COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 4/2025

NIS-2 im Griff

Unser aktuelles Whitepaper macht aus komplexen Vorgaben eine praxisnahe Roadmap.

Seite 6

KI-Starterpakete
Klar starten, sauber steuern – von der Idee zum geordneten Einsatz
Seite 12

Datenschutz-Audits im Sozialbereich
Pragmatisch planen und umsetzen
Seite 16

NIS-2 in der Praxis
So wurde eine Fachklinik prüffähig und resilient.
Seite 20

Norddeutsches
KI-Forum

Der 360°-Blick auf KI
in Unternehmen und Behörden

Künstliche Intelligenz verändert die Geschäftswelt rasant und bietet vielfältige Möglichkeiten für Unternehmen, Behörden und Kommunen. Das Norddeutsche KI-Forum bringt führende Köpfe, Innovatoren und Entscheidungsträger aus der Region zusammen, um gemeinsam die Zukunft der KI zu gestalten

JETZT TICKET BUCHEN!

18.–19. Februar 2026
Designhotel Wienecke XI, Hannover
ki-forum-nord.de

ALTHAMMER & KILL
H|S|V|N Kommunale Hochschule für Verwaltung in Niedersachsen
UVN Unternehmerverbände Niedersachsen

Editorial

Liebe Leserin, lieber Leser,

wir treffen viele Teams, die gerade viel stemmen – Termine, Entscheidungen, offene Fragen. Oft hören wir: Es wird nicht einfacher. Genau dafür ist dieses Heft gedacht. Es soll Ihnen Orientierung geben und den nächsten Schritt erleichtern.

Im Leitartikel geht es um das NIS-2-Umsetzungsgesetz (NIS2UmsuCG). Wir fassen zusammen, was für Leitung und Fachbereiche jetzt wichtig ist und zeigen, wie sich Vorgaben sinnvoll in bestehende Strukturen einfügen lassen. Dazu haben wir ein kompaktes Whitepaper vorbereitet, das Prioritäten und Reihenfolge klärt.

Ein weiteres Thema liegt uns besonders am Herzen: KI pragmatisch einführen. Unsere KI-Starterpakete bündeln die häufigsten Fragen aus Projekten. Welche Anwendungsfälle sind realistisch, wie dokumentiert man schlau, wo entstehen Risiken und wie behält man sie im Griff. Ziel ist ein Fahrplan, der zu Ihrer Organisation passt und sofort nutzbar ist.

Außerdem widmen wir uns Audits bei Dienstleistern und Lieferanten. Viele Abhängigkeiten liegen außerhalb der eigenen Systeme. Wir zeigen, wie ein schlankes Verfahren aussieht, welche Dokumentationen benötigt werden und wie Sie Prüfbarkeit als Routine etablieren statt als einmalige Aktion.

Zum Schluss berichten wir aus der Praxis zu NIS-2. Was hat Tempo gebracht, wo gab es Hürden und welche Entscheidungen haben Stabilität geschaffen.

Wenn Sie beim Lesen eine Stelle finden, die gerade zu Ihrer Lage passt, melden Sie sich gern. Ein kurzer Austausch bringt oft mehr Klarheit als eine lange Sitzung.

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*

Digitale Souveränität in der Praxis: Wege von der Vision zur Umsetzung

Digitale Souveränität ist kein Zustand, sondern ein Weg. Der Beitrag zeigt, wie Sie Abhängigkeiten sichtbar machen, Risiken priorisieren und realistische Schritte zur eigenen Gestaltungshoheit gehen. Digitale Souveränität ist ein Begriff, der in politischen Grundsatzpapieren ebenso präsent ist wie auf Fachkonferenzen, in IT-Abteilungen oder in Strategiepapieren großer Unternehmen. Doch häufig bleibt unklar, was damit konkret gemeint ist. Geht es um Datenschutz? Um staatliche Kontrolle über digitale Infrastrukturen? Oder um Alternativen zu dominierenden US-Cloudanbietern?

KLICK/SCAN

Privacy by Design: Warum Datenschutz für Startups kein Luxus ist, sondern Überlebensstrategie

KLICK/SCAN

Gemeint ist: Datenschutz nicht nachträglich einbauen, sondern von Anfang an ins Konzept integrieren. Privacy by Design ist deshalb keine juristische Pflichtübung, sondern ein strategisches Instrument. Es schafft Vertrauen, reduziert Risiken und öffnet Türen zu Kapital und Märkten

Business Impact Analyse – Grundlage für digitale Souveränität und Unternehmensresilienz

Die Business Impact Analyse ist ein systematischer Prozess, der darauf abzielt, die Auswirkungen eines Ausfalls von Geschäftsprozessen zu bewerten. Sie hilft Unternehmen dabei, die wichtigsten Abläufe zu identifizieren und zu priorisieren, Risiken zu erkennen und die Grundlage für Maßnahmen zur Sicherstellung der Betriebsfähigkeit zu schaffen.

KLICK/SCAN

NIS-2 in der Praxis: Was § 38 BISG von der Geschäftsleitung verlangt

In diesem Beitrag zeigen wir, was § 38 NIS2UmsuCG konkret fordert und wie sich die Anforderungen mit den übrigen Pflichten aus NIS-2 verzahnen. Zudem erhalten Sie pragmatische Hinweise, wie sich die gesetzlichen Vorgaben wirksam und nachweisbar in die Unternehmenspraxis überführen lassen.

KLICK/SCAN

Auditpflicht im Sozialwesen: So erfüllen Sie Ihre Datenschutzanforderungen rechtssicher

Neben der allgemeinen Datenschutz-Grundverordnung (DSGVO) normieren die Sozialgesetzbücher (SGB) zusätzliche Pflichten zumindest für Leistungsträger. Insbesondere betrifft dies die regelmäßige Kontrolle von Dienstleistern, die im Auftrag der Einrichtungen personenbezogene Daten verarbeiten (Art. 28 DSGVO). Im Beitrag zeigen wir auf, welche rechtlichen Grundlagen diese erweiterten Pflichten begründen, warum Dienstleister ggf. auch für Leistungserbringer umfassender zu prüfen sind, in welchem Turnus Audits stattfinden sollten und worauf es in der Praxis ankommt.

KLICK/SCAN

360°-Blick auf KI: Wirtschaft, Verwaltung und Unternehmen

Künstliche Intelligenz revolutioniert die Geschäftswelt und bietet enorme Chancen für Unternehmen aller Branchen sowie Behörden und Kommunen. Das Norddeutsche KI-Forum bringt führende Experten, Innovatoren und Entscheider aus der Region zusammen, um gemeinsam die Zukunft der KI zu gestalten.

Erleben Sie inspirierende Vorträge, praxisorientierte Workshops und anregende Diskussionsrunden rund um das Thema Künstliche Intelligenz. Vernetzen Sie sich mit Experten aus Wissenschaft, Verwaltung und Wirtschaft und entdecken Sie, wie KI bereits erfolgreich in norddeutschen Organisationen eingesetzt wird. Lassen Sie sich inspirieren und erkunden Sie die Potenziale für Ihr eigenes Unternehmen oder Ihre Behörde.

KLICK/SCAN

Zahl des Monats

119

So viele neue IT-Schwachstellen werden in Deutschland im Schnitt pro Tag bekannt. Das meldet das BSI in seinem aktuellen Lagebericht. Für die Praxis heißt das: ohne sauberes Patch- und Schwachstellenmanagement laufen Organisationen ständig hinterher – besonders kritisch für NIS-2-pflichtige Bereiche.

Veranstaltungen

connext VIVENDI **Kostenlose Webinarreihe in Kooperation mit Connext Vivendi**

Künstliche Intelligenz bietet der Pflege konkrete Entlastung – in Vivendi sogar schon heute. Gemeinsam mit Connext Vivendi zeigen wir, wo KI in den Vivendi-Modulen bereits sinnvoll unterstützt, welche Funktionen gerade entstehen und wie Sie rechtlich sauber sowie alltagstauglich vorgehen. Unser Anspruch: weniger Theorie, mehr Praxis – direkt im System, das Sie täglich nutzen.

14. Januar 2026
Generative KI in Vivendi verstehen: Grundlagen (LLM) & VIVA-Praxis
Was bedeutet „generative KI“ konkret und wie ist sie bereits heute in Vivendi integriert? Wir ordnen Large Language Models (LLMs) fachlich ein, erklären ihre Funktionsweise, Stärken sowie Grenzen und was für einen verantwortungsvollen Einsatz zu beachten ist.

KLICK/SCAN

27. Januar 2026
Dienstplanung mit KI: Modelle verstehen, richtig „trainieren“ & PEP Web Planungsautomatik
Ist Dienstplanung mit KI sicher? Was passiert mit den persönlichen Daten? Wie „lernt” eine KI und was bedeutet das für faire und schnelle Dienstpläne? Wir klären kompakt, wie Modelle generalisieren, warum Datenqualität wichtig ist und wie man ein Erwartungsmanagement betreibt.

