COMPLIANCE konkret

Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2022

TrustPid – das neue Datenschutzportal und seine Tücken

Kommt jetzt der Super-Cookie?
Seite 6

Gaia-X – kommt da noch was?
Gamechanger oder heiße Luft?
Seite 10

Verschlüsselung in der Cloud
Das müssen Sie zum Thema wissen
Seite 12

Das Lieferkettengesetz
Diese Pflichten ergeben sich daraus
Seite 18

Editorial

Liebe Leserin, lieber Leser,

über IT-Sicherheitsvorfälle wird täglich in den Medien berichtet. Doch wie ist es um die Lage in einzelnen Branchen konkret bestellt? Welche Verteidigungslinien und Schutzmaßnahmen sollten angegangen werden?

Gemeinsam mit der Arbeitsgruppe IT-Compliance vom Fachverband FINSOZ e.V. sind wir dieser Frage nachgegangen. Entstanden ist ein umfassender Lagebericht mit konkreten Handlungsempfehlungen für die Verbesserung der IT-Sicherheit im Gesundheits- und Sozialwesen. Neben Vorgehensweisen von Angreifenden werden im Bericht ebenso mögliche Abwehrsysteme aufgezeigt. So wird ein Überblick gegeben, sowohl über Datenschutz- und IT Sicherheitsvorfälle als auch über die Rechtslage.

Ein weiteres Thema dieser Ausgabe ist das Lieferkettensorgfaltspflichtengesetz. Ab 2023 sind Unternehmen ab 3.000 Mitarbeitenden dazu verpflichtet, ihrer menschenrechtlichen Verantwortung und Sorgfaltspflicht in ihren Lieferketten besser nachzukommen. Zu den Sorgfaltspflichten der Unternehmen zählen unter anderem die Einrichtung eines Risikomanagements und die Einrichtung eines Beschwerdeverfahrens im Falle von Rechtsverstößen.

So zeigt sich, dass jenes Gesetz ebenfalls eng mit der EU-Whistleblower-Richtlinie und der damit verbundenen Pflicht zum Einsetzen eines Hinweisgebersystems verknüpft ist. Hierbei kann der externe Compliance-Beauftragte Licht ins Dunkel bringen.

Im Interview sprachen wir mit Christian Bredlow, Geschäftsführer von Digital Mindset, wie er seine Kundinnen und Kunden durch die Herausforderungen der Digitalisierung begleitet und welche Rolle dabei Microsoft 365 spielt. Außerdem: Viele deutsche Firmen zeigen Interesse an Gaia X – wir werfen einen kritischen Blick auf das Projekt zum Aufbau einer Cloud- und Dateninfrastruktur.

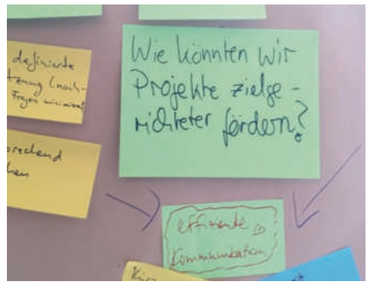
Wir wünschen Ihnen viel Spaß beim Lesen
und freuen uns auf den Diskurs mit Ihnen.

Thomas Althammer & Niels Kill

Darüber wird gesprochen

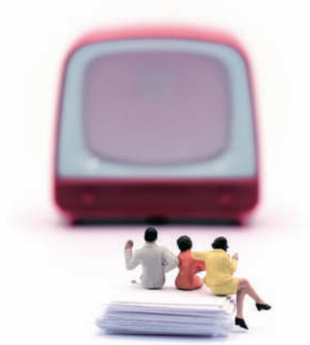
Diese und weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: *althammer-kill.de/news*

Hier klicken oder scannen!



Die Team-Tage 2022

Workshops, Quiz-Night, Brauereiführung – das waren die Althammer & Kill Team-Tage. Dieses Jahr trafen wir uns gesammelt im Sauerland in Meschede am Hennesee. Vom 7. bis 9. Juli hinterfragten wir Strukturen, suchten Lösungen für Probleme und lernten uns gegenseitig noch besser kennen. Bei dem ein oder anderen Kaltgetränk fällt das ja unter Umständen noch leichter.



Digitale Medizin: Datenschutz in der Videosprechstunde

Seit dem 01.04.2017 ist die Videosprechstunde als erste telemedizinische Leistung in die Regelversorgung aufgenommen. Wenn Arztpraxen und Kliniken Videosprechstunden anbieten wollen, haben sie sicherzustellen, dass der Datenschutz und das Patientengeheimnis in gleicher Weise gewahrt bleiben wie bei Vor-Ort-Sprechstunden.

Gastfreundlichkeit im Onlinehandel

Künftig sollen Onlinehändler noch „gastfreundlicher" werden, darauf einigten sich zumindest die Teilnehmer der DSK am 24. März 2022. Onlineshops sind somit nur noch mit einem sogenannten Gastzugang DSGVO konform. Das heißt, dass sich der Kunde künftig nicht bei jedem Onlinehändler registrieren muss. Vielmehr kann er – alternativ zum Anlegen eines Accounts im Onlineshop – als Gast bestellen. Hierfür muss der Kunde nur die für den konkreten Vertragsschluss notwendigen Daten angeben. Im Onlinehandel war es bisher regelmäßige Praxis, sich beim erstmaligen Bestellvorgang zu registrieren – dadurch muss der Kunde bei weiteren Bestellungen nur seinen Benutzernamen und sein Passwort eingeben.

Immer mehr Aufsichtsbehörden haben die Faxe(n) dicke

Immer mehr Aufsichtsbehörden haben sprichwörtlich die Faxen dicke. Erst recht, wenn es um die unverschlüsselte Übertragung von personenbezogenen Daten geht – eventuell sogar sensible. Bezogen auf die Datenübermittlung per Fax ist hierbei insbesondere an das Risiko des unbefugten Zugangs zu den versendeten Daten zu denken.

NGO Tour Recap

Nach 15 Stops, vielen hundert Kilometern und unzähligen Gesprächen ist die Microsoft NGO Tour nun vorbei. Wir haben vielen Vorträgen gelauscht und unsere eigene Keynote an jedem Tour-Stop präsentieren dürfen. Neben vielen interessanten Menschen, die wir an den zahlreichen Standorten kennenlernen durften, stellten wir fest, dass beim Thema Datenschutz im Kontext Microsoft 365 weiterhin viele Unsicherheiten existieren. Unser Vortrag trug dazu bei, für etwas mehr Klarheit zu sorgen.

Welche Daten dürfen in der Cloud gespeichert werden?

Viele Organisationen betreiben bisher Ihre IT-Infrastruktur in den eigenen Rechenzentren. Dabei können alle Daten und Informationen bedenkenlos auf den Dateiablageservern oder fachspezifischen Anwendungsservern gespeichert oder verarbeitet werden, denn die Daten und Informationen liegen in den eigenen Räumlichkeiten. Möglicherweise sollen nun aber wegen einer Strategieänderung Cloud-Ressourcen und -Dienste wie bspw. Microsoft-365-Produkte oder spezielle Fachanwendungen aus der Cloud genutzt werden. Folglich werden Informationen und Daten dann nicht mehr in den eigenen Rechenzentren gespeichert und verarbeitet, sondern bei einem externen Anbieter. Unbedacht sollten Sie diese strategische Änderung nicht umgesetzt werden.

Zahl des Monats

3.000

In Deutschland ansässige Unternehmen ab einer Größe von 3.000 Mitarbeitenden werden durch das Lieferkettensorgfaltspflichtengesetz dazu verpflichtet, ihrer menschenrechtlichen Verantwortung und Sorgfaltspflicht in ihren Lieferketten besser nachzukommen.

