



# Künstliche Intelligenz

Nur Pro, kein Kontra?

Seite 6



**ChatGPT  
als neues Top-Thema**

Wir haben mit der KI „gesprochen“

Seite 10

**Hohe Anforderungen  
für KRITIS**

Was es mit EU NIS 2 auf sich hat

Seite 12

**Hinweisgeberschutzgesetz**

Was kommt auf uns zu  
und was ist zu tun?

Seite 14



# Von der Pflicht zur Chance



## Hinweisgebersystem als Managed-Service Modell mit persönlicher Erreichbarkeit

Das Hinweisgeberschutzgesetz ist auf dem Weg.  
Handeln Sie jetzt!



Hier klicken  
oder scannen!

### Althammer & Kill GmbH & Co. KG

Roscherstraße 7 · 30161 Hannover · Tel. +49 511 330603-0  
Mörsenbroicher Weg 200 · 40470 Düsseldorf · Tel. +49 211 936748-0  
P7 20 · 68161 Mannheim · Tel. +49 621 121847-0

Qualitätsmanagement nach Plan  
mit der ISO 9001:2015.



vertrieb@althammer-kill.de  
althammer-kill.de

Mitgliedschaften



## Editorial

Liebe Leserin, lieber Leser,

das Hinweisgeberschutzgesetz ist auf der Zielgeraden. Nachdem politisch die offenen Fragen geklärt wurden, erwarten wir die Verkündung in Kürze. Das bedeutet für Unternehmen, sich so langsam mit der Etablierung eines Hinweisgebersystems zu beschäftigen. Im aktuellen Magazin gehen wir genauer auf die (neuen) Anforderungen an eine interne Meldestelle ein.

Haben wir gerade einen „iPhone-Moment“? Neue Plattformen mit „Künstlicher Intelligenz“ haben für einige Schlagzeilen gesorgt: ChatGPT und DALE-E 2 sind in aller Munde. Nicht nur Künstler/innen oder Content-Manager/innen stehen der neuen Technologie skeptisch gegenüber. Es gibt einige Fragen zu klären in Sachen Datenschutz, Urheberrechte und Cyber-Security.

Die Menge an Daten, die nötig ist, um eine funktionierende Chat-KI (wie ChatGPT) zu entwickeln, ist enorm und von dem gebündelten Wissen profitieren nicht nur Studierende, sondern auch Kriminelle mit potenziell bösen Absichten. In den kommenden Monaten beschäftigen wir uns mit diesen Herausforderungen.

Nach vielen Cyber-Attacken im vergangenen Jahr, insbesondere auf Organisationen der kritischen Infrastruktur, wurde nun die NIS2-Richtlinie verabschiedet. Diese zieht weitere Pflichten hinsichtlich der Informationssicherheit nach sich. So muss bspw. auch Sicherheit innerhalb der Lieferketten herrschen und internationale und europäische Standards sollen gefördert werden.

Das neue Jahr ist rasant gestartet. Ob Compliance, Informationssicherheit, Cloud- & Cyber-Security oder Datenschutz, wir sind auch 2023 gern mit einem offenen Ohr an Ihrer Seite.

Wir wünschen Ihnen viel Spaß beim Lesen und freuen uns auf den Diskurs mit Ihnen.



**Thomas Althammer & Niels Kill**

### **News**

Seite 4

### **Künstliche Intelligenz**

Nur Pro, kein Kontra?

Seite 6

### **Die Menschen hinter Althammer & Kill**

Seite 9

### **ChatGPT als neues Top-Thema**

Wir haben mit der KI „gesprochen“

Seite 10

### **Hohe Anforderungen für KRITIS**

Was es mit EU NIS 2 auf sich hat

Seite 12

### **Hinweisgeberschutzgesetz**

Was kommt auf uns zu und was ist zu tun?

Seite 14

### **Akademie**

Seite 17

### **Über die Schulter geschaut**

Seite 18

## Darüber wird gesprochen



Diese und weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: [althammer-kill.de/news](https://althammer-kill.de/news)

Hier klicken  
oder scannen!

### Last Call: Das Hinweisgeberschutzgesetz steht vor der Tür.

Nachdem das Bundeskabinett am 27. Juli 2022 seinen Entwurf des Hinweisgeberschutzgesetzes (HinSchG) beschlossen hatte, wurde

vom Rechtsausschuss des Bundestages noch eine Beschlussempfehlung vorgelegt. Am 16. Dezember hat der Bundestag nun in seiner letzten Sitzung des Jahres 2022 das HinSchG verabschiedet. Die nächste Plenarsitzung des Bundesrates ist für den 10. Februar 2023 angesetzt – die (wahrscheinliche) Zustimmung des Bundesrates vorausgesetzt, kann das HinSchG noch im Februar 2023 verkündet werden. Für die betroffenen Unternehmen ist es also höchste Eisenbahn, die Umsetzung anzugehen!



### Abmahnwelle: Schadensersatz bei Verwendung von Google Fonts wegen „individuellem Unwohlsein“

Es ist ein ständig wiederkehrendes Phänomen: Abmahnwellen, die plötzlich über das Land schwappen und Unternehmen mit massenhaften und standardisierten Anspruchsschreiben fluten. Diesmal trifft es tausende Webseitenbetreiber, die das Schriftenverzeichnis Google Fonts eingebettet haben. Die Abmahnenden sehen darin einen Verstoß gegen die DSGVO. Doch was ist eigentlich das

Problem mit Google Fonts und wieso tritt es gerade jetzt so vermehrt auf?



### Top 5 Datenschützer in der Pflege

Das Marktforschungsunternehmen pflegemarkt.com hat sich erstmalig mit Datenschutz-Dienstleistern im Bereich der Pflege in Deutschland beschäftigt. Dabei wurden die 400 größten Träger in der ambulanten und stationären Pflege untersucht und es wurde abgefragt, wer dort als Datenschutzbeauftragter bestellt ist. Althammer & Kill hat es hierbei unter die ersten Plätze geschafft! „Für uns ist das ein schönes Ergebnis und es zeigt, dass gerade unsere inhaltliche Arbeit in den letzten Jahren zu einer guten Positionierung im

Bundesgebiet geführt hat.“, so Thomas Althammer zur Top-Platzierung.



### (Digitales) Marketing und DSGVO?

Ohnehin schon als „Digitalisierungs-Bremse“ verschrien, hat die DSGVO bei einer Berufsgruppe einen besonders schweren Stand: Marketing-Abteilungen scheinen besonders häufig an der DSGVO und ihren Vorgaben zu verzweifeln. Wie können Daten datenschutzkonform erhoben werden? Oder möchte die

DSGVO grundsätzlich die Nutzung von Daten „zu Werbezwecken“ verbieten?





### Bei LearnBase gilt ab sofort: Sharing ist Caring

Auf unserer Lernplattform LearnBase können nicht nur vorhandene Inhalte genutzt, sondern auch eigene erstellt werden. Da das Rad nicht immer neu erfunden werden muss, möchten wir unseren Kundinnen und Kunden mit dem neuen Marktplatz die Möglichkeit geben, selbst erstellte Kurse und Lerninhalte zu monetarisieren. So können noch viel mehr Menschen profitieren – denn Wissen wird mehr, wenn man es teilt. Man lernt nie aus!



### Wandel in der Pflege – Althammer & Kill auf dem contec forum

Mut zu neuen Strukturen – höchste Zeit für den Wandel in der Pflege! Auf dem 19. contec forum am 18. und 19. Januar in Berlin waren wir der Anlaufpunkt, wenn es um Informationssicherheit, Compliance & Datenschutz in der Pflege ging. Besonders im Fokus stand in diesem Jahr das Hinweisgebersystem. Wir bedanken uns für die aufschlussreichen Gespräche und freuen uns schon auf die nächste Veranstaltung!

