COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 3/2023

Der lange Weg zum Hinweisgeberschutzgesetz

Alles, was Sie zur Umsetzung wissen müssen.
Seite 6

Das „Meta-Urteil" des EuGH
Die DSGVO auf dem Prüfstand
Seite 10

Genau hingeschaut: Microsoft Defender for Endpoint
Zu Unrecht unterschätzt?
Seite 12

Operational Technology als Herausforderung
Fast jedes Unternehmen betroffen
Seite 14

Editorial

Liebe Leserin, lieber Leser,

lebhaft wurde in den letzten Monaten über das Thema KI diskutiert. ChatGPT, Midjourney und ähnliche Dienste sind verblüffend und faszinierend zu gleich. Geht es nach dem Willen von Microsoft und anderen großen Tech-Konzernen, werden KI-Funktionen in viele Produkte des Alltags Einzug halten. Sind wir dafür schon weit genug? Lässt sich das mit strengen Anforderungen rund um Datenschutz und Compliance vertreten?

Laut Microsoft alles kein Problem, dank Microsoft 365 Copilot. Der neue Dienst soll nach Aussage des Unternehmens zum Einsatz kommen, um Geschäftsprozesse zu steuern. KI-Sprachmodelle werden genutzt, um individuelle Inhalte in Echtzeit zu generieren.

Und der Datenschutz? Microsoft betont, dass neben der effizienten Content-Generierung auch Datensicherheit gewährleistet ist. Copilot beachtet bestehende Sicherheits- und Datenschutzrichtlinien, isoliert Unternehmensdaten und gewährleistet Kontrolle. Die Einhaltung der KI-Grundsätze und Responsible AI Standards wird versichert… soweit die Theorie.

In der Praxis wird sich zeigen, wie das Ganze funktioniert. Der Einsatz von Copilot muss in jedem Fall individuell geprüft werden. Eine Analyse vertraglicher Regelungen und die Durchführung einer Datenschutz-Folgenabschätzung ist vor Einsatz des Tools unerlässlich. Die Vereinigung von KI und Unternehmensalltag erfordert sorgfältiges Abwägen von Innovation und Datenschutz. Microsoft 365 Copilot möchte da Wege ebnen, doch wie so oft bleibt die Verantwortung für eine datenschutzkonforme Nutzung bei Ihnen – den Organisationen.

Wir unterstützen Sie bei der Einführung von KI-Systemen, sprechen Sie uns gerne an!

Viel Spaß beim Lesen wünschen

Thomas Althammer & Niels Kill

Darüber wird gesprochen

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

Hier klicken oder scannen!

Wir sind TOP Consultant

Ein Auszeichnung, die uns sehr stolz macht: Der TOP Consultant Award ist ein Beratervergleich, der an der Wurzel ansetzt – unseren Kundinnen und Kunden. In einer anonymen, wissenschaftlich fundierten Befragung wurden verschiedene Parameter abgefragt, die auf unsere Professionalität, unsere Performance und nicht zuletzt die Zufriedenheit der Kundinnen und Kunden abzielte. Das Ergebnis der Befragung: Mit unserer Beraterleistung sind wir einer der TOP Consultants 2023.

Cybersecurity in der modernen Welt: Lücken, Risiken und Präventionsstrategien

In der heutigen digitalisierten Welt ist die Sicherheit unserer IT von entscheidender Bedeutung. Doch trotz der zunehmenden Abhängigkeit von IT-Systemen zeigen Studien immer wieder, dass sowohl öffentliche als auch private Sektoren in Deutschland erhebliche Schwachstellen in ihrer IT-Sicherheit aufweisen. Ein großer Teil dieser Schwachstellen ist auf veraltete Verschlüsselungsmethoden und den Mangel an Anpassungen an die weltweit mobil arbeitenden Menschen zurückzuführen.

Pur-Abo-Modelle – grünes Licht für „Daten-Paywalls"?

Daten sind bares Geld wert – dass Daten einen Geldwert haben und sich mit dem Handel von Daten viel Geld verdienen lässt, ist längst bekannt. Der Kauf und Verkauf von persönlichen Daten ist ein lukratives Milliardengeschäft.

FAQ zum Angemessenheitsbeschluss

Was ist das Trans-Atlantic Data Privacy Framework (TADPF)? Wie bewerten die Datenschutzbehörden (kirchlich und weltlich) den Angemessenheitsbeschluss? Und fällt mit dem Angemessenheitsbeschluss die Notwendigkeit einer Datenschutzfolgeabschätzung weg? Am 10.07.2023 hat die EU-Kommission ihren Angemessenheitsbeschluss für den neuen Datenschutzrahmen EU-USA (Data Privacy Framework) angenommen und damit wieder die rechtliche Basis für den Transfer personenbezogener Daten in die USA geschaffen. In unserem FAQ widmen wir uns den wichtigsten Fragen zum neuen Beschluss.

Team Althammer & Kill 2023

Der Juni in Bad Dürkheim lockt nicht nur Weinliebhaber in den Kurort, sondern auch das Team von Althammer & Kill. Bei den diesjährigen Team Tagen haben wir uns den Kollegen aus Mannheim genähert und sind in den Süden Deutschlands gefahren. Vor Ort haben wir nächste strategische Schritte und Ziele sowie die weiterführende Zusammenarbeit in Teams besprochen. Neben unternehmerischen Punkten, kam der Faktor "Team" natürlich auch nicht zu kurz. So konnten wir uns untereinander noch besser kennenlernen, Spiele spielen und neue Kolleginnen und Kollegen in unserer Mitte willkommen heißen. Nach knapp vier Tagen ging es dann wieder in die jeweilige Heimat.

Zahl des Monats

3

Am 10.07.2023, hat die EU-Kommission ihren Angemessenheitsbeschluss für den neuen Datenschutzrahmen EU-USA (Data Privacy Framework) angenommen und damit wieder die rechtliche Basis für den Transfer personenbezogener Daten in die USA geschaffen. Stellt sich nur die Frage, ob dieser tatsächlich Stand hält oder unter den strengen Augen der Datenschützer erneut gekippt wird. Wird Schrems, wie die Male davor, Klage erheben und damit ein drittes Mal zum Kippen des Beschlusses führen?

Veranstaltungen

18.–20.09.2023 Münster, Mövenpick-Hotel
BeB Fachtagung
Zukunft gestalten – Nachhaltig wirken!
Fachtagung Dienstleistungsmanagement 2023
https://beb-ev.de/veranstaltung/fachtagung-dienstleistungsmanagement-2023/

29. und 30. September in Marburg
Mitgliederversammlung Lebenshilfe e.V.
https://www.lebenshilfe.de/ueber-uns/mitgliederversammlung-der-lebenshilfe/

25.–26.10. 2023, Nürnberg
ConSozial
Die Leitmesse der Sozialwirtschaft
https://www.consozial.de/

08.11.2023 in Berlin
Paritätischer Pflegekongress
https://www.der-paritaetische.de/termin-detailansicht/paritaetischer-gesundheits-und-pflegekongress-2023/

Die neue Version der Orientierungshilfe zum Hinweisgeberschutzgesetz

Nach den aktuellen Entwicklungen steht fest, dass Unternehmen mit 250 Mitarbeitenden eine Meldestelle gemäß des Hinweisgeberschutzgesetz einrichten müssen. Für Unternehmen ab 50 Mitarbeitenden gilt eine Schonfrist bis zum 17.12.2023.

