ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden

KI-Systeme mit allg. Verwendungszweck (Art. 3 Nr. 66 KI-VO):
Ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen

Systemisches Risiko (Art. 3 Nr. 65 KI-VO):
Ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können.

5 Sanktionen bei Verstößen (Kapitel XII KI-VO)

Verstöße gegen die KI-VO können Konsequenzen nach sich ziehen. Von Verwarnungen und behördlichen Anordnungen bis hin zu Nutzungseinschränkungen oder gar Verboten. Für Anbieter von GPAI ohne systemische Risiken sind Geldbußen derzeit nicht vorgesehen, während bei GPAI+ und der Missachtung des Art. 5 (Verbotene Praktiken) erhebliche Strafen drohen können. Entscheidend für die Ermittlung der möglichen Strafen ist, gegen welche Vorgaben der KI-VO durch welche Akteure verstoßen wurde. Dies erhöht den Druck auf Unternehmen, ihre Compliance ernst zu nehmen, weil die Strafen bis in die Millionen gehen können, je nach Schwere des Verstoßes.

Was bedeutet das konkret für Unternehmen?

- **Bereich Einkauf:** Prüfen, ob eine KI-Software mit einem KI-Modell, das unter die Kategorie „KI-Modell mit allgemeinem Verwendungszweck (und systemischen Risiken)" fällt, eingekauft werden soll (Checkliste für den Einkauf).
- **Bereich IT und Compliance:** Prüfung bereits vorhandener Software, ob diese unter die Definition des KI-Modells oder des KI-Systems fällt. Technische Dokumentation, Risikoanalyse, Governance etablieren
- **Nutzende:** transparent über KI-Einsatz und Funktionsweise informieren
- **Geschäftsleitung:** Strategische Entscheidungen zu KI-Einsatz und Investitionen in Compliance treffen

Die Anforderungen verlangen ein interdisziplinäres Vorgehen bei Software-Projekten: IT-Spezialisten, Informationssicherheitsbeauftragte, Compliance-Verantwortliche, Einkaufsabteilung, Kommunikationsabteilungen und Datenschutz müssen eng zusammenarbeiten, um die KI-Nutzung rechtssicher und transparent zu gestalten.

Praxistipp: Frühzeitig handeln zahlt sich aus

Die KI-Verordnung gibt einen klaren Rahmen vor, doch die Umsetzung ist lösbar. Ein strukturierter Einstieg, klare Zuständigkeiten und passende Tools helfen Unternehmen, Risiken zu minimieren und regulatorische Anforderungen effizient zu erfüllen. Dabei eröffnet die Compliance zugleich Chancen: Ein verantwortungsvoller Umgang mit KI stärkt das Vertrauen von Auftraggebenden sowie Geschäftspartnerinnen und Geschäftspartnern und verbessert die Wettbewerbsfähigkeit. Althammer & Kill unterstützt Unternehmen dabei mit praxisbewährten Starterpaketen, die individuell angepasst werden können:

- **Mapping:** Welche GPAI-Systeme sind im Einsatz und wie werden sie genutzt?
- **Regel-Check:** Welche Vorschriften gelten für welche Modelle und wann?
- **Governance-Toolbox:** Vorlagen für Compliance-Strukturen, Rollen und Verantwortlichkeiten
- **Workshops und Schulungen:** Zielgerichtet, praxisnah und rechtssicher für alle relevanten Abteilungen

Fazit: KI braucht mehr als nur Technik

Die KI-Verordnung bringt dringend benötigte Klarheit in das Thema Künstliche Intelligenz und setzt neue, verbindliche Pflichten für alle Beteiligten. Wer sich frühzeitig auf die Anforderungen vorbereitet, kann Risiken wie Missbrauch, Haftungsfragen und Reputationsschäden minimieren. Gleichzeitig profitiert er von erhöhter Innovationskraft und einem nachhaltigen Wettbewerbsvorteil.

Der Schlüssel liegt in einem partnerschaftlichen, ganzheitlichen Ansatz mit kompetenten Beratenden, passgenauen Werkzeugen und einem strategischen Compliance-Management. Mehr Infos und unseren KI-Readiness-Check finden Sie auf unserer Webseite. Schauen Sie doch mal vorbei! &

KLICK/SCAN

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

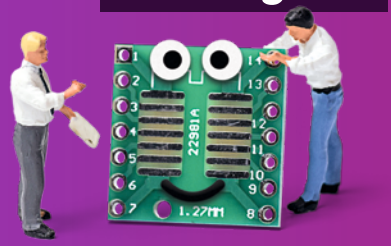
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

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