

mag

Buchen Sie
Ihr kostenfreies
Ticket für:
DFC Virtual,
Provide-tech,
Dikomm,
Provide-recruit

Datenschutz 2024: Lokomotive oder Bremsklotz?

Data Security - alles Zauberei?

Der Nutzen eines aktiven Daten-
schutzes bietet vielseitige Vorteile

Die Kreislaufwirtschaft und die Bedeutung
der zertifizierten Datenlöschung

Whistleblowinggesetz auf der Zielgeraden: Jetzt kommt das
Hinweisgeberschutzgesetz auch für kleine Unternehmen!

DATENSCHUTZ - LOKOMOTIVE ODER BREMSKLOTZ

QR-Code
mit dicoo-App
scannen und
Neues erleben!



QR-Code mit dicoo-App
scannen

Mit der dicoo rs+c[®] Methode

Das einzige Magazin mit
dem direkten Kontakt zwischen Leser, Autor und zurück!

www.digital-futuremag.de



MACHEN SIE IHR GEBÄUDE FIT FÜR DIE ZUKUNFT!

DAS WOHL SMARTESTE ENERGIE- UND GEBÄUDEMANAGEMENT FÜR INDUSTRIE & BÜROGEBÄUDE

Wir revolutionieren das Energie- und Gebäudemanagement mit speziell dafür entwickelten App-basierten Lösungen und schaffen so eine Kommunikationsinfrastruktur für intelligentes und effizientes Energiemanagement und alle relevanten Betriebsprozesse in Bestandsgebäuden. Im Besonderen profitieren davon Industrie- & Bürogebäude, sogenannte Mischflächen mit unterschiedlichsten Anforderungen an das Raumklima, die Luftqualität und flexibles Raum-Management.



**BIS ZU 90% ENERGIE & EMISSIONEN BEI BELEUCHTUNG SENKEN.
BIS ZU 30% BEI ALLEN WEITEREN VERBRÄUCHEN REDUZIEREN.**



SOFORTIGER ROI! Jetzt gratis KOSTEN-NUTZEN-ANALYSE durchführen



Editorial - Aufgeräumt und souverän: Die Essenz der geschäftlichen Datenverantwortung

Liebe Leserinnen und Leser,

auch wenn es für viele Unternehmensverantwortliche eine mitunter unangenehme, häufig auch stiefmütterlich behandelte Herausforderung darstellt: Im immer komplexer werdenden digitalen Zeitalter wird der Ruf nach Informationssicherheit, sowohl intern als auch in der Kundenkommunikation und in der Zusammenarbeit mit Partnern bzw. Dienstleistern, stetig lauter.

Das Bewusstsein für die Bedeutung von Datenintegrität und -schutz - gerade im Dickicht zunehmender regulatorischer Hürden, Compliance-Bestimmungen, Gesetzesverordnungen etc. - hat stark zugenommen. Dennoch umgeben viele Missverständnisse, sich hartnäckig haltende Irrtümer, vage Behauptungen oder gar gefährliches "Halbwissen" im öffentlichen Diskurs diese wichtigen Business-Themen.

Im aktuellen DFmag werfen wir daher einen ausführlichen Blick auf entscheidende Aspekte, die es nicht nur für große Player, sondern insbesondere auch KMU zu beachten gilt, damit wettbewerbskritisches Firmen-Know-how oder sensible Customer Data nicht in falsche, beispielsweise internetkriminelle Hände geraten.

Die vorliegende Ausgabe vermittelt Ihnen unter anderem durch unsere Interviews mit ausgewiesenen Experten entsprechendes Hintergrundwissen über Rechte und Pflichten, gibt Handlungsempfehlungen sowie Tipps zu den Dos und Don'ts in der derzeitigen Debatte.

So erklärt etwa der renommierte BISG-Vorstand und GDD-Mitglied Dr. Ralf W. Schadowski, worauf Sie achten sollten, damit der Datenschutz im kommenden Jahr eher zur Effizienz-Lokomotive als zum betrieblichen Bremsklotz wird. Fachanwalt Marc Oliver Giel von datamog räumt transparent mit immer noch weit verbreitenden Data Security-Mythen auf. Key-Kom-CEO Ralf Kamnitzer zeigt, welche vielseitigen Vorteile die aktive Nutzung der DSGVO Ihrer Organisation bringt. In einem Gastbeitrag beleuchtet Ruud de Wildt (Certus Software GmbH) anhand eines konkreten Best Practices aus der Kreislaufwirtschaft, mit welchen zertifizierten Methoden sich Daten auf sämtlichen elektronischen Geräten ordnungsgemäß wie nachhaltig löschen lassen, sobald sie nicht mehr kollektiv in einem größeren Arbeitsumfeld benötigt werden. Außerdem verrät Juristin Astrid Meyer-Krumenacker von amk-law in einem Impulsartikel, wie sich speziell für Mittelständler ab 50 Mitarbeitern Personalstärke, das für diese verpflichtende Hinweisgeberschutzgesetz noch bis Mitte Dezember fristgemäß umsetzen lässt.