Messen

Lassen Sie uns auf einer der nächsten Messen ins Gespräch kommen:

2.–4. November 2022, München
BeB Fachtagung
https://beb-ev.de/veranstaltung/fachtagung-dienstleistungsmanagement-2022/

15.–17. November 2022, Bielefeld
KommDigitale
https://kommdigitale.de/

7.–8. Dezember 2022, Nürnberg
ConSozial
https://www.consozial.de/

FINSOZ e.V. Digitalverband Sozialwirtschaft

IT-Sicherheit in der Sozialwirtschaft – Lagebericht & Leitfaden

Der Bericht, bei dem Thomas Althammer federführend mitwirkte, gibt einen Überblick zu Datenschutz- und IT-Sicherheitsvorfällen, erklärt Vorgehensweisen von Angreifern wie auch Verteidigungslinien zur Abwehr und liefert einen Überblick zur Rechtslage im Kontext IT-Sicherheit. Nicht-Mitglieder können den Bericht gegen eine Gebühr von 50,– € per E-Mail anfordern:
info@finsoz.de

Unser Podcast

„Maximale Langeweile" beschäftigt sich mit aktuellen Themen aus der Welt der Compliance. Besonderer Schwerpunkt bilden die Themen Datenschutz und Cyber-Security. Kontroverse Diskussionen werden dabei in den Vordergrund gerückt, während harte juristische oder technische Fakten eher den Unterbau bilden. „Maximale Langeweile" erscheint jeden zweiten Donnerstag auf Spotify, bei Apple Podcast und weiteren gängigen Podcast-Diensten.

TrustPid – das neue Datenschutzportal und seine Tücken

„Erhalte das freie Internet“ – Mit diesem Slogan wirbt der Mobilfunkkonzern Vodafone für sein neu entwickeltes Datenschutzportal TrustPid. Doch was ist TrustPid und inwiefern kann es wirklich zur Erhaltung eines kostenlosen Internets beitragen? Was ist bei der Nutzung zu beachten und warum schlagen Datenschützer Alarm?

Seit Einführung des Cookie-Banners, der Umsetzung eines lang erwarteten EuGH-Urteils, gibt es für den Internetnutzenden die Möglichkeit, unerwünschte Cookies auf Websites zu blockieren. Zum Unmut vieler Werbetreibenden, da dies personalisierte Werbung und entsprechendes Tracking erheblich erschwert.

Worum geht’s?

Händeringend wurde daher nach einem neuen Geschäftsmodell gesucht. Mobilfunkkonzerne, allen voran Vodafone, glauben nun mit TrustPid die Lösung für dieses Problem gefunden zu haben. Cookies sollen hierbei der Vergangenheit angehören und durch eine Art Web-ID ersetzt werden. Hierbei wird die Mobilfunknummer des Nutzenden in Kombination mit der IP-Adresse verwendet, um ein Pseudonym zu kreieren. Mithilfe dieser Kennung soll es Werbetreibenden ermöglicht werden, hieraus ein Personenprofil zu erstellen und Tracking-Aktivitäten zuzulassen.

Hier kommt wieder der Slogan ins Spiel, mit dem für TrustPid geworben wird. Dabei soll, laut einer Aussage aus dem Portal, der durchschnittliche Nutzende seinen Teil dazu beitragen, dass personalisierte Werbung im Internet weiterhin ermöglicht wird. Das Internet soll somit durch TrustPid weiterhin kostenlos und frei zugänglich bleiben. Grundsätzlich eine noble Aufgabe, die Vodafone sich hier vorgenommen hat. Doch wie funktioniert das Ganze?

Pseudonym und Super-Cookie

Die Methodik dahinter stützt sich laut Betreiber Vodafones auf die Rechtsgrundlage der Einwilligung. Hierbei bezeichnet Vodafone die Arbeitsweise von TrustPid als „transparent, sicher und DSGVO-konform“. Ob dies der Realität entspricht, ist fraglich. Zum einen scheint es bedenklich, eine Tracking-Sperre zu umgehen, die vom obersten europäischen Gericht als rechtskräftig notwendig erachtet wurde. Zwar erhalten Werbetreibende nur die pseudonyme Nennung, also nicht die konkrete Mobilfunknummer des Nutzers, jedoch bekommen sie durch TrustPid auch die Möglichkeit, dies einem Benutzerprofil zuzuordnen. Dieses Benutzerprofil wächst mit jedem Besuch einer neuen Website kontinuierlich. Diese Herangehensweise wird nicht ohne Grund von Kritikern als „Super-Cookie“ bezeichnet.

Als Vorreiter einer solchen Strategie kann man Vodafone aber keineswegs bezeichnen. Bereits 2012 entwickelte der US-Provider Verizon eine ähnliche Methode, seine Nutzenden zu tracken. Bereits damals musste der Konzern aufgrund des Einsatzes des „Super-Cookies“ eine Geldstrafe zahlen.

Dass die Idee von Mobilfunkprovidern umgesetzt wird, kommt nicht von ungefähr. Zukünftig könnten sie ihre Monopolstellung nutzen, um die Regelungen um den Cookie-Banner zu umgehen. Denn die Möglichkeit Mobilfunknummern zu verwenden, um Kennungen zu erstellen, hat nicht jeder. Denn selbst wenn durch den Browser Cookies gelöscht werden, oder eine IP-Adresse geändert wird, um dem Tracking zu entkommen, hat der jeweilige Mobilfunkbetreiber immer noch die Möglichkeit, einen Nutzer und dessen Verhalten durch die Kennung der Mobilfunknummer zu identifizieren.

Wie ist das mit dem Datenschutz?

Doch wie ist TrustPid datenschutzrechtlich tatsächlich aufgestellt? Ein Blick in das TrustPid-Portal verrät einiges. Die Website wirkt unausgereift und zeigt einmal mehr, dass sich das Projekt noch in der Testphase befindet.

Aus datenschutzrechtlicher Sicht zeigt sich das Portal nicht von seiner besten Seite. Zwar heißt es in der Datenschutzerklärung der Website: „Wir nehmen den Schutz der Privatsphäre unserer Nutzer sehr ernst“, doch selbst einfache Anforderungen scheinen auf den ersten Blick nicht erfüllt. Ein Impressum, welches rechtlich verpflichtend ist, befand sich zunächst nicht auf der Webseite– mittlerweile wurde hier nachgebessert.

Und auch mit der Thematik Google Analytics und den in mehreren Ländern der EU ausgesprochenen Untersagungen, hat man sich augenscheinlich nicht näher beschäftigt. Nach Auffassung des österreichischen Datenschutzbeauftragten böten die Standarddatenschutzklauseln (SCC) von Google kein angemessenes Schutzniveau, da Google der Überwachung durch US-Geheimdienste unterliegt und die aufgeführten Maßnahmen im SCC nicht ausreichend seien. Und genau dieses Analyse-Tool wird auf der Webseite von TrustPid verwendet.

„Dass die Idee von Mobilfunkprovidern umgesetzt wird, kommt nicht von ungefähr. Zukünftig könnten sie ihre Monopolstellung nutzen, um die Regelungen um den Cookie-Banner zu umgehen.“

Zuletzt aktualisiert wurden die Datenschutzhinweise auf der Website laut eigenen Angaben am 1. Juli 2022. Viele Stimmen aus der Presse haben sich zuvor eher kritisch über TrustPid geäußert und datenschutzrechtliche Mängel hervorgehoben. Hier versucht man nun wohl mit mehr Transparenz entgegenzuwirken, auch wenn weitere datenschutzrechtliche Fragestellungen, wie der Einsatz von Google Analytics, bestehen bleiben.

Zukunftsmusik?

Nichtsdestotrotz läuft das Projekt TrustPid bereits bei einigen Websitebetreibenden, wie beispielsweise Bild.de. Hier ploppt bei Besuch der Website ein Cookie-Banner auf, der TrustPid zwar nicht explizit erwähnt, die Nutzung des Portals in der Datenschutzerklärung jedoch näher beschrieben wird.

Zwar erklärt Bild.de in seiner Datenschutzerklärung auch, dass ein Widerruf der Einwilligung zum Tracking durch TrustPid jederzeit möglich sei. Klickt man aber auf den zur Verfügung gestellten Link, landet man auf der TrustPid-Startseite. Hier kann man sich zwar über die Vorzüge des Tools informieren, aber eine Möglichkeit zum Widerruf findet sich dort nicht. Obwohl der EU-Gesetzgeber verlangt, dass dieser genauso einfach abzugeben sein sollte, wie die Einwilligung selbst. Also, im Zeitalter des Internets und unter Berücksichtigung der Bequemlichkeit des durchschnittlichen Users, durch wenige Klicks.

Konfigurationen hinsichtlich einer Einwilligung bzw. eines Widerspruchs können nur mit einem Provider vorgenommen werden, der an TrustPid teilnimmt – bspw. Telekom-Nutzende gucken hierbei (noch) in die Röhre.