KLICK/SCAN

10. Februar 2026
Spracheingabe & NLP: Konzepte verstehen, Sprachsteuerung in PD Web nutzen
Natural Language Processing (NLP) macht Spracheingaben produktiv. Doch was passiert dabei genau? Wir erläutern, wie Erkennung, Verständnis und Generierung zusammenspielen und worauf es bei Qualität und Datenschutz ankommt.

KLICK/SCAN

Weitere Themen und Termine folgen.

NIS-2 im Griff: Von Pflicht zu Struktur

NIS-2 muss kein zusätzlicher Bürokratieblock werden. Unser Whitepaper macht aus komplexen Vorgaben eine praxisnahe Roadmap – mit Prioritäten, Meilensteinen und konkreten Ansatzpunkten für Geschäftsleitung, IT und Compliance.

Von Daniel Rauhut

Die meisten Einrichtungen spüren es schon im Alltag: Die Umsetzung der NIS-2-Anforderungen rückt nicht nur näher – sie ist längst Realität im Kalender. Die Übergangsfristen laufen, die ersten Fragebögen von Aufsichtsbehörden, Wirtschaftsprüfern und Versicherern landen in den Postfächern. Und plötzlich steht da schwarz auf weiß, was vorher oft abstrakt klang: Nachweise, Strukturen, Zuständigkeiten. Nicht mehr nur „Wir kümmern uns darum", sondern „Zeigen Sie uns bitte, wie genau Sie das tun." Genau deswegen haben wir ein aktuelles Whitepaper erstelllt. Dieser Artikel gibt Ihnen einen Einblick und macht hoffentlich Lust, tiefer einzusteigen.

Vom Schlagwort zur Pflicht: Was NIS-2 konkret verändert

Mit dem NIS2UmsuCG, einem neuen BSIG und den bestehenden Vorgaben aus IT-SiG 2.0 und DSGVO verschiebt sich der Fokus in Sachen Verantwortung klar in Richtung der Geschäftsleitung und den IT- und Informationssicherheitsverantwortlichen. Gefordert sind überprüfbare Strukturen, konsistente Prozesse und nachvollziehbare Entscheidungen – nicht nur gute Vorsätze oder der Hinweis, dass „man das schon immer so gemacht hat".

Für viele Organisationen bedeutet das:
- bekannte Anforderungen gewinnen deutlich an Schärfe,
- einzelne Insellösungen reichen nicht mehr aus,
- die Dokumentation wird zum strategischen Instrument oder zum Risiko.

Wer jetzt nur reagiert, wenn neue Anforderungen „von außen" hereinkommen, arbeitet im Dauer-Feuerwehrmodus: Einzelmaßnahmen hier, zusätzlicher Bericht dort, ein weiteres Tool, eine weitere Meldung. Die Folgen sind Lücken, Doppelstrukturen – und unangenehme Nachfragen der Aufsicht.

Gleichzeitig steckt in dieser Entwicklung eine Chance: NIS-2 kann der Anlass sein, aus verstreuten Aktivitäten ein tragfähiges Governance-Modell zu formen, das nicht nur „Pflicht erfüllt", sondern die Organisation langfristig stärkt.

Ein Geflecht aus Pflichten – und ein Zielbild, das Ordnung hineinbringt

Unser Whitepaper soll genau das zeigen: Es ordnet das Geflecht aus europäischen Vorgaben, nationalen Gesetzen und bereits etablierten Standards und übersetzt es in ein handhabbares Zielbild.

Im Mittelpunkt stehen unter anderem folgende Fragen:
- **Wie fügen sich NIS-2, BSIG, IT-SiG 2.0 und DSGVO sinnvoll zusammen?**
  Viele Anforderungen überschneiden sich, etwa bei Risikobewertung, Meldewegen oder Schulungspflichten. Das Whitepaper zeigt, wo Synergien liegen und wie sich Doppelarbeit vermeiden lässt.
- **Welche Einrichtung fällt in welche Kategorie – und was folgt daraus?**
  Ob „wesentliche" oder „wichtige" Einrichtung ist kein

Detail, sondern bestimmt Umfang, Tiefe und Zeitdruck der Umsetzung. Das Whitepaper erläutert, wie sich diese Einstufung konkret auf Prozesse, Rollen und Berichtspflichten auswirkt.
- **Was muss bis wann nachweisbar sein?**
  Von der Risikoanalyse über Incident-Management und Meldeprozesse bis hin zu Schulungen, Richtlinien und Dokumentation: Sie erhalten einen strukturierten Blick darauf, was kurzfristig, mittelfristig und langfristig erforderlich ist.

Statt abstrakte Paragraphen zu wiederholen, zeichnet das Whitepaper ein Zielbild, an dem sich Geschäftsleitung, IT, Informationssicherheit, Datenschutz und Compliance gemeinsam orientieren können – ohne alles neu erfinden zu müssen.

Informationssicherheit, Datenschutz, Notfallmanagement: getrennt gedacht, verzahnt umgesetzt

Viele Organisationen haben bereits Elemente aus Informationssicherheit, Notfallmanagement, Datenschutz und Risikomanagement etabliert:
- ein ISMS auf Basis von ISO 27001 oder BSI-Grundschutz,
- ein Notfallhandbuch mit Wiederanlaufplänen,
- Datenschutzkonzepte, Verarbeitungsverzeichnisse und TOMs,
- Risikoregister aus der Unternehmenssteuerung.

Das Problem: Häufig existieren diese Bausteine nebeneinander – entstanden aus unterschiedlichen Projekten, Prüfungen oder Vorgaben. NIS-2 fordert, diese Elemente stärker zu verzahnen.

Unser Whitepaper zeigt unter anderem:
- wie bestehende Risikomanagementprozesse genutzt werden können, um NIS-2-Anforderungen aufzunehmen, statt neue Parallelstrukturen zu schaffen,
- wie Notfall- und Wiederanlaufkonzepte so angepasst werden können, dass sie sowohl Anforderungen der Informationssicherheit als auch regulatorische Meldefristen berücksichtigen,
- wie Datenschutz und Informationssicherheit gemeinsam auftreten können – etwa bei der Bewertung von Dienstleistern, bei Cloud-Strategien oder bei KI-Anwendungen.

Das Ziel ist klar: Strukturen, die prüfbar sind, ohne die Organisation mit zusätzlicher Bürokratie zu überziehen.

12–18 Monate im Blick: Prioritäten statt Aktionismus

Ein Kernstück des Whitepapers ist eine praxisorientierte Roadmap für die nächsten 12–18 Monate. Sie hilft dabei, die vielen Anforderungen zu ordnen und zu priorisieren:
- **Kurzfristige Quick-Wins:**
  Wo lassen sich mit überschaubarem Aufwand sichtbare Verbesserungen erreichen – beispielsweise durch klare Zuständigkeitsregelungen, die Aktualisierung von Meldeprozessen oder die Definition eines einheitlichen Risikomaßstabs?
- **Mittelfristige Meilensteine:**
  Welche Projekte brauchen mehr Vorlauf, etwa der systematische Aufbau oder die Aktualisierung eines ISMS, die Überarbeitung von Dienstleistermanagement und Verträgen oder die Schulung von Leitungsorganen?
- **Langfristige Maßnahmen:**
  Wo geht es um strukturelle Veränderungen, etwa um die Verankerung von Informationssicherheit in der Unternehmensstrategie, die Anpassung der IT-Architektur oder die Etablierung eines kontinuierlichen Verbesserungsprozesses?

Statt einer langen Wunschliste erhalten Sie eine Arbeitsgrundlage, die in der Praxis verwendbar ist und die sich auch gegenüber Aufsicht, Wirtschaftsprüfern oder Versicherern sehen lassen kann.

Verantwortung in der Leitung – Orientierung für IT und Fachbereiche

Ein weiterer Fokus des Whitepapers liegt auf der Frage, wer was verantwortet:
- Welche Aufgaben liegen klar bei der Geschäftsleitung – etwa die Billigung des Sicherheitsniveaus, die Bereitstellung von Ressourcen oder die Festlegung von Risikobereitschaft?
- Welche Aufgaben sind operativ in IT, Informationssicherheit, Fachbereichen und Compliance zu verankern?
- Wie lassen sich diese Rollen so beschreiben, dass sie für Prüfungen nachvollziehbar und für Mitarbeitende im Alltag verständlich sind?

Auf diese Weise gewinnen Sie Klarheit über Verantwortungsbereiche und über die Art von Nachweisen, die bei Prüfungen oder im Ernstfall erwartet werden. Das Whitepaper bietet dafür Formulierungs- und Strukturhilfen, die Sie direkt als Grundlage für interne Regelwerke nutzen können.

Vom Pflichtprogramm zum Governance-Modell mit Mehrwert

NIS-2 ist kein isoliertes „IT-Thema“. Die Anforderungen greifen tief in Aufbau- und Ablauforganisation ein, betreffen Dienstleisterauswahl, Projektsteuerung, Budgetentscheidungen und Personalplanung. Wer den Auftrag nur als minimalistische Pflichtaufgabe versteht, wird auf Dauer viel Aufwand für wenig Effekt investieren.

