COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 2/2023

Automatisierter Datenklau

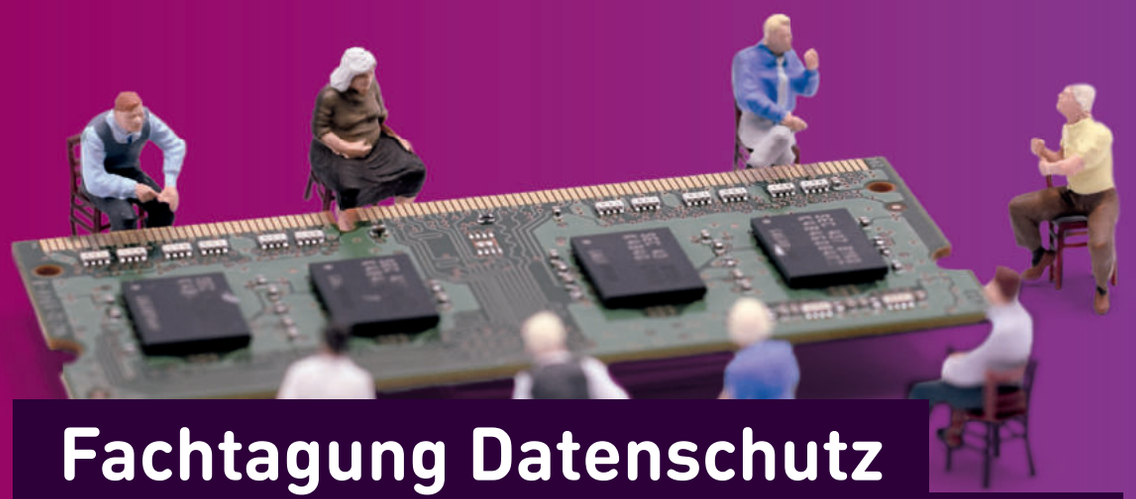
Facebook leidet unter Daten-Scraping
Seite 6

GPS im Firmenkontext
Das sollten Sie beachten
Seite 10

Kritische Ressourcen schützen
Mit Multi-Faktor-Identifizierung
Seite 12

Rollen im Compliance-Kontext
Die Ombudsperson
Seite 14

ALTHAMMER & KILL



Fachtagung Datenschutz und Informationssicherheit

in Sozialwirtschaft und Non-Profit-Organisationen

Die Cloud, KI & Cyber-Security in der Praxis wirksam zu gestalten ist eine große Herausforderung. Unsere Fachtagung für **interne Datenschutzbeauftragte** und **Datenschutzkoordinatoren**, IT-Verantwortliche sowie Informationssicherheit- und Digitalisierungsspezialisten bietet die ideale Möglichkeit zum Diskutieren und Mitwirken.

Alle Infos zum Thema

Save the date:
31.08.–01.09.2023
Paderborn

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

Editorial

Liebe Leserin, lieber Leser,

das Hinweisgeberschutzgesetz steht nach vielen Querelen in den Startlöchern. Durch die neuen Vorgaben gewinnt Compliance in vielen Unternehmen an Bedeutung. In diesem Zusammenhang bedarf es häufig der Besetzung neuer Stellen, wie bspw. dem Compliance-Beauftragten oder auch der Ombudsperson.

Wie sich diese beiden Rollen unterscheiden und inwiefern die Ombudsperson in Ihre Compliance-Strategie eingebunden werden kann, besprechen wir im Magazin. Oftmals bietet sich eine externe Vergabe an, um Kosten und Zeit zu sparen. Sprechen Sie uns gern an, wenn Sie an unseren neuen Angeboten Interesse haben.

In Sachen Datenschutz schafft es Facebook seit Jahren nicht aus den Schlagzeilen. In mehreren Urteilen ging es zuletzt um Datenscraping, also dem unerlaubten Auslesen von Inhalten mit Weiterverwendung durch Dritte. Wir stellen die Hintergründe und Auswirkungen vor.

Herzlich einladen möchten wir zu unserer ersten **Fachtagung „Datenschutz und Informationssicherheit“** mit Schwerpunkt Sozialwirtschaft und Non-Profit-Organisationen am **31.08. und 01.09.2023 in Paderborn**. Gemeinsam mit Expertinnen und Experten werden wir zu den Themen KI, Cloud und Cyber-Sicherheit diskutieren. Save the date!

Haben Sie Interesse an einem ähnlichen Format für andere Branchen? Wir sind bereits in ersten Überlegungen und würden uns über Ihr Feedback freuen.

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!

„ChatGPT: Schreibe einen Datenschutzartikel, der viele Klicks erhalten wird."

Von ChatGPT hat bestimmt schon jeder gehört. Seit der Veröffentlichung am 30. November 2022 meldeten sich innerhalb der ersten fünf Tage rund eine Million Nutzer an. Damit ist ChatGPT die am schnellsten wachsende Verbraucheranwendung, die es je gab. Auch qualitativ lassen sich die Texte häufig nicht beanstanden, aber was muss datenschutzrechtlich beachtet werden?

Quo vadis TADPF?

Das Abkommen soll die problematischen Datenexporte in die USA auf eine rechtssichere Grundlage stellen. Erklärtes Ziel des transatlantischen Datenschutzrahmens ist, durch Umsetzung der vereinbarten Executive Orders das Schutzniveau in den USA so anzuheben, dass ein Angemessenheitsbeschluss nach Art. 45 DSGVO wieder möglich wird. Wie schon während der Geltungsdauer des EU-US Privacy Shields wird also erneut ein sektorspezifischer Angemessenheitsbeschluss angestrebt.

Die Bedeutung von IT-Notfallplänen für Unternehmen

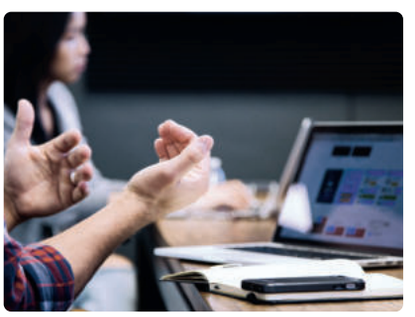
Die Implementierung effektiver IT-Notfallpläne ist in der heutigen, vernetzten Geschäftswelt unerlässlich, um Risiken zu minimieren und den Betrieb in Krisenzeiten aufrechterhalten zu können. Wir betrachten dabei die stetig wachsende Bedrohung durch Cyberangriffe, die menschlichen Aspekte – wie die psychische Belastung – sowie die Kosten für die Wiederherstellung ohne Notfallpläne.

HsH Akademie

Althammer & Kill und die Hochschule Hannover bilden Datenschutzmanager aus

Wirksamer Datenschutz braucht weit mehr als Kompetenz im Datenschutz-Recht. Um pragmatische Lösungen erarbeiten zu können, benötigen Datenschützer zusätzlich einiges an IT-Wissen. Und die wirksame Umsetzung in der Organisation erfordert Kenntnisse im Projekt- und Change-Management. Diese Aspekte kommen jedoch in der klassischen, Jura-zentrierten Datenschützer-Ausbildung zu kurz. Daher hat Althammer & Kill gemeinsam mit der Hochschule Hannover die ganzheitliche Weiterbildung „Datenschutzmanagement" konzipiert und erstmals durchgeführt: 16 frisch ausgebildete Datenschutzmanager dürfen sich über ihre Hochschul- und IHK-Zertifikate freuen. Der zweite Durchgang der Zertifikats-Weiterbildung startet im August 2023. Alle Infos finde Sie hier:

hs-hannover.de/weiterbildung/weiterbildungsangebot/datenschutzmanagement/



Rückblick: Infotag IT

„Security Awareness – Mitarbeitende als Schutz vor Cyber-Angriffen" – mit diesem Vortrag waren wir am 20. April auf dem „Infotag IT" des DRK, dem Paritätischen Wohlfahrtsverband und der WGKD vor Ort. Gemeinsam konnten wir uns über Entwicklungen und Trends im Bereich IT-Security austauschen und über neue Entwicklungen berichten.