Es bleibt abzuwarten, wie TrustPid sich entwickelt. Die datenschutzrechtlichen Bedenken stehen immer noch im Raum. Die Aufsichtsbehörde für Datenschutz in Nordrhein-Westfalen hat bereits die Wirksamkeit der Einwilligung der Nutzenden laut Presseberichten hinterfragt und eine datenschutzrechtliche Kontrolle des TrustPids angekündigt. &

Die Menschen hinter Althammer & Kill:

Sören Preuße

Ja hallo, wer bist du denn?

Sören: Hi, ich bin Sören, 29 Jahre alt und komme aus Harsum bei Hildesheim. Gelernt habe ich Industriekaufmann bei einem mittelständischen Unternehmen. Nach meiner Ausbildung hat es mich sofort in den Vertrieb gezogen, dem ich bis heute treu geblieben bin.

Wie lange arbeitest du schon bei Althammer & Kill?

Sören: Mittlerweile sind es etwas über 1,5 Jahre. Das Arbeiten und das Miteinander bei A&K machen sehr viel Spaß und ich freue mich auf weitere spannende Jahre.

Was sind Deine Aufgaben?

Sören: Ich berate und betreue potenzielle Neukunden und Bestandskunden von der Anfrage bis hin zur Angebotsannahme. Natürlich stehe ich den Kunden auch danach noch bei vertrieblichen Fragen zur Verfügung, aber im Grunde endet dort meine Arbeit. Abgestimmt auf die Bedürfnisse der Kunden erstelle ich individuelle Angebote und versuche Lösungen für ihre Hürden zu finden.

Was gefällt dir besonders an der Tätigkeit des Vertriebs-Mitarbeiters?

Sören: Am meisten gefällt mir der direkte Kontakt und Austausch mit den Kunden. Es macht Spaß, wenn man helfen kann und ein positives Feedback erhält.

Wie sieht dein Alltag als Vertriebs-Mitarbeiter bei Althammer & Kill aus?

Sören: Es ist ein guter Mix aus wiederkehrenden Aufgaben und neuen Herausforderungen. Als erstes plane ich den Tag, indem ich mein E-Mail-Postfach checke und meine anstehenden Aufgaben priorisiere. Danach gilt es diese Aufgaben abzuarbeiten – Angebote schreiben und Kundengespräche führen. Zwischendurch kommen immer mal wieder Telefonate von Interessenten rein oder es finden Kundentermine statt.

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

Sören: Etwas Besonderes war auf jeden Fall das erste Projekt, welches ich eigenständig vom Anfang bis zum Ende begleitet habe. Es fing an mit einer Anfrage zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Nach mehreren Angeboten und Gesprächen hat uns der Kunde schlussendlich beauftragt. Mittlerweile ist das Projekt abgeschlossen und der Kunde ist zufrieden, was mich natürlich auch zufrieden stimmt.

Welche Leistungen sind aktuell bei Kunden besonders gefragt?

Sören: Dauerbrenner ist die Stellung des externen Datenschutzbeauftragten. Datenschutz ist das Thema, mit dem A&K damals angefangen hat. Gerade in der Gesundheits- und Sozialbranche haben wir uns in diesem Bereich einen sehr guten Ruf erarbeitet. Durch die bevorstehende Umsetzung der EU-Whistleblower-Richtline wird aber auch das Thema Compliance immer interessanter, was man auch an der Häufigkeit der Anfragen merkt.

Welche war die skurrilste/lustigste/interessanteste Anfrage, die du in deiner Zeit hier bekommen hast?

Sören: Eine spezielle Anfrage kann ich da gar nicht nennen. Es kommen häufig interessante Anfragen rein. Einmal haben wir eine Anfrage von einem Unternehmen bekommen, welches ihren Hauptsitz auf der Isle of Man hat. Ich war etwas verwundert und musste den Namen erstmal googlen, da ich vorher noch nichts von dieser Insel gehört hatte. Mittlerweile ist die deutsche Tochtergesellschaft einer unserer Kunden.

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

Sören: Zunächst nehme ich mit dem Kunden Kontakt auf und vereinbare einen Termin für ein kurzes Kennenlernen. Der aktuellen Situation geschuldet, finden diese Termine meist per Videokonferenz oder Telefon statt. In dem Gespräch versuche ich durch gezielte Fragen die Bedürfnisse des Kunden herauszufinden. Im Anschluss setze ich mich an die Angebotserstellung. Im Optimalfall können wir den Kunden recht schnell von uns und unseren Leistungen überzeugen und die unterschriebene Angebotsannahme entgegennehmen. An diesem Punkt endet größtenteils mein Aufgabenbereich und das Projekt wandert zum Beratungsteam. &

Gaia-X – kommt da noch was?

Die Digitalisierung ist eines der zentralen Themen in Politik und Gesellschaft. Die Ampel-Regierung will Versäumnisse der letzten Jahre aufarbeiten und spricht von Künstlicher Intelligenz, Quantentechnologien und Cybersicherheit als digitale Schlüsseltechnologien. Auch das Wort Gaia-X fällt.

Doch was ist Gaia-X? Und wird Gaia-X eine gewichtige Rolle in der Digitalisierung spielen?

Das europäische Cloud-Ökosystem

Gaia-X ist ein Projekt des Bundesministeriums für Wirtschaft und Energie sowie der deutschen Wirtschaft und Wissenschaft, welches auf dem Digitalgipfel 2019 erstmalig der Öffentlichkeit präsentiert wurde. Es wird angestrebt, eine leistungs- und wettbewerbsfähige, sichere und vertrauenswürdige Dateninfrastruktur für Europa zu schaffen. Dabei orientiert sich das Projekt an den Leitprinzipien: Europäischer Datenschutz, Offenheit und Transparenz, Authentizität und Vertrauen, Souveränität und Selbstbestimmung, Freier Marktzugang und europäische Wertschöpfung, Modularität und Interoperabilität, Nutzerfreundlichkeit.

Das Projekt zielt darauf ab, dezentrale Infrastrukturdienste (insb. Cloud- und Edge-Instanzen) zu vernetzen und in einem homogenen, nutzerfreundlichen System zu vereinen. Basierend auf bereits existierenden Lösungen bzw. deren Weiterentwicklung sollen aus Europa wettbewerbsfähige Angebote für die Welt entwickelt werden. Daher stehen auch außereuropäischen Marktteilnehmern die Mitwirkung an diesem Projekt offen, sofern die formulierten Ziele der Datensouveränität, Datenverfügbarkeit und Interoperabilität geteilt werden. Im Januar 2021 wurde der gemeinnützige Verein Gaia-X European Association for Data and Cloud AISBL gegründet, der das Ziel hat, den technischen Rahmen zu entwickeln und die Dienste der Gaia-X Federation zu betreiben.

Seit Gründung haben sich dem Projekt 300 Mitglieder aus der ganzen Welt angeschlossen, wie bspw. Anbieter oder Nutzer von Dateninfrastrukturen, IT-Start-ups, Forschungseinrichtungen und Wirtschaftsverbände. Kernpunkte sind dabei die Interoperabilität auf Netzwerk-, Daten- und Dienstebene sowie eine Kollaboration zwischen Edge- und Cloud-Instanzen. Letzterer Aspekt erfordert das Aufbrechen von Datensilos und die Definition gemeinsamer Standards bzw. Datenschnittstellen. Sollte es gelingen, kann dies zu Effizienzvorteilen führen. Voraussetzung für ein Gelingen ist eine einheitlich existierende Referenzarchitektur für (redundante) Knotenpunkte innerhalb der Dateninfrastruktur, die eine optimale (Rechen-) Leistungsverteilung ermöglichen muss.

Identität und Vertrauen

Anders als die großen und weltweit agierenden Cloud-Anbieter möchte Gaia-X eine Vielzahl von (Cloud-)Angeboten verbinden und so ein Ökosystem unterschiedlichster Dienste darstellen. Um die Sicherheit im Ökosystem zu wahren sind die Parameter Identität und Vertrauen zentrale Eckpfeiler. Gaia-X verweist hierfür auf das Gaia-X Trust Modell, in dem verschiedene Akteure (Entitäten) die Einhaltung der Sicherheit definieren und schlussendlich auch prüfen. Im Zentrum des Gaia-X Trust Modells steht die Selbstbeschreibung. Selbstbeschreibungen sind W3C-überprüfbare Darstellungen, die in einem maschinenlesbaren Format alle Entitäten beschreiben.

