COMPLIANCE konkret

Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2024

Künstliche Intelligenz und Regulierung

Ein einheitlicher Rechtsrahmen für die EU

Seite 6

Wolfsburg-App
Datenschutz und Innovation im Fokus
Seite 10

ISO 27001:2022
Die neue Ära der Informationssicherheit
Seite 12

Das EU-Lieferketten-sorgfaltspflichtengesetz
Wie ist eigentlich der Stand?
Seite 16

Editorial

Liebe Leserin, lieber Leser,

in der dynamischen Welt der Technologie und Regulierungen gibt es kontinuierlich spannende Entwicklungen, die unser tägliches Leben und unsere Arbeitsweise beeinflussen. Ein bemerkenswertes Beispiel dafür ist die Stadt Wolfsburg, die das Thema Datenschutz bei der App-Entwicklung als Bindeglied zwischen Stadtverwaltung und Bürgerschaft von Anfang an mitgedacht hat. Die Wolfsburg-App zeigt dabei, wie der Schutz personenbezogener Daten erfolgreich in moderne Anwendungen integriert werden kann.

Auch die jüngste Aktualisierung der ISO/IEC 27001:2022 sorgt für Aufsehen. Diese neue Version der Norm bringt wesentliche Änderungen mit sich, die Unternehmen dabei unterstützen, ihre Informationssicherheitsmanagementsysteme weiter zu verbessern und auf aktuelle Bedrohungen abzustimmen. Wir haben die wichtigsten Neuerungen für Sie zusammengefasst und erklären, wie Sie diese effektiv umsetzen können.

Ein weiterer Meilenstein ist die Einführung der KI-Verordnung in der Europäischen Union. Diese wegweisende Regulierung zielt darauf ab, den Einsatz von Künstlicher Intelligenz sicherer und transparenter zu gestalten. Unternehmen stehen nun vor der Herausforderung, ihre KI-Systeme den neuen Anforderungen anzupassen, um ethische und rechtliche Standards zu erfüllen. Wir beleuchten die zentralen Punkte dieser Verordnung und bieten Ihnen einen Überblick über die notwendigen Anpassungen.

Nicht zuletzt rückt das EU-Lieferkettensorgfaltspflichtengesetz in den Fokus, das Unternehmen verpflichtet, die Einhaltung von Menschenrechts- und Umweltstandards in ihren Lieferketten zu gewährleisten. Diese Regelung stellt sicher, dass Verantwortung über die gesamte Wertschöpfungskette hinweg übernommen wird. In unserem Beitrag erfahren Sie, welche Maßnahmen zur Erfüllung dieser gesetzlichen Vorgaben erforderlich sind und wie nachhaltige Geschäftspraktiken gefördert werden können.

Wir hoffen, dass Ihnen diese Themen wertvolle Einblicke und Anregungen bieten. Viel Spaß beim Lesen wünschen

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*

Althammer & Kill-Teamtage: Sommer, Sonne, Sonnenschein!

Es war wieder so weit, die Teamtage standen vor der Tür. Nach einem produktiven Vormittag mit dem umfangreichen Thema „Prozessoptimierung", ging es dieses Jahr raus in die Eilenriede. Wir hatten beschlossen, uns auf eine Geocaching-Tour zu begeben. Die Tour hat uns das eine oder andere Rätsel abverlangt. Aber wir wären ja nicht Team Bildung, wenn wir es nicht lösen würden.

Aber das war noch nicht genug: Das Motto für den zweiten Tag unserer Teamtage lautete „Mit den Händen denken", und so konnten wir mit der Unterstützung von Michael Barsakidis die LEGO® Serious Play® Methode anwenden und verstehen. Mit dieser Methode ist es möglich, kreativ zu denken und gemeinsam komplexe Probleme zu lösen.

Unser Aufgabe war es „Innovative Lösungen für unsere nachhaltige Zukunft" zu entwickeln. Jede Person im Team visualisierte ihre Idee Stück für Stück bzw. Stein für Stein, um später gemeinsam aus den vielen individuellen Ideen eine große Idee zu präsentieren. Und ja, man ist wirklich nie zu alt, um mit Lego zu bauen und zu spielen – man lernt nie aus!

Was die neue KI-Verordnung für Unternehmen und Bürger bedeutet

Die neue KI-Verordnung (KI-VO) der EU trat am 1. August 2024 in Kraft. Was bedeutet das für Unternehmen und Bürger? Erfahren Sie alles über die Übergangsfristen, Risikoklassen und die strengen Anforderungen an Hochrisiko-KI-Systeme.

KLICK/SCAN

Künstliche Intelligenz: Grundlagen, Lernmethoden und Datenschutz

Was ist Künstliche Intelligenz (KI) überhaupt? Wie lernt sie und welche Arten des Lernens gibt es? Außerdem beleuchten wir wichtige Aspekte des Datenschutzes und der Informationssicherheit bei der Nutzung von KI-Systemen.

Künstliche Intelligenz (KI) ist längst nicht mehr nur ein Thema für Science-Fiction-Filme. Sie ist Teil unseres Alltags und findet Anwendung in vielen Bereichen wie Gesundheitswesen, Finanzen, Verkehr und Unterhaltung. Doch was genau verbirgt sich hinter diesem Begriff, und wie funktioniert KI eigentlich? In diesem Artikel geben wir Ihnen einen umfassenden Überblick über die Grundlagen der KI, ihre Lernmethoden und wichtige Datenschutzaspekte.

KLICK/SCAN

KATHOLISCHE UNIVERSITÄT EICHSTÄTT-INGOLSTADT

Studie zu Künstlicher Intelligenz: Sozialwirtschaft hält KI mehrheitlich für sehr wichtige Schlüsseltechnologie

Die Arbeitsstelle für Sozialinformatik an der Katholischen Universität Eichstätt-Ingolstadt hat mit Unterstützung von Althammer & Kill eine Studie zur Anwendung von Künstlicher Intelligenz (KI) in der Sozialwirtschaft durchgeführt.

Die Studie bietet einen Einblick in die Zukunft der Sozialwirtschaft. Sie beleuchtet nicht nur den aktuellen Stand der KI-Nutzung, sondern zeigt auch Potenziale und Herausforderungen auf. Für Führungskräfte und Verantwortliche ist sie eine gute Grundlage, um informierte Entscheidungen über den Einsatz von KI zu treffen. Die Studie kombiniert Expertenwissen mit praxisnahen Erkenntnissen und liefert wertvolle Orientierung in einer sich rasant entwickelnden digitalen Landschaft.

KLICK/SCAN

Zahl des Monats

4.000.000.000

Innerhalb des Jahres 2024 wird die Zahl der weltweiten Internetnutzer voraussichtlich die Marke von 4 Milliarden überschreiten. Diese beeindruckende Zahl unterstreicht nicht nur die weitreichende Digitalisierung unserer Gesellschaft, sondern hebt auch die wachsende Bedeutung von Datenschutz und Informationssicherheit hervor. Jeder dieser 4 Milliarden Nutzer hinterlässt digitale Spuren, die potenziell von Cyberkriminellen ausgenutzt werden können. Daher ist es entscheidend, dass sowohl Einzelpersonen als auch Unternehmen verstärkt in Sicherheitsmaßnahmen und Datenschutzpraktiken investieren.