Danke, dass wir dabei sein durften und danke an Maximilian Klose und Silvio Franke, dass ihr uns vor Ort in Frankfurt vertreten habt.

Zahl des Monats

53 %

der Menschen können nicht erkennen, ob ein Text von ChatGPT oder einem Menschen verfasst wurde. Dies ergab eine Studie von tooltester.com und zeigt damit, dass die KI einige Branchen, von IT bis Copywriting, nachhaltig erschüttern wird.

Wobei „AI generated content" auch seine Nachteile haben kann. So gaben in derselben Studie über 70 % der Befragten an, dass sie einer Marke weniger vertrauen würden, wenn diese auf durch KI geschrieben Inhalte setzt.

Veranstaltungen

31.08.–01.09. 2023, Paderborn
Fachtagung Datenschutz und Informationssicherheit für Unternehmen in der Sozialwirtschaft und Non-Profit-Organisationen

Die Cloud, KI & Cyber-Security in der Praxis wirksam zu gestalten ist eine große Herausforderung. Unsere Fachtagung bietet die ideale Möglichkeit zum Diskutieren und Mitwirken.

5 Jahre DSGVO und die Herausforderungen sind größer denn je. Verantwortliche in Sachen Datenschutz und Informationssicherheit haben allerhand zu tun. Selbst bei den „Basics" sind auch nach ein paar Jahren „Datenschutz-Routine" noch viele Fragen offen. Unsere Expertinnen und Experten geben zusammen mit externen Referenten spannende Impulse und vertiefen gemeinsam mit Ihnen auch Themen zum Datenschutz und zur Informationssicherheit, den Einsatz von KI in der Sozialwirtschaft und rechtliche Themen. Jetzt anmelden unter:

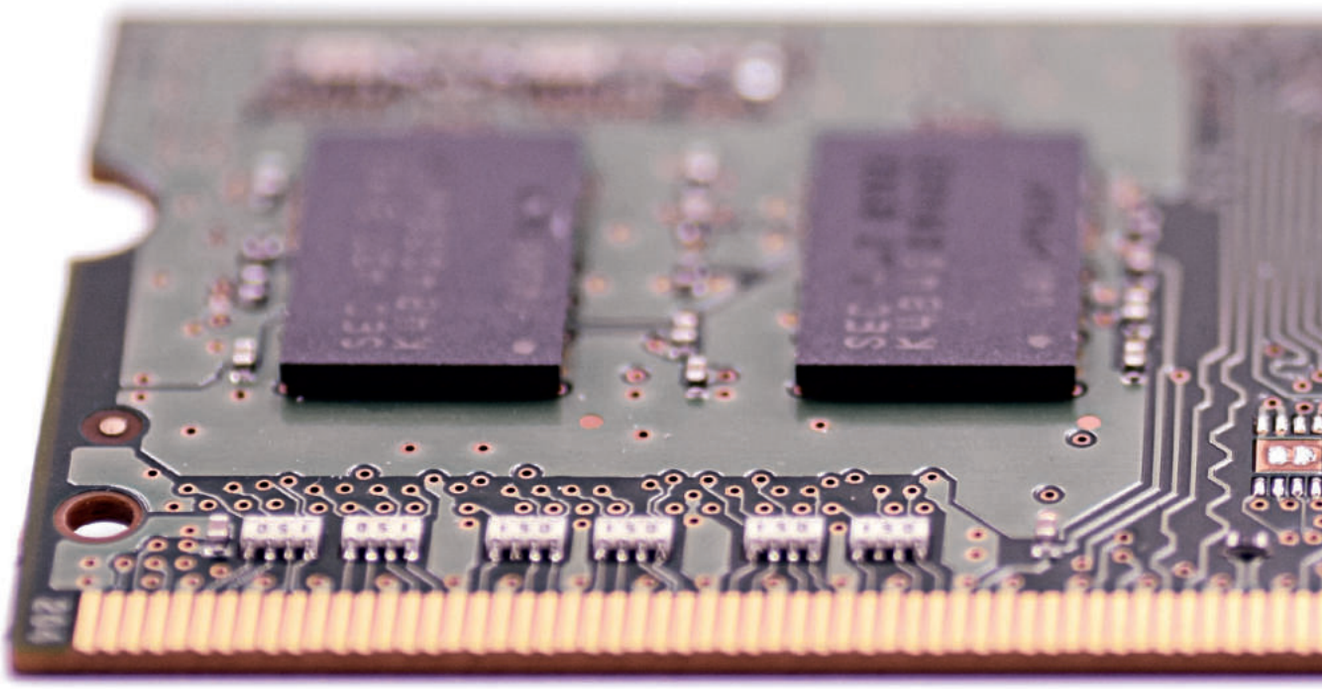
althammer-kill.de/fachtagung-datenschutz-informationssicherheit-in-sozialwirtschaft-und-non-profit-organisationen

05.–06.09. 2023, Kassel
health & care days
Digitalisierung in Krankenhäusern, sozialen Einrichtungen und Verbänden, Krankenkassen und Verwaltungsorganen
https://www.d-velop.de/events/health-and-care-days

14.09. 2023, Berlin
DRK Thementag „IT/Telekommunikation"
https://www.drkservice.de/veranstaltungen/tagungen/thementag-it-telekommunikation/

18.–20.09. 2023, Münster, Mövenpick-Hotel
BeB Fachtagung
https://beb-ev.de/veranstaltung/fachtagung-dienstleistungsmanagement-2023/

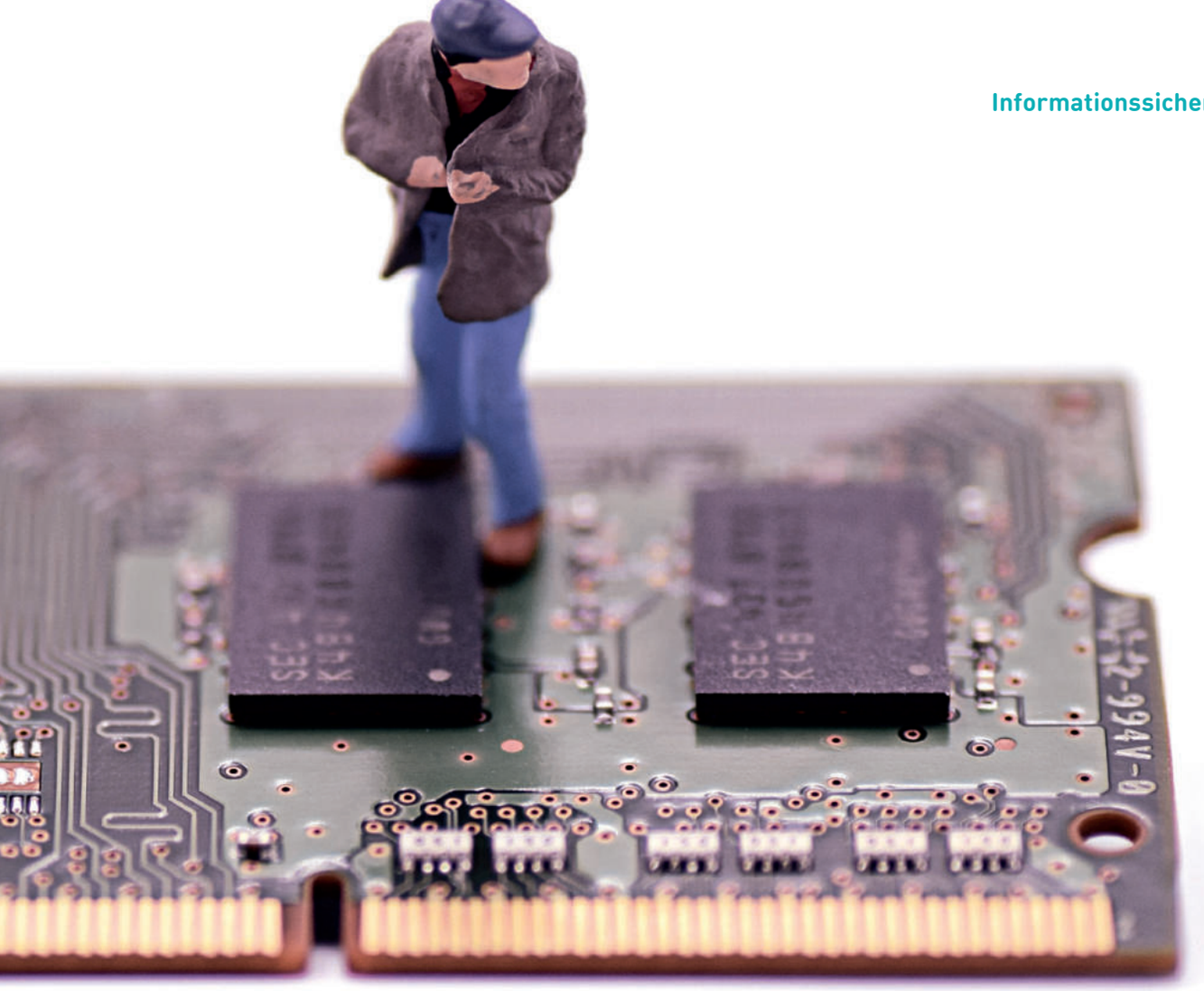
25.–26.10. 2023, Nürnberg
ConSozial
Die Leitmesse der Sozialwirtschaft
https://www.consozial.de/