In unserer neu aufgelegten Orientierungshilfe geben wir Ihnen das nötige Handwerkszeug, damit Sie die neue Richtlinie in Ihrer Organisation umsetzen können.

Jetzt hier kostenlos herunterladen:
https://www.althammer-kill.de/orientierungshilfe-hinweisgeberschutzsystems

Der lange Weg zum Hinweisgeberschutzgesetz

Whistleblower haben eine lange Tradition. Schon 1971 enthüllte Daniel Ellsberg die „Pentagon-Papers“ und damit die jahrelange Täuschung der Öffentlichkeit durch US-Verteidigungsministerium und das Weiße Haus über die Ziele des Vietnam-Kriegs.

Von Wulf Bolte und Frank Boje

2006 gründete der Australier Julian Assange die Plattform Wikileaks, auf der zum Beispiel 2010 die US-Soldatin Chelsea Manning hundertausende Dokumente über Vergehen der US-Militärs im Irak und Afghanistan-Krieg offenlegte. Der bekannteste Whistleblower ist wahrscheinlich Edward Snowden, der eine Menge geheimer Dokumente veröffentlicht hatte – in denen die teils hochproblematischen Vorgehensweisen der US-Sicherheitsbehörden dokumentiert waren und sind. Allen gemein ist, dass sie aufgrund ihrer Veröffentlichungen verfolgt und zum Teil inhaftiert worden sind.

Diese Beispiele zeigen, dass es einen geschützten Rahmen geben muss, in dem auf Missstände innerhalb von festen Strukturen hingewiesen werden kann. Die EU reagierte darauf mit der Whistleblower-Richtlinie (Richtlinie 2019/1937), mit der Personen geschützt werden sollen, die Verstöße gegen Unionsrecht melden, die das öffentliche Interesse beeinträchtigen. Nach mehreren Anläufen und etwas Verspätung ist am 02.07.2023 das “Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz (HinSchG))” in Kraft getreten.

Warum hat die Umsetzung so lange gedauert?

Nach der Veröffentlichung der EU-Richtlinie 2019/1937 am 23.10.2019 verging viel Zeit, bis die Bundesregierung begann; die Richtlinie in ein nationales Gesetz zu überführen. Erst am 13.04.2022 wurde der erste Referentenentwurf veröffentlicht zu dem über 50 Stellungnahmen eingingen. Bis zum ersten Gesetzentwurf der Regierung dauerte es dann weitere drei Monate – bis zum 27.07.2022. Nach dem Durchlaufen der parlamentarischen Instanzen konnte das Gesetz am 02.06.2023 im Bundesgesetzblatt verkündet werden und ist am 02.07.2023 in Kraft getreten.

Was fällt unter das Hinweisgeberschutzgesetz?

Persönlich gilt es für natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit Informationen über Verstöße erlangen und diese melden oder offenlegen. Sachlich handelt es sich dabei um Verstöße, die straf- oder bußgeldbewehrt sind, wenn die Vorschrift dem Schutz von Leben, Leib oder Gesundheit dient. Ferner gehören hierzu Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union, unter anderem aus den Bereichen Bekämpfung von Geldwäsche, Produktsicherheit, Umweltschutz, Lebensmittelsicherheit, Sicherheit in der Informationstechnik oder Datenschutz.

Was gibt es für besondere Schutz–mechanismen für den Hinweisgebenden?

Für den Schutz der Hinweisgebenden sieht der Gesetzgeber eine Reihe von Mechanismen vor. So sind Personen, die

im Rahmen der Tätigkeit für eine Meldestelle Informationen erlangen, zur Verschwiegenheit verpflichtet. Dieser Personenkreis benötigt für seine Tätigkeit die notwendige Fachkunde. Ferner hat die Meldestelle Vertraulichkeit sowohl über die meldende Person zu wahren, als auch über die Personen, die Gegenstand einer Meldung sind. Dieses gilt nicht bei grob fahrlässiger oder vorsätzlich falscher Meldung.

Was hat sich seit den ersten Entwürfen geändert?

Durch den langen parlamentarischen Weg mussten beim Hinweisgeberschutz einige Kompromisse eingegangen werden. So wurde unter anderem – dies ist eine der wichtigsten Neuerungen gegenüber dem Regierungsentwurf – die anonyme Meldung stark eingeschränkt. Zum einen muss eine Meldestelle kein System anbieten, welches eine anonyme Meldung ermöglicht, zum anderen ist die Bearbeitung von anonymen Hinweisen durch die Meldestelle nicht mehr verpflichtend. Dies lässt jedoch trotzdem den Raum, in Unternehmen oder Organisationen anonyme Meldungen zuzulassen.

Diese Möglichkeit reduziert die Hemmschwelle für Meldungen und bietet damit die Chance für eine effektive Qualitätsverbesserung. Ihre Mitarbeitenden kennen Ihren Arbeitsplatz am besten und können rechtzeitig auf Lücken in Prozessen aufmerksam machen. Nicht alle Mitarbeitenden sind so selbstsicher und couragiert, dass sie Missstände offen benennen und fühlen sich in der Anonymität geschützter.

Eine weitere Änderung betrifft die Sanktionen gegen Beschäftigungsgeber, die gegen die Regelungen des HinSchG verstoßen. Die Vorschriften sehen je nach der begangenen Ordnungswidrigkeit Bußgelder bis maximal EUR 50.000 vor. Hier waren im ersten Entwurf noch EUR 100.000 geplant. Ob mit der Reduzierung der Bußgeldhöhe der Bedeutung des HinSchG Rechnung getragen wird, und ob davon das richtige Signal ausgeht, möchten wir an dieser Stelle nicht weiter diskutieren.

Was ändert sich Ende des Jahres?

Seit dem 02.07.2023 müssen Beschäftigungsgeber mit mehr als 250 Mitarbeitenden ein System zur Abgabe von Hinweisen etabliert haben. Ab dem 01.12.2023 ist das Nicht-Einrichten bußgeldbewehrt.

Ab dem 17.12.2023 müssen auch Beschäftigungsgeber ab 50 Beschäftigten eine interne Meldestelle nach dem HinSchG einrichten. Zu den Beschäftigten zählen neben Arbeitnehmerinnen und Arbeitnehmern unter anderem auch die zu Ihrer Berufsbildung Beschäftigten, in Heimarbeit Beschäftigte, dem Beschäftigungsgeber überlassene Leiharbeiter und Menschen mit Behinderung, die in einer Werkstatt für behinderte Menschen beschäftigt sind.