Somit wird es für alle Rollen bzw. alle Angebote der Teilnehmer eine Selbstbeschreibung geben. Jede GAIA-X-Entität stellt schlussendlich Selbstbeschreibungen bereit, die von Dritten validiert und signiert werden. In Anlehnung an das Vokabular des W3C Verifiable Credentials Data Models wird eine Selbstbeschreibung wie folgt erstellt:

W3C-Begriff	Beispiel mit einem Rechenzentrum
Anspruch	Mein Rechenzentrum ist sicher.
Überprüfbare Bescheinigung	Die Bescheinigung eines unabhängigen Auditors, dass mein Rechenzentrum sicher ist (bspw. Zertifikat ISO 27001)
Überprüfbare Präsentation (Nachweis)	Ich zeige meinem Kunden das Zertifikat.
Emittent	Der Auditor
Inhaber	Ich selbst
Prüfstelle	Mein Kunde

Neben den Selbstbeschreibungen sollen Gaia-X-Gütesiegel bei der Auswahl von geeigneten Anbietern unterstützen. Technisch gesehen sind Gaia-X-Gütesiegel ebenfalls verifizierbare W3C-Berechtigungsnachweise – sie enthalten eine Versionsnummer, um eine kontinuierliche Weiterentwicklung des Regelwerks zu ermöglichen. Neue definierte Regeln im Ökosystem führen dementsprechend zu einer erneuten Validierungspflicht, um die Einhaltungen der Vorschriften zu bestätigen. Aktuell stehen drei Gütesiegel zur Verfügung (Level 1–3), welche aufsteigend strengere Regeln bzgl. der Sicherheit und des Datenschutzes einfordern.

Stichwort
W3C

Das W3C ist ein Industriekonsortium, das versucht, Standards für die Entwicklung des Webs und die Interoperabilität zwischen WWW-Produkten (World Wide Web) durch die Erstellung von Spezifikationen und Referenzsoftware zu fördern.

Kein Allheilmittel

Schaut man sich die Gütesiegel, welche als Signal für einen sicheren Anbieter dienen sollen, genauer an, stellte man Anfang des Jahres noch fest, dass die Gütesiegel nicht das halten, was sie versuchen zu versprechen. Für den Nachweis der Cybersicherheit wurde anfangs die Erfüllung des ENISA European Cybersecurity Scheme verlangt – ein Zertifizierungsverfahren, welches bisweilen noch nicht steht. Gängige Standards wie der C5 oder die ISO 27xxx-Reihe wurden nicht aufgeführt. Hier ist man zwischenzeitlich zurückgerudert und hat etablierte Standards der Informationssicherheit mit aufgenommen.

Beim Thema Datenschutz gehen die Gütesiegel derweil jedoch nicht weit genug. So fordert ausschließlich das höchste Gütesiegel (Level 3) einen obligatorischen Dienststandort in Europa. Vor dem Hintergrund des Schrems-II-Urteils und der anhaltenden Diskussion über die Befugnisse von u.a. den amerikanischen Geheimdiensten ist das zu wenig. Trotz eines europäischen Ökosystems kann Gaia-X somit datenschutzrechtlich keinen Mehrwert bieten – sofern die Drittlandsproblematik nicht politisch gelöst wird.

Ausblick

Kommt Gaia-X oder kommt es nicht? Und wird Gaia-X ein Gamechanger für die europäische Digitalisierung? Die Chancen stehen wohl eher schlecht als gut. So wurde Anfang des Jahres bekannt, dass die Ampelregierung die Fördermittel für (zumindest) Teilprojekte einstampfen möchte. Und auch erste Mitglieder brechen weg, wie bspw. der französische Cloudanbieter Scaleway. Dieser beklagt die steigende Dominanz amerikanischer Anbieter am Projekt. Ob Gaia-X noch eine europäische Erfolgsstory wird, bleibt daher (weiter) abzuwarten. &

Verschlüsselung in der Cloud

„Die Cloud“ ist ein Überbegriff für ganz vieles, was auch in unser Privatleben Einzug erhalten hat. Häufig werden keine eigenen Festplatten mehr genutzt, um Daten wie Urlaubsfotos, Dokumente usw. zu speichern, sondern es wird Speicherplatz bei einem Anbieter „gemietet“. Und genauso ist es auch im Organisationskontext.

Die Cloud ist ein Speicher, der „irgendwo anders“ steht und auf den über das Internet zugegriffen werden kann. Die Vorteile liegen klar auf der Hand: Organisationen müssen Speichermedien nicht mehr physisch vor Ort vorhalten, sondern können je nach Volumen beliebig viel Speicher hinzubuchen. Cloud-Speicher können so, den Bedürfnissen entsprechend, „von jetzt auf gleich“ skaliert werden und sind ein wesentlicher Baustein der Digitalisierung.

Welche Herausforderungen entstehen bei der Nutzung von Cloud-Angeboten?

Die größten Anbieter von Cloud-Lösungen stammen nicht aus Deutschland oder der EU. Die im Organisationskontext weitverbreitetsten Anbieter stammen aus den USA oder Asien. Dies bedeutet, dass viele der Services nicht immer zu 100 Prozent aus deutschen oder europäischen Rechenzentren angeboten werden können – d. h., dass Daten (auch mit Personenbezug) die EU verlassen und in Drittländern verarbeitet werden. In vielen Fällen kann somit ein Drittlandstransfer nicht ausgeschlossen werden – was zu datenschutzrechtlichen Herausforderungen führen kann.

IaaS, PaaS, SaaS – was verbirgt sich dahinter?

Cloud-Computing ist jedoch viel mehr als nur „das Speichern von Dokumenten“. Es werden drei Bereiche unterschieden: Infrastructur as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Durch den Verbund dieser drei Varianten kommen die Stärken des Cloud-Computings erst richtig zum Tragen.

IaaS: Der Cloud-Provider stellt den Nutzenden die üblichen Komponenten eines Rechenzentrums zur Verfügung, wie z. B. Hardware, Rechenleistung, Speicherplatz oder Netzwerkressourcen.

PaaS: Stellt eine Plattform für die Entwicklung von Anwendungen im Internet bereit. Dabei ist die Umgebung mit allem ausgestattet, was für die Entwicklung von neuer Software notwendig ist.

SaaS: Hierbei handelt es sich um ein Softwarevertriebsmodell, bei dem ein Cloud-Anbieter Anwendungen hostet und Nutzenden über das Internet zur Verfügung stellt. Ein lokales Installieren der Software ist dabei meist nicht notwendig. Das Microsoft 365-Angebot zählt zu diesen Softwarelösungen, wobei Microsoft sowohl das Hosting als auch die Software übernimmt.

Wie sicher sind Daten in der Cloud?

Große Cloud-Anbieter, sogenannte Hyperscaler, investieren viel Geld in ihre IT-Sicherheit, was sich u. a. in zahlreichen Zertifizierungen widerspiegelt. Die Rechenzentren sind darauf ausgelegt, Daten ausfallsicher zu speichern und jederzeit verfügbar zu haben. Neben der Sicherheit beim Cloud-Anbieter kommen jedoch weitere Faktoren hinzu, die es zu beachten gilt. Zunächst müssen die eingesetzten Anwendungen und Systeme von der Administration sicher konfiguriert werden – auch im Hinblick des Datenschutzes. Wenn möglich sollten Rechenzentren ausgewählt werden, die sich auf deutschem oder europäischem Boden befinden. Zudem greifen Nutzende meist mittels Log-in-Daten auf die ihnen zur Verfügung stehenden Daten zu. Neben einem wirksamen Rollen- und Rechtekonzept sollten auch Regelungen zur Verwendung von sicheren Passwörtern etabliert werden – bestenfalls mit einer Multifaktor-Authentifizierung. Genauso bedeutend ist auch die Überwachung der Updates und Releases des Cloud-Anbieters. Ggfs. müssen nach einem Update Konfigurationen durch die Administration vorgenommen werden, um den Anforderungen des Datenschutzes und der Informationssicherheit gerecht zu werden.

Warum ist Verschlüsselung so wichtig?