Daten-Scraping bei Facebook

Die negativen Schlagzeilen um den nicht datenschutzkonformen Umgang mit personenbezogenen Daten bei Facebook setzen sich weiter fort. So berichtete die Nachrichten-Website „Businessinsider.de“ bereits im April 2021 über einen sehr weitreichenden Fall von Daten-Scraping bei Facebook.

Von Urban Zimber



Unter Daten-Scraping versteht man das automatisierte Auslesen von Informationen aus Websites, um diese anderweitig zu speichern und zu nutzen. Zwischen Januar 2018 und September 2019 hatten Kriminelle auf diese Weise personenbezogene Daten von über 530 Mio. Facebook-Nutzenden mittels automatisierter Verfahren abgegriffen, die dann in einem frei zugänglichen Hacking-Forum veröffentlicht wurden.

Welche Daten sind betroffen?

Bei den abgegriffenen Daten handelte es sich weitgehend um öffentlich einsehbare Profildaten. Darunter der Nutzername von Facebook, Nutzer-ID, der dahinterstehende reale Name, Geburtsdatum, Geburtsort, teilweise E-Mail-Adressen und weitere Daten. Je nachdem, was die Nutzenden von sich preisgegeben hatten, konnten auch die Standortinformationen, Geschlechtsangaben, Beziehungsangaben, Daten über den Arbeitsplatz usw. enthalten sein.

Obwohl die Mobilfunknummer der Nutzenden in den „Sichtbarkeitseinstellungen“ standardmäßig als „nicht öffentlich einsehbar“ deklariert wurde, war auch diese enthalten.

Wie sind die Kriminellen vorgegangen?

Daten-Scraping war und ist zwar nach den Nutzungsbedingungen des Anbieters untersagt, dennoch gab es hierzu eine technische Möglichkeit.

Der Daten-Abruf erfolgte nicht über einzelne Nutzer-Profile, sondern über das digitale Contact Import Tools (CIT). Diese Kontaktimport-Funktion sollte Nutzenden einen Abgleich der auf ihrem Smartphone gespeicherten Kontakte ermöglichen, um diese auf der Facebook-Plattform zu finden und sich mit ihnen zu verbinden.

Zusätzlich zu den „Sichtbarkeitseinstellungen“ gibt es die „Suchbarkeitseinstellungen“. Die vorgegebene Standardeinstellung war für Telefonnummern als „für alle suchbar“ eingestellt. Dies nutzte auch die Kontaktimport-Funktion.

Kriminellen machten sich dies zunutze und stellten eine Verknüpfung auch bei nicht öffentlich gemachten Telefonnummern her. Sie konnten damit (zunächst unbekannte) Telefonnummern den zugehörigen Profildaten zuordnen. Die personenbezogenen Daten konnten anschließend zu einem Datensatz zusammengefügt werden.

Wie wurde der Vorfall bisher von den Gerichten bewertet?

Bisher machten zahlreiche Nutzende Schadensersatzansprüche wegen immaterieller Schäden gegen den Facebook-Mutterkonzern, die Meta-Platforms Ireland Ltd., auf der Grundlage des Art. 82 Abs. 1 DSGVO geltend. Die datenschutzrechtliche Bewertung ist entsprechend der hohen Anzahl an Urteilen vielfältig ausgefallen. Und die Ergebnisse der Gerichte liegen weit auseinander.

Ablehnende Urteile

Zunächst lehnten viele Gerichte einen Schadensersatzanspruch ab. Dabei wurde als Ablehnungsgrund unter anderem angeführt, dass Art. 82 DSGVO nicht einschlägig sei, kein Datenschutzverstoß vorliege, kein ersatzfähiger Schaden bestehe, ein Schaden nicht nachweisbar sei, die Betroffenheit vom Vorfall durch den Klagenden nicht ausreichend dargelegt worden sei oder keine schadensauslösende Pflichtverletzung der Beklagten vorliege.

Stattgebende Urteile

In letzter Zeit wurde Schadensersatz in einer Höhe zwischen 250 und 1.000 Euro immer häufiger zugesprochen und als immaterieller Schaden ein Kontrollverlust angenommen. Es bestehe eine immanente Gefahr, dass die Daten missbräuchlich und vermögensgefährdend von Dritten verwendet werden würden, was zu Stress, Unwohlsein und Komforteinbußen führe.

Welche Verstöße wurden festgestellt?

Die Gerichte stellten unter anderem folgende Verstöße gegen die DSGVO fest:

Verstoß gegen Art. 25 Abs. 2 DSGVO „Privacy by Default“: Danach hat der Verantwortliche datenschutzfreundliche Voreinstellungen zu treffen. Die Suchbarkeitseinstellung für Telefonnummern sei jedoch standardmäßig auf „Alle“ gesetzt gewesen, obwohl dies nicht für den Verarbeitungszweck (Durchführung des Schuldverhältnisses) erforderlich gewesen sei.

Verstoß gegen Informationspflicht, Art. 13 Abs. 1 lit. c) DSGVO: Danach sind der betroffenen Person bereits zum Zeitpunkt der Erhebung der personenbezogenen Daten unter anderem die Zwecke, für die die Daten verarbeitet werden sollen, mitzuteilen. Tatsächlich habe bei Abfrage der Telefonnummer aber keine Information der Nutzenden über die Kontaktimport-Funktion und die diesbezügliche Verwendung der Mobilfunknummer stattgefunden.

Verstoß gegen Art. 32 DSGVO: Danach ist der Verantwortliche verpflichtet, technische und organisatorische Maßnahmen (TOM) zu ergreifen, um im Hinblick auf die verarbeiteten personenbezogenen Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Anforderung sei nicht ausreichend umgesetzt worden. Es habe keine ausreichenden Sicherheitsmaßnahmen nach dem Stand der Technik gegeben, um eine Ausnutzung des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern. Dadurch sei eine unbefugte Offenlegung bzw. ein unbefugter Zugang ermöglicht worden. Es habe keine Einschränkung der Nutzung der Kontaktimport-Funktion gegeben, etwa durch eine Begrenzung der Anzahl der abrufbaren Mobilfunknummern. Es seien erst im Nachgang Verhinderungstechniken implementiert worden.

Verstoß gegen Meldepflicht, Art. 33 DSGVO: Die zuständige Datenschutzaufsichtsbehörde sei nicht rechtzeitig innerhalb der 72-Stunden-Frist informiert worden.

Verstoß gegen Informationspflicht der Betroffenen, Art. 34 DSGVO: Schließlich seien auch die Betroffenen selbst nicht über den Vorfall informiert worden, obwohl dies erforderlich gewesen wäre.

Was könnten Kriminelle mit den Daten machen?