Unser Ansatz – und das spiegelt sich im Whitepaper wider – ist ein anderer: Regulatorische Anforderungen sollen nicht bremsen, sondern helfen, Strukturen zu schaffen, die die Organisation auch in anderen Krisen- und Veränderungssituationen stärken. Dazu gehört beispielsweise:
- Transparenz über kritische Prozesse und Abhängigkeiten,
- einheitliche Kriterien für die Bewertung von Risiken,
- klare Eskalations- und Entscheidungswege,
- eine Kommunikationslinie, die auch in Stresssituationen trägt.

So entsteht ein Governance-Modell, das nicht nur NIS-2 „abarbeitet“, sondern die Resilienz der gesamten Organisation erhöht.

Und wenn die Zeit knapp ist?

Vielleicht erkennen Sie beim Lesen: Das alles passt schlecht zu ohnehin knappen Ressourcen. Sie sollen NIS-2 umsetzen, gleichzeitig andere EU-Vorgaben im Blick behalten, operative Projekte vorantreiben und den laufenden Betrieb sicherstellen.

Genau hier kann externe Unterstützung sinnvoll sein – nicht, um Verantwortung abzugeben, sondern um Zeit zu gewinnen und typische Fehler zu vermeiden. Durch erfahrene Beratung zur NIS-2-Richtlinie, zum neuen BSIG oder zu anderen EU-Anforderungen wie der DSGVO können Sie schneller zu einem belastbaren Umsetzungsstand kommen, als wenn jede Einrichtung für sich allein startet.

Wer besonders exponiert ist und noch keine dauerhaft besetzte Rolle für Informationssicherheit aufgebaut hat, kann zudem über eine Auslagerung nachdenken: Ein externer Informationssicherheitsbeauftragter bringt Erfahrung aus verschiedenen Projekten mit, kennt typische Prüfungsfragen und hilft dabei, Konformität mit Augenmaß umzusetzen, ohne die Organisation zu überfordern.

Ihr nächster Schritt: Vom Überblick zur eigenen Agenda

Dieser Artikel kann nur Schlaglichter setzen. Wenn Sie:
- ein klares Bild davon gewinnen möchten, wo Ihre Einrichtung heute steht,
- wissen wollen, welche Kategorie Sie trifft und welche Konsequenzen das hat,
- eine konkrete Agenda für die nächsten 12–18 Monate brauchen,
- und sich auf kommende Prüfungen und Nachfragen strukturiert vorbereiten möchten,

dann lohnt sich ein Blick in unser Whitepaper. Es liefert Ihnen keine abstrakte Gesetzeskommentierung, sondern eine praktische Arbeitsgrundlage – mit Zielbild, Prioritäten und Beispielen, wie Informationssicherheit, Notfallmanagement, Datenschutz und Risikomanagement so zusammenspielen, dass NIS-2 nicht zur Dauerbaustelle wird, sondern zu einem beherrschbaren Teil Ihrer täglichen Steuerung.

Nutzen Sie das Whitepaper als Ausgangspunkt für Ihre interne Diskussion – in der Geschäftsleitung, mit IT und Informationssicherheit, mit Datenschutz und Compliance. Und wenn Sie den Weg nicht allein gehen möchten, begleiten wir Sie gern: mit Erfahrung aus Projekten an der Schnittstelle von Technik und Recht – und mit dem Blick darauf, dass Konformität nicht automatisch Kostenexplosion bedeuten muss. &

Jetzt das aktuelle Whitepaper herunterladen

KLICK/SCAN

Das Whitepaper „NIS-2 Handlungsbedarf für Unternehmen und Organisationen“ ist ab sofort auf unserer Homepage zum kostenlosen Download abrufbar.

An der Schnittstelle von Recht und Technik

Joerg Heidrich im Porträt

Von Fabian Eggers

Wer Joerg Heidrich begegnet, trifft auf jemanden, der die digitale Transformation nicht nur rechtlich begleitet, sondern aktiv einordnet – seit über zwei Jahrzehnten. Der Fachanwalt für IT-Recht ist Kanzleiinhaber (Heidrich Rechtsanwälte), Justiziar und Datenschutzbeauftragter bei heise Medien und zusätzlich zertifizierter KI-Manager (IHK). Kurz: eine Stimme, die Technik, Recht und gelebte Praxis zusammenbringt.

Was ihn antreibt, fasst Heidrich selbst mit einem Augenzwinkern zusammen: „Speerspitzen-Jura" – die Freude daran, neue Entwicklungen früh zu verstehen und juristisch belastbar zu machen. So nüchtern dieser Anspruch klingt, so anspruchsvoll ist er im Alltag: Nicht selten erfordern digitale Innovationen ein rechtliches „Erstmapping", bevor Organisationen sichere Entscheidungen treffen können. Gerade bei Künstlicher Intelligenz zeigt sich das: Chancen und Risiken liegen nah beieinander, Marktdynamik und Regulierungsdichte wachsen parallel. Heidrich begrüßt Orientierung – warnt aber vor Übersteuerung. Beim AI Act sieht er Passagen, die Innovation eher bremsen könnten, als dass sie verlässlich leiten. Die Aufgabe der kommenden Monate bleibe deshalb, eine tragfähige Balance zu finden.

„Die Aufgabe der kommenden Monate bleibt, eine tragfähige Balance zu finden."

Seine Verbindung zu Althammer & Kill reicht in gemeinsame Konferenzen und Projekte zurück – aus fachlicher Nähe wurde Vertrauen. In unterschiedlichsten Vorhaben, von Datenschutzfolgenabschätzungen bis hin zu Kooperationen mit heise, schätzt Heidrich die Kombination aus technischer Expertise und juristischer Sorgfalt. Ein Beispiel dafür war das erste „Norddeutsche KI-Forum" Anfang 2025: ein Format, das zeigt, wie praxisnah sich Governance, Compliance und Produktentwicklung verzahnen lassen, wenn Teams mit einer Sprache sprechen.

Dass Digitalisierung zur strategischen Chefsache geworden ist, erlebt Heidrich täglich. In Medienhäusern, Behörden und Unternehmen steigen die Anforderungen zugleich in drei Dimensionen: IT-Sicherheit, Compliance und KI-Einführung. Wer das ernst nimmt, denkt nicht nur in Projekten, sondern in Programmen – mit klaren Verantwortlichkeiten, lernenden Prozessen und gelebter Transparenz. Für Heidrich beginnt erfolgreiche Umsetzung bei den Menschen: Schulungen sind wichtig, reichen allein aber nicht. Es braucht Dialogformate, die Skepsis adressieren, Kompetenz aufbauen und den Fortschritt sichtbar machen. Kurz: einen dauerhaften Rahmen, der digitale Veränderungen erklärt und begleitet.

Sein rheinisches Grundvertrauen („Et kütt wie et kütt") ist dabei kein Plädoyer fürs Abwarten, sondern für Gelassenheit mit System: Risiken benennen, Maßnahmen priorisieren, Verantwortungen klären und dann konsequent umsetzen. Diese Haltung passt zu Organisationen, die in hoch regulierten Umfeldern arbeiten: lieber Prüf- und Nachweisfähigkeit herstellen, als auf den „perfekten" Moment zu warten.

Gerade im Zusammenspiel von KI, Datenschutz und Informationssicherheit empfiehlt sich ein pragmatischer Dreiklang:

1. Den Einsatz von KI transparent dokumentieren.
2. Risiken entlang der Wertschöpfung steuern (vom Training über Zulieferungen bis zum Betrieb).
3. Die Belegschaft befähigen, damit Governance nicht als Hürde, sondern als Möglichmacher erlebt wird.

„Es braucht Dialogformate, die Skepsis adressieren, Kompetenz aufbauen und den Fortschritt sichtbar machen"

Wie sieht das im Alltag aus? Heidrich rät, KI-Vorhaben mit einem strukturierten Start zu versehen: ein klarer Anwendungsfall, ein schlanker rechtlicher Rahmen (Zweck, Rechtsgrundlage, Betroffenenrechte), technische Schutzmaßnahmen nach Stand der Technik – und ein Blick auf die Lieferkette, inklusive Hosting, Modelle und Integrationen. Wer diese Basiselemente sauber setzt, reduziert Reibung im laufenden Betrieb und gewinnt Zeit für das Wesentliche: den Mehrwert im Kerngeschäft.

Für die Zukunft wünscht er sich eine Debatte, die weniger in Extremen denkt und mehr in Lösungen: Technologieoffenheit dort, wo Innovation hilft; präzise Regeln dort, wo Schutz nötig ist. Und vor allem: Austausch auf Augenhöhe zwischen Technik, Recht und Management. Denn nur wenn alle drei Perspektiven zusammenkommen, entsteht die Handlungsfähigkeit, die moderne Organisationen brauchen.