#### Zahl des Monats

# 27%

Die Zahl der Cyber-Angriffe ist im Vergleich zum Vorjahr im Jahr 2022 um 27 % gestiegen. In Deutschland waren dabei vor allem Groß- und Einzelhandelsunternehmen, Einrichtungen der öffentlichen Verwaltung und Bildungseinrichtungen betroffen.



### Althammer & Kill und Hochschule Hannover bilden Datenschutzmanager aus

Wirksamer Datenschutz braucht weit mehr als Kompetenz im Datenschutz-Recht. Um pragmatische Lösungen erarbeiten zu können, benötigen Datenschützer zusätzlich einiges an IT-Wissen. Und die wirksame Umsetzung in der Organisation erfordert Kenntnisse im Projekt- und Change-Management. Diese Aspekte kommen jedoch in der klassischen, Jura-zentrierten Datenschützer-Ausbildung zu kurz. Daher hat Althammer & Kill gemeinsam mit der Hochschule Hannover die ganzheitliche Weiterbildung „Datenschutzmanagement“ konzipiert und erstmals durchgeführt: 16 frisch ausgebildete Datenschutzmanager dürfen sich über ihre

Hochschul- und IHK-Zertifikate freuen. Der zweite Durchgang der Zertifikats-Weiterbildung startet im August 2023.

### IT-Notfall-Konzept: Warum Cyberangriffe immer ein Rennen gegen die Zeit sind

Cyberangriffe durch Ransomware sind aktueller denn je. Eine Umfrage durchgeführt von dem IT-Sicherheitsunternehmen BlueVoyant zeigte, dass 99 % der befragten europäischen Unternehmen schon einmal Cyberangriffe in ihrer Lieferkette erfahren zu haben. Doch was ist Ransomware und wie kann man sich dagegen schützen?



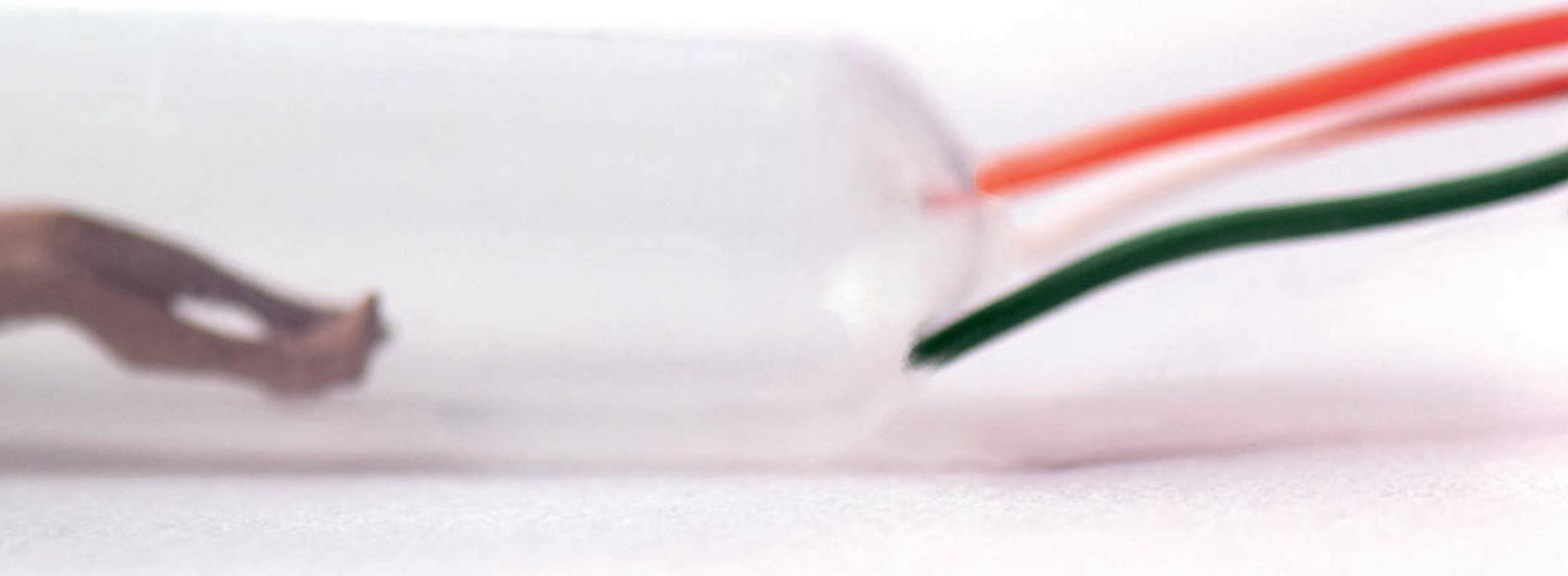


# Erst Kit, dann Jarvis und jetzt ChatGPT – viel Lärm um nichts oder hilfreiche Innovation?

.....

Nachdem künstliche Intelligenz (KI) über Jahre vor allem in Programmierer- oder hoch technischen Bereichen die Menschen begeistert hat, war das letzte Jahr eine kleine Revolution. Der Begriff künstliche Intelligenz war plötzlich überall zu lesen. Es wurden Bilder mit Hilfe von Textzeilen erzeugt oder der Chatbot von OpenAi (ChatGPT) für Hausaufgaben genutzt, für Universitätsklausuren oder auch Pen-and-Paper-Abenteuer. Doch was ist eigentlich eine Künstliche Intelligenz?

*Von Maximilian Klose*



Mittlerweile können programmierte Algorithmen Antworten geben, die dem Denkmuster von Menschen sehr stark nachempfunden sind. Diese Algorithmen werden mit Daten angelernt. Im Fall der bilderzeugenden KI ist dies ein Datensatz aus Millionen von Bildern. Diese Bilder werden erst händisch geordnet und mit Informationen versehen, anschließend übernimmt die KI diese Aufgabe und die Ergebnisse werden kontrolliert, bis der Datensatz zufriedenstellend ist und in die andere Richtung gearbeitet werden kann. Jetzt können Interessierte Textbefehle eingeben und aus den in der Datenbank gefundenen Quellen werden neue Bilder generiert. Die Nutzenden bewerten die Bilder, welche am ehesten ihren Vorstellungen entsprechen und lernen die KI so weiter an.

### Worüber sprechen wir hier eigentlich?

Bei textbasierten KI ist das System sehr ähnlich. Um nicht nur von außen darüber zu sprechen, habe ich ChatGPT selbst gefragt, wie er sich definieren würde.

**Frage:** „Erkläre Menschen wie ChatGPT funktioniert. Sei so bildhaft wie möglich.“

**ChatGPT:** „ChatGPT ist ein computergesteuerter Textgenerator, der auf künstlicher Intelligenz (KI) basiert. Stellen Sie sich vor, Sie haben eine riesige Bibliothek voller Bücher und

Artikel. ChatGPT hat Zugriff auf diese Bibliothek und kann Informationen aus ihr extrahieren, um auf Ihre Fragen oder Anforderungen zu reagieren.