Es könnten Social-Engineering-Angriffe, wie Phishing per E-Mail, Telefonanrufe oder SMS von Betrügern durchgeführt werden. Die Gefahr, auf solche Angriffe hereinzufallen, steigt mit der Anzahl der erlangten Daten an, da mit Hilfe der erlangten Informationen eine authentischere Gestaltung ermöglicht wird.

Fazit

Der Scraping-Skandal und die darauffolgenden Gerichtsurteile zeigen einmal mehr auf, dass immer wieder datenschutzrechtliche Probleme bei Facebook an die Öffentlichkeit gelangen. Dass Facebook nicht datenschutzkonform agiert, ist unter Datenschützern kein Geheimnis. Die Vorteile und Risiken einer Nutzung von Facebook sollten deshalb immer sorgfältig gegeneinander abgewogen werden. &

Die Menschen hinter Althammer & Kill:

Winona Wenning

Ja hallo, wer bist du denn?

Winona: Hallo, mein Name ist Winona und ich gehöre zum A&K Standort in Düsseldorf – dort wohne ich auch. Ich habe Law & Economics studiert und während meines Erasmus-Jahrs in Zagreb ein tolles Seminar zum Datenschutzrecht besucht. So bin ich mit dem Bachelor of Laws Anfang 2018 als Beraterin im Datenschutz ins Berufsleben gestartet. Privat bin ich am liebsten draußen unterwegs auf dem Mountainbike oder auf Ski.

Wie lange arbeitest du schon bei Althammer & Kill?

Winona: Ich bin im Oktober 2022 zu Althammer & Kill gekommen und wurde gleich so gut aufgenommen, dass ich manchmal schon das Gefühl habe bereits viel länger dabei zu sein.

Was sind deine Aufgaben?

Winona: Im Bereich Beratung liegt der Fokus auf dem Kunden und seinem Bedarf. Ich berate und betreue einen festen Kundenstamm. Daneben wirke ich an Projektaufträgen und der Betreuung der Kunden meiner Teamkollegen mit. Thematisch liegt mein Fokus dabei auf dem Datenschutz. Dies bedeutet in der langfristigen Betreuung neben dem Aufbau des Datenschutzmanagementsystems auch die Beantwortung vieler Einzelfragen aus dem Alltag des Kunden, in die man sich reindenken muss.

Was studierst du?

Winona: Ich studiere Wirtschaftsrecht mit der Vertiefungsrichtung Legal Tech.

Warum hast du dich für dieses Studium entschieden?

Winona: Es hat mich einfach in den Fingern gejuckt, meinem Bachelor noch einen Master of Law anzuschließen. Dieser war gar nicht so leicht zu finden. Fächer wie Entscheidungstheorie, Compliance, Haftungsrecht, und sogar Internetrecht & Datenschutz stehen auf dem Plan. Das zusätzliche Wissen kommt also gleich zur Anwendung.

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

Winona: Das frage ich mich manchmal auch. Glücklicherweise ist mein Studium an der FOM auf die Bedürfnisse von Berufstätigen zugeschnitten und kommt mir in der Kombination mit dem flexiblen Arbeitsmodell bei A&K sehr entgegen. Mit geschickter Planung und effizienter Arbeit für Prüfungsleistungen kommt so auch das Privatleben nicht zu kurz. Trotzdem muss ich manchmal auf dem Weg zwischen Büro und Vorlesungssaal ganz schön in die Pedale treten.

Wie sieht dein Alltag bei A&K aus?

Winona: Berater-Alltag – gibt es das überhaupt? Einen idealen Tag im Büro starte ich mit einer kurzen Sichtung von Posteingang und Tickets, bevor ich mit meiner ersten größeren Aufgabe für den Tag starte. Die Zeit bis zur Mittagspause nutze ich gerne für die intensive Arbeit an komplexen Aufgaben wie Berichten und Stellungnahmen. Nach der Mittagspause geht es mit Kundenterminen weiter, oder dem Austausch mit dem Team. Dienstreisen oder zeitkritische Anfragen bringen diese Struktur aber auch gerne mal durcheinander.

Was schätzt du besonders am Beruf des Beraters?

Winona: Viele Routineaufgaben und einen monotonen Alltag gibt es als Berater kaum. Genau das gefällt mir. Ich muss mich immer wieder auf neue Menschen einstellen und in neue Sachverhalte einarbeiten. Dabei lernt man auch viel über die Branchen der Kunden. Das kann manchmal ganz schön fordernd sein, aber das macht, mit dem Rückhalt aus dem Team, den Job einfach spannend.

Welche Themen werden deiner Meinung nach besonders wichtig werden in den kommenden Wochen und Monaten?

Winona: Ich habe gerade erst meine Vertiefungsrichtung für den Master ausgesucht: Legal Tech, also die Digitalisierung und Automatisierung von Rechtsdienstleistungen. Hierbei ist der Einsatz künstlicher Intelligenz durch die aktuellen Entwicklungen noch mehr in den Fokus gerückt. Es bleibt also spannend, ob Chat GTP als weiteres Tool auch unseren Arbeitsalltag verändern wird. &

GPS-Ortung im Fuhrparkmanagement – einfach so möglich?

Der Fuhrpark eines Unternehmens, besonders im Bereich der Logistik oder Disposition, muss gut funktionieren. Gerne werden zur Koordinierung von Ressourcen, Benzinverbrauch, Geschwindigkeitsmessungen und ggf. zum Diebstahlschutz die GPS-Ortung eingesetzt. Dabei gibt es jedoch diverse Punkte zum Datenschutz zu beachten.

Von Jessica Henning

Die GPS-Ortung kann vielseitig eingesetzt werden. In der Pflege wurden Systeme entwickelt, die es Pflegenden erlaubt, Patienten mit hohem Bewegungsdrang nachverfolgen zu können. Hat beispielsweise ein Alzheimer-Patient ein Hin- bzw. Weglaufbedürfnis, kann diese Person nach gründlicher Abwägung mit GPS-Armband oder -Kette ausgestattet werden.

Stichwort
GPS-Ortung

GPS ist die Abkürzung für „Globales Positionsbestimmungssystem". Dieses System wurde in den 1950er Jahren vom US-Militär entwickelt und dient dazu, den Standort eines bestimmten Objektes zu ermitteln und zu überwachen.

Bei GPS handelt es sich um Signale, die Satelliten aussenden. Das bedeutet, um GPS zu nutzen, braucht es keine andere Funktechnologie (wie z. B. WiFi). Man kann aber auch das Mobilfunknetz nutzen, um Standorte zu ermitteln (Triangulation).

Durch das Netzwerk des Globalen Navigationssatellitensystems GNSS können verschiedene Satelliten verwendet werden. Dadurch kann eine frühere und Echtzeit-Navigationsinformation über eine zurückgelegte Strecke geliefert werden.

Die meisten Unternehmen setzen jedoch die GPS-Ortung im Bereich der Logistik und Disposition ein. Fahrzeuge können dadurch gezielt eingesetzt werden, sodass das am nächstgelegenen Fahrzeug zum Einsatz fahren und so eine schnelle Reaktionsmöglichkeit seitens des Unternehmens gewährleistet werden kann. Die Systeme werden auch zur Koordinierung von Ressourcen, Benzinverbrauch, Geschwindigkeitsmessungen und ggf. zum Diebstahlschutz eingesetzt.

Die GPS-Ortung kann sowohl passiv als auch aktiv ausgelegt werden. Beim passiven Abruf ist die GPS-Ortung nur dann aktiv, wenn jemand die Daten abruft (z. B. bei der Paket-Verfolgung). Beim aktiven System ist die Ortung dauerhaft und kann auch bei vergangenem Einsatz abgerufen werden (z. B. beim Navigationssystem).

Die Prinzipien des Datenschutzes

Da die Ortungssysteme mit einem Objekt verknüpft sind, werden personenbezogene bzw. personenbeziehbare Daten erfasst und ausgewertet. Sobald es um die Verarbeitung solcher Daten geht, gilt immer die Datenschutz-Grundverordnung (DSGVO). Dabei müssen die Grundsätze aus Art. 5 der DSGVO eingehalten werden. Bei der GPS-Ortung sind das **Verbot mit Erlaubnisvorbehalt**, das **Prinzip der Zweckgebundenheit** und die **Datenminimierung** von signifikanter Bedeutung.