Was wurde am Hinweisgebersystem von Althammer & Kill geändert?

Auch wir von A&K haben uns Gedanken gemacht, wie wir die gesetzlichen Vorgaben umsetzen und das Hinweisgeberschutzsystem noch attraktiver für Sie gestalten können. So wurden von uns folgende Änderungen implementiert:

- **Stellung der externen Ombudsperson**
  Damit der interne Aufwand für Sie so gering wie möglich ist, stellen wir auch gerne die Ombudsperson für Sie. Der Gesetzgeber schreibt vor, dass Personen, die mit Aufgaben einer internen Meldestelle betraut sind über die notwendige Fachkunde verfügen und die Tätigkeit nicht zu Interessenkonflikten führen darf.
- **Möglichkeit, auch Beschwerden und Lieferkettenproblematiken über das System zu melden**
  Um einen möglichst großen Nutzen von einem Hinweisgebersystem zu haben, können Sie dieses auch für andere Problematiken öffnen. Nutzen Sie dasselbe System als internes Beschwerdeportal oder für Meldungen nach dem Lieferkettensorgfaltspflichtengesetz.
- **Einfache Sprache**
  Nach dem Gesetz stellt der Beschäftigungsgeber den Beschäftigten klare und leicht zugängliche Informationen über das interne Meldeverfahren zur Verfügung. Deshalb sind alle Informationen zu unserem Hinweisgeberschutzportal auch in einfacher Sprache verfügbar.
- **Unterteilung der Standorte und Muttergesellschaften**
  Über ein leicht zu bedienendes Konfigurationstool lassen sich Besonderheiten in Ihrer Organisation darstellen, sodass für die hinweisgebende Person immer klar ist, an wen sie sich wenden kann.
- **Individualisierung von Erscheinungsbild passend zur internen CI**
  Auch wenn das Hinweisgebersystem nicht Teil ihrer IT-Infrastruktur ist, möchten Sie, dass es in Ihrem Look-and-Feel erscheint. Dafür können wir Ihr Firmenlogo einbinden und für ein einheitliches Erscheinungsbild Ihre Firmenfarbe verwenden. &

Die Menschen hinter Althammer & Kill:

Johannes Endres

Ja hallo, wer bist du denn?

Johannes: Moin. Ich bin Johannes Endres. Aufgewachsen bin ich am Niederrhein, aber seit 1996 lebe ich in Hannover. 1984 konnte ich zum ersten Mal meine Finger an einen Computer legen (Apple II, die Alten erinnern sich). Damals hieß das automatisch, dass man programmiert. Diese Faszination hat mich nie mehr losgelassen.
Bei allem Spaß an den positiven Möglichkeiten der Technik habe ich daraus auch große Aufmerksamkeit für die Gefahren des Missbrauchs entwickelt. Diese Kombination führte mich nach dem Studium (Physik) in die gemeinsame Redaktion von c't und heise online. Dort haben wir die Auswirkungen auf die Privatsphäre bei allen technischen Themen mit betrachtet; und so wurde Datenschutz zu einem meiner Schwerpunktthemen.
In meinen fast 20 Jahren im Heise-Verlag habe ich es vom Volontär zum Chefredakteur gebracht. Anschließend habe ich mich als Berater selbständig gemacht.

Wie lange arbeitest du schon bei Althammer & Kill?

Johannes: Im Juli 2020 durfte ich mich dem Althammer-&-Kill-Team anschließen.

In welcher Position bist du tätig und was sind deine Aufgaben?

Johannes: Derzeit bin ich Leiter des Bereichs Beratung und gleichzeitig weiterhin in einigen Projekten als Berater für Datenschutz und Informationssicherheit eingebunden.

Was gefällt dir besonders an der Tätigkeit des Beraters?

Johannes: Datenschutz hat rechtliche, technische, organisatorische und wirtschaftliche Aspekte. Daher gelingt ein effektiver Schutz der Privatsphäre nicht, wenn ein Jurist oder ein IT-ler alleine in seinem Kämmerlein arbeitet.

Es macht mir besonderen Spaß, mit meinen Kunden Lösungen zu erarbeiten, die alle diese Blickwinkel so kombinieren, dass die Privatsphäre der betroffenen Personen wirksam geschützt wird. Durch meine Programmierer-Erfahrung kann ich oft technische Umsetzungen mitgestalten und als ehemaliger Journalist kann ich zwischen den Beteiligten übersetzen.

Wie sieht dein Alltag bei Althammer & Kill aus?

Johannes: Mein Alltag besteht in erster Linie aus Kommunikation – mit meinen Kolleginnen und Kollegen sowie mit den Kunden.

Welche Entwicklungen gibt es innerhalb der Beratung (Stichwort Teamsport)?

Johannes: Früher waren Beratende bei uns Einzelkämpfer. Jede und jeder hat ihre und seine Kunden ganz allein betreut. Das führte zwar zu einem sehr engen Kontakt, hatte aber zum Beispiel in der Urlaubszeit große Nachteile. Außerdem ist unser Themenfeld komplexer geworden, sodass nicht jeder in allen Bereichen Experte sein kann.
Wir sind deshalb dabei, uns auf eine Zusammenarbeit in kleinen Teams umzustellen: Jede Gruppe aus Beratenden kümmert sich umfassend um gemeinsame Kunden. Dazu haben wir Teams mit den verschiedenen Kompetenzen zusammengestellt. Diese Teams haben 4 bis 6 Mitglieder, sodass die Kunden ihre Ansprechpartner ebenso kennen, wie die Beratenden ihren jeweiligen Kunden-Stamm. Das bringt natürlich auch Änderungen in der täglichen Arbeitsweise mit sich. Aber schon in der aktuellen Urlaubs-Saison zeigt sich, wie gut das Konzept in der Praxis funktioniert.

Welche Themen werden deiner Meinung nach besonders wichtig im Bereich IT und Datenschutz?

Johannes: Das große Thema heißt derzeit Künstliche Intelligenz.
Die Technik ist ja nicht neu, aber die Entwicklung der Hardware in den letzten Jahren verhilft neuen Anwendungen zum kommerziellen Durchbruch. Das rückt die Fragen zum Datenschutz und zur Informationssicherheit in den Fokus.
Da gibt es einerseits den Reflex „das verstehe ich nicht, das muss verboten werden", andererseits den vollkommen unkritischen Einsatz ohne Vorstellung von den Grenzen der KI. Beides halte ich für gefährlich. Hier mit unseren Kunden einen sinnvollen Weg zu finden, wird in den nächsten Monaten viele interessante Aufgaben bringen. &

Das „Meta-Urteil" des EuGH

Ein wegweisendes Urteil (vom 04.07.2023, Az. C-252/21) zur Entscheidungsbefugnis der Wettbewerbsbehörde und zur Zusammenführung von Nutzerdaten beim Meta-Konzern, das die praktische Anwendung der DSGVO auf den Prüfstand stellte. Wir zeigen auf, was dahintersteckt.