Veranstaltungen

19.–20. Februar 2025, Hannover

Norddeutsches KI-Forum – Der 360°-Blick auf KI in Wirtschaft, Verwaltung & 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 mit KI zu gestalten.

Erleben Sie inspirierende Keynotes, praxisnahe Workshops und spannende Diskussionsrunden rund um das Thema Künstliche Intelligenz. Tauschen Sie sich mit Vordenkern aus Wissenschaft, Behörden und Wirtschaft aus und knüpfen Sie wertvolle Kontakte. Entdecken Sie, wie norddeutsche Verwaltung und Unternehmen bereits heute KI erfolgreich einsetzen und welche Potenziale sich für Ihr eigenes Unternehmen eröffnen.

KLICK/SCAN

Unsere Orientierungshilfe zur NIS-2-Richtlinie

NIS-2 steht für "Network und Information Security 2". Das Ziel der Richtlinie ist die Etablierung eines einheitlichen Mindeststandards für die Sicherheit in der gesamten EU. Jedoch ergeben sich aus der Richtlinie viele Fragen: Wer ist genau betroffen? Wie kann ich den Ansprüchen der Richtlinie gerecht werden und welche Maßnahmen müssen konkret ergriffen werden? Wir zeigen in unserer Orientierungshilfe, wie sie mit NIS-2 umgehen können.

KLICK/SCAN

Künstliche Intelligenz (KI) und Regulierung – ein einheitlicher Rechtsrahmen für die EU

Der Einsatz Künstlicher Intelligenz (KI) wird aufgrund der zahlreichen Anwendungsmöglichkeiten und der zunehmenden Verfügbarkeit für viele Nutzende verstärkt diskutiert. KI ist in vielen Bereichen bereits im Einsatz. Sie unterstützt als Chatbot den Kundensupport, bietet Hilfe bei Formulierungen, hilft beim Programmieren oder übersetzt Texte und Gespräche in andere Sprachen.

Von Urban Zimber

Neben den Chancen werden auch die Risiken des KI-Einsatzes diskutiert. Es stellt sich die Frage, welche Gefahren KI aktuell und in Zukunft mit sich bringen kann. Um diesen Chancen und Risiken zu begegnen, hat die Europäische Union mit der KI-Verordnung (AI-Act) rechtliche Leitplanken für den Einsatz von KI innerhalb der EU gesetzt.

Was ist KI?

Die Meinungen darüber, was Künstliche Intelligenz genau ist, gehen auseinander. Es gibt keine allgemein gültige Definition, da der Begriff Intelligenz nicht genau bestimmt ist.

Die folgenden Definitionsversuche geben jedoch eine ähnliche Richtung vor:

„Künstliche Intelligenz ist die Eigenschaft eines IT-Systems, »menschenähnliche«, intelligente Verhaltensweisen zu zeigen."
— Bitkom e. V. und Deutsches Forschungszentrum für Künstliche Intelligenz

„Unter Künstlicher Intelligenz (KI) verstehen wir Technologien, die menschliche Fähigkeiten im Sehen, Hören, Analysieren, Entscheiden und Handeln ergänzen und stärken."
— Microsoft Corp.

„Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren."
— Europäisches Parlament

Eine abstrakte und differenzierte Definition findet sich in Artikel 3 Absatz 1 der neuen KI-Verordnung (KI-VO) der EU: „KI-System" – ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren und nach dem Einsatz Anpassungsfähigkeit zeigen kann. Es kann aus den Eingaben, die es erhält, ableiten, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen."

Arten von KI

Es wird zwischen traditioneller KI und generativer KI unterschieden.

Traditionelle KI (prädiktive KI): Mustererkennung und Vorhersagen anhand von Wahrscheinlichkeiten, wie z. B. Datenanalyse und Zukunftsprognosen.

Generative KI: Kann eigenständig Inhalte aus ihren Trainingsdaten produzieren, also neue, originelle

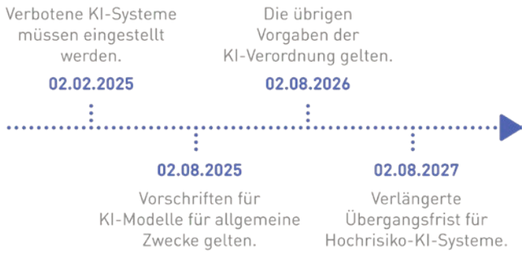
Inhalte erschaffen. Dazu gehört maschinelles Lernen (Training aus Daten). Beispiele: Erschaffung von Kunstwerken, Textgenerierung, Bildgenerierung (aus Textbeschreibungen), Erstellung realistischer Videos aus Textanweisungen.

Regulierungen der KI

Bereits im April 2021 hatte die EU-Kommission den ersten europäischen Rechtsrahmen für KI vorgeschlagen. Darin wurde empfohlen, dass KI-Systeme, abhängig von dem Risiko, das sie für die Nutzenden darstellen, analysiert und eingestuft werden. Die einzelnen Risikostufen unterliegen stärkerer oder weniger strenger Regulierung.

Nachdem der Rat der Europäischen Union am 21. Mai 2024 die KI-VO verabschiedet hat, wurde das weltweit erste umfassende Regelwerk zur Anwendung von KI auf den Weg gebracht. Der Verordnungstext umfasst 113 Artikel und wird durch 180 Erwägungsgründe ergänzt. Die Verordnung wurde am 12. Juli im Amtsblatt der EU veröffentlicht und tritt 20 Tage später, also am 1. August 2024 in Kraft.

Es gelten gestaffelte Übergangsfristen nach Inkrafttreten:



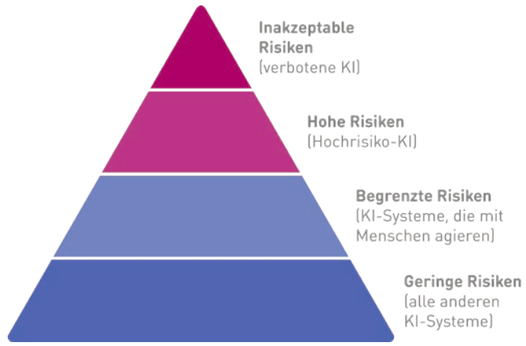
Ziele der KI-VO

Die Ziele der KI-VO werden in Artikel 1 Nummer 1 der KI-VO beschrieben:

- Verbesserung des Funktionierens des Binnenmarktes
- Förderung der Einführung menschenbezogener und vertrauenswürdiger KI
- Gewährleistung eines hohen Niveaus des Schutzes der Gesundheit, der Sicherheit, der in der Charta verankerten Grundrechte, einschließlich der Demokratie, der Rechtsstaatlichkeit und des Umweltschutzes vor den schädlichen Auswirkungen von KI-Systemen in der Union und Unterstützung von Innovationen

Überblick zur KI-VO

Die KI-VO definiert keinen allumfassenden Rechtsrahmen für KI, sondern verfolgt einen horizontalen, risikobasierten Ansatz, der sich vorrangig auf Produktsicherheitsaspekte für KI-Systeme konzentriert. Ein besonderer Fokus liegt auf KI-Systemen, die aufgrund ihres Risikopotentials für Grundrechte und sensible Rechtsgüter strengeren Regulierungen unterliegen. Dieser Ansatz unterscheidet Verpflichtungen ausgehend von dem Risikograd der Nutzung von KI-Systemen, unabhängig von der zugrunde liegenden Technologie. Dabei werden KI-Systeme in vier Risikoklassen unterteilt:



Damit setzt die KI-Verordnung regulatorische Maßnahmen gezielt dort ein, wo ein Risiko für die öffentliche Ordnung oder Grundrechte besteht. Inakzeptable Risiken verletzen fundamentale Rechte und sind verboten, z. B. ein Social-Scoring-System. Hohe Risiken können zu einem potentiell hohen Schaden führen und unterliegen umfangreichen Anforderungen. Begrenzte Risiken werden mit Transparenzpflichten reguliert. Niedrige Risiken unterliegen keiner weiteren Regulierung.