Vielleicht ist es genau diese Mischung aus Zuversicht und Präzision, die Heidrich auszeichnet. Man könnte sagen: Er bringt Ordnung in das Tempo der Digitalisierung – ohne es zu drosseln. Ein gutes Vorbild für alle, die Verantwortung für KI-Einsatz, Datenschutz, Informationssicherheit und Compliance tragen und die Digitalisierung als das verstehen, was sie sein sollte: ein Möglichmacher. &

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

KI-Starterpakete: klar starten, sauber steuern

Von der Idee zum geordneten Einsatz: Unsere KI-Starterpakete bündeln die notwendigen rechtlichen, organisatorischen und technischen Schritte, damit Anwendungen wie Spracherkennung oder Assistenzsysteme im Alltag funktionieren, ohne Rechts- oder Sicherheitslücken zu hinterlassen.

Von Jessica Henning

Viele Organisationen stehen heute an einem ähnlichen Punkt: KI ist bereits da – mal sichtbar, mal leise im Hintergrund. In der Bürokommunikation sind ChatGPT und Microsoft Copilot präsent, in der Sozialwirtschaft unterstützen Lösungen wie „voize" die Pflege-Dokumentation oder es werden KI-gestützte Funktionen in Systemen aus dem Vivendi-Umfeld genutzt.

Die Frage ist selten, ob KI eingesetzt wird. Entscheidend ist: Welche Funktionen sind vorgesehen? Welche Daten fließen wohin? Und wie lässt sich das Ganze nachvollziehbar, regelkonform und tragfähig gestalten?

Aus Gesprächen mit IT, Datenschutz, Informationssicherheit und Fachbereichen kennen wir die wiederkehrenden

Hürden: unklare Zuständigkeiten, uneinheitliche oder unvollständige Vertragslagen, spärliche Dokumentation, Unsicherheit bei Rechtsgrundlagen und eine allgemeine Skepsis, ob man „schon genug" abgesichert ist. Hinzu kommen steigende Anforderungen – von DSGVO, DSG-EKD oder KDG bis zur EU-KI-Verordnung.

Es braucht also kein weiteres Grundsatzpapier, sondern eine strukturierte Vorgehensweise, die die vorhandenen Systeme und Routinen aufgreift und in geordnete Bahnen lenkt.

Warum ein Starterpaket?

Der Begriff „Starterpaket" meint kein Produkt „von der Stange". Gemeint ist ein schlanker, klar umrissener Rahmen, der wiederkehrende Prüfschritte bündelt und dadurch Aufwand reduziert. Der Ansatz ist besonders sinnvoll, wenn Systeme und Funktionsumfänge bekannt sind: etwa Spracherkennung im Pflegealltag oder definierte KI-Module in Fachanwendungen.

Solche spezialisierten Lösungen lassen sich konsistenter bewerten als große, offene Modelle. Das verringert Reibung im Projekt, beschleunigt Entscheidungen und sorgt dafür, dass Ergebnisse prüffähig dokumentiert vorliegen.

Ausgangslage und Zielbild

Sie haben sich ein spannendes KI-Tool eingekauft und stehen nun vor der Herausforderung, die datenschutzrechtlichen und regulatorischen Anforderungen (DSGVO, DSG-EKD, KDG, KI-VO) vollständig umzusetzen?

Durch unsere umfassende Erfahrung können wir Ihnen helfen, mit gezielten Fragen genaustens aufzunehmen, welche Funktionen produktiv genutzt werden könnten, welche Dienstleister involviert sind und welche Schnittstellen zu betrachten sind. Daraus ergibt sich, welche Features in Ihrer Organisation genutzt werden sollen und welche Funktionen deaktiviert werden müssten. Diese Einordnung ist entscheidend – sie sorgt dafür, dass Technik und Governance Schritt halten und Ihr Unternehmen jederzeit compliant bleibt.

Was im Leistungsumfang steckt:

- Vertrags- und Informationslage ordnen. Auftragsverarbeitungsverträge werden angepasst, Informationspflichten (z. B. Datenschutzhinweise) überprüft und vereinheitlicht.
- Datenverarbeitungen nachvollziehbar machen. Verarbeitungstätigkeiten werden konkret beschrieben: Zweck, Datenarten, Empfänger, Aufbewahrung, Löschung. Subunternehmer und Übermittlungen in Drittländer werden transparent erfasst.
- Rechtsgrundlagen festlegen. Für die jeweiligen Funktionen werden tragfähige Rechtsgrundlagen bestimmt und dokumentiert, warum diese passen.
- Training durch Anbieter prüfen. Ist anbieterseitiges KI-Training auf Produktivdaten vorgesehen, wird die Deaktivierung bewertet und, wo möglich und sinnvoll, vorgenommen.
- Nutzungshinweise werden erstellt, die regeln, welche Maßnahmen von den Mitarbeitenden beachtet werden müssen.
- Risiken einschätzen und klassifizieren. Sowohl eine Schwellwertanalyse nach den geltenden Datenschutzgesetzen wird durchgeführt als auch eine Risikoklassifizierung nach KI-VO.
- Sie erhalten eine Mustervorlage zur Erstellung einer Datenschutz-Folgenabschätzung mit Produktspezifischen Informationen und einem Risikoschema als Ausfüllhilfe.
- Ergebnisse bündeln. Alles mündet in einen kompakten Bericht: Nachvollziehbare Entscheidungen, klare Freigaben und noch offene Punkte.

So läuft es ab

1. **Orientierung:** In einem Kick-off werden Ziele, Use Cases und Rahmenbedingungen sortiert. Der Fokus liegt auf konkreten Anwendungen, nicht auf hypothetischen Möglichkeiten.
2. **Absicherung:** Verträge, Prozesse und Systeme werden entlang der oben genannten Prüfpunkte bewertet. Wo Lücken sichtbar werden, werden sie dokumentiert und mit pragmatischen Maßnahmen hinterlegt – von Konfigurationseinstellungen über Prozessschritte bis zu kurzen Textbausteinen für Informationspflichten.
3. **Betrieb und Regeln:** Eine schlanke Nutzungsrichtlinie fasst klare Spielregeln zusammen. Sie ist bewusst knapp gehalten, damit sie im Alltag genutzt wird. Damit soll vor allem organisatorischen Risiken vorgebeugt werden.

Ein Beispiel aus der Praxis

Eine Einrichtung plant, Sprachaufzeichnungen zur Pflegedokumentation produktiv zu nutzen. Im Starterpaket werden Aufnahme- und Übertragungsstrecken beschrieben, inklusive Zwischenspeicher und Löschfristen. Rollen werden geschärft: Wer darf Audio anlegen, wer transkribieren, wer freigeben? Es wird geprüft, ob Audio-Daten für Trainingszwecke beim Anbieter verbleiben und welche Opt-out-Möglichkeiten bestehen.

Die Informationspflichten werden um einen klaren Abschnitt ergänzt („Einsatz von Sprachverarbeitung"). Ergebnis: Die Funktion wird freigegeben – mit definierten Grenzen (z. B. keine Erfassung besonders sensibler Inhalte per Sprache in bestimmten Situationen) und einer kurzen Einweisung für die Teams. Der Mehrwert ist spürbar, die Regeln sind klar, die Dokumentation vollständig.

Besonderheiten in der Sozialwirtschaft

Hier treffen hohe Schutzbedarfe auf komplexe Trägerstrukturen und knappe Ressourcen. KI kann den Alltag spürbar entlasten – zugleich verlangt sie eine besonders sorgfältige Ausgestaltung.

Die Starterpakete adressieren typische Fragen: Ist der Auftragsverarbeitungsvertrag ausreichend? Sind alle Informationspflichten erfüllt? Wie ist die Risikoklassifizierung? Sind alle spezifischen technischen und organisatorischen Maßnahmen bedacht worden? Wie werden externe Leistungen (z. B. Transkriptionsdienste) eingebunden, ohne die Kontrolle über Daten zu verlieren? Der Ansatz ist nicht „branchenspezifisch eng", aber sensibel für diese Rahmenbedingungen.

Was am Ende zählt

Ziel ist nicht ein weiterer Ordner im Regal, sondern eine freigegebene, nutzbare und nachvollziehbar dokumentierte KI-Anwendung. Die Teams wissen, was erlaubt ist und was nicht. Leitung und Aufsicht erhalten belastbare Nachweise. IT und Informationssicherheit haben eine Grundlage, auf der sie technisch weiterarbeiten können. Und wenn sich Rahmenbedingungen ändern – neue Funktionen, geänderte Anbieterbedingungen oder neue rechtliche Vorgaben – lässt sich die Entscheidung mit denselben Schritten aktualisieren.

Ziel ist nicht ein weiterer Ordner im Regal, sondern eine freigegebene, nutzbare und nachvollziehbar dokumentierte KI-Anwendung.