Von Urban Zimber

Der EuGH hat sich zunächst mit der Frage auseinandergesetzt, ob das Bundeskartellamt zum Schutz des Wettbewerbs auch die Einhaltung von Datenschutzvorschriften prüfen darf. Zudem hat sich der EuGH näher mit den möglichen Rechtsgrundlagen zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Zusammenführung von Nutzerdaten zwecks personalisierter Werbung durch den Meta-Konzern befasst.

Facebook stellt für seine Werbekunden zur zielgerichteten Werbung sog. Off-Facebook-Daten zur Verfügung. Als Off-Facebook-Daten werden die Nutzerdaten konzerneigener Dienste wie Instagram, WhatsApp und von Websites weiterer Anbieter bezeichnet, die ohne eine ausdrückliche Erlaubnis der Betroffenen miteinander verknüpft wurden.

Hintergrund

Das Bundeskartellamt hatte Meta im Jahr 2019 in einem Beschluss untersagt, die Nutzung des sozialen Netzwerks in den damaligen Allgemeinen Nutzungsbedingungen von der Verarbeitung von Daten über die Aktivität des Nutzers außerhalb von Facebook abhängig zu machen und diese ohne Einwilligung zu verarbeiten.

Gegen den Beschluss legte der Meta-Konzern Beschwerde beim OLG Düsseldorf ein. Das OLG-Düsseldorf wendete sich zur Vorabentscheidung an den EuGH, um eine Auslegung des Europäischen Rechts herbeizuführen.

Konkret wollte das OLG Düsseldorf vom EuGH u. a. wissen, ob das Bundeskartellamt das Datenschutzrecht prüfen und mittelbare Verstöße sanktionieren darf. Weiter sollte geklärt werden, auf welche Rechtsgrundlage sich Meta bei der Datenverarbeitung von Off-Facebook-Daten berufen kann.

Zur Entscheidungsbefugnis des Bundeskartellamts

Die Frage zur Entscheidungsbefugnis des Bundeskartellamts beantwortete der EuGH dahingehend, dass diese vorliegt, falls es darum geht, den Missbrauch einer marktbeherrschenden Stellung festzustellen und Maßnahmen zur Abstellung festzulegen. Auch Nutzugsbedingungen eines Unternehmens, die gegen den Datenschutz verstoßen, könnten ggf. den Missbrauch einer marktbeherrschenden Stellung belegen. Die Prüfung erfolge dann aber nur zu dem Zweck, den Missbrauch einer marktbeherrschenden Stellung festzustellen und ggf. Maßnahmen dagegen ergreifen zu können.

Die Einhaltung von Datenschutzanforderungen wird damit vom EuGH als potenziell wettbewerbsrelevant anerkannt.

Die Feststellungen der Wettbewerbsbehörden trete aber nicht an die Stelle der zuständigen Datenschutzaufsichtsbehörden. Es bestehe eine Abstimmungspflicht mit den zuständigen Datenschutzbehörden und die Pflicht zur loyalen Zusammenarbeit. Es müsse eine Berücksichtigung jeder Entscheidung oder Untersuchung der zuständigen Aufsichtsbehörde gewährleistet sein. Ein Gebrauch von den Befugnissen nach Art. 58 DSGVO (Untersuchungsbefugnisse, Abhilfebefugnisse usw.) sei den Datenschutzbehörden vorbehalten.

Zur Rechtfertigung für die Erfassung der Off-Facebook-Daten äußerte sich der EuGH wie folgt:

Vertragserfüllung

Eine Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 lit. b) DSGVO liege nur dann vor, wenn die Verarbeitung objektiv unerlässlich sei, um einen Zweck zu erfüllen, der notwendiger Bestandteil, der für die betroffene Person bestimmten Vertragsleistung sei. Der Umstand, dass die Verarbeitung im Vertrag erwähnt werde, oder für die Erfüllung des Vertrages von Nutzen sei, sei in diesem Zusammenhang unerheblich. Es sei vielmehr entscheidend, dass die Verarbeitung für die ordnungsgemäße Vertragserfüllung notwendig sei.

Die Personalisierung sei für den Nutzer zwar hilfreich, da damit die Einblendung von Werbung im Interesse des Nutzers ermöglicht werde, um die grundlegenden Dienste des Netzwerks anzubieten, sei die Personalisierung aber nicht erforderlich.

Berechtigte Interessen

Eine Erforderlichkeit der Datenverarbeitung zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten nach Art. 6 Abs. 1 lit. f) DSGVO sei nur gegeben, wenn drei Voraussetzungen vorliegen:

Die Verarbeitung müsse zur Verwirklichung dieses berechtigten Interesses absolut notwendig sein, es dürfe kein entgegenstehendes Nutzerinteresse bestehen und den Nutzern müsse das Interesse mitgeteilt werden (Informationspflicht Art. 13 Abs. 1 lit. d) DSGVO).

Einwilligung

Zur Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO stellte der EuGH fest, dass die Möglichkeit der Verweigerung bestehen müsse, ohne infolgedessen auf die Dienste verzichten zu müssen.

Zu den Erfordernissen einer Einwilligung wird auf den **Erwägungsgrund 42** zur DSGVO verwiesen. Dort heißt es in Satz 5: „Es sollte nur dann davon ausgegangen werden, dass sie (die betroffene Person) ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat[..a.]."

Auch bei einer marktbeherrschenden Stellung sei grundsätzlich eine Freiwilligkeit der Einwilligung möglich. Es müsse hier aber möglich sein, die Verweigerung der Einwilligung auf das Netzwerk selbst und auch auf Off-Facebook-Daten zu beziehen.

Dementsprechend findet sich in Satz 2 des **Erwägungsgrundes 43** folgende hilfreiche Interpretation zur Zwanglosigkeit einer Einwilligung wieder: „Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, […]oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

Fazit

Mit der Entscheidung des EuGH wurde die Stellung des Bundeskartellamtes als Wettbewerbsbehörde gestärkt. Um den Missbrauch einer marktbeherrschenden Stellung durch Meta zu begründen, durfte das Bundeskartellamt auch die Vorgaben der DSGVO prüfen. Damit wurde eine Weichenstellung für die Durchsetzung des Datenschutzrechts vorgenommen.

Hinsichtlich der Rechtfertigung der fraglichen Datenverarbeitung anhand der Vorgaben aus der DSGVO, hat der EuGH keine abschließenden Entscheidungen für den Einzelfall getroffen, sondern Leitlinien mit praktischer Relevanz für sämtliche Unternehmen entwickelt.