Anwendungsbereich

Hauptadressierte der KI-VO sind die Anbietenden von KI-Systemen (Artikel 2 Nummer 1 (a) KI-VO). Darunter versteht die KI-VO „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickeln lässt und es unter eigenem Namen oder eigener Marke in Verkehr bringt oder in Betrieb nimmt, unabhängig davon, ob dies entgeltlich oder unentgeltlich geschieht“ (Artikel 3 Absatz 3 KI-VO).

Die Pflichten der Anbietenden sind insbesondere in Artikel 16 KI-VO geregelt. Sie müssen vor allem die Anforderungen

von Artikel 8 bis 15 KI-VO vor dem Inverkehrbringen und der Inbetriebnahme eines KI-Systems erfüllen. Anbietende müssen ein Risikomanagementsystem zur Überwachung aufbauen (Artikel 19 KI-VO) und eine hohe Qualität der verarbeiteten Datensätze sicherstellen (Artikel 10 KI-VO). Zudem sind Transparenz und menschliche Aufsicht über die KI (Artikel 13, 14 KI-VO) zu gewährleisten.

Weiterhin fallen Bereitstellende unter die KI-VO. Als solche werden „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System unter eigener Aufsicht einsetzt, es sei denn, das KI-System wird im Rahmen einer persönlichen, nicht beruflichen Tätigkeit verwendet“ definiert (Artikel 3 Absatz 4 KI-VO). Die Pflichten der Bereitstellenden sind überwiegend in Artikel 26 KI-VO geregelt. Weitere Adressierte sind u.a. Importierende und Vertreibende von KI-Systemen (Artikel 2 Nummer 1 (d) KI-VO) und betroffene Personen, die sich in der Union befinden (Artikel 2 Nummer 1 (g) KI-VO).

Artikel 2 Nummer 1 KI-VO bestimmt zudem den räumlichen Anwendungsbereich. Die KI-VO gilt für Anbietende, die KI-Systeme innerhalb der EU in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob sie in der EU ansässig sind oder nicht (Artikel 2 Nummer 1 (a) KI-VO). Bereitstellende von KI-Systemen unterliegen den Vorschriften der KI-VO, wenn sie ihren Niederlassungsort in der EU haben oder dort ansässig sind (Artikel 2 Nummer 1 (b) KI-VO).

Die KI-VO ist auch für Anbietende und Betreibende in Drittstaaten anwendbar, wenn das von dem KI-System erzeugte Ergebnis in der Union verwendet wird (Artikel 2 Nummer 1 (c) KI-VO). Dies zielt darauf ab, eine Umgehung der KI-VO und die unregulierte Datenübermittlung in Drittstaaten zu verhindern.

Rechtsdurchsetzung

Zur Rechtsdurchsetzung werden mehrere Behörden auf nationaler sowie auf EU-Ebene etabliert. Eine zentrale Rolle nimmt dabei das neu gegründete EU AI Office ein.

Datenschutzrechtliche Aspekte bei KI-Anwendungen

KI-Anwendungen müssen neben der KI-Verordnung auch den datenschutzrechtlichen Vorschriften standhalten. Die DSGVO ist bei KI-Anwendungen weiterhin anwendbar (Artikel 2 Nummer 7 KI-VO). Einzelne Ausnahmen davon finden sich in Artikel 10 Absatz 5 und Artikel 59 KI-VO.

Fazit

Bereits vor dem Einsatz von KI-Anwendungen sollte eine Vorabprüfung stattfinden, um die relevanten Pflichten zu identifizieren. Ähnlich wie bei der Datenschutzgrundverordnung (DSGVO) führt auch in der KI-VO ein risikobasierter Ansatz dazu, dass höhere Risiken zu einer strengeren Regulierung führen.

Neben der Einordnung unter die KI-VO sind weiterhin die datenschutzrechtlichen Vorgaben und die Informationssicherheit von zentraler Bedeutung. &

Impressum

Redaktion/V. i. S. d. P.:
Fabian Eggers, Michael Defland, 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

Wolfsburg-App: Digitale Stadtverwaltung weiterentwickelt – Datenschutz und Innovation im Fokus

Die Wolfsburg-App vereinfacht den Alltag und stärkt die Verbindung zwischen Stadtverwaltung und Bürgerinnen und Bürgern. Herausforderungen und Lösungen in der Entwicklung und Sicherheit.

Von Jessica Henning

Die Stadt Wolfsburg hat einen großen Schritt in Richtung digitale Transformation gemacht, indem sie die Wolfsburg-App eingeführt hat. Diese App zielt darauf ab, den Alltag der Stadtbewohnenden durch eine zentrale App für zahlreiche stadtbezogene Dienste zu erleichtern. Im Rahmen des Projekts wurden Herausforderungen bewältigt, insbesondere im Bereich Datenschutz und Cybersecurity. Ein wesentlicher Bestandteil des Erfolgs der App war die enge Zusammenarbeit mit der Cybersecurity- und Datenschutzberatung von Althammer & Kill.

Ziele und Funktionen der Wolfsburg-App

Die Wolfsburg-App bündelt eine Vielzahl von stadtbezogenen Dienstleistungen und bietet den Bürgerinnen und Bürgern ein umfassendes Werkzeug für alltägliche Anliegen. Die App umfasst unter anderem eine Handypark-Funktion und einen Mängelmelder. Diese Dienste sollen vor allem den Servicegedanken für die Bewohnerinnen und Bewohner stärken.

Zu den neuen Funktionen gehört die Anzeige aktueller Kraftstoffpreise an Tankstellen. Dies ermöglicht den Nutzenden, Preise zu vergleichen und so gezielt günstigere Tankmöglichkeiten in ihrer Nähe zu wählen. Der Mängelmelder erlaubt es, Defekte wie beschädigte Gehwege oder kaputte Ampeln schnell und unkompliziert zu melden, wobei der Bearbeitungsstatus transparent verfolgt werden kann.

Herausforderungen und Lösungsansätze

Ein zentrales Anliegen bei der Entwicklung der Wolfsburg-App war die Einhaltung hoher Datenschutz- und Sicherheitsstandards. Bei der Verarbeitung von persönlichen Daten, wie etwa Standortdaten, mussten strenge gesetzliche Vorgaben eingehalten werden.