Durch die Nutzung von Cloud-Diensten werden Daten im Ruhezustand beim Anbieter abgelegt (Data at rest) und während der Verarbeitung über das Internet übertragen (Data in transit). Beide Formen der Verarbeitung, also das bloße Speichern und das Übertragen, müssen mittels einer wirksamen Verschlüsselung abgesichert werden, um eine unbefugte Offenlegung der Daten zu verhindern. Hierzu existieren verschiedene Verfahren. Bei der Übermittlung

Stichwort
Drittlandtransfer

Sofern Auftragsverarbeiter aus Drittländern in die Verarbeitung personenbezogener Daten eingebunden werden, bedarf es einer Rechtsgrundlage für die Übermittlung der Daten. Zudem ist die Rechtslage insb. im Hinblick auf die Befugnisse von Geheim- und Nachrichtendiensten im Zielland zu überprüfen. Im Zweifel sind zusätzliche technische, organisatorische und vertragliche Maßnahmen zu vereinbaren.

kommen in den meisten Fällen gängige und sichere Transportverschlüsselungen zum Einsatz, die vom Cloud-Anbieter vorgegeben werden. Bei der Datenspeicherung existieren hingegen mehrere Verfahren, für die sich Organisationen aktiv entscheiden können – sogenannte „Hold your own key"- und „Bring your own key"-Verfahren (HYOK/BYOK).

Bei HYOK wird der Schlüssel zum Entschlüsseln der Daten von der Organisation selbst bereitgehalten und dem Cloud-Anbieter nicht zur Verfügung gestellt. Dieses Verfahren wird vor allem bei besonders sensiblen Daten verwendet, da so ein Zugriff durch den Cloud-Anbieter (bspw. auf Anfrage von Geheim- und Nachrichtendiensten) auf Klardaten ausgeschlossen werden kann.

Beim BYOK-Verfahren bringt die Organisation einen eigenen Schlüssel mit, speichert diesen jedoch ebenfalls beim Cloud-Anbieter. Nicht unüblich ist sogar, dass der Schlüssel beim Cloud-Anbieter direkt erzeugt wird. Dieses Verfahren macht es der Organisation einfach, ein Verschlüsselungsverfahren anzuwenden, doch liegen der Schlüssel und die verschlüsselten Daten eben beim selben Anbieter. Hier muss die Organisation darauf vertrauen, dass der Cloud-Anbieter die Daten nicht eigenmächtig entschlüsselt, z.B. auf Anfrage und Druck von Geheim- oder Nachrichtendiensten.

Neben diesen beiden Formen existieren weitere Verschlüsselungsmechanismen, die z. T. auf HYOK/BYOK aufsitzen und teilweise darüber hinausgehen. Sogenannte Third Party Gateways verschlüsseln bspw. Daten, noch bevor diese zum Cloud-Anbieter übermittelt werden.

Stichwort
Verschlüsselung

Bei einer Verschlüsselung werden Daten in eine für unbefugte Person nicht mehr lesbare Form verwandelt. Hierbei kommen digitale Schlüssel in symmetrischen oder asymmetrischen Verschlüsselungsverfahren zum Einsatz. Die verschlüsselten Daten können erst mithilfe des „richtigen" Schlüssels in ein lesbares Format entschlüsselt werden.

Sicher vor Hackern dank verschlüsselter Daten?

Trotz vermeintlich sicherer Verschlüsselung und abgeriegelter Rechenzentren schaffen es Hacker immer wieder auf Daten zuzugreifen und diese selbst zu verschlüsseln und/oder zu kopieren. Dabei nutzen Angreifende meist keine versteckte Hintertür (z. B. durch Schwachstellen in Systemen). Hacker haben es auf die Zugangsdaten der Mitarbeitenden abgesehen. Werden diese erlangt, können die Angreifenden durch den „Haupteingavng", also die webbasierte Login-Seite, in das System einsteigen. Hier gilt es zum einen die Mitarbeitenden bzgl. der Gefahren von Phishing-Mails, Social Engineering und Co. zu sensibilisieren und gleichzeitig technische und organisatorische Abwehrmaßnahmen einzurichten, um einen Einstieg bestmöglich abzuwehren (Multi-Faktorauthentifizierung, Zero-Trust-Strategie, usw.). &

Impressum

Redaktion/V. i. S. d. P.:
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

Digitalisierung nachhaltig umsetzen

Während manche Organisationen mittlerweile komplett papierlos arbeiten, scheinen manche erst vor Kurzem auf Farbfax umgestiegen zu sein - Veränderungen in Unternehmen sind nicht leicht umgesetzt. Christian Bredlow von Digital Mindset, gab uns im Interview einen Einblick in seine Tätigkeit.

Christian, Büro oder Homeoffice? Was ist der neue gemeinsame Nenner nach Corona für Eure Kunden?

Christian: Die Mischung macht's! Wir beobachten bei den wenigsten Kunden eine „Entweder-Oder-Entscheidung". Also nur Büro oder nur Homeoffice. Im Durchschnitt liegt die Homeoffice-Quote bei 3,5 Tagen in der Woche. Das macht in den meisten Fälle auch viel mehr Sinn als z. B. alle Mitarbeitenden jeden Tag ins Büro zu beordern. Denn wieso sollten Mitarbeiter*innen ins Büro zurückkehren, um wie im Homeoffice zu arbeiten? Auch Pflegeeinrichtungen, die wir im Rahmen von Digital Business Hannover begleiten durften, haben das für sich erkannt und für administrative Tätigkeiten das Homeoffice ermöglicht. Das Büro der Zukunft hingegen wird bei vielen unsere Kunden ein Raum der Begegnung, des Teamgefüges und der kreativen Zusammenarbeit sein.

Wie begleitet ihr Organisationen in Sachen Digitalisierung und woher kommt die Expertise?

Christian: Unser grundlegender Ansatz ist es, Organisationen durch Inspiration von außen zu zeigen, was in der Welt um uns herum schon alles passiert und dass das mit der Digitalisierung nicht mehr weg geht, noch dass man davor Angst haben muss. Im Wesentlichen erfolgt das durch meine Keynotes, unsere Workshops oder Inspirationsreisen zu anderen Unternehmen.

Auf die Inspiration folgt dann die Veränderung – und zwar von innen. Gemeinsam mit Teams aus Führungskräften und Mitarbeitenden gestalten wir digitale Fitnessprogramme und machen aus weniger-digitalen Organisationen wie wir es nennen „Connected Companies".

Das Besondere an uns Digitalisierungslotsen und- lotsinnen: Wir alle kommen aus der Praxis und die Basis unserer Arbeit sind unsere eigenen Erfahrungen mit der digitalen Transformation.

Welche Herausforderungen stellt Ihr gemeinsam mit den Kunden fest?

Christian: Eine der größten Herausforderungen, die wir durch die Bank weg gemeinsam mit unseren Kunden feststellen, ist einen identischen Grad der Digitalisierung bei allen Beschäftigten herzustellen und Bedenken gegenüber der Digitalisierung auszuräumen.

Privat sind wir doch alle irgendwie digitaler, oder? Wir bezahlen beim Bäcker mit unserer Smartwatch, fahren mit Elektrorollern durch die Stadt und kommunizieren privat doch eher über Messenger als über E-Mails. Auf der Arbeit legen die meisten ihr digitales Mindset und ihren digitalen Pragmatismus dann meist ab. Und da setzen wir an und zeigen, wie Digitalität auch im Arbeitsalltag funktionieren kann.

Da braucht es oft nur ein paar gute Beispiele, wie z. B. der Dreh von Lernvideos mit dem Smartphone statt in einem voll ausgestatteten Studio und dann klappt's auch mit der Veränderungsbereitschaft.

Welche Rolle spielt die Einführung von Microsoft 365 oder vergleichbarer „Modern Workplace"-Lösungen?

Christian: Nun, das passende Tool ist die Basis für die digitale Zusammenarbeit und kann Unternehmen jeglicher Branchen dabei unterstützen neue und vernetzte Formen der Kollaboration einzuführen. Ob Microsoft 365, die Google G Suite, Coyo oder Slack – Software-Lösungen gibt es ja mittlerweile genug.

Aber viel wichtiger ist neben dem Tool auch die Etablierung des nötigen Mindsets. Denn was bringt einem das beste Tool, wenn keiner weiß, welche Möglichkeiten das Tool bietet oder es schlicht weg nicht genutzt wird. Digitalisierung ist eben nicht nur eine Frage der Technologie, sondern vielmehr eine veränderte Geisteshaltung.

Digitalisierung ist keine Frage der Technologie? Aber was ist dann die Rolle von Software überhaupt?