Der Streit geht nun zurück an das OLG Düsseldorf. Dort wird entschieden, ob die Untersagungsentscheidung in dem Bescheid des Bundeskartellamts von 2019 rechtmäßig war. Dabei wird unter Berücksichtigung des Urteils des EuGH geprüft werden, ob ein Rechtfertigungsgrund aus der DSGVO für die Verarbeitung der zusammengeführten Nutzerdaten besteht. &

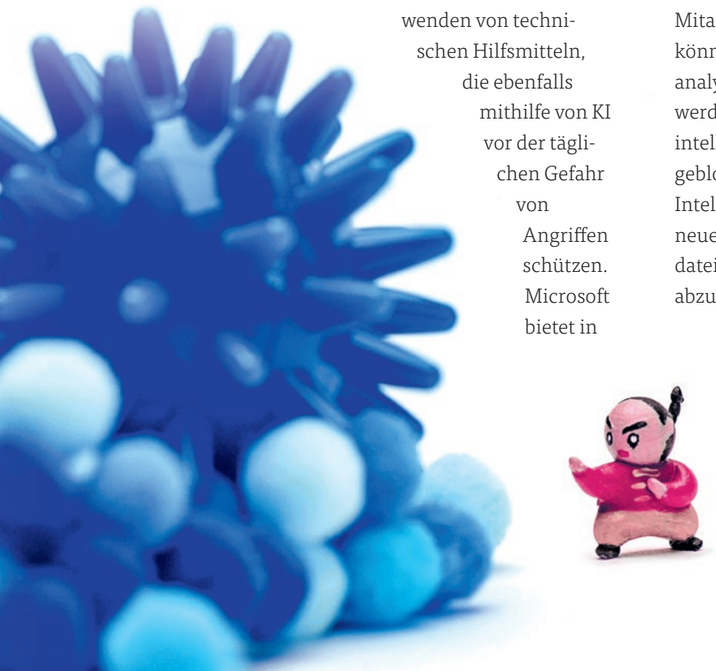
Viren, Malware & Co.: Schützt der Microsoft Defender for Endpoint Ihr Unternehmen?

Viren, Malware und Co. stellen eine große Bedrohung für Unternehmen dar. Doch wie kann man sich davor schützen? Microsoft bewirbt den hauseigenen Defender for Endpoint als effektive Lösung, die die Endgeräte der Nutzer und dadurch die Unternehmen vor Schäden bewahren soll. In diesem Beitrag betrachten wir, ob der Defender for Endpoint unterschätzt oder tatsächlich nur ein weiteres zu vernachlässigendes Tool ist.

Von David Armbrust

Viren, Malware und andere Schadprogramme stellen heutzutage eine ernstzunehmende Bedrohung für Unternehmen dar. Sie können nicht nur Daten und Informationen stehlen oder löschen, sondern auch gesamte IT-Infrastrukturen zum Stillstand bringen. Umso wichtiger ist es, dass sich Unternehmen mit einem effektiven Schutz gegen diese Bedrohungen wappnen.

Da Angriffe immer öfter die Unterstützung von künstlicher Intelligenz nutzen, ist eine weitere Maßnahme das Verwenden von technischen Hilfsmitteln, die ebenfalls mithilfe von KI vor der täglichen Gefahr von Angriffen schützen. Microsoft bietet in unterschiedlichen Lizenzplänen eine Fülle an Security- und Compliance-Lösungen – wie auch den Defender for Endpoint. Dieser wurde in den letzten Monaten immer wieder positiv bewertet. Doch was genau ist der Defender for Endpoint und wie schützt er Ihr Unternehmen?



Was ist der Defender for Endpoint?

Der Microsoft Defender for Endpoint ist eine von vielen Sicherheitsfeatures aus dem vielseitigen Microsoft-Portfolio und schützt plattformübergreifend die Endgeräte der Mitarbeitenden. Über eine zentrale Managementkonsole können Konfigurations- und Sicherheitsprobleme schnell analysiert und darauf reagiert werden. Bedrohungen werden automatisiert überwacht und können mit Hilfe von intelligenten Entscheidungsalgorithmen beobachtet oder geblockt werden. Es steckt hier also eine Art künstliche Intelligenz dahinter. Dadurch ermöglicht es der Defender, neue polymorphe und metamorphe Schadsoftware sowie dateilose und dateibasierte Bedrohungen zu erkennen und abzuwehren. Der Defender arbeitet im Hintergrund und überwacht alle Aktivitäten auf den Endgeräten der Mitarbeitenden.

Funktionsweise des Defender for Endpoint im Detail

Im Detail betrachtet arbeitet der Defender for Endpoint auf Basis von Cloud-Technologie und künstlicher Intelligenz. Dabei werden alle Geräte im Netzwerk überwacht und verdächtige Aktivitäten erkannt. Hierbei wird nicht nur auf bekannte Bedrohungen geachtet, sondern auch auf noch unbekannte Angriffsmethoden. Durch die Integration von Machine-Learning-Modellen ist es dem Defender for Endpoint möglich, Muster in den Datenströmen zu erkennen und darauf zu reagieren. So kann die Software schnell auf neue Bedrohungen reagieren und entsprechende Maßnahmen ergreifen, bevor es zu einem Schaden kommt.

Zusätzlich bietet der Defender for Endpoint auch Funktionen zur Risikobewertung (Risiken werden nur aufgrund der verarbeiteten Anmeldedaten berücksichtigt) von Geräten und Benutzern sowie zur Verwaltung von Sicherheitsrichtlinien. Dadurch können IT-Administratoren schnell auf potenzielle Schwachstellen im Netzwerk reagieren und diese beheben. Die Cloud-basierte Architektur des Defenders ermöglicht es, dass die Software ständig auf dem neuesten Stand ist und automatisch Updates erhält. Außerdem können Bedrohungen in Echtzeit erkannt werden, da die Daten aus verschiedenen Quellen zusammengeführt und analysiert werden. Darüber hinaus bietet der Defender for Endpoint auch eine umfassende Firewall-Funktionalität sowie ein Verhaltensanalyse-System, das ungewöhnliche Aktivitäten innerhalb des Netzwerks erkennen und blockieren kann.

„Bedrohungen werden automatisiert überwacht und können mit Hilfe von intelligenten Entscheidungsalgorithmen beobachtet oder geblockt werden“

Zuletzt ermöglicht es der Defender, über eine zentrale Verwaltungsoberfläche alle Geräte und Aktivitäten im Netzwerk einzusehen.

Wie sieht es mit dem Datenschutz aus?

Der Defender for Endpoint arbeitet auf Basis von Cloud-Technologien und künstlicher Intelligenz bzw. Machine-Learning. Dadurch benötigt er für einen einwandfreien Bedrohungsschutz die Verbindung zum Internet, nicht nur um global Informationen zu aktuellen Bedrohungen abzufragen, sondern auch, um Daten der Benutzersysteme zu teilen (Telemetriedaten). Zu diesen Daten zählen u.a. Dateidaten (z.B. Dateinamen, Größen und Hashes), Prozessdaten (ausgeführte Prozesse, Hashes) und Registrierungsdaten, Netzwerkverbindungsdaten (Host-IPs und Ports).