Die Notwendigkeit, umfassende Datenschutzmaßnahmen zu implementieren, erforderte eine enge Zusammenarbeit mit Fachleuten im Bereich Sicherheits- und Datenschutzberatung. „Die Herausforderung bestand darin, eine App zu entwickeln, die sowohl benutzerfreundlich als auch sicher ist. Besonders im Hinblick auf den Datenschutz mussten wir sicherstellen, dass alle gesetzlichen Anforderungen erfüllt, werden“, erklärt ein Vertreter der Stadtverwaltung.

Sicherheitsüberprüfung und Datenschutz

Die Überprüfung der App umfasste mehrere Phasen. Zunächst wurde eine ausführliche Datenschutzfolgenabschätzung durchgeführt. Diese Analyse half unter anderem dabei, mögliche Risiken bei der Verarbeitung personenbezogener Daten zu identifizieren und zusätzliche geeignete Schutzmaßnahmen zu entwickeln. Im späteren Verlauf wurden durch einen Penetrationstest (Pentest), vor Veröffentlichung der App, Unstimmigkeiten aufgedeckt und dann entsprechende Verschlüsselungstechnologien für die Datenübertragung implementiert, um sicherzustellen, dass die Daten der Nutzenden vor unbefugtem Zugriff geschützt sind.

Zusätzlich wurden, vor der Implementierung neuer Funktionen, umfassende Risikoanalysen und Pentests durchgeführt. Diese Tests ermöglichten es, Schwachstellen in der App zu identifizieren und zu beheben, bevor die App für die Öffentlichkeit freigegeben wurde. „Unsere Arbeit konzentrierte sich darauf, potenzielle Sicherheitslücken und Risiken frühzeitig zu erkennen und Lösungen zu entwickeln, die den Anforderungen an den Datenschutz entsprechen und die Nutzenden in ihren Persönlichkeitsrechten zu schützen“, beschreibt Jessica Henning, Beraterin für das Projekt, die Vorgehensweise.

Integration von Nutzenden-Feedback

Ein weiterer wesentlicher Aspekt der Entwicklung war die Integration des Feedbacks der Nutzenden. Die Stadtverwaltung legt großen Wert darauf, dass die App den tatsächlichen Bedürfnissen der Bürgerinnen und Bürger entspricht. Rückmeldungen wurden gesammelt und analysiert, um gezielte Verbesserungen vorzunehmen.

„Die Herausforderung bestand darin, eine App zu entwickeln, die sowohl benutzerfreundlich als auch sicher ist. “

Die Feedback-Schleifen ermöglichten es, die App kontinuierlich an die Anforderungen der Nutzenden anzupassen. „Die Rückmeldungen der Bürgerinnen und Bürger waren entscheidend für die Weiterentwicklung der App. Sie halfen uns dabei, die Funktionen zu optimieren und sicherzustellen, dass die App den Erwartungen der Nutzenden entspricht“, so ein Sprecher der Stadtverwaltung.

Zusammenarbeit mit Fachleuten

Im Rahmen des Projekts war die Unterstützung durch Fachleute im Bereich Datenschutz und Cybersecurity von großer Bedeutung. Die Expertise dieser Beratenden war entscheidend für die Umsetzung der hohen Sicherheits- und Datenschutzanforderungen. Die Beratung umfasste nicht nur die technische Ausgestaltung, sondern auch die rechtlichen Aspekte, die bei der Verarbeitung personenbezogener Daten berücksichtigt werden mussten.

„Durch die enge Zusammenarbeit mit Sicherheitsexpertinnen und -experten konnten wir sicherstellen, dass die Wolfsburg-App sowohl sicher als auch benutzerfreundlich ist“, erklärt die Stadtverwaltung. Diese Unterstützung ermöglichte es, datenschutzfreundliche Lösungen schon frühzeitig bei der Entwicklung zu implementieren und sicherzustellen, dass die App alle relevanten Vorschriften einhält.

Erweiterung und kontinuierliche Verbesserung

Die Wolfsburg-App ist als Langzeitprojekt angelegt, das kontinuierlich weiterentwickelt wird. Die Planung sieht vor, dass regelmäßig neue Funktionen hinzugefügt werden, um den sich ändernden Bedürfnissen der Bürgerinnen und Bürger gerecht zu werden. Zu den geplanten Erweiterungen gehören zusätzliche stadtbezogene Dienstleistungen und Optimierungen basierend auf dem Feedback der Nutzenden.

„Die kontinuierliche Weiterentwicklung der App ist ein wesentlicher Bestandteil unseres Projekts. Wir planen, die App regelmäßig, um neue Funktionen zu erweitern, um den Alltag der Stadtbewohnenden weiter zu verbessern“, betont die Stadtverwaltung. Die regelmäßige Aktualisierung und Anpassung an neue Anforderungen stellen sicher, dass die App stets den aktuellen Bedürfnissen der Nutzenden entspricht.

Fazit

Die Wolfsburg-App stellt einen bedeutenden Fortschritt in der Digitalisierung der Stadtverwaltung dar. Durch die enge Zusammenarbeit mit Fachleuten für Datenschutz und Cybersecurity konnte die Stadt Wolfsburg eine App entwickeln, die sowohl funktional als auch sicher ist. Die erfolgreichen Maßnahmen zur Gewährleistung des Datenschutzes und die kontinuierliche Verbesserung der App sind entscheidende Faktoren für deren Erfolg.

Die App bietet den Bürgerinnen und Bürgern eine zentrale Plattform für zahlreiche stadtbezogene Dienste und bringt diese näher. „Die Wolfsburg-App soll allen Menschen, die in Wolfsburg wohnen und die Stadt besuchen, den Alltag erleichtern und Zeit sparen“, lautet das Ziel der Stadtverwaltung. &

ISO 27001:2022 – die neue Ära der Informationssicherheit

Von Cloud-Security bis Risikomanagement: Wie Unternehmen mit der überarbeiteten Norm ihre Sicherheitsstrategien verbessern und zukünftige Bedrohungen meistern.

Von Maximilian Klose

Die ISO/IEC 27001-Norm, ursprünglich 2005 eingeführt und zuletzt 2013 überarbeitet, adressiert die ständig wachsenden Anforderungen an die Informationssicherheit. Die Überarbeitung aus dem Jahr 2022 zielt darauf ab, den aktuellen technologischen Entwicklungen und Bedrohungen gerecht zu werden. Dieser Artikel beleuchtet die Unterschiede zwischen der ISO 27001:2013 und der ISO 27001:2022, erläutert die neuen Anforderungen und wegfallenden Elemente und erklärt, welche Schritte Unternehmen gehen müssen, um die neue Norm zu erfüllen.

ISO/IEC 27001 ist eine international anerkannte Norm, die Anforderungen an Informationssicherheits-Managementsysteme (ISMS) festlegt. Sie bietet Organisationen einen strukturierten Ansatz zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und schützt somit vor Bedrohungen wie Cyberangriffen und Datenlecks.