Christian: Wie erwähnt: Die Software ist zum Werkzeug geworden, das die neuen Arten der Zusammenarbeit überhaupt erst ermöglicht. Wissensmanagement, mobiles Arbeiten über die Welt verteilt – all das können Tools wie M365 oder Slack.

Damit das Ganze aber auch Erfolg hat und sich besagte Formen der Zusammenarbeit etablieren können, braucht es eben auch das richtige, digitale Mindset. Dafür ist wichtig, dass einmal durch Führungskräfte kommuniziert wird, warum dieses Werkzeug überhaupt eingeführt wird, um alle Mitarbeitenden mitzunehmen. Und im Anschluss braucht es Anwendungskompetenz, Anwendungskompetenz und Anwendungskompetenz – die Mitarbeitenden müssen befähigt werden, die Tools zu bedienen und das zu ihrem Nutzen.

Wie helfen Eure Programme beim Recruiting und dem Gewinn von neuen Mitarbeitenden?

Christian: Nun, ich glaube nicht, dass ich irgendwem etwas Neues erzähle, wenn ich vom derzeitigen Fachkräftemangel, der in quasi allen Branchen zu beobachten ist, spreche. Umso wichtiger ist es, dass Unternehmen und Organisationen attraktiv auf potenzielle Bewerberinnen und Bewerber wirken und auch fernab der festen Jobbeschreibungen Talenten einen Einstieg ermöglichen.

Ein besonders guter Weg dafür ist auf jeden Fall, wenn die eigenen Mitarbeitenden ihren Freunden, Familien und Geschäftspartnern in (sozialen) Netzwerken positiv über ihre Arbeit und den Arbeitgeber berichten. Einer meiner Kollegen z. B. feiert jedes Jubiläum auf LinkedIn mit einem Bild aus seiner Zeit bei der Digital Mindset. Die dazugehörigen Skills, auf Social Media aktiv zu sein und dem Ganzen eine Chance zu geben, leiten sich ja in den meisten Fällen aus der Nutzung von Kollaborationswerkzeugen ab. &

Kurzvorstellung **Digital Mindset**

Die Digital Mindset GmbH begleitet Unternehmen durch die digitale Transformation. Unter dem Ansatz „Inspiration von außen, Veränderung von innen" hilft die Digital Mindset Organisationen dabei, digitale Zusammenhänge zu verstehen, digitale Potentiale zu identifizieren und diese in nachhaltigen Geschäftserfolg umzuwandeln.

Digitalisierung vs. Datenschutz?

Eine Meinung von Simon Lang

„Datenschutz setzt Unternehmen unter Druck" – so betitelt der bitkom e.V. eine im September vegangenen Jahres durchgeführte Studie. Drei von vier Unternehmen gaben an, der Datenschutz hätte sie bereits bei Innovationen ausgebremst.

Ist der Datenschutz damit größter Widersacher beim Thema Digitalisierung?

Weit gefehlt, wie ich meine. Der Datenschutz stellt den Anspruch, die Rechte und Freiheiten natürlicher Personen zu schützen – im analogen und im digitalen Bereich. Hier unterscheidet der Datenschutz nicht.

Als Datenschützer beobachte ich seit längerem, dass viele analoge Prozesse ein wesentlich höheres Risiko bei der Verarbeitung personenbezogener Daten tragen als digitale Prozesse, da softwareseitig bei der Absicherung von Daten wirksam unterstützt werden kann. Die Digitalisierung sollte daher der beste Freund eines jeden Datenschützers sein.

Wenn von „Innovationen" im Kontext Datenschutz geschrieben wird, verbergen sich dahinter jedoch oftmals Verarbeitungsvorgänge wie (unrechtmäßige) Big Data Analysen oder Profiling von Kundendaten bzw. Daten von Mitarbeitenden. Und diese können tatsächlich im klaren Gegensatz zu datenschutzrechtlichen Grundsätzen stehen. Das ist jedoch kein Konstruktionsfehler der DSGVO, sondern genau so gewollt.

Missbräuchliche Verarbeitungen von Daten zum Zwecke der eigenen Gewinnmaximierung und auf dem Rücken der Rechte und Freiheiten natürlicher Personen stellen für mich keine „Innovationen" dar, da sie keinen gesellschaftlichen Nutzen stiften oder legitime Geschäftsprozesse effektiver machen.

Die Frage muss daher lauten: Bremst der Datenschutz gewollte und nützliche Innovationen aus?

Ich meine nein. Legitime Vorhaben im digitalen Raum können sich auf eine breite Palette an Rechtsgrundlagen stützen – man muss eben nur wissen, wie man den Datenschutz richtig anwendet. Digitalisierer und Datenschützer müssen sich (endlich) an einen Tisch setzen und gemeinsam kluge Innovationen ausarbeiten.

Dann klappt's auch mit der längst überfälligen Digitalisierung unserer Gesellschaft. &

Neue Compliance-Anforderungen: das Lieferkettengesetz

Am 1. Januar 2023 soll es so weit sein: das „Gesetz über die unternehmerische Sorgfaltspflicht in Lieferketten“ (Lieferkettengesetz) tritt in Kraft. Es ergeben sich direkte und indirekte Pflichten für Unternehmen und Organisationen in Deutschland.

Obwohl sich bereits in der Vergangenheit viele Unternehmen und Organisationen im Rahmen ihres Umwelt- und Nachhaltigkeitsmanagement auch der Liefer- und Wertschöpfungskette gewidmet und ihre Bemühungen ausgebaut haben, soll das Lieferkettengesetz diese Kür zur Pflicht machen.

Nach dem Gesetz soll Nachhaltigkeit in der Lieferkette künftig keine freiwillige Selbstverpflichtung mehr sein. Stattdessen sollen definierte Sorgfaltspflichten gelten. Das Gesetz verfolgt das Ziel, dem Schutz grundlegender (internationaler) Menschenrechte Rechnung zu tragen und legt konkrete Anforderungen an ein verantwortungsvolles und nachhaltiges Wirtschaften fest. Betroffene Unternehmen und Organisationen müssen sich spätestens ab dem 1. Januar 2023 mit folgenden neun Punkten beschäftigen:

1. Die Einrichtung eines bzw. Anpassung des vorhandenen Risikomanagementsystems
2. Die Festlegung einer betriebsinternen Zuständigkeit
3. Die Durchführung regelmäßiger Risikoanalysen
4. Die Abgabe einer Grundsatzerklärung
5. Die Verankerung von Präventionsmaßnahmen im eigenen Geschäftsbereich und gegenüber unmittelbaren Zulieferern
6. Das Ergreifen von Abhilfemaßnahmen
7. Die Einrichtung eines Beschwerdeverfahrens
8. Die Umsetzung von Sorgfaltspflichten in Bezug auf Risiken bei mittelbaren Zulieferern
9. Die Dokumentation und die Berichterstattung

Wer ist davon betroffen?

Vom Lieferkettengesetz betroffen sind zunächst Unternehmen und Organisationen mit Hauptverwaltung, Hauptniederlassung, Verwaltungssitz oder satzungsmäßigem Sitz in Deutschland, die mindestens 3.000 Mitarbeitende beschäftigen. Gleichzeitig werden bei Konzernen mit Sitz in Deutschland die konzernangehörigen Gesellschaften im Ausland hinzugerechnet.

Ab 2024 sinkt die Grenze auf 1.000 Mitarbeitende. Doch auch für KMU wird das Gesetz mittelbar relevant, da davon auszugehen ist, dass unmittelbar betroffene Unternehmen und Organisationen ihre gesetzlichen Pflichten an ihre Zulieferer weiterreichen werden.

Risikomanagement und Beschwerdeverfahren

Auch wenn Risikomanagement im Kontext Compliance nichts gänzlich Neues ist, wird die Pflicht nun gesetzlich verankert. Der Gesetzgeber verlangt „ein angemessenes und wirksames Risikomanagement zur Einhaltung der Sorgfaltspflichten“ einzurichten und in alle maßgeblichen Geschäftsabläufe zu verankern. Diesbezüglich wird eine Risikoanalyse zur Pflicht, die einmal im Jahr sowie anlassbezogen durchzuführen ist.