Durch die im Jahr 2023 eingeführte EU-Datengrenze wird zwar der Großteil der Kundendaten in europäischen Rechenzentren gespeichert und verarbeitet, jedoch werden Telemetriedaten der Benutzersysteme pseudonymisiert und verschlüsselt an Microsoft-Rechenzentren in den USA übermittelt und dort nur per Secure Admin Workstations (SAW) mit Just-In-Time-Zugriffsberechtigungen getrennt von anderen Nutzerdaten verarbeitet. Microsoft selbst sagt dazu, dass dies ein notwendiger Schritt ist, da in den USA die Kompetenzzentren für die Analyse, Erkennung und Weiterentwicklung von Algorithmen sitzen. Diese Rechenzentren sind allerdings wie alle anderen Rechenzentren zertifiziert.

Zudem sollte nichts an der allgemein vertretenen Strategie bzgl. des Einsatzes von US-Dienstleistern geändert werden, um nicht in absehbarer Zeit wieder Rechtsunsicherheiten bei den Datenverarbeitungen und Datenübermittlungen ausgesetzt zu sein. Zwar gilt seit dem 10.07.2023 das Angemessenheitsabkommen zwischen der EU und den USA, jedoch ist es möglich, dass der Angemessenheitsbeschluss durch den EuGH ein weiteres Mal gekippt wird. Ferner hat der EuGH während des Anfechtungsverfahrens die Möglichkeit, das neue Abkommen so lange auszusetzen, bis das Verfahren beendet wurde. Eine Entscheidung ist erst in den kommenden Jahren zu erwarten.

Fazit

Durch die Auswahl geeigneter Maßnahmen lassen sich Sicherheitsrisiken und Angriffe vermeiden. Besonders hilfreich können daher Systeme sein, die den Benutzern durch KI-Unterstützung unter die Arme greifen. Der Defender for Endpoint bietet für Unternehmen eine umfassende Lösung, die durch fortschrittliche Funktionen verdächtige Aktivitäten erkennen und blockieren kann. Durch die nahtlose Zusammenarbeit mit anderen Microsoft-Produkten bietet er so ein umfassendes Sicherheitsnetzwerk. Jedoch ist die Einhaltung von Datenschutzgesetzen und -bestimmungen, wie der Europäischen Datenschutz-Grundverordnung (DSGVO), ein entscheidender Faktor bei der Implementierung von Microsoft-Lösungen und sollte auch trotz neuem Angemessenheitsbeschluss nicht vernachlässigt werden. &

Operational Technology als Herausforderung: Fast jedes Unternehmen betroffen

Unsere Netzwerke sind immer häufiger mit Geräten und Systemen verbunden, die auf den ersten Blick nicht als „Computer“ im klassischen Sinne erkannt werden. Ein ganzheitlicher Blick auf (IT-)Sicherheit gewinnt an Bedeutung.

Von Thomas Althammer

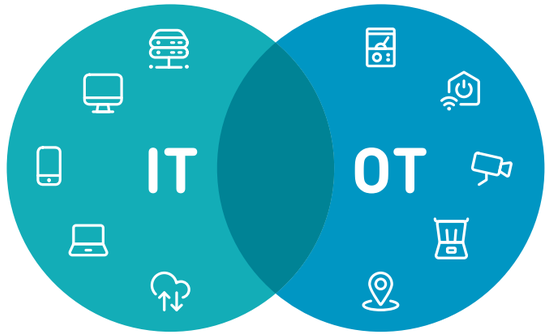
Die Digitalisierung schreitet voran und bringt Geräte mit sich, die nicht wie ein Computer oder ein Laptop aussehen. Gemeint sind Dinge wie Telefonanlagen, WLAN-Lautsprecher, Medizinprodukte oder Schließsysteme, die immer häufiger über Netzwerkschnittstellen verfügen. Im industriellen Umfeld wird IT-lastige Betriebstechnik aus Hardware und Software zur Steuerung von Anlagen als Operational Technology (OT) bezeichnet.

Traditionell gesehen beschreiben Informationstechnologie (IT) und OT verschiedene Welten, die in den letzten Jahren immer mehr zusammenwachsen. Selbst vermeintlich „normale“ Haushaltsgeräte wie Geschirrspüler, Backöfen und Kühlschränke verfügen immer häufiger über WLAN-Anschlüsse, Apps und extern steuerbare Technik. Moderne Gebäudesteuerung wie Wärmepumpen und Solaranlagen, aber auch Telefonanlagen sind ohne Computertechnik nicht mehr denkbar. Neben Telefonanlagen basieren spezielle Systeme wie Lichtrufanlagen oder Medizintechnik immer häufiger auf IT-Komponenten oder verfügen über Schnittstellen in IT-Netzwerke.

Wer kümmert sich um diese Systeme? Sind Verantwortlichkeiten klar festgelegt? Können Gefahren oder Sicherheitsvorfälle von diesen Systemen ausgehen oder könnten diese Systeme Ziel von Cyberattacken werden?

Internet der Dinge

Der Begriff Operational Technology ist keineswegs neu. Es existieren verschiedene Synonyme und artverwandte Bezeichnungen wie “Internet of Things (IoT)” oder „Industrie 4.0“. Das Prinzip dahinter ist, dass Geräte und Systeme immer weiter über Schnittstellen miteinander vernetzt werden, Informationen austauschen und somit sich gegenseitig beeinflussen können.



Der Windsensor auf dem Dach sorgt dafür, dass Außen-Jalousien automatisch bei Sturm eingefahren werden. Früher wurde dafür ein Kabel direkt verlegt. An diese Stelle tritt heute eine Wetterstation mit Netzwerk- oder WLAN-Anbindung, die digital die Witterungsinformationen an die Gebäudesteuerung überträgt.

Alle Branchen betroffen

Jedes Gerät mit einem Netzwerkanschluss enthält – so kann man sich das vorstellen – einen kleinen Computer. Dieser ist meist auf die konkret benötigten Funktionen angepasst, ist aber dennoch grundsätzlich ein Angriffsziel in Sachen Sicherheit und kann unter Umständen auch für andere Zwecke missbraucht werden. So konnten in der Vergangenheit beispielsweise WLAN-Kameras von außen gekapert und ferngesteuert werden. Im Rahmen von Penetrationstests wurde gezeigt, dass über Schwachstellen in solchen Überwachungskameras Zugriff auf das gesamte IT-Netzwerk erlangt werden konnte. Systeme im Umfeld von OT sollten bei der Betrachtung von IT-Risiken in Absicherungskonzepte mit einbezogen werden. Dazu gehören im weiteren Sinne auch Drucker, Kopierer, Zutrittskontrolle, Lichtsteuerung und viele andere Geräte mit digitalen Schnittstellen.