Unterschiede zwischen ISO 27001:2013 und ISO 27001:2022

Die Revision der ISO/IEC 27001 im Jahr 2022 bringt umfassende Änderungen sowohl in der Struktur der Norm wie auch im Inhalt. Der Anhang A der Norm, der die Controls enthält, wurde überarbeitet und modernisiert. Die Anzahl der Controls wurde von 114 auf 93 reduziert, indem einige Controls zusammengelegt und andere entfernt wurden. Diese verbleibenden Controls sind in vier Hauptkategorien unterteilt: organisatorische, personelle, physische und technologische Maßnahmen.

Elf neue Controls wurden eingeführt, darunter Threat-Intelligence, die Nutzung der Cloud, Sicherheitsanforderungen für Informations- und Kommunikationstechnologie (IKT), und die sichere Softwareentwicklung. Der Fokus auf Risikomanagement wurde verstärkt, und Unternehmen müssen detailliertere Prozesse zur Risikoidentifizierung, -bewertung und -behandlung implementieren. Die neuen Versionen legen größeren Wert auf die Kriterien und die Effektivität von sicherheitsrelevanten Controls. Unternehmen müssen nachweisen, dass ihre Controls nicht nur implementiert, sondern auch wirksam sind.

Spezifische Änderungen der ISO 27001:2022

Die Einführung neuer Controls, wie die systematische Sammlung und Analyse von Bedrohungsinformationen, erlaubt es Unternehmen, auf sich entwickelnde Bedrohungen proaktiv zu reagieren. Spezifische Controls zur Sicherung von Cloud-Diensten wurden hinzugefügt, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten in der Cloud sicherzustellen. Die Norm beinhaltet Controls für eine sichere Softwareentwicklung, die im gesamten Softwareentwicklungszyklus Sicherheitsaspekte berücksichtigen. Des Weiteren wurden Anforderungen zur Verwaltung von Benutzerzugriffen präzisiert, um sicherzustellen, dass nur autorisierte Personen Zugriff auf sensible Informationen haben.

Stichwort
Controls

Controls in der ISO/IEC 27001:2022 sind Schutzmaßnahmen, die Unternehmen einsetzen, um ihre Informationen vor Gefahren wie Datenverlust oder unbefugtem Zugriff zu schützen. Sie können technisch sein, wie Firewalls, oder organisatorisch, wie Sicherheitsrichtlinien. Diese Maßnahmen helfen, Risiken zu reduzieren und die Informationssicherheit zu gewährleisten.

Die Anforderungen an den Einsatz kryptografischer Methoden wurden an den neuesten Stand der Technik angepasst. Die Controls zur Verwaltung von Sicherheitsanforderungen an Lieferanten und Dienstleister wurden verstärkt. Unternehmen müssen sicherstellen, dass auch Drittanbieter angemessene Sicherheitsmaßnahmen implementieren. Ein weiteres wichtiges Element der neuen Norm ist die verstärkte Fokussierung auf die Leistungsbewertung des ISMS durch regelmäßige Audits und die Verwendung von Metriken und Key Performance Indicators (KPIs).

Konsequenzen für Unternehmen und deren ISMS

Unternehmen, die nach ISO 27001:2013 zertifiziert sind, haben in der Regel eine Übergangsfrist von zwei bis drei Jahren, um auf die neue Version umzusteigen. Es ist entscheidend, dass sie ihre internen und externen Audits entsprechend planen und frühzeitig mit der Zertifizierungsstelle Kontakt aufnehmen. Eine umfassende Gap-Analyse hilft, die Unterschiede zwischen dem aktuellen ISMS und den Anforderungen der ISO 27001:2022 zu identifizieren. Basierend auf den Ergebnissen sollten Unternehmen ihre ISMS-Dokumentation überprüfen und aktualisieren, insbesondere die Risikobewertungs- und Risikomanagementprozesse. Die Integration der neuen Controls in das ISMS erfordert möglicherweise technische Anpassungen, vor allem in den Bereichen Cloud-Security und sichere Softwareentwicklung. Um das Bewusstsein für die neuen Anforderungen zu stärken, sollten Schulungsprogramme und Awareness-Kampagnen durchgeführt werden. Das Engagement des Managements ist dabei entscheidend, da es die Entscheidung über die Bereitstellung von notwendigen Ressourcen trifft.

Praktische Tipps und Empfehlungen

Eine sorgfältige Planung und Umsetzung ist der Schlüssel zur erfolgreichen Umstellung auf die ISO 27001:2022. Ein detaillierter Zeitplan, ein engagiertes Projektteam und eine gründliche Gap-Analyse sind entscheidend. Die Aktualisierung der Dokumentation und Prozesse sowie die Implementierung neuer Controls sollten unter Einhaltung der neuen Anforderungen erfolgen. Mitarbeiterschulungen und Sensibilisierungskampagnen sind notwendig, um das Verständnis und die Umsetzung der neuen Controls zu fördern.

Technische Maßnahmen sollten implementiert und getestet werden, um die Effektivität der neuen Controls zu überprüfen. Regelmäßige Tests und Bewertungen, wie interne Audits und Penetrationstests, tragen dazu bei, die Wirksamkeit der Sicherheitsmaßnahmen zu gewährleisten. Frühzeitige Kommunikation mit der Zertifizierungsstelle und gründliche Auditvorbereitung sind unerlässlich, um die Rezertifizierung zu erleichtern.

Langfristige Vorteile der Umstellung

Die Umstellung auf die ISO 27001:2022 bietet langfristige Vorteile, die über die unmittelbare Erfüllung von Anforderungen hinausgehen. Die neuen Controls ermöglichen es Unternehmen, proaktive Sicherheitsmaßnahmen gegen aktuelle und zukünftige Bedrohungen zu ergreifen und ihre Resilienz gegenüber Cyberangriffen zu erhöhen. Die Norm stärkt das Vertrauen der Stakeholder in die Informationssicherheit des Unternehmens und verbessert dessen Reputation auf dem Markt. Die Einhaltung internationaler Vorschriften wird erleichtert, wodurch das Risiko von Compliance-Verstößen reduziert wird.

Fazit

Die ISO/IEC 27001:2022 stellt sicher, dass Unternehmen auf aktuelle Herausforderungen und Bedrohungen der Informationssicherheit vorbereitet sind. Die sorgfältige Planung und Umsetzung der neuen Anforderungen ermöglicht es Unternehmen, ihre Sicherheitslage zu stärken, Prozesse zu optimieren und eine Sicherheitskultur zu etablieren. Die Umstellung auf die neue Norm bietet nicht nur Compliance-Vorteile, sondern auch strategische Chancen zur Verbesserung der Sicherheitsstrategie und des Geschäftserfolgs. Unternehmen, die diese Chance nutzen, positionieren sich als vertrauenswürdige Partner in der globalen Geschäftswelt und sind besser gerüstet, um in einer digitalisierten und vernetzten Umgebung erfolgreich zu sein. &

Die Menschen hinter Althammer & Kill:

Frank Boje

Ja hallo, wer bist du denn?

Frank: Guten Morgen! Ich heiße Frank und habe ursprünglich Industriekaufmann gelernt. Eine Kollegin nennt mich immer Frank, „die Wundertüte“, weil ich so vielfältig bin. Vor Althammer & Kill habe ich Zahncreme für Hunde verkauft, war kaufmännischer Leiter bei einem gemeinnützigen Verein und habe viele Jahre Anwender-Support für Software in der Altenpflege geleistet.