Blick nach vorn

Die Starterpakete setzen bewusst bei spezialisierten Anwendungen an, weil dort schnelle, eindeutige Ergebnisse möglich sind. Auf dieser Basis lassen sich später auch breit einsetzbare Sprachmodelle wie ChatGPT oder Copilot strukturierter einführen. Der Weg bleibt derselbe: klare Ziele, transparente Datenflüsse, begründete Rechtsgrundlagen, dokumentierte Entscheidungen.

Fazit

KI entfaltet ihren Nutzen, wenn Technik und Ordnung zusammenpassen. Ein geordnetes Vorgehen nimmt Unsicherheit aus dem Alltag, macht Entscheidungen schneller und hält die Nachvollziehbarkeit hoch – ohne den praktischen Einsatz auszubremsen. Das KI-Starterpaket ist dafür ein robuster Rahmen: nicht spektakulär, aber wirksam. &

Sie möchten mehr über unsere KI-Starterpakete erfahren?

Kontaktieren Sie uns, wir unterstützen Sie gern!

Ihr Vertriebsteam
vertrieb@althammer-kill.de
Tel. +49 511 330603-0

Althammer & Kill Akademie

KLICK/SCAN

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

17. Dezember 2025 // 15. April 2026 – kostenloses Webinar

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

Tauchen Sie ein in die Welt der kommenden 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.

25. Februar 2026 –kostenloses Webinar

Ihre Roadmap zur erfolgreichen KI-Richtlinie

Künstliche Intelligenz bietet enormes Potenzial für Effizienz, Innovation und neue Geschäftsmodelle. Gleichzeitig bringt sie aber auch rechtliche, ethische und organisatorische Herausforderungen mit sich. Wer KI erfolgreich einsetzen will, braucht deshalb klare Leitplanken: eine verständliche und praxisnahe Richtlinie, die Chancen nutzt und Risiken beherrschbar macht.

18. März 2026 – 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?

22.–24. Februar 2026 – Online-Seminar

Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Mit dem esseziellen Grundlagenwissen zur kompetenten Ansprechperson in Datenschutzfragen. Mit Zertifikat, welches Ihre Datenschutzkompetenz dokumentiert und gegenüber der Aufsichtsbehörde, Vorgesetzten, Geschäftspartnern und Mitarbeitenden ausweist.

4. Februar 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. Mit Abschluss dieser Schulung leisten Sie zugleich einen wichtigen Beitrag zur Erfüllung Ihrer Pflichten gemäß des im NIS-2-Umsetzungsgesetz geänderten § 38 BSIG – insbesondere im Hinblick auf die Qualifizierung der Geschäftsleitung in Fragen der Cybersicherheit.

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

Datenschutz-Audits bei Dienstleistern im Sozialbereich

Soziale Einrichtungen verarbeiten besonders schutzwürdige Daten. Risikobasierte Audits von Auftragsverarbeitern sind Pflicht und Chance zugleich: Sie erhöhen Sicherheit, Transparenz und Verlässlichkeit in der Zusammenarbeit. Dieser Beitrag zeigt, welche rechtlichen Maßstäbe gelten und wie Sie Audits pragmatisch planen und umsetzen.

Von Sören Hartmann und Winona Wenning

Im Alltag läuft vieles reibungslos: Software liefert Daten, der Dienstleister hostet stabil, Verträge sind unterschrieben. Genau deshalb rutschen Prüfungen leicht nach hinten. Bis eine Nachfrage der Aufsicht, ein Systemwechsel oder ein Vorfall zeigt, wie wichtig ein nüchterner Blick von außen ist. Ein Audit holt die Zusammenarbeit aus dem Bauchgefühl in die Nachvollziehbarkeit: Was ist vereinbart, was wird tatsächlich getan, wo gibt es Lücken und welche Punkte verdienen Priorität? Es geht nicht um Misstrauen, sondern um Verlässlichkeit im Betrieb. Je klarer die Fakten, desto leichter lassen sich Entscheidungen treffen, Budgets begründen und Maßnahmen wirksam nachverfolgen.

Soziale Einrichtungen wie Wohlfahrtsverbände, Pflegeeinrichtungen oder Träger der Kinder- und Jugendhilfe stehen dabei vor besonderen Herausforderungen, wenn es um den Schutz personenbezogener Daten Ihrer Klienten geht.

Neben der Datenschutz-Grundverordnung (DSGVO) normieren die Sozialgesetzbücher (SGB) zusätzliche Pflichten zumindest für Leistungsträger. Insbesondere betrifft dies die regelmäßige Kontrolle von Dienstleistern, die im Auftrag der Einrichtungen personenbezogene Daten verarbeiten (Art. 28 DSGVO).

Recht	Risiko	Vertrauen
Pflicht nach DSGVO Art. 28: Auftragsverarbeiter regelmäßig prüfen.	**Datenpannen vermeiden:** Schwachstellen früh erkennen und schließen.	**Verlässliche Partnerinnen und Partner?** Qualität und Reifegrad objektiv belegen.
Nachweisbarkeit: Dokumentierte Audits als Beleg für Compliance.	**Lieferketten-Transparenz:** Kritische Abhängigkeiten sichtbar machen.	**Transparente Zusammenarbeit:** Klare Maßnahmen und Fristen vereinbaren.
Technisch und organisatorisch: Wirksamkeit der TOMs belegen.	**Kontinuität sichern:** Ausfall- und Wiederanlauffähigkeit prüfen.	**Reputationsschutz:** Professioneller Umgang stärkt Außenwirkung.
Spezialvorgaben Sozialdaten: Strengere Maßstäbe bei besonders schützenswerten Daten.	**Aktuelle Bedrohungen:** Patch-, Zugriffs- und Backup-Management bewerten.	**Gemeinsamer Standard:** Erwartungen und KPIs verbindlich machen.
Verträge leben: AVV-Anforderungen in der Praxis verifizieren.	**Priorisieren statt Gießkanne:** Fokus auf Prozesse mit hoher Kritikalität.	**Langfristige Stabilität:** Weniger Überraschungen, mehr Planbarkeit.

Warum Audits bei Dienstleistern?

Audits machen Pflichten sichtbar, senken Risiken und stärken die Zusammenarbeit. Im Folgenden zeigen wir auf, welche rechtlichen Grundlagen diese erweiterten Pflichten begründen, warum Dienstleister ggf. auch für Leistungserbringer umfassender zu prüfen sind, in welchem Turnus Audits stattfinden sollten und worauf es in der Praxis ankommt.

Rechtliche Grundlagen

Die DSGVO verpflichtet Verantwortliche (also auch soziale Einrichtungen) dazu, nur mit Auftragsverarbeitern zusammenzuarbeiten, die hinreichende Garantien für die Einhaltung des Datenschutzes bieten (Art. 28 Abs. 1 DSGVO). Diese Pflicht ist nicht mit der Unterzeichnung eines Auftragsverarbeitungsvertrages erledigt – der Verantwortliche muss sich auch aktiv davon überzeugen, dass die Vorgaben eingehalten werden.

Darüber hinaus enthalten die Sozialgesetzbücher (insbesondere § 80 SGB X sowie § 35 SGB I) erhöhte Anforderungen. Sie verpflichten zunächst Leistungsträger, die Einhaltung datenschutzrechtlicher Vorgaben bei ihren Auftragsverarbeitern regelmäßig zu kontrollieren und zu dokumentieren. § 80 Abs. 1 Nr. 1 SGB X sieht ausdrücklich vor, dass sich Sozialleistungsträger bei der Auftragsverarbeitung von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen müssen. Auch im SGB V, SGB VIII und SGB XI finden sich ergänzende Verweise auf den Schutz von Sozialdaten, die über die allgemeinen DSGVO-Anforderungen hinausgehen.

Zwar finden sich dort keine expliziten Regeln für Leistungserbringer, jedoch macht der deutsche Gesetzgeber an dieser Stelle klar: Die Verarbeitung von personenbezogenen Daten im Sinne von Sozialdaten birgt ein erhöhtes Risiko, dem mit erhöhten Sicherheitsmaßnahmen begegnet werden muss. Damit gilt: Für soziale Einrichtungen sind Audits bei Dienstleistern keine Kür, sondern ggf. notwendige Maßnahme.

Welche Dienstleister sind zu auditieren?

Grundsätzlich sieht der Art. 28 DSGVO bereits vor, dass Auftragsverarbeitungen nur durch Dienstleister erbracht werden,

Stichwort
Art. 28 DSGVO Auftragsverarbeiter

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

welche hinreichende Garantien bieten, dass die Verarbeitung im Rahmen des geltenden Datenschutzrechts erfolgt, die Rechte der Betroffenen geschützt werden und ausreichende technische und organisatorische Maßnahmen implementiert wurden.

Außerdem sieht Abs. 3 lit. h vor, dass der zugrundeliegende Auftragsverarbeitungsvertrag neben der Nachweispflicht des Auftragsverarbeiters auch eine explizite Kontrollmöglichkeit durch „Überprüfungen – einschließlich Inspektionen -, die vom Verantwortlichen oder anderen von diesem beauftragten Prüfer durchgeführt werden“ vor. Kurzgesagt: Jeder Auftragsverarbeitungsvertrag muss dem Verantwortlichen das Recht für Audits, auch vor Ort, zusichern.