Zudem wird festzulegen sein, wer innerhalb des Unternehmens dafür zuständig ist, das Risikomanagement zu überwachen – hier wird etwa die Benennung eines Menschenrechtsbeauftragten aufgeführt. Analogien gibt es darüber hinaus etwa zur EU-Hinweisgeberrichtlinie, die noch in diesem Jahr in einem nationalen Gesetz münden dürfte. So verlangen beide Rechtstexte ein Meldeverfahren, um auf Missstände aufmerksam machen zu können.

Im Kontext des Lieferkettengesetzes soll es Personen ermöglicht werden, auf menschenrechtliche und umweltbezogene Risiken sowie auf Verletzungen menschenrechts- oder umweltbezogener Pflichten hinzuweisen.

Sanktionsmöglichkeiten

Die Einhaltung dieses Gesetzes soll das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) kontrollieren. Die BAFA soll die Möglichkeit erhalten, gegen Unternehmen Zwangsgelder von bis zu 50.000 €, oder bei vorsätzlichen bzw. fahrlässigen Verstößen gegen Sorgfaltspflichten Bußgelder zu verhängen. Sofern schwere Verstöße bekannt werden, ist auch der Ausschluss von der Vergabe öffentlicher Aufträge für einen Zeitraum von bis zu drei Jahren möglich.

Ausblick

Auf Compliance-Beauftragte kommen spannende Zeiten zu. Mit der nationalen Umsetzung der EU-Hinweisgeberrichtlinie wird noch in diesem Jahr gerechnet, da Deutschland die Umsetzungsfrist Ende letzten Jahres verstreichen lassen hat. Gleichzeitig sorgt das Lieferkettengesetz dafür, dass ein Risikomanagement im Kontext Menschen- und Umweltrechte eingehalten und nachgewiesen werden muss. Zudem fordern beide Gesetzestexte die Etablierung eines Beschwerde- bzw. Hinweisverfahrens, welches sich jedoch zumindest technisch wohl über eine Plattform darstellen lassen könnte.

Besonders interessant wird es zudem zu beobachten, wie auf europäischer Ebene eine Lieferkettenrichtlinie ausgestaltet wird. Diesbezüglich ist man bereits in Vorbereitung und erste Details zur Richtlinie wurden bekannt. So ist es gut möglich, dass die europäische Richtlinie über das deutsche Gesetz hinausgeht. Dies hätte dann zur Folge, dass Unternehmen und Organisationen zeitnah ihre eigenen Bemühungen auf Basis des Lieferkettengesetzes nachbessern müssen, um den europäischen Ansprüchen gerecht zu werden. &

In eigener Sache

Gerne beraten wir Sie zum Lieferkettengesetz und zur Umsetzung der EU-Hinweisgeberrichtlinie und stellen Ihnen unsere Lösungen vor.
Sprechen Sie uns einfach an!

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

Zwischen Studium, E-Learning und AV-Verträgen

Regina Bergers Rolle im Unternehmen lässt sich nicht so leicht zusammenfassen, denn als Werkstudentin unterstützt sie an verschiedensten Stellen.

Wie sich Studium und Arbeit vereinbaren lassen, worauf es bei der Konzeption von Schulungen ankommt und welche Trends sich beim E-Learning abzeichnen, erzählt Regina in unserem Format „Über die Schulter geschaut".

Was genau machst du bei Althammer & Kill bzw. LearnBase?

Regina: Im Moment bin ich als Werkstudentin tätig und beschäftige mich primär mit der Content-Erstellung für unsere LearnBase E-Learnings. Seit Neustem gebe ich auch Autorenschulungen und zeige unseren Kunden wie sie selbst Kursinhalte mit dem Autorentool unserer LearnBase erstellen können. Hinzu kommen noch einige spontane Aufgaben, die ich von unserem Beraterteam bekomme, wie z.B. die Prüfung eines AV-Vertrags oder verschiedene Rechercheaufgaben.

Was studierst du?

Regina: Ich studiere im Moment Jura an der Leibniz-Universität Hannover. Davor habe ich noch ein Sozialarbeitsstudium an der Hochschule Hannover absolviert.

Wie sieht dein Alltag bei A&K und LearnBase aus?

Regina: Einen fest geregelten Alltag habe ich so gesehen nicht. Oft kommen spontane Aufgaben auf mich zu, über die ich mich sehr freue. Mein Alltag ist also nie eintönig.

Wie gehst du bei der Erstellung von E-Learning Content vor?

Regina: Zuallererst recherchiere und sammle ich zuverlässige Quellen. Sobald ich genug Wissen zusammengetragen habe, ist der nächste Schritt die Erstellung einer Struktur. Dabei muss ich mir dann überlegen, wie ich das Thema aufteilen will, wie viele Bausteine ich dafür brauche und was in welchen Baustein gehört.

Nach diesem Schritt hole ich mir das erste Feedback ein. Ist hier alles in Ordnung, geht es direkt weiter mit dem Storyboard, d.h. ich überlege mir für jede Folie, welche Bilder, Texte oder interaktiven Elemente ich verwenden möchte. Auch nach diesem Schritt hole ich mir ein Feedback ein. Nach der Freigabe des Storyboards mache ich mich daran, mein Storyboard auf unserer LearnBase umzusetzen.

Bei der Umsetzung muss man wiederum flexibel sein. Oft merkt man, dass einige Ideen nicht funktionieren und z. B. Hintergrundbild und Bilder nicht zusammenpassen oder dass zu viel Text auf den einzelnen Folien ist. Man muss also so lange ausprobieren, bis alles harmonisch aussieht und der Inhalt passt. Wenn die Bausteine fertig sind, werden sie an einen Kollegen weitergegeben, der dann die Qualitätssicherung durchführt. Oft werden die Bausteine dann noch ins Englische übersetzt und natürlich wieder von einem Kollegen überprüft. Wichtig ist hierbei, dass ich mir nach jedem Schritt ein Feedback einhole, sodass wir uns in einer ständigen Korrekturschleife befinden und Fehler schnell behoben werden.

Worauf muss deiner Meinung nach besonders geachtet werden, wenn es um die Erstellung von E-Learning Content geht?

Regina: Meiner Meinung nach sollte besonders auf das Gleichgewicht zwischen Inhaltsvermittlung und Spaß geachtet werden. Gamification ist hier das Stichwort. Bei der Erstellung von Inhalten ist es zudem wichtig, von einem Kursdesign wegzukommen, das eher an reine PowerPoint-Präsentationen erinnert. Stattdessen sollte man Interaktionen einbauen und Elemente verwenden, die verschiedene Lerntypen ansprechen. Natürlich muss die Qualität der Inhalte immer im Auge behalten werden.

Wie schaffst du es, Studium, Arbeit und Privatleben unter einen Hut zu bekommen?

Regina: Ich arbeite viel mit Zeitplänen und To-Do-Listen. Für jede Woche überlege ich mir, wann ich etwas erledigen muss und z.B. feste Termine habe oder, bis wann ich etwas erledigt haben möchte. Im nächsten Schritt schaue ich dann, wann ich zwischen diesen Terminen freie Zeit habe, und koordiniere mein Privatleben entsprechend. Natürlich erlaube ich mir eine gewisse Flexibilität.

Bei der Planung arbeite ich auch viel mit Pufferzonen. Wenn zum Beispiel eine Arbeit zum 30. September abgegeben werden muss, plane ich, sie bis zum 20. September fertig zu haben, um einen Puffer für spontane Ereignisse zu haben.

Inwiefern hat dich die Pandemie in deinem Studium und deiner Arbeit eingeschränkt?

Regina: Zunächst einmal ist der soziale Faktor, den Studium und Arbeit normalerweise mit sich bringen, weggebrochen. Eines der größten Probleme war daher der Aufbau von Kontakten, gerade weil das Studium von Austausch und Diskussion lebt. Glücklicherweise hatte ich mein erstes Semester noch vor Ort, sodass ich mir eine kleine Gruppe aufbauen konnte, mit der ich während der Pandemie in Kontakt war. Neben dem Studium habe ich viel im Homeoffice gearbeitet, wobei ich hier kaum Veränderungen bemerkt habe. Der direkte Kontakt wurde zwar eingeschränkt, aber die Zusammenarbeit und der Austausch waren weiterhin problemlos möglich.