Wieso Althammer & Kill?

Frank: Auch wenn sich das jetzt anhört, als wollte ich mich einschmeicheln; aber ich bin schon einmal von Thomas eingestellt worden, damals noch in der Softwarebranche und ich fand die Arbeit mit Thomas äußerst spannend. In dem Unternehmen habe ich dann später schon Verantwortung für den Datenschutz übernommen und so meine Leidenschaft für das Thema entdeckt. Als dann eine Stelle bei Althammer & Kill ausgeschrieben war, habe ich mich gleich beworben.

Wie lange arbeitest du schon bei Althammer & Kill?

Frank: Als Althammer & Kill am 29. Februar 10-jähriges Jubiläum gefeiert hat, hatte ich mein 5-jähriges.

Was machst du so den ganzen Tag?

Frank: Althammer & Kill betreut eine große Anzahl von kleinen Kunden, die nur ein geringes Budget für den Datenschutz zur Verfügung haben. Diese Kunden heißen bei uns Kompakt-Kunden. Häufig handelt es sich dabei um kleine Vereine oder Startup-Unternehmen. Sie erledigen viele Dinge selbst mit Werkzeugen, die von uns zur Verfügung gestellt werden. Diese Kunden betreue ich und unterstütze Sie bei der Nutzung der Werkzeuge, oder berate Sie, wenn ein umfangreicherer Sachverhalt zu klären ist. Zusätzlich habe ich noch eine Handvoll von Beratungskunden, bei denen ich als Datenschutzbeauftragter bestellt bin, und die von mir beraten werden.

Welche Art von Anfragen und Problemen bearbeitest du am häufigsten?

Frank: Die Kompakt-Kunden haben die gleichen Fragen wie andere. Häufig geht es um den Einsatz von bestimmten Softwareprodukten und den damit verbundenen Vereinbarungen zur Auftragsverarbeitung, oder um Datenschutzvorfälle, bei denen die Kunden eine Einschätzung benötigen, ob eine Meldepflicht besteht oder nicht. Da in unseren Info-Centern viele Vorlagen für unsere Kompakt-Kunden vorhanden sind, können Sie sich aber auch viele Fragen selbst beantworten.

Gibt es ein besonderes Erfolgserlebnis oder eine positive Kundenrückmeldung, an die du dich gerne erinnerst?

Frank: Eigentlich nicht. Ich freue mich jedes Mal wenn ein Kunde zufrieden ist und uns eine entsprechende Rückmeldung gibt. Egal, ob wir dem Kunden bei der Erstellung der Datenschutzhinweise für die Webseite oder bei der Aktualisierung des Verarbeitungsverzeichnisses geholfen haben. Besonders groß ist die Freude natürlich, wenn wir über einen zufriedenen Kunden einen Neukunden gewinnen konnten. Das macht mich schon ein bisschen stolz, wenn ich meinen Teil dazu beigetragen habe.

Was gefällt dir besonders an der Arbeit hier?

Frank: Wir sind ein tolles Team bei Althammer & Kill. Dazu kommt, dass die Herausforderungen jeden Tag neu sein können. Du weißt nie, wer als nächstes anruft, oder welche Aufgaben die nächste E-Mail mit sich bringt. Das macht die Arbeit so abwechslungsreich.

Wann war deine Arbeit erfolgreich?

Frank: Wenn wir unserem Kunden weiterhelfen und ihm eine pragmatische Lösung für seine Fragen anbieten können.

Worauf freust du dich in naher Zukunft besonders?

Frank: Die neuen Technologien, insbesondere die Künstliche Intelligenz (KI), werden in naher Zukunft immer mehr in den Vordergrund rücken. Diese Technologien benötigen Unmengen von Daten, damit sie funktionieren. Daher ist es umso wichtiger, darauf zu achten, welche Daten von der KI verarbeitet werden und welche Daten die KI „zum Lernen“ erhält. Der Datenschutz wird in solchen Projekten einen viel höheren Stellenwert bekommen und man muss darauf achten, dass kein Missbrauch betrieben wird. Das wird eine spannende Herausforderung.

Althammer & Kill Akademie

KLICK/SCAN

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

10. September 2024 – kostenloses Webinar

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

In einer zunehmend digitalisierten Welt ist die Sicherheit von Netz- und Informationssystemen für den reibungslosen Betrieb und die Kontinuität von Unternehmen und kritischen Infrastrukturen von entscheidender Bedeutung.

Die NIS-2-Richtlinie, die jüngste Weiterentwicklung der NIS-Richtlinie (Network and Information Security), zielt darauf ab, die Cybersicherheit innerhalb der Europäischen Union weiter zu stärken und an die sich ständig verändernde Bedrohungslage anzupassen.

24. September 2024 – Online-Seminar

Workshop Verarbeitungsverzeichnis DSGVO, DSG-EKD & KDG

Zu den wesentlichen datenschutzrechtlichen Pflichten der Verantwortlichen und der Auftragsverarbeitenden gehört nach Art 30 DSGVO, § 31 DSG-EKD und § 31 KDG das Führen eines Verzeichnisses aller Verarbeitungstätigkeiten. Damit zählt das Verarbeitungsverzeichnis zu den speziellen Nachweispflichten gegenüber den Aufsichtsbehörden.

Der Workshop vermittelt und erarbeitet praxisorientiert die rechtlichen Grundlagen zum Führen eines solchen Verzeichnisses.

Ihre Ansprechpartnerin:

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

26. September 2024 – kostenloses Webinar

Vorbereitung auf NIS-2: Strategien für Gesundheits- und Sozialeinrichtungen

Mit dem aktuellen Referentenentwurf zum NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) wird deutlich, was auf Organisationen zukommt. Einrichtungen im Gesundheits- und Sozialwesen und andere Non-Profit-Unternehmen müssen im Rahmen ihrer Leistungsangebote prüfen, ob und in welchem Umfang sie von den neuen Vorgaben betroffen sind. Wir zeigen auf, was schon heute absehbar ist, welche Auflagen auf die Branche zukommen und wie NIS-2-Vorgaben nachhaltig in Organisationen umgesetzt werden können.

Sie erfahren, welche neuen gesetzlichen Anforderungen an die Gestaltung der IT-Sicherheit im Gesundheitswesen und in sozialen Einrichtungen gestellt werden. Wir erläutern im Detail, wie die Vorgaben durch die NIS-2-Verordnung und ergänzende Gesetzgebung in Deutschland zu verstehen und anzuwenden sind, um Maßnahmen zur Informationssicherheit und die Ausfallsicherheit von IT-Systemen in Organisationen zu verbessern.

20.–21. Januar 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. Sie haben einen internen oder externen Datenschutzbeauftragten? Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

Was macht eigentlich das EU-Lieferkettensorgfaltspflichtengesetz?

Schon am 23.02.2022 hatte die EU-Kommission einen ersten Vorschlag für eine europäische Lieferketten-Richtlinie vorgelegt: Unternehmen innerhalb der Europäischen Union sollen verpflichtet werden, die negativen Auswirkungen ihrer Wirtschaftstätigkeit, insbesondere in Bezug auf ihre globalen Lieferketten, auf Menschenrechte und Umwelt zu reduzieren. Erfahren Sie in diesem Beitrag alles Wichtige über Hintergrund, Inhalt und Komplexität bei der Umsetzung des EU-Lieferkettensorgfaltspflichtengesetzes.