Gemäß dem **Verbot mit Erlaubnisvorbehalt** ist eine Verarbeitung grundsätzlich verboten. Ausnahmen bestehen, wenn eine Einwilligung der betroffenen Person vorliegt oder ein gesetzlicher Ausnahmefall gem. Art. 6 vorliegt.

Gemäß der **Zweckgebundenheit** und **Datenminimierung** dürfen Daten nur im notwendigsten Umfang für einen zuvor definierten Zweck verarbeitet werden. Bevor die GPS-Ortung eingesetzt werden darf, muss also festgelegt werden, **welcher Zweck** erfüllt werden soll, **wie viele Daten** für die Zweckerfüllung erforderlich sind und auf **welche Rechtsgrundlage** die Verarbeitung gestützt werden soll.

„Private Daten können durch das GPS-System verarbeitet werden, wodurch der Arbeitgebende Informationen erhalten kann, die über das Maß des Beschäftigungsverhältnisses hinausgeht."

Es gilt also schon bei der Auswahl des Systems zu schauen, ob dieses mit den Prinzipen des Datenschutzes im Einklang steht und die rechtlichen Vorgaben beachtet.

Die Rolle des Beschäftigtendatenschutzes

Ergänzend zur DSGVO gilt ebenfalls das Bundesdatenschutz-Gesetz (BDSG). In § 26 BDSG sind maßgebliche Normen zum Beschäftigtendatenschutz festgehalten. Demnach darf eine Verarbeitung nur stattfinden, wenn sie für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Sollten keine Tarifverträge, Betriebs- oder Dienstvereinbarung vorliegen, kann die Verarbeitung auch aufgrund einer freiwilligen Einwilligung erfolgen. Da die Freiwilligkeit wegen des Abhängigkeitsverhältnisses jedoch schwierig zu gewährleisten ist, müssen besondere Anforderungen beachtet werden.

GPS-Ortung im Beschäftigungsverhältnis

Sollen Mitarbeitende per GPS-Ortung getrackt werden, darf dies **ausschließlich** zum vorher definierten Zweck, wie z. B. Einsatzkoordinierung, Abrechnung oder Arbeitszeitkontrolle (bei gesetzlich vorgeschriebenem Fahrtenschreiber) erfolgen. Sollte ein Unternehmen die Daten dazu nutzen, die Arbeitsleistung oder das Verhalten seiner Arbeitnehmer zu kontrollieren, stellt dies einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Mitarbeitenden dar und ist somit **rechtswidrig**.

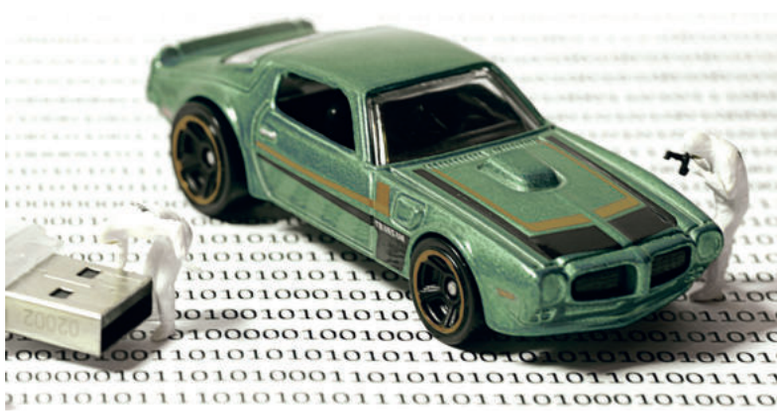
Private Nutzung der Kraftfahrzeuge

Einige Arbeitgebende erlauben die private Nutzung von den zur Verfügung gestellten Kraftfahrzeugen. Diese Fahrzeuge sollten nicht mit einem GPS-Ortungssystem ausgestattet sein, da Arbeitnehmende dadurch unter den Kontrolldruck des Arbeitgebenden fallen können. Private Daten können durch das GPS-System verarbeitet werden, wodurch der Arbeitgebende Informationen erhalten kann, die über das Maß des Beschäftigungsverhältnisses hinausgeht. Die Privatsphäre des Arbeitnehmenden ist nicht mehr geschützt. Die GPS-Ortung sollte also entweder nicht eingebaut sein oder durch den Arbeitnehmenden außerhalb der Arbeitszeit abschaltbar sein.

Was ist also zu tun?

Arbeitgebende sollten die Systeme sorgfältig unter den Aspekten des Datenschutzes auswählen. Dabei sollte zwingend beachtet werden, dass nur die notwendigsten Daten und Funktionen eingesetzt werden. Alle Daten zur Mitarbeitendenüberwachung müssen abgeschaltet werden. Ziehen Sie schon bei diesem ersten Schritt Ihren Datenschutzbeauftragten hinzu, um die datenschutzrechtliche Konformität mitzubetrachten. Es gilt eine gründliche Interessensabwägung und ggfs. eine Risikoabwägung in Form einer Datenschutz-Folgenabschätzung durchzuführen und zu dokumentieren. Dabei ist besonders wichtig zu beachten, ob nicht mildere Mittel zur Zweckerfüllung existieren. Falls ein Betriebsrat oder eine Mitarbeitendenvertretung im Unternehmen eingesetzt wird, muss diese vor dem Einsatz des Systems hinzugezogen werden. Zentral ist ebenfalls die Information der Mitarbeitenden gem. Art. 13 DSGVO. Aufgrund der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO sollte die Information schriftlich erfolgen und vom Mitarbeitenden bestätigt werden.

Die Systeme zur GPS-Ortung sollen grundsätzlich nur nach sorgfältiger Nutzen-Risiko-Analyse eingesetzt werden. &



Multi-Faktor-Authentifizierung – das sollten Sie wissen

In der heutigen digitalen Welt ist die Sicherheit von Informationen und Systemen für Unternehmen von größter Bedeutung. Eine effektive Methode, um den Zugang zu kritischen Ressourcen und Daten zu schützen, ist die Multi-Faktor-Authentifizierung (MFA). In diesem Artikel betrachten wir datenschutzfreundliche MFA-Methoden und deren Bedeutung für Unternehmen.

Von Maximilian Marius Klose

MFA kombiniert zwei oder mehr Authentifizierungsfaktoren, um die Identität eines Benutzers zu bestätigen. Die gebräuchlichsten Faktoren sind etwas, das der Benutzer weiß (z. B. ein Passwort), etwas, das der Benutzer besitzt (z. B. ein Smartphone oder Hardware-Token) und etwas, das den Benutzer unverwechselbar macht (z. B. ein Fingerabdruck). Datenschutzfreundliche MFA-Methoden, wie der Time-based One-Time Password Algorithmus (TOTP), benötigen keine Internetverbindung, um zu funktionieren und bieten somit zusätzliche Sicherheit und Datenschutz.

Obwohl MFA-Apps wie der Microsoft- oder Google-Authenticator bequem sind, sollte man beachten, dass einige Anbieter Cloud-Dienstleister aus den USA sind, was Datenschutzbedenken hervorruft. Um die Sicherheit weiter zu erhöhen, werden hier häufig Telemetriedaten verwendet. Diese Daten enthalten teilweise den Standort, Informationen über das Gerät aber auch IP-Adressen. Aus Datenschutzsicht sollten diese Daten nicht mit einem Dienstleister außerhalb der EU geteilt werden. Hier sollte abgewogen werden, ob die Authentifizierung mit einem der großen Cloud-Dienstleister der richtige Weg ist.

Geht das auch datenschutzkonform?

Eine der datenschutzfreundlichsten MFA-Methoden ist die Verwendung von Hardware-Token. Diese Geräte generieren Passcodes, die vom Benutzer bei der Anmeldung eingegeben werden. Da sie nicht mit dem Internet verbunden sind, bieten sie höhere Sicherheit und Datenschutz. Die Anschaffung dieser Token ist jedoch mit Kosten verbunden und das Risiko, ihn zu verlieren, darf ebenfalls nicht unbetrachtet bleiben.