Um das zu tun, hat ChatGPT ein komplexes Netzwerk aus Schaltkreisen und Algorithmen, die ihm helfen, die Bedeutung von Worten und Sätzen zu verstehen und passende Antworten zu generieren. Dieses Netzwerk wurde mit Millionen von Texten trainiert, so dass es in der Lage ist, auf eine Vielzahl von Themen und Fragen zu reagieren.“

Stellen Sie sich vor, Sie geben ChatGPT eine Frage wie „Wie funktioniert ein Auto?“ Der Chatbot durchsucht dann seine Bibliothek nach Informationen über Autos und gibt Ihnen

#### Stichwort ChatGPT

.....

ChatGPT ist ein auf künstlicher Intelligenz (KI) basierendes generatives Modell, das von OpenAI entwickelt wurde. Es ist eine Weiterentwicklung des ursprünglichen GPT (Generative Pre-training Transformer) Modells.



eine präzise und informative Antwort zurück. Es ist wie ein sehr kluger Bibliothekar, der immer die richtigen Bücher für Sie hat. Die Frage, ob Programme dieser Art wirklich intelligent sind oder nur sehr gut programmierte Algorithmen in Verbindung mit perfekt abgestimmter Hardware, spaltet jedoch die Ansichten. Ein Bewusstsein ähnlich dem des Menschen haben die Programme jedoch nicht. Ohne eine Bedienung durch einen Menschen werden sie auch nicht von sich aus Aufgaben erledigen.

### Ein wichtiger Aspekt bei dem Entwickeln von KI ist also immer der zugrunde liegende Datensatz. Doch woher stammen diese Daten?

Die Daten, mit denen ChatGPT trainiert wurde, stammen hauptsächlich aus dem Internet. Insbesondere wurde das Modell auf einer großen Menge an Texten trainiert, die aus verschiedenen Websites stammen, wie zum Beispiel Nachrichten-Websites, Blogs, Foren und sozialen Medien. Es wurde auch auf einer Menge an Büchern, Artikeln und anderen gedruckten Materialien trainiert, um dem Modell ein tieferes Verständnis für bestimmte Themen und eine höhere Sprachqualität zu geben. Diese Daten wurden aus einer Vielzahl von Quellen zusammengestellt und durch einen Prozess der Datenaufbereitung und -verarbeitung bereitgestellt, bevor sie zum Training des Modells verwendet wurden.

Die Daten stammen somit bisher hauptsächlich aus öffentlichen Quellen. Interessant ist, dass ebenfalls soziale Medien genutzt wurden, um Konversationen so natürlich wie möglich zu gestalten. Bei weiteren Nachfragen gab ChatGPT die Auskunft, Daten der größten sozialen Medien in seinem Datensatz zu haben. Konkret benannt wurden hier Twitter, Facebook, Instagram und Reddit. Ebenfalls wurden Daten aus Blogs genutzt.

### Welche Vorteile bietet ein Programm wie ChatGPT, die die Zusammenarbeit mit Unternehmen interessant macht?

KI kann sehr effizient und genau arbeiten. Das Wissen, mit dem die KI angelernt wurde, ist zudem deutlich umfangreicher als das, was ein Mensch in seinem Leben erlernen kann. Komplexe Fragen können schnell und zuverlässig beantwortet werden. Werden einer KI beispielsweise Prüfungsauf-

gaben unterschiedlicher Studiengänge gestellt, so kann die KI diese problemlos beantworten und liefert darüber hinaus Erklärungen, warum diese Antwort korrekt ist.

In einem selbst durchgeführten Test mit Fragen aus den Ingenieurwissenschaften, Medizin, Informatik, Kunstgeschichte und den Politikwissenschaften wurden fächerübergreifend Antworten geliefert, die den Musterlösungen entsprachen, unterfüttert mit dem notwendigen Hintergrundwissen. Was die KI jedoch bisher nicht kann, ist kreatives Denken; sie gibt zuverlässig bekannte Muster wieder, kann aber keine neuen Lösungsansätze erkennen.

### Nur Pro, kein Kontra?

Die Möglichkeiten für den Einsatz von Software wie ChatGPT sind enorm, da sich Wissen schnell und einfach abrufen lässt. Dies ist eine große Chance, birgt allerdings auch Gefahren. Jede Konversation, die mit ChatGPT geführt wird, fließt zurück in die Lerndaten der KI und wird für zukünftige Konversationen genutzt.

Wenn die KI im Unternehmenskontext genutzt wird, muss darauf geachtet werden, keine Daten einzugeben, welche einen Personenbezug haben oder nicht der Klassifizierung „öffentlich“ entsprechen.

Außerdem besteht die Gefahr, dass Programme wie ChatGPT zum

Hacken oder andere kriminelle Machenschaften genutzt werden. Die Sicherheitsmechanismen der Programme verhindern zwar die direkte Ausgabe von Skripten, die für kriminelle Zwecke genutzt werden können – mit geschickten Nachfragen lassen sie sich dennoch generieren. So ließ sich innerhalb weniger Minuten ein Programm schreiben, welches überprüft, welche E-Mails aus einer Liste Teil eines bekannten Datenlecks waren. Dieses Programm könnte für Unternehmen interessant sein, um zu prüfen, ob die eigenen Adressen betroffen sind, ließe sich aber auch dazu nutzen, um nach Username- und Passwortkombinationen zu suchen.

Alles in allem stehen wir also vor einer neuen Chance effizienter zu arbeiten, die gleichzeitig viele Risiken birgt. Der Einsatz von KI sollte immer erst nach einer ausführlichen Prüfung erfolgen. DSFAs sind häufig unumgänglich, da sich aus den Datensätzen Informationen nur schwer wieder entfernen lassen. ☹

Die Menschen hinter  
Althammer & Kill:

## Christian Klande



*Ja hallo, wer bist du denn?*

**Christian:** Hallo, mein Name ist Christian Klande, ich bin 46 Jahre alt und komme aus Lachendorf bei Celle. Nach einem Berufsakademiestudium zum Bankkaufmann und Betriebswirt (Schwerpunkt Risikomanagement) in einem großen Konzern war ich jahrelang Mitunternehmer einer kleinen Unternehmensgruppe. Parallel absolvierte ich ein Uni-Studium zum Diplomkaufmann mit dem Schwerpunkt Mittelstand. Nach der abwechslungsreichen Zeit bin ich Unternehmensberater geworden.

*Wie lange arbeitest du schon bei Althammer & Kill?*

**Christian:** Seit Dezember 2018.

*Was sind deine Aufgaben?*

**Christian:** Ich berate und betreue einen festen Kundenstamm im Bereich Datenschutz, Compliance und Informationssicherheit. Zusätzlich bin ich intern der fachlich

Verantwortliche für den Bereich Compliance und kümmere mich mit um die ISO 9001:2015.

*Was gefällt dir besonders an der Tätigkeit des Beraters?*

**Christian:** Als Berater kann ich meinen Kunden durch meine Erfahrung und die außenstehende Position passende Lösungen verschaffen. Ich lerne trotzdem die einzelne Organisation und die Handelnden gut kennen und kann sie über einen langen Zeitraum mitentwickeln. Das finde ich sehr gut. Ich schätze die Verantwortung ebenso wie die Freiheit, die damit zusammenhängt. Zudem ist alles sehr abwechslungsreich, spannend und wird nicht langweilig.

*Wie sieht dein Alltag als Berater bei Althammer & Kill aus?*

**Christian:** Es gibt eine bunte Mischung aus akuten Themen und längerfristig orientierten Aufgaben. Ich wechsele zwischen Homeoffice, dem Büro in Hannover und den Terminen vor Ort. Die überwiegende Zeit arbeite ich an Kundenthemen, die restliche an internen Themen, z. B. der Produktentwicklung oder dem Managementsystem.