Von Arne Wolff

Das neue EU-Lieferkettengesetz , welches international als Corporate Sustainability Due Diligence Directive (CSDDD oder auch CS3D) betitelt wird, wurde nach zähem Ringen am 24.04.2024 vom EU-Parlament und am 24.05.2024 vom Europäische Rat formell verabschiedet. Am 05.07.2024 wurde die Direktive im Amtsblatt der Europäischen Union veröffentlicht und ist somit am 25.07.2024 in Kraft getreten. Die EU-Mitgliedstaaten müssen die Richtlinie anschließend innerhalb von zwei Jahren in nationales Recht umsetzen – Deutschland wird dazu höchstwahrscheinlich das seit Januar 2023 geltende Lieferkettensorgfaltspflichtengesetz (LkSG) anpassen.

LkSG vs. CSDDD: Das deutsche und das europäische Lieferkettengesetz im Vergleich

Das Lieferkettensorgfaltspflichtengesetz (LkSG) und Corporate Sustainability Due Diligence Directive (CSDDD) unterscheiden sich in Umfang und Schwerpunkt.

Das LkSG deckt ein breites Spektrum an Risiken im Zusammenhang mit Menschenrechten und Umwelt ab, darunter:
- Zwangsarbeit
- Diskriminierung
- Rechte indigener Völker
- Schutz von Umweltlebensräumen und Forstwirtschaft

Drei spezifische umweltbezogene Abkommen werden ebenfalls vom Gesetz adressiert: die Minamata-Konvention, die Stockholmer Konvention und die Basler Konvention.

Das CSDDD ist weniger spezifisch, was den Umfang der zu bewertenden Menschenrechts- und Umweltaspekte angeht. Die Unternehmen werden verpflichtet, negative Auswirkungen, die während des gesamten Produktionslebenszyklus entstehen, allgemein zu identifizieren und zu adressieren, indem sie Maßnahmen ergreifen, um Missstände zu korrigieren. Beschränkte sich der Geltungsbereich des LkSG auf den eigenen Geschäftsbereich, die unmittelbaren Lieferanten und – bei konkreten Hinweisen – die mittelbaren

Lieferanten, umfasst der CSDDD die gesamte Wertschöpfungskette und alle wesentlichen vor- und nachgelagerten Geschäftsbeziehungen. Die vorgelagerte Wertschöpfungskette schließt alle Aktivitäten des Unternehmens ein, die zur Herstellung eines Produktes oder Erbringung von Dienstleistungen (Anbau, Zulieferer) beitragen.

Die nachgelagerte Kette bezieht sich auf sämtliche Aktivitäten der Geschäftspartner eines Unternehmens, beispielsweise Transport, Lagerung, Vertrieb oder Entsorgung. Abnehmer und Verbraucher fallen nicht darunter.

Geltungsbereich

Das LkSG gilt für alle juristischen Personen mit mehr als 1.000 Beschäftigten in Deutschland, die CSDDD nur für Kapitalgesellschaften (GmbH, AG, KG, KGaA, OHG), wobei die Schwelle stufenweise abgesenkt wird:
- **2027:** mehr als 5.000 Mitarbeitende, weltweiter Umsatz über 1,5 Mrd. €
- **2028:** mehr als 3.000 Mitarbeitende, weltweiter Umsatz über 900 Mio. €
- **2029:** mehr als 1.000 Mitarbeitende, weltweiter Umsatz über 450 Mio. €

Geldbußen

Bei Verstößen sieht das CSDDD Geldbußen bis zu fünf Prozent des weltweiten Nettoumsatzes vor – damit deutlich mehr als das LkSG, bei dem es zwei Prozent sind.

Es werden im EU-Lieferkettensorgfaltspflichtengesetz (CSDDD) jedoch mehr Rechtsbereiche geschützt. Auch eine eigenständige zivilrechtliche Haftungsregelung wird ergänzt.

EU-LkSG: Umsetzungsschwierigkeiten für Unternehmen

Die Umsetzung des EU-Lieferkettensorgfaltspflichtengesetzes birgt verschiedene Herausforderungen für Unternehmen. Eine der Hauptschwierigkeiten besteht darin, die gesamte Lieferkette zu erfassen, zu überwachen und zu kontrollieren. Oftmals sind Lieferketten komplex und global, wodurch es schwierig ist, alle beteiligten Unternehmen und Standorte zu identifizieren.

Darüber hinaus fehlen teilweise die erforderlichen Ressourcen und Kompetenzen, um eine angemessene Überprüfung durchzuführen. Auch können unterschiedliche Rechtsvorschriften in den verschiedenen EU-Staaten zu Inkonsistenzen und Unsicherheiten führen, was die Umsetzung zusätzlich erschwert. Eine effektive Umsetzung des Gesetzes trotz dieser Herausforderungen ist entscheidend, um Menschenrechtsverletzungen und Umweltschäden entlang der Lieferketten zu verhindern und die unternehmerische Verantwortung zu stärken.

Althammer & Kill: Ihre kompetenten Compliance-Experten

Die Verabschiedung verbindlicher Compliance-Anforderungen und -Standards zur menschenrechtlichen Sorgfaltspflicht ist ein wichtiger Schritt hin zu einer verantwortungsvolleren und nachhaltigeren Weltwirtschaft. Eine EU-weite Regelung schafft Chancengleichheit und verleiht dem Anliegen ungleich mehr Gewicht.

Deutsche Unternehmen, die noch nicht unter das LkSG fallen, sollten jetzt prüfen, ob sie zum erweiterten Geltungsbereich des EU-Lieferkettensorgfaltspflichtengesetzes (CSDDD/CS3D) gehören.

Wenn Sie Unterstützung bei dieser Einschätzung benötigen, wenden Sie sich an Althammer & Kill für eine individuelle Compliance-Beratung. Von der Durchführung von Risikoanalysen über die Entwicklung und Implementierung von Richtlinien, Strategien und Verfahren bis hin zu Schulungen für Mitarbeitende – mit Fachwissen und langjähriger Erfahrung helfen wir Organisationen dabei, die Anforderungen des Gesetzes zu erfüllen. &

Hinter den Kulissen des Vertriebsalltags

Die Kunst des Zuhörens und Verstehens im Vertrieb.
So entstehen Lösungen, die wirklich passen.

Wer bist du? Welche Ausbildung hast du?

Silvio: Ich bin Silvio, 46 Jahre alt. Nach zwei technischen Ausbildungen bin ich seit über 20 Jahren im Vertrieb tätig, spezialisiert auf IT/Software und Beratungsdienstleistungen im Gesundheits- und Sozialwesen. Mein technisches Know-how und Vertriebserfahrung ermöglichen es mir, meine Kunden optimal zu unterstützen und passende Lösungen anzubieten.

Wie lange arbeitest du schon bei Althammer & Kill?

Silvio: Ich arbeite seit 2,5 Jahren bei Althammer & Kill.