Erstaudit	Vor Beginn der Zusammenarbeit oder unmittelbar danach.
Regelmäßige Folgeaudits	Alle 1–3 Jahre, abhängig von der Sensibilität der Daten und dem Risiko der Verarbeitung. Außerdem können zusätzliche, weniger aufwendige Kontrollpunkte zwischen zwei Audits den Turnus erhöhen.
Anlassbezogene Audits	Wenn es Hinweise auf Datenschutzverstöße gibt oder wenn sich die Verarbeitung wesentlich ändert (z. B. neue IT-Systeme, Cloud-Umzüge).

Gemeinhin wird die sog. Auftragskontrolle als Teil der technischen und organisatorischen Maßnahmen verortet. Art. 32 Abs. 1 i.V.m. lit. d DSGVO umfasst auch die Überprüfung und Bewertung der Angemessenheit der Maßnahmen des Auftragsverarbeiters, welche der Verantwortliche letztlich mitverantwortet. Häufig wird hierbei eine Prüfung durch Fragebögen oder Checklisten, welche der Dienstleister beantworten soll, genutzt, wenn denn nicht sowieso gänzlich darauf verzichtet wird.

Als Maßnahme zur Wahrung der Sicherheit der Verarbeitung ist die Dienstleisterprüfung hinsichtlich ihrer Umsetzung im Einzelfall genauso zu bewerten, wie jede andere Maßnahme: Umfang und Form einer Sicherheitsmaßnahme bestimmt sich unter anderem an der Wahrscheinlichkeit und Schwere des Risikos für Betroffene, sowie dem für die jeweilige Verarbeitung personenbezogener Daten notwendigen Schutzniveau (vgl. Art. 32 Abs. 1 S. 1, Abs. 2 DSGVO).

Daraus folgt: Wer für unkritische Auftragsverarbeitungen seine Kontrolltätigkeit auf bloße Selbstprüfungen beschränkt, wird womöglich zu dem Ergebnis kommen, dass für die Verarbeitung von Sozialdaten durch Dienstleister ein höherer Prüfungsumfang notwendig wird. Denkbar für ein selbstdurchgeführtes oder extern beauftragtes Audit sind typischerweise

- generelle IT-Dienstleister (Hosting, Software, Cloud-Services)
- oder spezifische Fachanbieter
- Aktenvernichtungsunternehmen
- externe Callcenter oder Abrechnungsstellen

Wichtig: Auch kleine, scheinbar „unbedeutende" Auftragsverarbeiter können unter diese Pflicht fallen, sobald sie Zugriff auf entsprechende personenbezogene Daten – insbesondere Sozialdaten – haben.

In welchem Abstand müssen Audits erfolgen?

Das Gesetz nennt keinen festen Turnus. Aus der Praxis und den Anforderungen der Aufsichtsbehörden haben sich jedoch die nebenstehenden Maßstäbe etabliert.

Soziale Einrichtungen sollten daher ein Auditkonzept entwickeln, das die Häufigkeit risikobasiert festlegt und dokumentiert.

Besondere Anforderungen im Sozialrecht im Vergleich zur DSGVO

Während die DSGVO eher allgemein von „hinreichenden Garantien" spricht, sind die Sozialgesetzbücher strenger:

- Sozialdaten gelten als besonders schutzwürdig (vgl. § 35 SGB I). Schon kleinste Verstöße können erhebliche Konsequenzen haben.
- Die Pflicht zur Kontrolle ist aktiv und regelmäßig – ein bloßer Verweis auf Zertifikate oder Selbstauskünfte reicht in der Regel nicht aus.
- Dokumentationspflichten sind besonders betont: Einrichtungen müssen nicht nur prüfen, sondern ihre Kontrollen auch nachvollziehbar festhalten.

Daraus folgt: Diese Pflicht adressiert soziale Einrichtungen nicht direkt, jedoch sollte die Einschätzung des deutschen Gesetzgebers bei der Risikobewertung im Rahmen ihrer Tätigkeit einfließen. Einrichtungen müssen bei der Auswahl und Kontrolle ihrer Dienstleister deutlich sorgfältiger vorgehen, als es in anderen Branchen üblich ist.

Praktische Umsetzung

Ein Datenschutz-Audit umfasst typischerweise:

1. Prüfung der Verträge (AV-Verträge nach Art. 28 DSGVO und ergänzende Vereinbarungen).
2. Bewertung der technischen und organisatorischen Maßnahmen (z. B. Zugriffskontrollen, Verschlüsselung, Backup-Konzepte, Prozessuales Vorgehen).
3. Interviews, Begehung und Nachweise: Gespräche mit Verantwortlichen, Einsicht in Zertifikate, Prüfberichte oder interne Richtlinien zur Prüfung der Umsetzung.
4. Dokumentation und Bericht: Ergebnisdarstellung mit Empfehlungen und ggfs. Maßnahmenplan.

Pflicht und Nutzen – in allen Branchen

Die regelmäßige Überprüfung von Auftragsverarbeitern ist keine Spezialität des Sozialbereichs, sondern eine Vorgabe der DSGVO, die jede Organisation betrifft, sobald Dienstleister personenbezogene Daten verarbeiten.

Sinn und Zweck sind überall gleich: Transparenz über Schutzmaßnahmen schaffen, Verantwortlichkeiten in der Lieferkette klären und die eigene Nachweisfähigkeit gegenüber Aufsichtsbehörden und interner Revision stärken. Richtig angelegt, ist ein Audit keine Momentaufnahme, sondern Teil eines kontinuierlichen Verbesserungsprozesses – mit klaren Prioritäten entlang von Risiko und Kritikalität.

Praktisch wird es besonders dort wichtig, wo sensible Daten im Spiel sind (z. B. im Gesundheits- oder Finanzwesen), wenn es um Beschäftigtendaten geht, wenn Dienstleisterketten komplex werden und/oder internationale Datenflüsse hinzukommen.

Auch Systemwechsel, Sicherheitsvorfälle oder neue regulatorische Anforderungen sind gute Anlässe, genauer hinzusehen. Ob intern durchgeführt oder mit externem Blick: Entscheidend ist, dass Audits pragmatisch, nachvollziehbar dokumentiert und wirksam nachverfolgt werden. So entsteht Schritt für Schritt mehr Sicherheit – ohne den Betrieb auszubremsen.

Fazit

Datenschutz-Audits sind für soziale Einrichtungen möglicherweise gesetzlich verpflichtend – zwar nicht direkt nach den Sozialgesetzbüchern, aber vielleicht auf Grund des risikobasierten Ansatzes der DSGVO.

Wer diese Pflicht vernachlässigt, riskiert nicht nur Bußgelder, sondern auch das Vertrauen von Klientinnen und Klienten. &

Jetzt durchstarten im Datenschutz!

HsH Akademie

In einer Zeit rasanter Digitalisierung werden Datenschutzexperten dringender denn je gebraucht – als interne/r Datenschutzbeauftragte/r, Consultant oder selbstständig im Datenschutzumfeld. Genau hierfür bietet die HsH-Akademie in Kooperation mit heise academy und Althammer & Kill die Weiterbildung „Datenschutzmanagement – Theorie, Praxis und Karriere im Datenschutz" an.

Was Sie erwartet

- Rechtliche Grundlagen inkl. DSGVO, besonderer Kategorien personenbezogener Daten und internationale Aspekte – vermittelt von Experten von Althammer & Kill und der Hochschule Hannover.
- Technischer und organisatorischer Datenschutz: Verschlüsselung, Cloud-Betrieb, Awareness, Risikomanagement.
- Change Management: Wandelprozesse gestalten, Widerstände managen, agile Projektmethoden.
- Praxistransfer: Datenschutz-Folgenabschätzung, Verarbeitungsverzeichnisse, Datenpannen-Prozesse, KI-Bezug.
- Abschluss: Hochschulzertifikat und optional IHK-Zertifikat, 6 ECTS.