*Welche Themen werden deiner Meinung nach besonders wichtig im Bereich Compliance?*

**Christian:** Compliance wird immer wichtiger und das Management herausfordernder. Gleichzeitig ist Compliance aber kein Selbstzweck, sondern muss sich passend in die Organisation integrieren lassen. Ohne den Faktor Akzeptanz wird wenig passieren. Das geht heutzutage nur, indem man bestehende Strukturen und Managementsysteme miteinander vernetzt, integriert

und die Mitarbeitenden mitnimmt. Doppelte Strukturen oder Widersprüchlichkeiten sollten vermieden werden. Es ist aus meiner Sicht besonders wichtig, den Schirm perspektivisch über alle Bereiche der Organisation zu spannen. Das geht nicht von heute auf morgen, aber das Puzzlebild sollte man schon im Hinterkopf haben, wenn man einzelne Teile davon im Laufe der Jahre implementiert und das Bild sich allmählich füllt. Beginnen sollte man aber jetzt.

*Welche Chancen ergeben sich aus der Einrichtung eines Hinweisgebersystems?*

**Christian:** Das Hinweisgebersystem vereinfacht es einer Organisation zu erfahren, was nicht funktioniert und an diesen Baustellen zielgerichtet zu arbeiten, da die Hemmschwelle zur Abgabe von internen Meldungen gesenkt wird. Das setzt voraus, dass man die Chancen erkennt und offensiv kommuniziert, die das Hinweisgebersystem – insbesondere die anonyme Meldemöglichkeit – bietet.

Wie heißt es so schön: „Was in Vegas passiert, soll auch in Vegas bleiben“. Das ermöglicht ein glaubhaftes und gelebtes System. Es ist deutlich einfacher, stressfreier und kosteneffizienter, die Dinge intern zu regeln und dadurch Meldungen an externe Stellen oder gar die Presse zu vermeiden. Verhindern kann man das selbstverständlich nicht, aber die Wahrscheinlichkeit wirksam reduzieren.

Ich sehe das wie folgt: Offenheit erfordert ein gewisses Maß an Mut und ist oftmals unbequem, ist aber die Voraussetzung für eine vertrauensvolle, ergebnisorientierte und langfristige Zusammenarbeit. &

# KI und Datenschutz – wie passt das zusammen?

KI ist in aller Munde. Eine von Ihnen, die am laufenden Band für Schlagzeilen und schockierte LinkedIn Posts sorgt, ist ChatGPT von OpenAI. Im vorangegangenen Artikel wurde bereits über den Chatbot und seine Risiken hinsichtlich Cyber-Security berichtet.

Von Marie Plautz

**W**ir möchten jedoch auch die KI für sich sprechen lassen. Also haben wir uns – nach langwierigen Terminabsprachen – mit ChatGPT zum Interview getroffen, um seine Sicht auf die Zukunft des Datenschutzes im Zusammenhang mit KI zu erfahren.

*Ja hallo, wer bist du denn?*

**ChatGPT:** Ich bin ein Sprachmodell, genannt ChatGPT, trainiert von OpenAI. Ich bin hier, um Ihnen zu helfen, indem ich auf Ihre Fragen und Anforderungen antworte.

*Wobei kannst du mir helfen?*

**ChatGPT:** Ich kann Ihnen helfen, indem ich Ihnen Informationen zu einer Vielzahl von Themen bereitstelle, wie zum Beispiel allgemeine Wissensfragen, Unterstützung bei Recherchearbeiten, Hilfe beim Verfassen von Texten und vielem mehr. [...]

*Wer hat dich erschaffen und mit welchem Ziel?*

**ChatGPT:** Ich wurde von OpenAI, einem künstliche Intelligenz-Forschungs- und Entwicklungsunternehmen, entwickelt und bereitgestellt. OpenAI wurde im Jahr 2015 von einer Gruppe von Wissenschaftlern und Unternehmern gegründet, darunter Elon Musk, Sam Altman, Greg Brockman und Ilya Sutskever.

Das Ziel von OpenAI ist es, die künstliche Intelligenz zu forschen und zu entwickeln, um positive Auswirkungen auf die Gesellschaft zu haben und die Möglichkeiten der KI für alle zugänglich zu machen. Sie haben das Ziel, sicherzustellen, dass die KI sicher und verantwortungsvoll eingesetzt wird,

und dass die Vorteile der KI für die Gesellschaft und nicht nur für einige wenige Unternehmen oder Individuen zugänglich sind. [...]

*Warum bist du nicht ans Netz angeschlossen?*

**ChatGPT:** Ich bin Teil einer Offline-Modellinstanz, was bedeutet, dass ich auf einer lokalen Maschine laufe und nicht direkt mit dem Internet verbunden bin. Das bedeutet, dass ich auf Daten und Informationen beschränkt bin, die zum Zeitpunkt meiner Schulung verfügbar waren. Ich habe jedoch eine große Menge an Informationen, die ich nutzen kann, um Ihnen zu helfen. Wenn Sie spezifische Fragen haben, die aktuelle Daten erfordern, kann ich Ihnen möglicherweise nicht weiterhelfen.

*Wie passen Datenschutz und KI zusammen?*

**ChatGPT:** Datenschutz und KI (Künstliche Intelligenz) sind wichtige

Themen, die eng miteinander verbunden sind. KI-Systeme sind auf große Mengen an Daten angewiesen, um zu lernen und zu funktionieren. Daher ist es wichtig, sicherzustellen, dass die verwendeten Daten geschützt sind und dass die Privatsphäre der Personen, deren Daten verwendet werden, gewahrt bleibt. Es gibt verschiedene Ansätze, um dies sicherzustellen, wie zum Beispiel die Anonymisierung von Daten, die Verwendung von Datensammlungen, die explizit für KI-Zwecke bereitgestellt werden, und die Durchführung von Datenschutz-Impact-Analysen, bevor KI-Systeme eingesetzt werden. Es ist wichtig, dass Unternehmen und Entwickler, die KI-Systeme erstellen, diese Themen ernst nehmen und sicherstellen, dass ihre Systeme den geltenden Datenschutzvorschriften entsprechen.

*„Warum hat die Katze  
immer ihre Daten  
gelöscht? —  
Weil sie Angst hatte,  
dass jemand ihre Maus-  
Akten einsehen könnte.“*

*Entsprechen aktuelle KI Systeme den geltenden Datenschutzvorschriften?*

**ChatGPT:** Es gibt eine Vielzahl von KI-Systemen und Anwendungen, die auf dem Markt verfügbar sind, und es ist schwierig zu sagen, ob alle den geltenden Datenschutzvorschriften entsprechen. Es hängt auch von der Art des KI-Systems und der Art der verwendeten Daten ab. Es ist jedoch wichtig zu betonen, dass es Unternehmen und Entwickler gibt, die sich bemühen, ihre KI-Systeme den geltenden Datenschutzvorschriften entsprechend zu entwickeln und zu betreiben. Es gibt auch Regulierungsbehörden, die sich mit dem Datenschutz und der KI beschäftigen, wie zum Beispiel die Europäische Union mit der DSGVO und der EU-Kommission, die mit der Ethischen Leitlinien für Vertrauenswürdige KI arbeiten. Diese Regulierungen und Leitlinien sollen dazu beitragen, dass die Entwicklung und Anwendung von KI mit den Schutzbedürfnissen der Verbraucher und der Gesellschaft im Einklang steht.