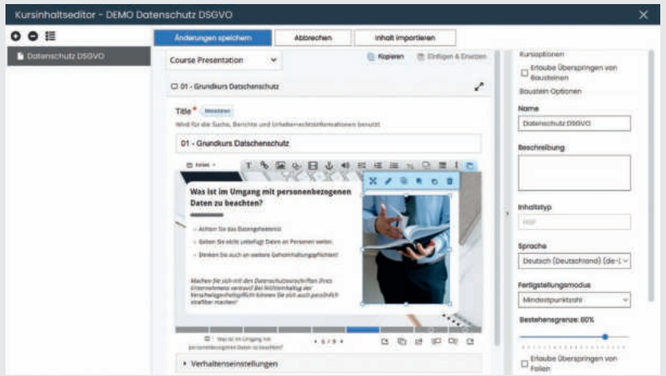
Was für eine Rolle hat hierbei E-Learning in deinem Privat-/Studienleben gespielt?

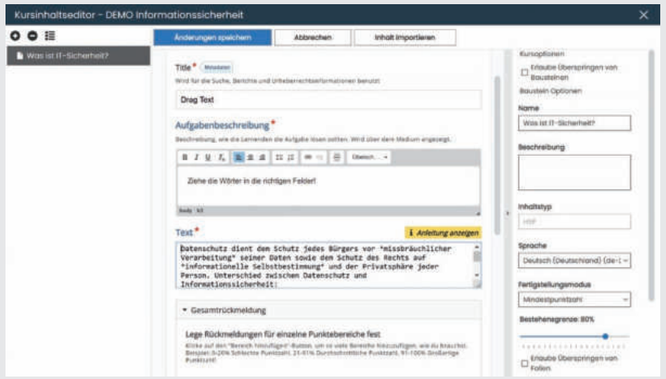
Regina: Gerade während der Pandemie hat sich mein Lernalltag zu einem großen Teil in die digitale Welt verlagert. Unsere Kurse haben online stattgefunden und das entweder synchron oder asynchron als aufgezeichnetes Video. Vor allem asynchrone Veranstaltungen hatten den Vorteil, dass man nicht an einen festen Stundenplan gebunden war,

Stichwort
LearnBase

LearnBase ist eine sich fortwährend weiterentwickelnde moderne Lernplattform. Sie unterstützt Unternehmen bei der Konzeption und Umsetzung von E-Learning Maßnahmen – sowohl mit bereits erstelltem Content als auch der Möglichkeit, eigene E-Learnings zu erstellen.

Mehr Informationen:
learnbase.de





Beim Gestaltungsprozess eines E-Learnings gibt es einiges zu beachten. Nicht nur die Fakten müssen stimmen, sondern der Kurs soll auch ansprechend aussehen und die Lernenden aktiv mit einbinden.

sondern frei planen konnte, wann welcher Kurs absolviert bzw. nachgearbeitet wird. Dies erfordert jedoch auch viel Disziplin.

Was das Privatleben betrifft, so kann ich sagen, dass ich E-Learning, wie die meisten von uns, ebenfalls viel nutze. Wir lesen Online-Artikel, hören Podcasts, sehen uns Videos und Tutorials an oder nutzen Apps, um neue Fähigkeiten zu erlernen. E-Learning spielt also auch in meinem Leben eine große Rolle.

Was willst du nach deinem Studium machen?

Regina: Einen genauen Plan habe ich noch nicht. Ich weiß aber, dass ich nach meinem Schwerpunktstudium in IT-, IP- und Datenschutzrecht in diesem Bereich weiterarbeiten möchte. Ich könnte mir auch gut vorstellen, nach dem Staatsexamen einen Master in IT- und IP-Recht zu machen. Außerdem würde ich gerne wieder mehr Erfahrungen im Ausland sammeln.

Gibt es Trends, die sich bei E-Learning Content abzeichnen?

Regina: Aktuell scheint sich der eLearning-Bereich in Richtung Micro-Learning oder Blended-Learning zu entwickeln. Unter Micro-Learning versteht man das Erlernen neuen Wissens durch die Verwendung kurzer und zielgerichteter Informationsblöcke. Ein Informationsblock beansprucht dabei meist nur zwischen 1–10 Minuten. Der Vorteil hier ist natürlich, dass man solche Kurse problemlos in den Alltag integrieren kann und nicht ein, zwei Stunden seines Tages fürs Lernen freihalten muss. Blended-Learning meint hingegen die Verknüpfung von Präsenzunterricht und Computer-gestütztem Lernen. E-Learning wird hier also als sinnvolle Ergänzung oder Vertiefungsmöglichkeit für das klassische Lernen genutzt. Aber auch Gamification ist ein wichtiger Trend.

Welche Elemente sind bei Unternehmen besonders gefragt?

Regina: Da E-Learning so aufbereitet werden kann, dass verschiedene Lerntypen angesprochen werden können, ist das Interesse besonders an solchen Elementen groß, die alle Lerntypen ansprechen: Audioelemente für Menschen, die eher auditiv lernen; Videos, Bilder und Texte für den visuellen Lerntyp oder interaktive Quiz-Elemente, die den problemorientierten Lerntyp abholen. Auch die Barrierefreiheit wird ein immer wichtigeres Thema.

Was glaubst du, in welche Richtung wird sich E-Learning in Zukunft weiterentwickeln?

Regina: Ich glaube, dass immer mehr Unternehmen die Vorteile von E-Learning für sich entdecken und es zu einem festen Bestandteil ihrer Weiterbildungsstrategie machen werden. Die Präsenz von E-Learning wird gerade durch die zunehmende Digitalisierung aller Prozesse immer präsenter werden. &

Veranstaltungen und Termine

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

Hier klicken oder scannen!

14. September 2022 – Webinar
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.

Durch die EU-Whistleblower Richtlinie müssen Systeme eingerichtet werden, die Hinweisgebern wie Edward Snowden erlauben, offen zu sprechen und dabei Anonymität zu bewahren. Die Rede ist von Hinweisgebersystemen.

Wir stellen Ihnen das Hinweisgebersystem von Althammer & Kill vor, das sich ganz einfach bei Ihnen einbinden lässt, alle Daten völlig anonym behandelt und die Anforderungen an die neue Richtlinie optimal erfüllt.

26.–29. September 2022 – Online-Seminar
ISO 27001 Professional - Information Security Officer

Unser ISO 27001 Professional-Seminar vermittelt Ihnen das weiterführende Fachwissen der international anerkannten Norm für Informationssicherheit ISO 27001 und ergänzender Normen. In dem viertägigen Kurs vermitteln wir Ihnen auf Basis des erfolgreichen Foundation Zertifikates tiefgreifendes Wissen und bereiten Sie so auf das erfolgreiche Bestehen der Zertifikatsprüfung vor.

Nach Abschluss des Seminares haben Sie die Möglichkeit an einer Zertifikatsprüfung der international anerkannten ICO-Cert teilzunehmen (zzgl. Prüfungsgebühr) und bei bestandener Prüfung besitzen Sie durch das erworbene Zertifikat den Nachweis der fachlichen Kenntnisse zur Normenreihe ISO27X.

Voraussetzung für das Zertifikat ist das erfolgreiche Bestehen der Zertifikatsprüfung und das vorhandene Zertifikat ICO ISMS 27001:2018 Foundation.

11. Oktober 2022 – Online-Seminar
Datenschutz in Online-Marketing und Social Media

Egal ob die eigenen Webseiten, das E-Mail-Marketing oder die Ansprache der Zielgruppen über Social Media, Datenschutz spielt eine besondere Rolle. Diese Art der Kommunikation und Außendarstellung hat ihre besonderen Herausforderungen.

Dazu gehört es einerseits zu wissen, was überhaupt auf den eigenen Webseiten (im Hintergrund) passiert und andererseits ob z. B. Plug-ins, die eine Schnittstelle zu Anbietern, wie Facebook, Google Maps oder YouTube aufgrund der USA-Problematik noch ohne Risiken einfach eingebunden werden können.

6. Dezember 2022 – Online-Seminar
Privacy by Design – Datenschutz für Software-Entwickler

Wenn Software die Datenschutz-Gesetze verletzt, drohen Bußgelder und Reputations-Schäden. Je später im Entwicklungsprozess der Datenschutz berücksichtigt wird, desto teurer und zeitaufwendiger sind die Reparaturen. Unser Seminar vermittelt an praktischen Beispielen das Grundwissen, um von Anfang an Datenschutz-freundliche Entscheidungen zu treffen und umzusetzen.

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

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
Mörsenbroicher Weg 200 · 40470 Düsseldorf · Tel. +49 211 936748-0
Kaiserring 10–16 · 68161 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