Weitere Alternativen bilden Open-Source Apps, die ebenfalls den TOTP unterstützen und ohne Telemetriedaten eine sichere Anmeldung gewährleisten können. Diese Apps bieten meistens denselben Schutz, wie die Apps der großen Cloud-Dienstleister, jedoch ohne die Anbindung an externe Stellen. Bei diesen Apps wird bei der Einrichtung ein „Secret“ ausgetauscht, welches es einem Dienst und einem Smartphone erlaubt, zur gleichen Zeit denselben numerischen Code zu generieren.

Wird nun das Smartphone vom Internet getrennt oder jegliche Weitergabe von Telemetriedaten unterbunden, so wird der auf dem Smartphone generierte Code dennoch mit dem eines Dienstes bzw. des Servers übereinstimmen. Möglichkeiten wie Geo-Blocking oder Geo-Fencing sind jedoch mit dieser Variante der MFA nicht möglich.

Eine gute Investition

Insgesamt ist es unerlässlich, eine MFA-Strategie zu implementieren. Durch die Auswahl geeigneter MFA-Methoden und -Anbieter sowie die kontinuierliche Anpassung an die sich ändernde Bedrohungslandschaft und Technologieentwicklung können Sie ihre Ressourcen und Daten schützen und gleichzeitig die Privatsphäre Ihrer Nutzenden wahren. Die kontinuierliche Weiterentwicklung der MFA-Technologie ermöglicht es Ihnen, Ihre Sicherheitsstrategien an die sich ändernden Bedrohungen und Herausforderungen anzupassen.

Die Integration von Künstlicher Intelligenz (KI) und maschinellem Lernen in MFA-Lösungen kann die Erkennung ungewöhnlicher Aktivitäten und potenzieller Sicherheitsrisiken verbessern. Hierbei sollte aber ebenfalls bedacht werden, dass die Unterstützung von KI mit der Erhebung von Daten verbunden ist, die im Hintergrund das Nutzerverhalten analysieren.

Balance zwischen Nutzen und Nutzerfreundlichkeit

Ein weiterer wichtiger Aspekt bei der Implementierung von MFA ist die Benutzerfreundlichkeit. Wenn MFA-Methoden zu komplex oder umständlich sind, kann dies dazu führen, dass Mitarbeitende sie nicht konsequent nutzen oder Umgehungswege suchen. Daher sollten Unternehmen darauf achten, dass die gewählten MFA-Lösungen einfach zu bedienen und in den Arbeitsablauf der Mitarbeitenden zu integrieren sind. Schulungen können hier das Maß an Akzeptanz deutlich erhöhen.

Neben der Implementierung von MFA sollten Notfallpläne und Verfahren zur Wiederherstellung immer mitgedacht werden. Der Verlust eines Smartphones oder eines Hardwaretokens ist eine Gefahr, die nicht unbeachtet bleiben darf, da die Verfügbarkeit von Daten sonst gefährdet sein könnte. Es empfiehlt sich somit, Backup-Authentifizierungsmethoden mitzudenken, die gleichzeitig jedoch nicht die Sicherheit mindern.

Wo geht die Reise hin?

Die Zukunft von MFA wird durch neue Technologien und Trends geprägt sein, die den Datenschutz und die Sicherheit weiter verbessern können, gleichzeitig jedoch genau betrachtet werden müssen. Die Blockchain-Technologie zum Beispiel bietet Möglichkeiten für dezentralisierte Identitätslösungen, bei denen Authentifizierungsinformationen nicht von einem zentralen Anbieter gespeichert werden, sondern in einem verteilten Netzwerk. Diese dezentralisierten Lösungen zeichnen sich dadurch aus, dass nur der Mensch, der das Verfahren nutzt, alle Informationen hat. Kein Dienstleister und keine andere Person besitzt alle Daten, über die verteilten „Teilstücke“ der Daten lässt sich jedoch zweifelsfrei eine Identität nachweisen.

Bildlich wäre hier der Vergleich mit einem sehr umfangreichen Puzzle, bei dem beispielsweise 1000 Menschen ein Teil des Puzzles verschlossen in einer kleinen Kiste in der Hand haben und vor einem schwarzen Vorhang sitzen. Hinter dem Vorhang sitzt die Person, die Ihre Identität bestätigen möchte. Sie hat alle Schlüssel für die Kisten, lässt sich eine Kiste nach der anderen geben und setzt sie zusammen, bis das Puzzle komplett ist.

Fazit

Durch die Auswahl geeigneter MFA-Methoden, Anbieter und Sicherheitsmaßnahmen können Unternehmen ihre IT-Sicherheit und Datenschutzpraktiken optimieren und gleichzeitig die Benutzerfreundlichkeit und Effizienz ihrer Authentifizierungssysteme gewährleisten. Die Einhaltung von Datenschutzgesetzen und -bestimmungen, wie der Europäischen Datenschutz-Grundverordnung (DSGVO), ist ein weiterer entscheidender Faktor bei der Implementierung von MFA-Lösungen. &

Brauchen Sie Hilfe?

Unternehmen müssen sicherstellen, dass ihre MFA-Methoden und -Systeme die Anforderungen dieser Gesetze und Bestimmungen erfüllen, um mögliche Strafen oder Rechtsstreitigkeiten zu vermeiden. Dazu gehört auch die Durchführung von Datenschutz-Folgenabschätzungen und die Implementierung von Datenschutzprinzipien wie Datenminimierung und Privacy by Design. Gerne unterstützen wir Sie bei der Einführung von MFA in Ihrem Unternehmen. Sprechen Sie uns an!

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

Die Ombudsperson

Das Thema Compliance wird ein immer wichtigerer Bereich in Unternehmen. Dadurch werden neue Rollen im Betrieb geschaffen, darunter auch die Ombudsperson. Doch was verbirgt sich hinter diesem Begriff und was unterscheidet die Ombudsperson vom Compliance-Beauftragten?

Von Jessica Henning

Compliance ist das Einhalten von jeglichen Gesetzen, Regeln und Vorschriften sowie von internen Richtlinien und Standards in einer Organisation. Unternehmen haben die Verantwortung sicherzustellen, dass sie in allen Aspekten ihres Geschäfts ethisch und rechtmäßig handeln und die Rechte und Interessen aller Stakeholder, einschließlich Mitarbeitenden, Kunden, Aktionären u. ä. beachten.

Compliance hat in den letzten Jahren stark an Bedeutung gewonnen, da Unternehmen immer stärker reguliert werden und das Risiko von Strafen, Klagen und Reputationsschäden steigt. Rechtliche und finanzielle Risiken sollen minimiert und das Vertrauen von Kunden, Investoren, Mitarbeitenden und anderen Interessengruppen in das Unternehmen erhalten werden. Daher ist Compliance zu einem wichtigen Teil des Risikomanagements und der Unternehmensführung geworden.

Was ist eine Ombudsperson?

Der Begriff Ombudsmann bezeichnete ursprünglich eine Person, die als Vertreter des Volkes gegenüber der Regierung fungierte. Heute wird der Begriff Ombudsperson auch im Bereich der Wirtschaft und des Rechts verwendet, um eine unabhängige Vermittlerrolle zu beschreiben.

Eine Ombudsperson im unternehmerischen Sinne ist eine unabhängige Person, die als Ansprechpartner für Mitarbeitende und Geschäftspartner dient, um Beschwerden oder Bedenken in Bezug auf die Einhaltung von Regeln und Gesetzen im Unternehmen entgegenzunehmen.

Die Aufgaben der Ombudsperson im Bereich Compliance umfassen

- die Entgegennahme von Hinweisen auf Regelverstöße,
- die unabhängige Prüfung und Aufklärung dieser Hinweise,
- Erstellung von Lösungen, sowie
- das Aussprechen von Empfehlungen zur Verbesserung der Compliance im Unternehmen.

Die Ombudsperson soll dabei nicht nur als „Kummerkasten" dienen, sondern auch aktiv dazu beitragen, dass Verstöße vermieden werden und eine Kultur der Compliance im Unternehmen gefördert wird.