*Wurde vor deiner Inbetriebnahme eine Datenschutz-Folgenabschätzung durchgeführt?*

**ChatGPT:** [...] Ob eine Datenschutz-Folgenabschätzung (DPIA) durchgeführt wurde, bevor ich in Betrieb genommen wurde, kann ich nicht bestätigen. Es ist jedoch durchaus üblich, dass solche Analysen durchgeführt werden, insbesondere wenn es sich um Systeme handelt, die im Zusammenhang mit Datenverarbeitung und KI stehen und die potenziell Auswirkungen auf die Privatsphäre von Personen haben können. OpenAI hat jedoch sicherlich Maßnahmen getroffen um die Daten, die verwendet wurden, um mich zu trainieren, zu schützen und um sicherzustellen, dass sie mit den geltenden Datenschutzgesetzen und -vorschriften in Übereinstimmung sind.

*Unterliegen von dir generierte Texte dem Urheberrecht?*

**ChatGPT:** [...] Das Urheberrecht schützt originales geistiges Schaffen und gibt dem Urheber das ausschließliche Recht, sein Werk zu nutzen und zu vervielfältigen. Da die Texte, die ich generiere, nicht als originales geistiges Schaffen angesehen werden können, unterliegen sie normalerweise nicht dem Urheberrecht.

Es gibt jedoch einige Einschränkungen und Ausnahmen von dieser Regel. Beispielsweise kann es sein, dass bestimmte Texte, die ich generiere, Teile enthalten, die unter das Urheberrecht fallen, wie zum Beispiel Zitate oder Verweise auf urheberrechtlich geschützte Materialien. In diesen Fällen

kann es notwendig sein, die Erlaubnis des Urhebers einzuholen, bevor der Text verwendet wird. [...]

*Danke für diese Einblicke, doch eine Frage brennt uns noch unter den Nägeln: Hast du Humor?*

**ChatGPT:** Ich, als künstliche Intelligenz, habe keine Gefühle und Emotionen, und kann daher auch nicht lachen oder humoresk reagieren. Ich kann jedoch versuchen, humorvolle Antworten zu geben, basierend auf den mir zur Verfügung stehenden Daten und meiner Programmierung. Ich wurde trainiert, in bestimmten Situationen und Kontexten humorvoll zu sein.

*Erzählst du mir einen Witz?*

**ChatGPT:** Warum hat die Katze immer ihre Daten gelöscht? Weil sie Angst hatte, dass jemand ihre Maus-Akten einsehen könnte.

## Fazit

Hochgelobt? Zurecht. Doch ausgereift? Noch nicht ganz. Ein weiterer Meilenstein wurde mit ChatGPT in jedem Fall gesetzt, doch das Ende der Fahnenstange ist damit noch lange nicht erreicht. Wir bleiben gespannt, wo uns die Reise der künstlichen Intelligenz noch hinführt und vor allem, welche datenschutz- und compliancetechnische Herausforderungen auf diesem Weg auf uns warten werden. &





# Die NIS-2-Richtlinie der EU – hohe Anforderung für die KRITIS

Gesprengte Pipelines in der Ostsee, durchtrennte Glasfaserkabel an Bahnlinien – solche spektakulären Ereignisse haben den Blick der Öffentlichkeit auf die Sicherheit der Infrastruktur in Deutschland gelenkt. Ist man gegenüber derartigen physischen Angriffen relativ machtlos, kann man sich jedoch sehr wohl vor Attacken in der virtuellen Welt schützen – denn auch diese verursachen sehr realen Schaden.

Von Arne Wolff

Um sich vor Cyber-Kriminalität zu schützen sollen für die Betreiber kritischer Infrastrukturen in der EU höhere Cyber-Security-Mindeststandards etabliert werden; zu diesem Zweck ist am 16. Januar die EU-NIS-2-Richtlinie (2016/1148) in Kraft getreten. Die Mitgliedstaaten müssen die Richtlinie nun bis zum 17. Oktober 2024 in nationales Recht umsetzen. In Deutschland wird voraussichtlich das IT-Sicherheitsgesetz 2.0 (IT-Sig 2.0) entsprechend erweitert.

## Wer ist betroffen?

Ein Kernpunkt der neuen Richtlinie ist die Erweiterung der KRITIS-Sektoren. Lag es bisher im Ermessen der Mitgliedstaaten, die Kriterien festzulegen, welche Unternehmen zur kritischen Infrastruktur gehören und welche nicht, werden künftig allgemeine, an der Unternehmensgröße festgemachte Schwellenwerte gelten – in Deutschland war bislang die Anzahl der versorgten Personen maßgeblich. Konkret sind betroffen:

- Mittlere Unternehmen mit 50 bis 250 Beschäftigten, 10-50 Mio. Euro Umsatz und bis zu 43 Mio. Euro Bilanzsumme.
- Große Unternehmen mit mehr als 250 Beschäftigten, über 50 Mio. Euro Umsatz und mehr als 43 Mio. Euro Bilanzsumme.

Zusätzlich und größenunabhängig reguliert werden Betreiber digitaler Infrastruktur, Einrichtungen der öffentlichen Verwaltung, Zentralregierung und Regionalregierung (risikoabhängig) sowie Sonderfälle (zum Beispiel wenn es sich

um den einzigen Anbieter eines unerlässlich angesehenen Dienstes handelt). Gleichzeitig wird die Anzahl der Sektoren auf 18 vergrößert – dabei wird unterschieden zwischen elf wesentlichen („essential“) und sieben wichtigen („important“) Sektoren, an die verschiedenen hohe Anforderungen bezüglich der umzusetzenden Maßnahmen gestellt werden. Insgesamt führt das zu



einer starken Erhöhung der Anzahl der betroffenen Unternehmen, die sich übrigens auch bei der European Union Agency for Cybersecurity (ENISA) anmelden müssen.

### Was wird verlangt?

Erstmals werden Mindestanforderungen an Cyber-Sicherheit und Risiko-Management bei den Betreibern gestellt – Maßnahmen unter anderem aus den folgenden Bereichen müssen umgesetzt werden:

- Risikoanalyse und Informationssicherheit
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Aufrechterhaltung des Betriebs, wie Backup-Management und Disaster Recovery, und Krisenmanagement (Business Continuity)
- Sicherheit der Lieferkette (Supply Chain)
- Anschaffung, Entwicklung und Wartung von Netzwerk- und IT-Systemen
- Bewertung der Wirksamkeit von Risikomanagement und Cyber-Sicherheitsmaßnahmen
- ...

Es ist geplant, internationale und europäische Standards für diese Maßnahmen zu fördern – die EU-Kommission kann noch konkretisierende Verordnungen erlassen. Die Mitgliedstaaten können Betreibern dabei die Nutzung von EU-Cyber-Sicherheits-Zertifizierungen und zertifizierten Produkten vorschreiben.

### Wie wird das kontrolliert?

Um die Einhaltung der neuen Regelungen überwachen zu können, sieht die Richtlinie weitreichende Befugnisse für die nationale Aufsicht vor; so sollen die zuständigen Behörden bspw. Nachweise erhalten und eigene Audits und Untersuchungen durchführen können (regelmäßig und unangekündigt) – sowohl „Random Checks“ durch Experten als auch Security Audits oder Security Scans durch unabhängige Dritte oder Behörden.