Wie hat es dich nach Althammer & Kill verschlagen?

Silvio: Ich kenne Thomas Althammer seit über 10 Jahren. Als 2022 die Gelegenheit zur vertrieblichen Unterstützung bei Althammer & Kill kam, brachte ich mein umfassendes Vertriebs-Know-how im IT/Software- und Beratungsbereich gerne ein.

Was sind deine Aufgaben? Wie sieht dein Alltag aus?

Silvio: Meine Hauptaufgabe ist es, mit Kunden über ihre Herausforderungen zu sprechen und maßgeschneiderte Lösungen zu entwickeln. Mein Alltag umfasst intensive Kundenkommunikation, Zusammenarbeit mit unserem Expertenteam und den Austausch mit Verbänden, die unseren fachlichen Input schätzen. Wichtig: Die Kaffeemaschine muss immer in Reichweite stehen.

Warum bist du Vertriebler geworden?

Silvio: Mich reizt die Schnittstelle zwischen Unternehmen und Kunden. Ich entwickle gemeinsam mit den Kunden konkrete Ideen, die echten Nutzen bringen. Die selbstbestimmte und lösungsorientierte Arbeitsweise im Vertrieb begeistert mich. Vertrieb ist meine Leidenschaft.

Wie unterscheidet sich der Vertrieb einer Dienstleistung vom Vertrieb eines Produkts?

Silvio: Der Vertrieb von Produkten und Dienstleistungen unterscheidet sich vor allem in der Art und Weise, wie der Kundennutzen vermittelt wird. Bei einem Produkt ist der Nutzen oft klar und direkt ersichtlich. Dienstleistungen hingegen sind flexibler und variabler, was bedeutet, dass es besonders wichtig ist, genau mit dem Kunden über seine spezifischen Bedürfnisse und Anforderungen zu sprechen. Dabei handelt es sich oftmals um Kriterien, die sich nicht klar in Zahlen oder Ja/Nein ausdrücken lassen.

Erst wenn der genaue Bedarf ermittelt ist, kann man einen maßgeschneiderten Leistungsumfang anbieten. Wenn man dem Kunden nicht aufmerksam zuhört oder nicht genügend nachfragt, besteht die Gefahr, dass das Angebot nicht optimal auf seine Bedürfnisse abgestimmt ist und der Kunde sich nicht gut betreut fühlt.

Wie läuft der Prozess von der ersten Interessenbekundung hin zur Unterschrift des Kunden ab?

Silvio: Der Prozess beginnt damit, dass ich bei meinem Gesprächspartner Interesse wecke und Themen anspreche, über die er möglicherweise noch nicht nachgedacht hat. Wenn es mir gelingt, seine Neugier zu wecken und eine Vertrauensbasis aufzubauen, entsteht die Grundlage für eine mögliche Zusammenarbeit. Dieses Vertrauen entscheidet darüber, ob der Kunde uns als Teil der Lösung sieht und eine Zusammenarbeit in Betracht zieht. Sobald dieses Vertrauen aufgebaut ist und der Bedarf klar definiert wurde, entwickeln wir gemeinsam einen maßgeschneiderten Lösungsansatz, der letztendlich zu einer Zusammenarbeit führt.

Welche Themen beschäftigen unsere Kundinnen und Kunden besonders?

Silvio: Derzeit beschäftigen sich viele Organisationen intensiv mit dem Thema Informationssicherheit. Sie suchen nach Lösungen, um das Bewusstsein und die Sicherheitsstrukturen innerhalb ihrer Unternehmen zu stärken. Dieses Thema wird nicht mehr nur von IT-Leitern, sondern auch von Geschäftsführern und Vorständen als äußerst wichtig angesehen.

„Ein guter Vertriebsprofi hört aufmerksam zu und stellt gezielte Fragen.“

Zusätzlich stehen viele Unternehmen vor der Herausforderung, mit den schnellen Entwicklungen im Bereich der Künstlichen Intelligenz (KI) Schritt zu halten. Da es in diesem Bereich noch nicht den Erfahrungshorizont von Jahrzehnten gibt, sehen sich viele vor großen Fragen und Unsicherheiten. KI bietet zwar immense Möglichkeiten und kann einen erheblichen Nutzen für Unternehmen bringen, aber es ist entscheidend, von Anfang an den Einsatzrahmen klar zu definieren und die Mitarbeiter entsprechend zu schulen, um den Datenschutz nicht zu gefährden.

Was gefällt dir besonders an deiner Tätigkeit bei Althammer & Kill?

Silvio: Besonders schätze ich das selbstbestimmte Arbeiten bei Althammer & Kill, das von großem Vertrauen geprägt ist. Viele Arbeitgeber streben danach, ein solches Arbeitsumfeld zu schaffen, doch nur wenigen gelingt es tatsächlich. Bei Althammer & Kill erleben wir eine Zusammenarbeit auf Augenhöhe, bei der alle Beteiligten gemeinsame Ziele verfolgen. Das ist für mich das Beste, was einem Unternehmen passieren kann und trägt maßgeblich zu meiner Zufriedenheit und Motivation bei.

Was waren bisher deine Highlights bei Althammer & Kill?

Silvio: Ein besonderes Highlight war unser erstes Teamevent, bei dem ein Beraterkollege und ich spontan die Idee hatten, trotz der niedrigen Temperaturen im nahegelegenen See am Abend schwimmen zu gehen. Anfangs waren wir nur zu zweit und wurden von den anderen Kollegen etwas belächelt. Doch nach kurzer Zeit gesellten sich immer mehr dazu, und innerhalb von 15 Minuten waren über 20 Personen im See – ein riesiger Spaß! Dieses Ereignis hat uns nicht nur viel Freude bereitet, sondern auch gezeigt, wie stark der Teamgedanke bei Althammer & Kill gelebt wird.

Wie schaffst du es, fremde Menschen immer wieder in Gespräche zu verwickeln? Wie geht’s du auf Leute zu?

Ein guter Vertriebsprofi hört aufmerksam zu und stellt gezielte Fragen. Durch aktives Zuhören und präzises Nachfragen zeige ich echtes Interesse und finde heraus, welche Themen für mein Gegenüber relevant sind. So stelle ich eine authentische Verbindung her und führe bereichernde Gespräche. &

ALTHAMMER & KILL

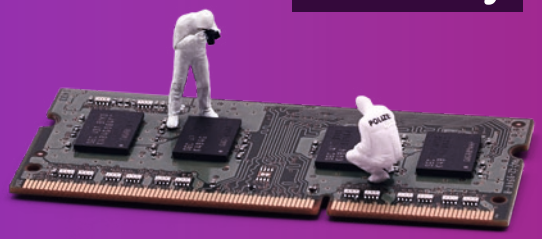
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

Wir sind Digitalisierungskenner, Datenversteher und Vorwärtsdenker –
Ihr Experte für Datenschutz, Informationssicherheit, Cloud- & Cyber-Security und Compliance.
Unsere 45 Mitarbeitenden bringen Digitalisierung und Datenschutz bundesweit in Einklang.

Datenschutz

Informations-sicherheit

Cloud- & Cyber-Security



Compliance

althammer-kill.de

KLICK/SCAN