Der Unterschied zwischen Ombudsperson und Compliance-Beauftragtem

Im Gegensatz zur Ombudsperson ist der Compliance-Beauftragte eine interne Funktion im Unternehmen. Er ist für die Überwachung und Durchsetzung der Einhaltung von Regeln und Gesetzen verantwortlich und arbeitet mit den Geschäftsbereichen bzw. Bereichsleitern sowie der Geschäftsführung zusammen. Der Compliance-Beauftragte hat also eine aktive Rolle im Unternehmen.

Die Ombudsperson hingegen hat eine unabhängige Position und dient als Ansprechpartner für Mitarbeitende und Geschäftspartner, die Bedenken oder Hinweise auf Regelverstöße haben. Sie ist nicht in die täglichen Geschäftsabläufe involviert und kann somit eine objektive und unabhängige Bewertung vornehmen, ohne Angst haben zu müssen, arbeitsrechtliche Konsequenzen zu erleiden.

Die Rolle der Ombudsperson in der Compliance

Eine Ombudsperson kann auf verschiedene Weisen in die Compliance-Strategie eines Unternehmens eingebunden werden. Eine Möglichkeit besteht darin, eine interne Ombudsstelle einzurichten, die von der Geschäftsleitung oder dem Vorstand unabhängig ist und direkt an diesen berichtet.

Die interne Ombudsstelle kann von Mitarbeitenden, Kunden und anderen Stakeholdern kontaktiert werden, die Bedenken hinsichtlich des Verhaltens des Unternehmens oder seiner Mitarbeitenden haben. Die Ombudsperson kann dann die Beschwerde untersuchen, einschließlich des Sammelns von Informationen und Interviews mit Beteiligten, und Empfehlungen zur Lösung des Problems geben.

Eine andere Möglichkeit besteht darin, eine externe Ombudsstelle zu engagieren, die von einem unabhängigen Dritten betrieben wird und auch von Mitarbeitenden, Kunden und anderen Stakeholdern kontaktiert werden kann. Die externe Ombudsstelle kann auch Schulungen für Mitarbeitende anbieten, um das Bewusstsein für Ethik und Compliance zu schärfen und das Risiko von Fehlverhalten zu reduzieren.

Die Rolle der Ombudsperson im Compliance-Management ist nicht nur auf die Untersuchung von Beschwerden beschränkt. Sie können auch Empfehlungen zur Verbesserung der Compliance-Strategie geben und dazu beitragen, die Einhaltung von Standards und Richtlinien zu fördern. Sie können beispielsweise Schulungen für Mitarbeiter konzeptionieren, um sicherzustellen, dass diese die relevanten Vorschriften und Standards verstehen und befolgen.

Eine wichtige Aufgabe der Ombudsperson besteht ebenfalls darin, eine offene und vertrauliche Kommunikation mit Mitarbeitenden und anderen Stakeholdern zu fördern. Dies ist entscheidend, um sicherzustellen, dass Probleme frühzeitig erkannt werden und dass Mitarbeitende Bedenken ohne Angst vor Vergeltungsmaßnahmen oder arbeitsrechtlichen Konsequenzen äußern können.

Eine weitere wichtige Funktion der Ombudsperson ist, als Vermittler zwischen den verschiedenen Stakeholdern zu

Stichwort
Stakeholder

Der Begriff Stakeholder bezeichnet Personen (Kunden, Mitarbeitende, Lieferanten) oder Gruppen (Institutionen, Aktionäre), die von der Durchführung, des Verlaufs oder Ergebnisses eines Projektes oder Prozesses betroffen sind oder dieses beeinflussen können.

fungieren. Sie können dazu beitragen, Konflikte zu lösen und Lösungen zu finden, die im Interesse aller Beteiligten liegen.

Die Herausforderungen bei der Umsetzung einer Ombudsstelle

Die Einrichtung einer Ombudsstelle innerhalb der Compliance-Strategie bringt Herausforderungen mit sich, so ist z. B. sicherzustellen, dass die Ombudsperson unabhängig und frei von Einflüssen durch die Geschäftsleitung oder andere Interessengruppen ist.

Ebenso muss die Ombudsperson über die erforderlichen und umfangreichen Kenntnisse und Fähigkeiten in diversen Fachbereichen verfügen, um komplexe Fälle zu untersuchen und Lösungen zu finden.

„Die Umsetzung einer Ombudsstelle in der Compliance-Strategie kann Herausforderungen mit sich bringen, insbesondere in Bezug auf Unabhängigkeit, Kompetenz und Akzeptanz."

Auch wenn die Ombudsperson der Schweigepflicht unterliegt, kann es schwierig sein, Mitarbeitende und andere Stakeholder davon zu überzeugen, ihre Bedenken an die Ombudsstelle zu richten, insbesondere wenn sie Angst vor schwerwiegenden Konsequenzen haben.

Darüber hinaus können die Kosten für die Einrichtung und den Betrieb einer Ombudsstelle hoch sein. Es gilt abzuwägen, ob eine externe Ombudsstelle beauftragt werden soll oder ein Mitarbeitender die erforderlichen Kenntnisse besitzt bzw. die nötigen Ressourcen zur Verfügung stehen, Mitarbeitende dahingehend fortzubilden.

Fazit

In einer Welt, in der Ethik und Compliance immer wichtiger werden, spielen Ombudspersonen eine wichtige Rolle bei der Sicherstellung der Einhaltung von Standards und der Vermeidung von Fehlverhalten. Eine Ombudsstelle kann dazu beitragen, Probleme frühzeitig zu erkennen, Konflikte zu lösen und das Bewusstsein für Compliance in der Organisation zu fördern.

Die Umsetzung einer Ombudsstelle in der Compliance-Strategie kann Herausforderungen mit sich bringen, insbesondere in Bezug auf Unabhängigkeit, Kompetenz und Akzeptanz. Unternehmen müssen daher sorgfältig abwägen, welche Art von Ombudsstelle am besten geeignet ist. Das Team von Althammer & Kill übernimmt die Rolle der externen Ombudsperson oder freut sich über die Beratung und Begleitung interner Ombudsstellen.

Insgesamt ist die Rolle der Ombudsperson entscheidend, um sicherzustellen, dass Unternehmen ethisch und rechtmäßig handeln und die Rechte und Interessen aller Stakeholder respektieren. &

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. Juni 2023 – kostenloses Webinar

Datenschutz-Folgenabschätzung

Jede Einführung neuer Verarbeitungsprozesse bedarf einer Datenschutz-Folgenabschätzung. Die Datenschutz-Folgenabschätzung soll dazu dienen, die möglichen Risiken zu verringern und dieses zu dokumentieren. Sie stellt dadurch ein wichtiges Instrument der Rechenschaftspflicht dar. Eine methodische Herangehensweise ist notwendig, ohne dass eine bestimmte Form vorgeschrieben ist.

Sobald aus der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen hervorgeht, verlangt Art. 35 DSGVO vorab eine Abschätzung der Folgen vom Verantwortlichen. Daneben veröffentlichen die Datenschutzbehörden Listen für Thematiken, in denen immer eine Datenschutz-Folgenabschätzung durchzuführen ist. In unserem Webinar führen wir Sie in die Vorgehensweise und mögliche Methodik einer Datenschutz-Folgenabschätzung ein.

5. Juli 2023 – kostenloses Webinar

Security Awareness: Der Weg zur Human Firewall

„Hier nochmal die Datei, die du von mir wolltest" – auf einen Link geklickt und schon ist alles weg.

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. Wenn nicht können sie jedoch die Schwachstelle sein, die Angreifende ausnutzen. Cyber-Security im Zeitalter von Cloud und Co. bedeutet vor allem, dass ein Bewusstsein bei Mitarbeitenden geschaffen werden muss. Im Seminar lernen Sie, wie Sie sich und Ihr Unternehmen schützen, wie Sie Angriffe erkennen und wie einfach es ist, eine Phishing-Kampagne durchzuführen.