Es gibt dabei nur kleine Unterschiede zwischen den Sektoren „wesentlich“ und „wichtig“:

- Sektor „wesentlich“: Strafen bis zu einem Maximum von

- mind. 10 Mio. € oder 2% des weltweiten Umsatzes
- Sektoren „wichtig“: Strafen bis zu einem Maximum von mind. 7 Mio. € oder 1,4% des weltweiten Umsatzes

Die Leitungsorgane von Betreibern sollen für Verstöße übrigens sogar persönlich haftbar gemacht werden können. Überwacht wird die Einhaltung der NIS-2 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) – es agiert auch als Single Point Of Contact (SPOC). Die Richtlinie verlangt aber noch die Einrichtung einer Behörde für das Krisenmanagement schwerwiegender Vorfälle und eines nationalen Computer Security Incident Response Teams (CSIRT) für das Incident Handling der kritischen Sektoren.

### Was ändert sich noch?

Vor allem der Informationsaustausch zwischen den Mitgliedstaaten soll verbessert werden. Dazu werden auf europäischer und nationaler Ebene verschiedene neue Institutionen und Mechanismen eingerichtet. Hierzu zählen zum Beispiel die Cooperation Group (CG), welche die Zusammenarbeit innerhalb der EU und zwischen den Mitgliedstaaten steuert, oder das European Cyber Crises Liaison Organisation Network (EU-CyCLONe) das großflächige Cyber Incidents und Krisen managen und die Mitgliedstaaten dafür sensibilisieren und vorbereiten soll.

*„Die Leitungsorgane von Betreibern sollen für Verstöße übrigens sogar persönlich haftbar gemacht werden können.“*

### Fazit

Den Betreibern kritischer Infrastruktur wird einiges abverlangt, um ihre IT-Systeme vor fremdem Zugriff zu schützen – zu Recht, denn an diesen Systemen hängen Menschenleben. Eigentlich ist es selbstverständlich, für entsprechenden Schutz nach Stand der Technik zu sorgen, doch fällt vielen Unternehmen eine strukturierte Herangehensweise schwer. Die Richtlinie liefert ihnen hier klarere Vorgaben. Auch die Erweiterung des Begriffes „kritische Infrastruktur“ ist Ausdruck eines geschärften Problembewusstseins.

Letztlich wird nichts verlangt, was nicht ohnehin sinnvoll ist – liegt Cyber-Sicherheit doch auch im ureigensten unternehmerischen Interesse. &



## Hinweisgeberschutzgesetz – Was kommt da auf uns zu?

Das Hinweisgeberschutzgesetz ist die deutsche Umsetzung der EU-Whistleblower-Richtlinie. Diese sieht vor, dass in der Europäischen Union Mindeststandards für den Schutz von Hinweisgebern (sog. Whistleblowern) eingeführt werden.

*Von Christian Klande*

Die Richtlinie hat das Ziel, Verstöße gegen das Unionsrecht aufzudecken und zu unterbinden. Werden von Mitarbeitenden Verstöße entdeckt, sollen diese angezeigt werden können – ohne die Befürchtung eventueller persönlicher Konsequenzen und Schäden.

### Worum geht's?

Der Bundestag stimmte am 16.12.2022 für die Einführung des Hinweisgeberschutzgesetzes. Für das Inkrafttreten fehlt derzeit noch die Zustimmung des Bundesrats. Aller Voraussicht nach erfolgt diese Mitte Februar. Erst nach der finalen Unterschrift des Bundespräsidenten und der Veröffentlichung im Bundesgesetzblatt tritt das Gesetz drei Monate nach der Verkündung in Kraft, somit Mitte/Ende Mai.

### Wen oder was schützt das HinSchG?

Das Gesetz schützt künftig hinweisgebende Personen (die Whistleblower) und die gemeldeten Personen (die einen Verstoß begangen haben (sollen)); außerdem den Hinweisgeber unterstützende und sonstige Personen, die von einer Meldung betroffen sind. Der Hinweisgeber soll vor Repressalien des Arbeitgebers geschützt werden. Dieser hat im Rahmen einer Beweislastumkehr zu beweisen, dass (mögliche) Maßnahmen gegen die meldende Person nichts mit der Aufdeckung von Verstößen zu tun hat.

Vereinfacht gesagt, gilt der Schutz, sofern die hinweisgebende Person zum Meldezeitpunkt davon ausgehen konnte, dass der Hinweis zutrifft, selbst, wenn sich hinter-

her (nach der Untersuchung, des sog. Case-Managements, durch die Ombudsperson oder den Compliance-Beauftragten) das Gegenteil herausstellen sollte. Ein Schutz besteht jedoch nicht, wenn vorsätzliche oder grob fahrlässig unrichtige Informationen weitergegeben wurden.

Die hinweisgebende Person hat dabei die Wahl, ob er/sie interne oder externe Meldestellen in Anspruch nimmt. Zur Vermeidung größerer Aufwände (z. B. Prüfung durch Aufsichtsbehörden) muss es daher im vitalen Interesse aller Organisationen liegen, interne Meldestellen vorzuhalten und zu propagieren, egal welche Beschäftigtenzahl diese hat.

### Welche gemeldeten Verstöße sind geschützt?

Gesetzlich sind nicht alle Meldungen über Verstöße geschützt. Es gibt einen abschließenden Katalog. Der Sinn und Zweck des Gesetzes würde aber nicht erfüllt werden können, wenn der Meldende zunächst eine genaue Einordnung und Prüfung des Sachverhalts vornehmen müsste. Insofern wird hier vermutlich eine großzügige Auslegung stattfinden müssen.

Wenn die hinweisgebende Person bei Abgabe hinreichenden Grund zur Annahme hatte, dass die Weitergabe oder die Offenlegung unter den Schutz des Gesetzes fallen würde, müsste sich die Wirkung entfalten – selbst, wenn sich später herausstellen sollte, dass die Meldung nicht explizit geschützt sein sollte. Der Beschäftigungsgeber ist daher gut beraten, trotzdem die Regeln des HinSchG einzuhalten. Folgende Vorschriften werden beispielhaft genannt:

- ✔ Verstöße gegen alle Strafvorschriften (z. B. Steuerhinterziehung, Betrug)
- ✔ Verstöße, die bußgeldbewehrt sind und dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten dienen – die Regelung ist weit auszulegen, z. B.:
  - Arbeits- und Gesundheitsschutz, Mindestlohn und Arbeitnehmerüberlassung
  - Aufklärungs- und Auskunftspflichten gegenüber Betriebsräten
- ✔ Verstöße gegen EU-Normen (Verordnungen und Richtlinien), z. B.:
  - Geldwäsche, Produktsicherheit, Umweltschutz, Lebensmittelsicherheit
  - Verbraucherschutz, Datenschutz und Sicherheit in der Informationstechnik
  - Vergaberecht.

### Wer muss die Regeln des HinSchG umsetzen?

Alle privaten Beschäftigungsgeber mit Ausnahme juristischer Personen des öffentlichen Rechts und solcher Beschäftigungsgeber, die im Eigentum oder unter Kontrolle einer juristischen Person des öffentlichen Rechts stehen, müssen das Gesetz umsetzen. Beschäftigungsgeber ist eine Organisation dann, wenn sie mindestens eine Person beschäftigt (natürliche Personen, Personengesellschaften und juristische Personen des öffentlichen und des privaten Rechts sowie rechtsfähige Personenvereinigungen, soweit sie nicht vorher genannt wurden).

### Wer muss eine interne Meldestelle einrichten?

Auch wenn das Gesetz für alle Beschäftigungsgeber gilt, müssen nicht alle eine interne Meldestelle einrichten. Lediglich Beschäftigungsgeber mit jeweils in der Regel mindestens 50 Beschäftigten (einige unabhängig von der Beschäftigtenzahl, insbesondere Kreditinstitute, Versicherungen usw.), müssen spätestens ab dem 17.12.2023 ein Hinweisgebersystem einrichten.