Netzwerk überprüfen und absichern

Systeme im Umfeld von OT sind nicht per se unsicher, sind sie aber von außen erreichbar und nicht von anderen IT-Systemen abgeschottet, können sie durch Konfigurationslücken oder veraltete Software (sogenannter Firmware) zu einer Schwachstelle im Netzwerk werden. Die folgende Tabelle stellt eine Reihe von Schutzmaßnahmen vor, um für einen möglichst sicheren Betrieb zu sorgen.

Maßnahme	Beschreibung
Zuständigkeit	Klären Sie Zuständigkeiten: Wer ist im Unternehmen konkret für den Betrieb und die Wartung von OT-Systemen verantwortlich?
Inventarisierung	Führen Sie eine Bestandsaufnahme durch und legen Sie ein Verzeichnis von allen Geräten und Systemen im Netzwerk an – nicht nur Computer, Laptops und Server.
Sichere Konfiguration	Überprüfen Sie die Konfiguration der eingesetzten Systeme, insbesondere wenn diese von Fremdfirmen in Betrieb genommen wurden. Nutzen Sie starke Passwörter.
Updates und Patch-Management	Installieren Sie regelmäßig verfügbare Updates/Patches der jeweiligen Hersteller. Wird vom Hersteller keine Wartung mehr angeboten, prüfen Sie einen Austausch der Systeme.
Backup und Wiederherstellung	Auch Operational Technology kann Daten verlieren oder ausfallen. Führen Sie in angemessenen Abständen ein Backup der Konfiguration/Daten durch.
Datenträger/Cloud-Dienste	Ergreifen Sie Schutzmaßnahmen für mobile Datenträger oder eine etwaige Cloud-Anbindung, z. B. durch Verschlüsselung.
Netzwerk-Segmentierung	Unterteilen Sie Ihr Netzwerk in verschiedene Zonen und Segmente. Sorgen Sie für eine Absicherung der Zugänge und Übergänge in Ihrer Firewall bzw. in Ihrem Netzwerk-Management
Protokollierung und Überwachung	Überwachen Sie Meldungen der Systeme und sorgen Sie dafür, dass Auffälligkeiten erkannt werden, z. B. durch eine Alarmierung.
Ereignismanagement	Treffen Sie Vorkehrungen für Probleme und Ausfälle: mit einem Incident-Response-Konzept wappnen Sie sich für Störungen oder Sicherheitsvorfälle.
Schulung	Schulen Sie Ihre Mitarbeitenden und sorgen Sie für Bewusstsein, damit Auffälligkeiten erkannt und gemeldet werden.

Ganz konkret empfiehlt sich ein Schwachstellen-Scan und eine Überprüfung auf Anfälligkeiten. Dies sollte in regelmäßigen Abständen wiederholt werden, denn Geräte und Systeme, die nicht auf den ersten Blick als Computer erkannt werden, werden meist nicht mit Updates oder Patches versorgt – sodass sich Schwachstellen zu einer tickenden Zeitbombe entwickeln können.

In eigener Sache

Sprechen Sie uns bei weitergehendem Beratungsbedarf gern an!

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

Datenschutzmanagement, Runde zwei

Nach der positiven Resonanz auf den ersten Kooperationskurs mit der Hochschule Hannover ging nun zum zweiten Mal der Kurs „Datenschutzmanagement“ an den Start.

Im Wechsel aus Online- und Präsenzphasen können Interessierte sich über ein Semester lang tiefgehend mit Datenschutz und damit verbundenen Aspekten beschäftigen. Hier trifft wissenschaftliche Theorie der Lehrendenden auf praktische Expertise aus dem Arbeitsalltag der Beratenden von Althammer & Kill. Alle Inhalte werden dabei anhand von Beispielen greifbar gemacht.

Die Module

Datenschutzrecht: Im Modul Datenschutzrecht liegt der Fokus sowohl auf den nationalen als auch auf den internationalen und kirchlichen Grundlagen des Datenschutzes. Exkurse in weitere Bestimmungen wie dem Telekommunikation-Telemedien-Datenschutz-Gesetz runden das Modul ab.

Technische und organisatorische Maßnahmen: Im technischen Datenschutz geht es auch, aber nicht nur, um Mobile Device Management, die Cloud, Malware oder Patch-Management. Der Faktor Mensch ist ein relevanter Sicherheitsfaktor und wird deshalb ebenfalls ausgiebig behandelt.

Praxistransfer und Umsetzung: Dieses Modul widmet sich der praktischen Umsetzung von zentralen Datenschutz-Faktoren. Sie erlernen unter anderem, wie Sie eine Datenschutz-Folgenabschätzung erfolgreich umsetzen, wie ein Verarbeitungsverzeichnis erstellt und gepflegt wird und was im Falle einer Datenpanne zu tun ist.

Change Management: Datenschutz erfordert oft Änderungen an Strukturen und Prozessen. Um diese innerhalb eines Unternehmens einzuführen, bedarf es Fingerspitzengefühls. Im Modul Change Management lernen Sie verschiedene Ansätze zur Beherrschung und Steuerung von Wandel kennen und erfahren, wie Widerstände umgangen werden können.

Kurs verpasst?

Wer die Anmeldung verpasst hat, kann sich schon jetzt bei Christina Ahrberg von der Hochschule Hannover für den nächsten Kurs vormerken lassen: *weiterbildung@hs-hannover.de*

Mehr zum Thema: *https://www.althammer-kill.de/hochschulzertifikatskurs-datenschutzmanagement*

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*

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

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

Althammer & Kill Akademie

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

Hier klicken oder scannen!

20. September 2023 – kostenloses Webinar
Das Hinweisgebersystem von Althammer & Kill

Wir erklären die Richtlinie, zeigen Anforderungen und Pflichten auf und stellen Ihnen das Hinweisgebersystem von Althammer & Kill vor.

Dieses lässt sich ganz einfach bei Ihnen einbinden, behandelt alle Daten völlig anonym und erfüllt die Anforderungen an die Richtlinie optimal. So können Sie Ihre Meldestelle einfach und nach der EU-Whistleblower-Richtlinie implementieren.

27. September 2023 – kostenloses Webinar
Microsoft 365, AWS & Co. – sicher in die Cloud

Microsoft 365, Amazon Web Services und Co. sind ein Problemfall für Datenschützer – denn es sind sogenannte „Cloud-Dienste“.

Wir stellen Ihnen die datenschutzrechtliche Einordnung und Umsetzungsmöglichkeiten unter praktischen Gesichtspunkten vor, zeigen worauf Entscheider im Rahmen ihrer IT-Strategie achten sollten und welche rechtlichen Herausforderungen bei der Einführung von cloud-basierten Diensten gemeistert werden müssen.

4. Oktober 2023 – kostenloses Webinar
Security Awareness: Der Weg zur Human Firewall

Systeme werden immer sicherer und dennoch sind erfolgreiche Hacker-Angriffe an der Tagesordnung.