So bauen wir gemeinsam Ihre „Human Firewall".

18.–19. September 2023 – Online-Seminar

Datenschutzkoordinator/in DSGVO, DSG-EKD und KDG

Auch wenn keine Datenschutzbeauftragten bestellt werden müssen, sind Datenschutzgesetze und -regelungen einzuhalten und umzusetzen. Hier kommt der Datenschutzkoordinator bzw. die Datenschutzkoordinatorin als fachliche Unterstützung der Unternehmensleitung und Mitarbeitenden ins Spiel. Sie haben einen internen oder externen Datenschutzbeauftragten? Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

Am Ende des Seminars haben Sie die Möglichkeit, an einer Prüfung mit dem Zertifikatsabschluss „Datenschutzkoordinator/in" teilzunehmen. Dieses Zertifikat dokumentiert Ihre Datenschutzkompetenz gegenüber der Aufsichtsbehörde, Vorgesetzten, Geschäftspartnern und Mitarbeitenden Ihrer Organisation.

Ihr Ansprechpartnerin:

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

Mit Verständnis und Einfühlungsvermögen

Arne ist bei Althammer & Kill nicht mehr wegzudenken.

Arne hat bei Althammer & Kill bereits mehrere Stellen bekleidet und einige Büros durchlaufen. Vor allem die gelebte Diversität hat es ihm angetan.

Welche Ausbildung oder welches Studium hast du absolviert?

Arne: Ich habe Informatik – genauer gesagt „Angewandte/Praktische Informatik mit Anwendungsfach Mathematik" – an der TU Clausthal studiert und mit Diplom (die älteren erinnern sich) abgeschlossen.

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

Arne: Das war eigentlich eher zufällig. Ich war auf der Suche und mein damaliger Kollege Ralf, der damals schon (und heute immer noch) die Gestaltung für Althammer & Kill machte, meinte, ich solle doch mal Thomas fragen – den kannte ich flüchtig von einer Geburtstagsfeier bei Ralf. Wir haben uns dann einfach mal getroffen und der Rest ist Geschichte. 😉

Das war zu der Zeit, als die DSGVO gerade in Kraft getreten war und viele Unternehmen sich zum ersten Mal ernsthaft mit Datenschutz auseinandergesetzt haben – entsprechend viel gab es zu tun. Gestartet bin ich mit einer Aufgabenverteilung von 50 % Beratung und 50 % Entwicklung/IT-Administration, das hat sich aber über die Jahre immer wieder verschoben – viele Bereiche sind dazugekommen oder weggefallen. Derzeit habe ich gerade begonnen, mich um das Wissensmanagement zu kümmern, aber auch weiter um IT-Administration, Customizing, unsere eigenen Internetauftritte, das Verfassen redaktioneller Beiträge, …

Wie sieht dein Arbeitsalltag aus?

Arne: Abgesehen von einer Handvoll wiederkehrenden Administrationsaufgaben ist das sehr unterschiedlich, je nachdem, was halt aktuell so ansteht. Ich lege mir immer einige Aufgaben für den Tag zurecht – zum Beispiel Vorlagen aktualisieren oder neu erstellen, Änderungswünsche für unsere unterschiedlichen Softwaretools umsetzen, Artikel redigieren beziehungsweise selbst schreiben oder Themen und Termine für Webinare und Blogbeiträge verteilen,

die wir in der Redaktionskonferenz besprochen haben – aber oft überlebt die Planung den Morgenkaffee nicht…

Was gefällt dir besonders an der Tätigkeit?

Arne: Die Abwechslung und der gute Mix aus Routine und Herausforderung. Ich kann mir meine Arbeit weitgehend selbst organisieren, bekomme immer Unterstützung, wenn ich sie brauche und einfordere und kann so meine Komfortzone immer mehr erweitern.

Du bist ja nicht mehr aktiv in der Beratung tätig. Was fehlt dir daran/Was hat dir daran besonders viel Spaß gemacht?

Arne: Wahrscheinlich die große Bandbreite der Kundenfragen und das direkte Feedback. Es kamen sehr unterschiedliche Fragestellungen von den Kunden – teilweise ganz allgemeine, teilweise sehr spezielle. Es erfordert ein grundlegendes Verständnis für die Bedürfnisse des Kunden und oft auch ein gewisses Einfühlungsvermögen, um eine Lösung zu finden, die sowohl gesetzeskonform als auch praktikabel ist. Wenn das gelingt und der Kunde zufrieden ist, kann das sehr befriedigend sein.

Welche Anfragen bekommst du von Kolleginnen und Kollegen am häufigsten?

Arne: Am häufigsten wohl IT-Probleme, wie sie jeder schon mal hatte – irgendetwas funktioniert plötzlich nicht mehr oder zumindest nicht mehr so wie gewohnt. Das reicht von kleineren Software-Merkwürdigkeiten bis hin zu Hardwareausfällen und verlangt mal die eine, mal die andere Herangehensweise – oft weiß man erstmal nicht, welche und muss „strukturiert rumprobieren". Erfahrung hilft, ist aber auch keine Garantie für Erfolg. Insbesondere im Microsoft-365-Umfeld muss man ständig am technologischen Ball bleiben, weil die Entwicklung fortwährend voranschreitet. Aktuell gibt es zum Beispiel verstärkt die Tendenz, künstliche Intelligenz einzusetzen – nach meinem Dafürhalten mehr getrieben durch die mediale Aufmerksamkeit auf dem Thema und weniger durch echten Bedarf. Ich glaube, dass derzeit etliche Unternehmen Produkte herausbringen

„Es erfordert ein grundlegendes Verständnis für die Bedürfnisse des Kunden und ein gewisses Einfühlungsvermögen, eine Lösung zu finden, die sowohl gesetzeskonform als auch praktikabel ist."

und Features implementieren, die die Marktreife eigentlich noch gar nicht erreicht haben, weil sie unter hohem Druck stehen, als innovativ gelten zu müssen. Gerade aus Datenschutzsicht birgt das Risiken, die man permanent im Auge behalten muss.

Wie eng arbeitest du mit anderen Abteilungen zusammen?

Arne: Unterschiedlich – bei IT-Admin-Themen vor allem individuell und abteilungsübergreifend, da Technik-Probleme entweder nur Einzelne betreffen, mit denen man dann gemeinsam auf Fehlersuche geht, oder aber alle, wenn grundlegende Systeme gestört sind und man sich innerhalb des IT-Teams austauscht. Mit den Beratenden habe ich natürlich besonders viel im Wissensmanagement zu tun, schließlich sind sie das primäre Objekt meiner Bemühungen – sie schaffen das Wissen, das ich dann einsammle, aufbereite und zugänglich mache. Mit dem Marketing muss ich mich vor allem bei der Pflege unserer Websites und der redaktionellen Arbeit abstimmen und die Verwaltung ist meistens der interne Auftraggeber für das Customizing der von uns eingesetzten Software.

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

Arne: Das Arbeitsklima. Die Kollegen. Das eigenverantwortliche Arbeiten. Das Vertrauen, das jedem entgegengebracht wird. Grundsätzlich habe ich nie das Gefühl, dass Gewinnmaximierung die Triebfeder unserer Tätigkeit ist, sondern das Bestreben, gute Arbeit zu leisten und nachhaltige Kundenbeziehungen zu unterhalten. Und das gilt auch für die Beziehung zwischen Arbeitgeber und Arbeitnehmer. Es wird immer versucht, alles möglich zu machen.

Ebenso wichtig finde ich auch, dass hier Diversität, Integration und Gleichberechtigung wirklich gelebt werden – also nicht bloß angestrebt, gefördert und unterstützt. Ich habe es hier nie erlebt, dass irgendjemand wegen Geschlecht, Alter, Herkunft oder sonstiger personenbezogener Eigenschaften besonderer Kategorie anders behandelt worden wäre (vgl. Art. 9 Abs. 1 DSGVO 😉) – im Gegenteil, die vielen unterschiedlichen Lebenserfahrungen und Perspektiven werden als Stärke erkannt. Als schwuler Mann in meinem Alter kenne ich das auch anders. &

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