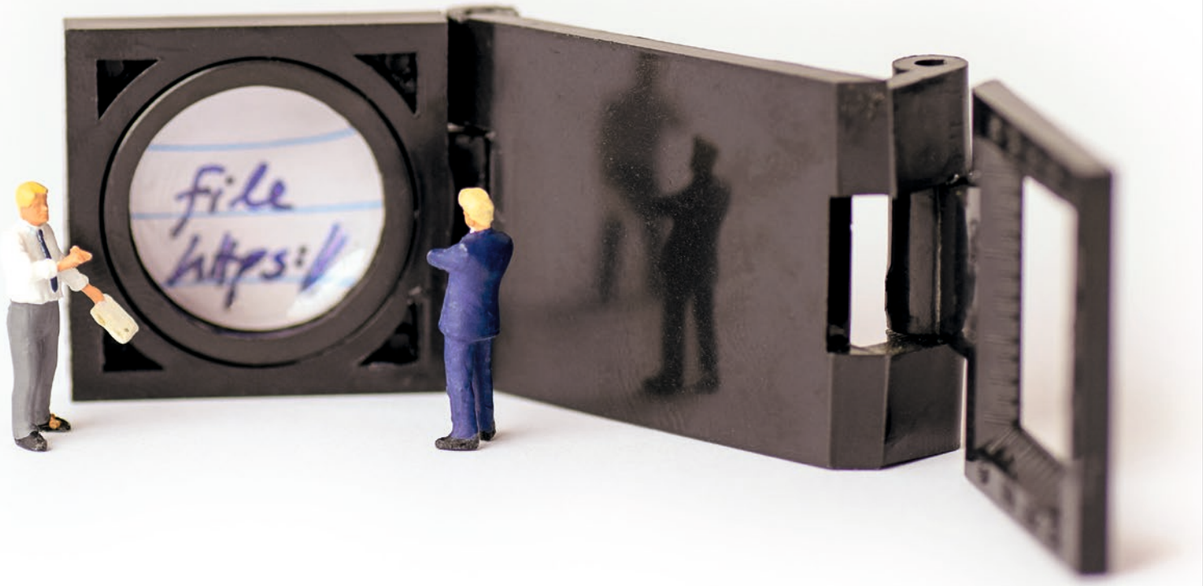
Für wen ist das genau? Für Fach- und Führungskräfte, die sich im Datenschutz qualifizieren wollen – als Datenschutzbeauftragte/r, Consultant oder selbstständig Beratende/r.

Warum teilnehmen? Sie erwerben fundiertes Datenschutzwissen – rechtlich, technisch und organisatorisch – und lernen von führenden Expertinnen und Experten aus der Praxis. Damit sind Sie bestens positioniert, um in einer Schlüsselrolle mitzugestalten und echte Wirkung zu erzielen.

Kursdauer: 4 Monate (Beginn 26.02.2026)
Kombination aus Präsenz- und Onlinephasen
Frühbucher-Rabatt bis 15.12.2025 möglich.

KLICK/SCAN

Mehr Infos & Anmeldung:
https://www.hs-hannover.de/hsh-akademie/weiterbildungen-a-z/datenschutzmanagement



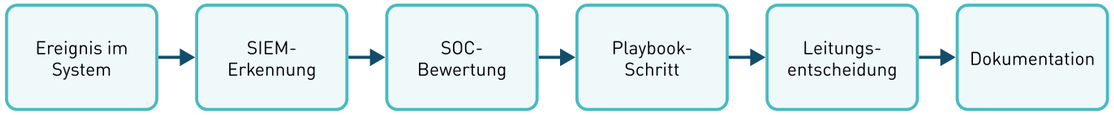
NIS-2 in der Praxis: Wie eine Fachklinik prüffähig wurde

So wurde eine Fachklinik prüffähig und resilient. Althammer & Kill und die Blueteam GmbH schaffen ein gemeinsames Lagebild und eine verlässliche Arbeitsweise.

Von Wulf Bolte und Sarah Friedrich

Ein angekündigtes Audit bringt Bewegung in bewährte Abläufe. Eine Fachklinik mit rund 180 Betten entschied sich in dieser Situation für einen nüchternen, alltagstauglichen Weg: zuerst Sichtbarkeit schaffen, dann Zuständigkeiten klären und parallel die Nachweise aufbauen, die im Ernstfall Bestand haben.

Blueteam übernahm die operative Beobachtung und Bewertung im Security Operations Center. Althammer & Kill verankerte die Ergebnisse in Governance, Verantwortung und prüffähiger Dokumentation. Die juristischen Hintergründe zu NIS-2, dem NIS2UmsuCG sowie dem neuen BSIG werden in einem separaten Beitrag dieses



Der Projektablauf in der Übersicht

Magazins erläutert. Hier möchten wir die Umsetzung in der Praxis aufzeigen.

Einleitung

Sie kennen diese Ausgangslage wahrscheinlich aus eigener Erfahrung. Der Betrieb läuft, Systeme sind historisch gewachsen, Fachbereiche arbeiten mit unterschiedlichen Anwendungen, die IT hält die Infrastruktur in Gang. Was fehlt, ist ein durchgängiges Lagebild, das von der Serverebene bis in die Leitungsebene reicht. Als in der Fachklinik die Prüfankündigung eintraf, stand zunächst die Frage im Raum, ob ein Haus dieser Größe wirklich betroffen sei. Die ersten Gespräche und eine kurze Bestandsaufnahme nahmen diese Unsicherheit heraus und brachten etwas Wichtigeres zutage. Ohne zentrale Sicht auf Ereignisse, ohne klare Meldewege und ohne belastbare Dokumentation bleibt Sicherheit eine Annahme. Genau an diesem Punkt setzt die Zusammenarbeit zwischen Blueteam und Althammer & Kill an. Es geht nicht um den großen Wurf auf einen Schlag. Es geht um einen verlässlichen Arbeitsrhythmus, in dem Erkennen, Entscheiden und Nachweisen gut ineinandergreifen.

„Viele Häuser unterschätzen, wie schnell sich Angriffe in ihrer Infrastruktur bewegen. Mit unseren SOC-Analysen konnten wir zeigen, dass Sichtbarkeit der erste Schritt zur Sicherheit ist.“

Matthäus Kozlowski, Geschäftsführer Blueteam

Ausgangslage in der Fachklinik

Die Diagnose zu Beginn war ehrlich und frei von Dramatisierung. Protokolle wurden an mehreren Stellen aufgezeichnet, aber nicht durchgängig korreliert. Einzelne Anwendungen lösten Alarme aus, doch die Wege von der Meldung zur Entscheidung waren je nach System unterschiedlich. Aufgaben waren beschrieben, allerdings nicht einheitlich geübt. Die Dokumente lagen vor, allerdings in einer Form, die für den Alltag brauchbar war, jedoch nicht darauf ausgelegt, einer Prüfung standzuhalten. Backups existierten, aber die Frage, wie lange ein Wiederanlauf dauert und an welcher Stelle Engpässe entstehen, war nicht regelmäßig getestet worden. Der wichtigste Befund lautete daher schlicht: Es fehlte ein gemeinsames Lagebild, das sowohl die IT als auch die Leitung in gleicher Weise verstanden und nutzen konnten. Ohne dieses Lagebild ist es schwierig, Pflichten aus der NIS-2 und dem neuen BSIG im Alltag verlässlich zu erfüllen, selbst wenn die Technik aus Sicht einzelner Komponenten gut funktioniert.

Wie die Zusammenarbeit entstand

Der Impuls zur Zusammenarbeit kam aus der Prüfperspektive. Die Klinik wollte wissen, welche Schritte kurzfristig Wirkung entfalten und zugleich Bestand im Audit haben. Althammer & Kill brachte dafür eine strukturierende Sicht ein, die an der Schnittstelle von Technik und Recht ansetzt. Es ging um Rollen, Eskalationsstufen, Meldeketten und vor allem um Nachweise, die nicht nur formuliert, sondern gelebt werden. Schnell wurde deutlich, dass diese Struktur nur so gut ist, wie die operative Wahrnehmung der Ereignisse. Bei der Frage, wie rund um die Uhr relevante Vorgänge erkannt, bewertet und priorisiert werden, fiel die Wahl auf Blueteam. Ausschlaggebend war die Fähigkeit, ein Security Operations Center zügig bereitzustellen, ein Managed-SIEM aufzusetzen, Alarme nach Wirkung zu priorisieren und das Ganze in Berichten so aufzubereiten, dass sie in der Leitung nicht erklärt werden müssen, sondern zum Arbeiten einladen.
Aus dieser Konstellation ergab sich eine klare Arbeitsteilung. Blueteam liefert beobachtbare Fakten, bewertet Auffälligkeiten und schlägt Handlungen vor. Alt-

hammer & Kill übersetzt diese Ergebnisse in Verantwortung, Risikoabwägung und prüffähige Dokumentation. Beide Seiten vereinbarten kurze Iterationen. Jede technische Maßnahme erhält sofort ihren Platz in Zuständigkeiten und Nachweisen. Jede organisatorische Vorgabe wird zugleich mit Daten aus dem Betrieb hinterlegt. So entsteht ein Kreislauf, der weder in Technikdetails stecken bleibt, noch im Papierhaften verharrt.