Wie passt das zusammen? Menschen können ein effektiver Schutz gegen Angriffe sein, wenn sie die Bedrohung kennen. Cyber-Security im Zeitalter von Cloud und Co. bedeutet vor allem, dass ein Bewusstsein bei Mitarbeitenden geschaffen werden muss.

11. Oktober 2023 – 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.

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

25. Oktober 2023 – kostenloses Webinar
Bring Your Own Device – Fallstricke vermeiden

Privathandy im Firmenkontext? Bring your own device (BYOD) ist hier das Zauberwort.

Aus der Perspektive der Informationssicherheit und des Datenschutzes ist der BYOD-Ansatz jedoch risikobehaftet und es ist eine sorgfältige Abwägung erforderlich. Wir zeigen Risiken auf und geben Maßnahmenempfehlungen aus Datenschutz- und Informationssicherheits-Perspektive.

Haben Sie Fragen?

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

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

Frisch dabei und trotzdem mittendrin

Auch wenn sie noch zu den Dienstjüngeren gehört,
hat Alexandra ihren Platz im Team schon längst gefunden.

Wir haben ihr nach gut einem Jahr bei Althammer & Kill über die Schulter geschaut.

Wer bist du? Welche Ausbildung hast du?

Hallo, Ich bin Alexandra von Senden. Nach dem Abitur habe ich zunächst eine Ausbildung im Einzelhandel absolviert, danach ein Abendstudium zur Kommunikationswirtin drangehängt, habe aber mittlerweile einen bunten Lebenslauf über Selbständigkeit und diverse Werbe- und Multimedia-Agenturen.

Wie lange arbeitest du schon bei Althammer & Kill?

Ich bin seit August 2022 dabei – aber es fühlte sich von Anfang an sehr vertraut an. Ich hatte eine tolle Einarbeitung und so viele nette KollegInnen, dass der Einstieg leichtfiel.

Wie hat es dich zu Althammer & Kill verschlagen?

Unverhofft kommt oft – so wurde mein letzter Arbeitgeber von dem Hersteller der Software, die wir als Platinum-Reseller vertrieben haben, leider aufgekauft und damit alle

entlassen; nur die Geschäftsführer wurden übernommen. Das war nach 26 Jahren, die ich dort bereits arbeitete, etwas plötzlich. Aber ich fand über die geläufigen Jobportale schnell die ausgeschriebene Stelle bei Althammer & Kill. Entschieden habe ich mich dafür, weil es gut zu meinem Aufgabenspektrum passte.

Was sind deine Aufgaben?

Im Grunde genau das, was ich vorher unter anderem auch gemacht habe: Der Schwerpunkt liegt im Auftragsmanagement mit etwas Officemanagement drumherum. Das heißt, ich bekomme die beauftragten Leads vom Vertrieb und wandele diese in Aufträge um, lege Auftragsrollen an, erstelle Verträge und Urkunden für den Kunden und informiere den zuständigen Berater über den neuen Auftrag, damit er mit dem Kunden Kontakt aufnehmen kann.

Was gefällt dir besonders an deiner Tätigkeit?

Ich mag es nicht, wenn man nicht über den Tellerrand schaut, daher passt der Job umso besser. Es ist für mich ideal, in dieser Schnittstellenfunktion zwischen Vertrieb und Berater zu arbeiten. Auch mit der Buchhaltung ergeben sich Berührungspunkte, wenn z. B. etwas storniert oder angepasst werden muss. Mit den Kunden habe ich ebenso gelegentlich Kontakt, wenn es manchmal Änderungswünsche oder Fragen zum bestehenden Auftrag gibt.

Wie sieht dein Alltag bei Althammer & Kill aus?

Morgens checke ich erst mal die allgemeinen Postfächer und verteile die eingegangenen Anfragen. Dann haben wir um 9:00 das Vertriebsdaily, was sehr wichtig ist für die Schnittstellenfunktion zwischen Vertrieb und Beratung. Dabei ergeben sich auch immer mal wieder Dinge, die neu definiert, oder Abläufe, die umstrukturiert werden müssen. Spätestens dann muss ein Kaffee sein 😉. Ansonsten bearbeite ich dann überwiegend die eingegangenen Aufträge und was noch so anliegt. Einmal wöchentlich stimme ich mich mit der Organisationsentwicklung ab, da geht es meist um Prozesse und aktuelle Themen, da ist es sehr wichtig immer am Ball zu bleiben und Dinge anzupassen.

„Ich hatte eine tolle Einarbeitung und so viele nette KollegInnen, dass der Einstieg leichtfiel.“

Welches Projekt hat dir in deiner Zeit bei Althammer & Kill am besten gefallen?

Ich arbeite nicht wirklich projektbezogen – aber da wir Anfang 2023 eine Softwareumstellung hatten, mussten in allen Bereichen viele Prozesse angepasst oder neu gedacht werden. Es macht mir sehr viel Spaß, Abläufe zu optimieren oder welche zu entwickeln, wo noch keine sind. Kurz nach meinem Eintritt bei Althammer & Kill ging es verstärkt um das Hinweisgeberschutzgesetz, das war so ein Beispiel, wo es galt, ein neues Produkt in die bestehenden Abläufe zu integrieren.

Deine Aufgabenbereiche sind sehr vielfältig. Wie schaffst du es da, den Überblick zu behalten?

Ja, manchmal geht es sehr turbulent zu, wenn man gerade konzentriert in einer Sache steckt und es an der Tür oder das Telefon klingelt und vielleicht gleichzeitig noch ein Kollege eine Frage hat, ein Essen bestellt und ein Seminarraum gebucht werden soll… – ach ja, da waren auch noch zwei Umzüge von unseren Standorten in Mannheim und Düsseldorf zu organisieren. Da muss man sich schon Zeitfenster blocken, in denen man mal nicht zu sprechen ist. Aber zum Glück ist ja nicht jeder Tag so.

Welche Bitte oder Anfrage erhältst du von Kolleginnen und Kollegen am häufigsten?

Das ist schwer zu verallgemeinern. Irgendwie ist jeder Tag anders und auch die Fragen. Oft sind es Fragen zu Aufträgen oder zu Abläufen.

Welche war die interessanteste Begegnung, die du jemals an der Eingangstür von Althammer & Kill hattest?

Schon zweimal traf ich Dienstleister aus meiner beruflichen Vergangenheit hier wieder – das war ein schönes Wiedersehen.

Worauf freust du dich morgens am meisten, wenn du ins Büro kommst?

Also der Kaffee bei uns im Büro ist schon sehr lecker! Und die KollegInnen sind auch alle supernett. Und der Rest ist die Überraschung, was mich so erwartet. &

ALTHAMMER & KILL

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
Standort Düsseldorf: Tel. +49 211 936748-0
Standort Mannheim: Tel. +49 621 121847-0

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

Qualitätsmanagement nach Plan mit der ISO 9001:2015.

Mitgliedschaften

NIEDERSACHSEN DIGITAL · BvD e.V. · FINSOZ · GDD