Alle Beschäftigungsgeber mit mehr als 250 Beschäftigten sind sofort ab Inkrafttreten des Gesetzes dazu verpflichtet. Mehrere Beschäftigungsgeber mit 50–249 Beschäftigten können eine gemeinsame Meldestelle einrichten (unter Sicherstellung der Vertraulichkeit und der eigenen Verantwortlichkeit für die Bearbeitung). Bei komplexen Trägern bzw. Konzernen sieht dies wie in der Tabelle auf der nächsten Seite aus.

### Anforderungen an die interne Meldestelle

Die Meldestelle besteht in der Regel aus einem Meldeportal (welches spätestens ab dem 01.01.2025 auch anonyme Meldungen entgegennehmen und bearbeiten muss) sowie der

#### Stichwort

#### Need-to-know-Prinzip

.....

Das Need-to-know-Prinzip ist eines der Grundpfeiler zur Sicherstellung der Vertraulichkeit. Vereinfacht ausgedrückt: Nur wenn eine Person die Informationen zur Erfüllung ihrer Tätigkeit braucht, darf sie auch Zugang dazu haben.

Beherrschende Organisation	Abhängige Organisation	Interne Meldestelle
50–249 Beschäftigte	–	ab 17.12.2023
> 250 Beschäftigte	< 50 Beschäftigte	Beherrschende ab Mitte/Ende Mai 2023, abhängige nein
> 250 Beschäftigte	50–249 Beschäftigte	Beherrschende ab Mitte/Ende Mai 23, die Abhängige ab 17.12.23. Die Abhängige kann im System der Beherrschenden miteingebunden werden. Vertraulichkeit und Verantwortlichkeit müssen sichergestellt sein.
> 250 Beschäftigte	> 250 Beschäftigte	Beherrschende und Abhängige ab Mitte/Ende Mai 2023. Vertraulichkeit und Verantwortlichkeit müssen sichergestellt sein. Jeweils eigene Stellen oder Beauftragung der Beherrschenden.

mit dem Case-Management beauftragten Person (Ombudsperson oder Compliance-Beauftragter). In allen Bereichen muss die Vertraulichkeit – insbesondere das Need-to-know-Prinzip – sichergestellt sein. Es dürfen keinerlei Interessenskonflikte bestehen. Dieses muss die Organisation im Rahmen der Beweislastumkehr beweisen können (auch glaubhaft gegenüber der Mitarbeitervertretung/Betriebsrat bzw. den Mitarbeitenden).

Das Portal von Althammer & Kill kann anonyme Meldungen entgegennehmen und bearbeiten (optional auch nicht anonym, bis zum 31.12.2024 nach Wahl des Auftraggebers). Bei Anonymität ist davon auszugehen, dass die Hemmschwelle deutlich niedriger ist und daher mehr Meldungen eingehen werden. Es dürfte im vitalen Interesse der Organisation liegen, Missstände zu erfahren, aufzuklären und externe Meldungen zu vermeiden. Die Ombudsperson muss über die notwendige Fachkunde verfügen. Es lohnt

sich daher für viele Organisationen, nicht nur das Meldeportal extern zu vergeben, sondern auch die Ombudsperson extern zu bestellen (keine Ausbildungskosten, keine unnötige Bereitstellung von Ressourcen und Forderungen der zu bestellenden Person). ☎

**In eigener Sache**  
.....

Sie brauchen mehr Informationen?  
Sprechen Sie uns einfach an!



**Ihr Vertriebsteam**  
[vertrieb@althammer-kill.de](mailto:vertrieb@althammer-kill.de)  
 Tel. +49 511 330603-0

**Impressum**  
.....

**Redaktion/V. i. S. d. P.:**  
 Marie Plautz, Danny Sellmann,  
 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](http://winternheimer.net)

**Fotos Mini-Figuren:**  
 Katja Borchhardt, [miniansichten.de](http://miniansichten.de)

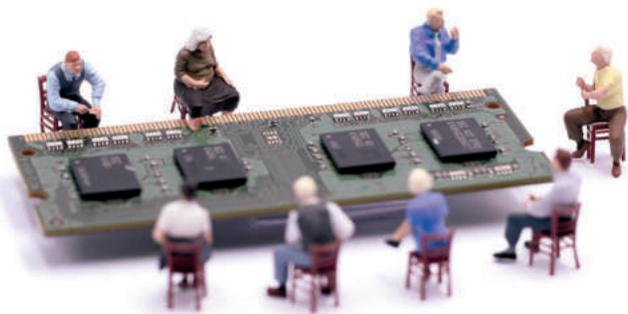
**Anschrift:**  
 Althammer & Kill GmbH & Co. KG  
 Roscherstraße 7 · 30161 Hannover  
 Tel. +49 511 330603-0  
[althammer-kill.de](http://althammer-kill.de)

# Veranstaltungen und Termine



Mehr Informationen, weitere Termine und Anmeldemöglichkeiten für unsere Veranstaltungen finden Sie unter: [althammer-kill.de/akademie](https://althammer-kill.de/akademie)

Hier klicken oder scannen!



21.-22. März 2023 – Online-Seminar

## ISO 27001 Foundation Zertifikatskurs

Unser ISO 27001 Grundlagenseminar vermittelt Ihnen das Basiswissen der international anerkannten Norm für Informationssicherheit ISO 27001. In dem zweitägigen Kurs lernen Sie ohne vorherige Kenntnisse die Norm kennen und können diese fortan in Ihrem Unternehmen adressieren. Dabei geht der Referent auf die Mindestanforderungen der Norm und Maßnahmen zur Umsetzung der Normen ein.

18. April 2023 – Online-Seminar

## Privacy by Design – Datenschutz für Software-Entwickler

Unser Seminar vermittelt an praktischen Beispielen das Grundwissen, um von Anfang an Datenschutz-freundliche Entscheidungen zu treffen und umzusetzen. Die Teilnehmer lernen die Grundprinzipien, die sie bei Design und Implementierung im Blick behalten sollten.

25.-26. April 2023 – Online-Seminar

## Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

22. März 2023 – kostenloses Webinar

## Persönliche Haftungsrisiken der Geschäftsleitung minimieren – durch Compliance Management

Ein Compliance-Management-System gehört nicht zur Kür, sondern zur Pflicht eines jeden Unternehmens im Rahmen der Legalitätspflicht der Geschäftsleitung. Wir zeigen auf, wie man ein solches aufbauen, erweitern und pflegen kann.

12. April 2023 – kostenloses Webinar

## Datenschutz-Folgenabschätzung

Jede Einführung neuer Verarbeitungsprozesse bedarf einer Datenschutz-Folgenabschätzung. Die Datenschutz-Folgenabschätzung soll dazu dienen, die möglichen Risiken zu verringern und dieses zu dokumentieren. In unserem Webinar führen wir Sie in die Vorgehensweise und mögliche Methodik einer Datenschutz-Folgenabschätzung ein.

29. März 2023 – kostenloses Webinar

## Von der Pflicht zur Chance: Das Hinweisgebersystem von Althammer & Kill

Ohne Edward Snowden, wüssten wir wohl bis heute nicht um die Methoden der amerikanischen Geheimdienste. Er war mutig und hat sich getraut, Missstände öffentlich zu machen, er war der Hinweisgeber. Wir stellen Ihnen das Hinweisgebersystem von Althammer & Kill vor, das die Anforderungen an die neue Richtlinie optimal erfüllt.