Der Projektstart: Pragmatik vor Perfektion

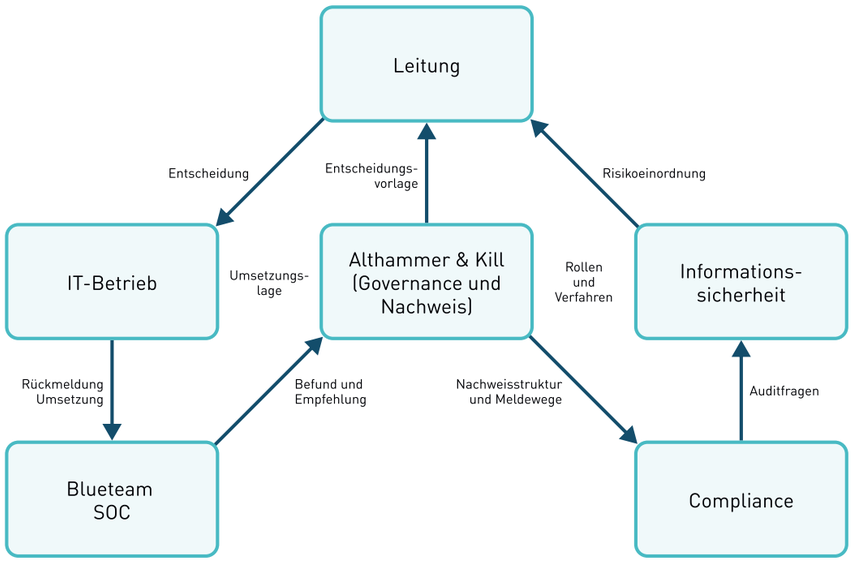
Die ersten Tage galten der Orientierung. Statt eines großen Programms mit umfangreichen Zielbildern wurde ein schlanker Ablauf für typische Ereignisse definiert. Wer meldet was an wen? Welcher Kanal gilt zu welcher Uhrzeit? Welche Reaktionszeit ist realistisch und wann ist die Leitung einzubinden? Parallel wurden die wichtigsten Quellen an die zentrale Auswertung angebunden. Nicht alles, was technisch möglich ist, ergab in der ersten Welle Sinn. Entscheidend war eine erste Lageübersicht, die nicht mit Meldungen überflutet, sondern Entscheidungen ermöglicht.

Diese Priorisierung war die erste echte Weichenstellung. Alarme sind künftig keine abstrakten Nummern mehr, sondern Anlässe, eine Konsequenz zu ziehen. Mit wenigen gezielten Use Cases wurde erkennbar, wo ungewöhnliche Muster auftreten, welche Konten besondere Aufmerksamkeit erfordern und welche Systeme für den Betrieb kritisch sind. Die Mannschaft vor Ort merkte rasch, dass es nicht um Kontrolle geht, sondern um Verlässlichkeit. Wenn klar ist, wer in welcher Situation handelt und wie eine Entscheidung dokumentiert wird, entsteht Ruhe in den Abläufen. An diesem Punkt zeigte sich bereits ein Nebeneffekt, der in vielen Häusern unterschätzt wird. Gespräche verlagerten sich weg von ungeklärten Zuständigkeiten hin zu greifbaren Entscheidungen, die sich nachvollziehen lassen.

Sichtbarkeit wird Routine

Mit der Anbindung weiterer Quellen wuchs das Lagebild. Blueteam etablierte einen Rhythmus, in dem Ereignisse nicht nur erkannt, sondern nach einem festen Schema bewertet werden. Die Berichte sind auf Verständlichkeit angelegt. Sie zeigen nicht nur, was passiert ist, sondern ordnen die Relevanz ein und schlagen ein Vorgehen vor. Dadurch steigt die Qualität der Gespräche in der Linie. Es geht nicht mehr darum, ob etwas geschehen ist, sondern darum, wie die Organisation damit umgeht. Althammer & Kill überführte diese Ergebnisse parallel in Rollen und Nachweise.

Eine technische Maßnahme, etwa eine geänderte Konfiguration oder eine neue Anbindung, wird nicht isoliert betrachtet. Sie bekommt ihren Platz im Verfahren, in der Zuständigkeit und in den Kriterien, die in der Prüfung benötigt werden. Auf diese Weise wird aus fortlaufender Technikarbeit eine prüffähige Routine. Das ist unspektakulär, aber genau das macht den Unterschied. Wer geordnet arbeitet, kann gelassen geprüft werden.



Die Mitte des Projekts: SOC und Governance greifen ineinander

Etwa ab Woche fünf veränderte sich der Charakter des Projekts.

Aus der initialen Orientierung wurde ein verlässlicher Betrieb. Blueteam führte feste Intervalle für das Schwachstellenmanagement und für den Endpunktschutz ein. Die Lageberichte bekamen Kennzahlen, die nicht nur zählen, sondern erklären, ob eine Maßnahme wirkt. Althammer & Kill verdichtete diese Ergebnisse zu Risikobewertungen und ordnete sie in den Verbesserungsprozess ein.

In der Praxis bedeutet das, dass es zu einer beobachteten Auffälligkeit nicht nur einen technischen Eintrag gibt, sondern eine begründete Entscheidung, die sich zu einem späteren Zeitpunkt nachverfolgen lässt. Die Leitung erhält damit eine Sicht, die nicht nach Spezialwissen verlangt, sondern den Kern trifft. Wo stehen wir heute? Was hat gewirkt? Was steht als Nächstes an? Für die Fachklinik war diese Klarheit der entscheidende Schritt. Aus einer Reihe von Maßnahmen wurde eine Linie, die im Alltag trägt.

„NIS-2-Compliance ist keine Frage der Größe, sondern der Verantwortung. Auch kleinere Häuser brauchen Strukturen, um Sicherheit dauerhaft leben zu können.“

Wulf Bolte, Althammer & Kill

Die Generalprobe: Das Audit als Alltagstest

Zwei Wochen vor der externen Prüfung führte das Team eine interne Generalprobe durch. Es wurden typische Szenarien in kurzen Schleifen durchgespielt. Dabei ging es nicht um perfekte Antworten, sondern um Souveränität. Wer übernimmt in welcher Minute? Wo wird dokumentiert? Welche Begründung trägt? Schnell zeigte sich, dass die größte Stärke nicht im Auswendiglernen von Abläufen liegt, sondern in der Klarheit der Übergaben. Wenn die IT eine Lage bewerten kann und die Leitung auf dieser Basis entscheiden kann, entstehen wenige Reibungen und kaum Zeitverluste.

Das eigentliche Audit verlief folgerichtig geordnet. Wichtiger als die Bewertung war die Erkenntnis, dass die Organisation die Lage nicht nur technisch im Griff hat, sondern auch kommunikativ. Die gleiche Faktenlage liegt beiden Seiten vor. Entscheidungen werden auf dieser Basis getroffen und nachvollziehbar festgehalten. Genau das ist gemeint, wenn von gelebter Sicherheit gesprochen wird.

Was sich sichtbar verändert hat

Im Alltag der Fachklinik sind heute mehrere Verschiebungen spürbar. Das Lagebild ist zentral und verständlich. Alarme werden nicht mehr an ihrer Anzahl gemessen, sondern an der Qualität der Entscheidungen, die sie auslösen. Die Leitung und die IT sprechen über dasselbe Bild und können Entscheidungen zeitnah treffen. Die Dokumentation ist kein Selbstzweck, sondern dient als Arbeitsgrundlage. Sie zeigt den Stand der Dinge, nicht nur die Absicht. In der Prüfung lassen sich Maßnahmen und Entscheidungen nachvollziehen. Das schafft Vertrauen. Gleichzeitig ist die Organisation realistisch geblieben.

Es geht nicht um einen Endzustand, sondern um einen wiederkehrenden Prozess. Die Pflege der Playbooks, die Überprüfung von Kontakten und das regelmäßige Üben sind Teil der Routine geworden. Niemand erwartet, dass nie etwas Ungewöhnliches passiert. Der Unterschied liegt darin, ob die Organisation darauf vorbereitet ist, es zu erkennen, geordnet zu handeln und es nachvollziehbar zu dokumentieren.

Was bleibt

Das Projekt zeigt: Echte Informationssicherheit entsteht dort, wo Technik und Governance ineinandergreifen – unabhängig von der Größe der Organisation. Sie entsteht dort, wo operative Beobachtung und Führungsverantwortung zusammenfinden. Wo Zuständigkeiten so beschrieben sind, dass Menschen sie leben können. Und wo Nachweise so geführt werden, dass sie nicht nur der Revision genügen, sondern im Alltag Orientierung geben. NIS-2, NIS2UmsuCG und das neue BSIG schaffen den Rahmen für diese Aufgabe. Entscheidend ist die Ausgestaltung vor Ort. In der Fachklinik wurde aus einer Prüfankündigung ein Arbeitsrhythmus, der die Organisation stärkt. Nicht, weil jede technische Möglichkeit ausgeschöpft wurde, sondern weil die richtigen Dinge zur richtigen Zeit getan wurden. Das ist eine ermutigende Botschaft für alle, die vor ähnlichen Aufgaben stehen. &

ALTHAMMER & KILL

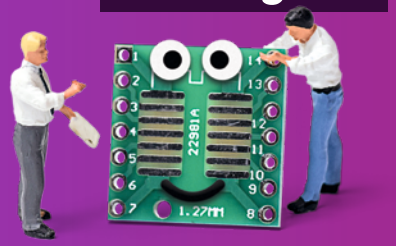
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

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