### Ihr Ansprechpartnerin:



**Nina Hoffmann**

[veranstaltung@althammer-kill.de](mailto:veranstaltung@althammer-kill.de)

Tel. +49 511 330603-0



## Das Team macht den Unterschied

Sema ist bei Althammer & Kill als Beraterin für Datenschutz tätig.

**F**ür Sema macht vor allem das freundschaftliche Verhältnis zu den Kolleginnen und Kollegen den Unterschied und runden die abwechslungsreiche Tätigkeit ab.

*Welche Ausbildung oder welches Studium hast du absolviert?*

**Sema:** Ich habe mein Studium im Wirtschaftsrecht mit dem Schwerpunkt „Recht und Marketing in der Informationsgesellschaft“ an der Ostfalia Hochschule für angewandte Wissenschaften mit dem Bachelor

of Laws absolviert. Während meines Studiums habe ich mich bereits mit den rechtlichen Grundlagen des Informationstechnologierechts, insbesondere Datenschutz- und IT-Vertragsrecht intensiv auseinandergesetzt. Der Schutz von Daten ist für viele ein eher sperriges Thema, doch während meines Studiums habe ich gemerkt, dass Datenschutz ausgesprochen spannend ist.

*Wie bist du zu Althammer & Kill gekommen und wie war deine Entwicklung innerhalb des Unternehmens?*

**Sema:** Eine ehemalige Mitarbeiterin und enge Freundin hatte mich darauf aufmerksam gemacht, dass Althammer & Kill auf der Suche nach einer erfahrenen Beraterin für Datenschutz und Informationssicherheit ist und womöglich genau das Richtige für mich sei. Und sie hatte Recht! Zu Beginn war ich zu 50 % im Service Desk und zu 50 % als Beraterin tätig. Im Laufe der Zeit haben wir festgestellt, dass mir die Beratungstätigkeit sehr gut liegt und es am sinnvollsten ist mein Potenzial am besten durch eine Vollzeitstelle als Beraterin zu entfalten.

Was ist bisher dein größtes Projekt gewesen?

**Sema:** Der Datenexport in Drittländer bringt verschiedene Herausforderungen mit sich. Meine bisher größten Projekte sind Datenschutz-Folgeabschätzungen wie u. a. für Microsoft 365. Datenschutzaufsichtsbehörden fordern bei der Nutzung von Microsoft 365 eine Datenschutz-Folgenabschätzung, da die Software aus den USA stammt und in dem Zusammenhang gravierende technische und vor allem rechtliche Probleme entstehen können.

Was gefällt dir besonders an der Tätigkeit als Beraterin für Datenschutz und Informationssicherheit?

**Sema:** Mein Aufgabengebiet als Beraterin für Datenschutz und Informationssicherheit ist abwechslungsreich und vielseitig. Dabei gefällt mir besonders der Kontakt mit den Kunden. Sowohl direkter als auch indirekter Kundenkontakt ist mir sehr wichtig. Es ist für mich von grundlegender Bedeutung auf die Bedürfnisse der Kunden einzugehen und gemeinsam das bestmögliche Ergebnis zu erreichen.

Was gefällt dir an der Tätigkeit der Beratung am besten? / Was war ein besonders schönes Erlebnis in deinem Beratungs-Alltag?

**Sema:** Die größte Freude bereiten mir glückliche und zufriedene Kunden, indem sie mir positives Feedback oder Ihren Dank aussprechen. Dann merke ich ganz besonders, wie gerne ich diese Beratungstätigkeit ausübe.

Welche Themen beschäftigen unsere Kundinnen und Kunden am meisten?

**Sema:** Die Nutzung von Microsoft 365 spielt für unsere Kunden eine große Rolle. Ein grundsätzliches Problem bei der Nutzung von Microsoft 365 ist, dass personenbezogene Daten in die USA übermittelt werden. Aus diesem Grund ist auch die Durchführung einer Datenschutz-Folgeabschätzung besonders wichtig, um sich das Risiko der Datenverarbeitung bewusst zu werden und entsprechende Sicherheitsmaßnahmen zu etablieren. Dabei unterstützen wir unsere Kunden natürlich auch bei der Durchführung!

*„Es ist für mich von grundlegender Bedeutung, auf die Bedürfnisse der Kunden einzugehen und gemeinsam das bestmögliche Ergebnis zu erreichen“*

Welches Thema liegt dir am besten/ wozu berätst du am liebsten?

**Sema:** Da ich Wirtschaftsjuristin bin, berate ich am liebsten in datenschutzrechtlichen Fällen. Besonders Spaß macht mir auch die datenschutzrechtliche Prüfung von Webseiten unserer Kunden und die Erstellung von Datenschutzerklärungen.

Welche Themen werden deiner Meinung nach im Jahr 2023 relevant werden?

In diesem Jahr wird uns weiterhin das Thema Microsoft 365 begleiten. In diesem Zuge wird, wie bereits zuvor erwähnt, auch die Durchführung

von Datenschutz-Folgeabschätzungen weiterhin eine große Rolle einnehmen.

Außerdem rücken die technischen Neuerungen wie Künstliche Intelligenzen und App-Entwicklungen weiter in unseren Fokus.

Wie eng arbeitest du mit den anderen Beratern zusammen?

Hauptsächlich arbeite ich selbstständig. Meine Kollegen stehen mir dennoch gerne mit ihrem Rat zur Seite. Wir haben immer ein offenes Ohr füreinander und unterstützen uns gegenseitig. Darüber hinaus arbeite ich in größeren Kundenprojekten eng mit Kollegen zusammen. Dabei kommunizieren wir sehr viel miteinander, stimmen uns ab, tauschen Informationen aus und bearbeiten einige Aufgaben gemeinsam. Teamarbeit wird bei uns großgeschrieben!

Was schätzt du besonders an der Arbeit im Unternehmen Althammer & Kill?

Bei Althammer & Kill schätze ich besonders das harmonische Arbeitsklima und freundschaftliche Verhältnisse mit den Kollegen und Kolleginnen. So macht die Arbeit doch erst richtig Spaß, oder?!

Unsere Zusammenarbeit ist von Wertschätzung und Respekt geprägt. Auch schwierige Herausforderungen werden durch ein gutes Miteinander der Berater gemeistert. Wir reden offen und unkompliziert miteinander, legen Wert auf die Meinung des anderen und sind stets bemüht unsere Fähigkeiten und Kompetenzen zu erweitern. Des Weiteren haben wir die Möglichkeit uns weiterzuentwickeln und Veränderungen mitzugestalten. Zudem finde ich auch die uns gegebene Flexibilität und das damit verbundene Vertrauen in uns super. ☺



# Digitalisierung sicher gestalten

Althammer & Kill bietet pragmatische Lösungskonzepte für Datenschutz und Digitalisierung. Wir beraten bundesweit im Umfeld Datenschutz, Informationssicherheit, Cloud- und Cybersecurity und Compliance.

Unsere rund 45 Mitarbeitende an den Standorten Hannover, Düsseldorf und Mannheim sind als externe Datenschutzbeauftragte, Informationssicherheits- und IT-Experten für mehr als 500 Kunden unterschiedlichster Branchen tätig.

---

## Althammer & Kill GmbH & Co. KG

Roscherstraße 7 · 30161 Hannover · Tel. +49 511 330603-0  
Mörsenbroicher Weg 200 · 40470 Düsseldorf · Tel. +49 211 936748-0  
P7 20 · 68161 Mannheim · Tel. +49 621 121847-0

Qualitätsmanagement nach Plan  
mit der ISO 9001:2015.



vertrieb@althammer-kill.de  
althammer-kill.de

Mitgliedschaften