Ich wünsche Ihnen nun bei der Lektüre viele neue Erkenntnisse zu potenziellen Chancen und zielführenden Möglichkeiten, um strategisch-technologisch inspiriert eigene Präventionsvorhaben und -maßnahmen bedarfsgerecht(er) angehen, weiterentwickeln oder optimieren zu können.

Viel Spaß beim Lesen!



Ihr Michael Mattis
Herausgeber



>> Bitte mit DICOO-App scannen

KONTAKT



AMC MEDIA NETWORK GmbH & Co. KG
Otto-Hesse-Straße 19 - T9
64293 Darmstadt
Michael Mattis
+49 6151 - 957577 -0
michael.mattis@amc-media-network.de
www.amc-media-network.de

PS: Jetzt kostenlos auf dicoo eintragen!
Nutze die Plattform und präsentiere Dein Unternehmen,
sammle Leads und Kontakte.

DFmag
Powerd by



INHALT

DEZEMBER 2023



DATENSCHUTZ 2024: LOKOMOTIVE ODER BREMSKLOTZ?

6

IM INTERVIEW MIT DR. RALF W. SCHADOWSKI, VORSTAND IM BUNDESFACHVERBAND DER IT-SACHVERSTÄNDIGEN BISG E.V. UND AKTIVES MITGLIED IN DER GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT GDD E.V.

- 2 Clear Light GmbH - **Anzeige**
- 3 Editorial
- 6 Datenschutz 2024: Lokomotive oder Bremsklotz? - **Interview**
- 10 Silicon Valley Europe - **Anzeige**
- 11 Dicoo - **Anzeige**
- 12 Data Security - alles Zauberei? Aufräumen mit weitverbreiteten Mythen im Datenschutz - **Interview**
- 14 Provide-recruit - **Anzeige**
- 17 Dikomm - **Anzeige**
- 18 Der Nutzen eines aktiven Datenschutzes bietet vielseitige Vorteile - **Interview**
- 22 Die Kreislaufwirtschaft und die Bedeutung der zertifizierten Datenlöschung - **Gastbeitrag**



DER NUTZEN EINES AKTIVEN DATENSCHUTZES BIETET VIELSEITIGE VORTEILE

18

IM INTERVIEW MIT RALF KAMNITZER, EINEM SEHR ERFAHRENEEN DATENSCHÜTZER IM RHEIN-MAIN-GEBIET



DATA SECURITY - ALLES ZAUBEREI? AUFRÄUMEN MIT WEITVERBREITETEN MYTHEN IM DATENSCHUTZ

IM INTERVIEW MIT MARC OLIVER GIEL VON DATAMOG

24 **DIGITAL FUTURE**congress Virtual -
Anzeige

26 Whistleblowinggesetz auf der
Zielgeraden: Jetzt kommt das
Hinweisgeberschutzgesetz auch für
kleine Unternehmen! - **Gastbeitrag**

29 **DIGITAL FUTURE**mag Mediadaten
1000° E-PAPER - **Anzeige**

30 Gastbeitrag von Dipl.-Chem.oec.
Stephanie Ta, Authorised Officer/ Pro-
kuristin Syntlogo GmbH - **Gastbeitrag**

36 Provide-tech - **Anzeige**
Mediadaten - **Anzeige**



22

DIE KREISLAUFWIRTSCHAFT UND DIE BEDEUTUNG DER ZERTIFIZIERTEN DATENLÖSCHUNG

GASTBEITRAG VON RUUD DE WILDT,
CERTUS SOFTWARE GMBH



26

WHISTLEBLOWINGGESETZ AUF DER ZIELGERADEN: JETZT KOMMT DAS HINWEISGEBERSCHUTZGESETZ AUCH FÜR KLEINE UNTERNEHMEN!

EIN GASTBEITRAG VON ASTRID MEYER-KRUMENACKER,
RECHTSANWÄLTIN

DATENSCHUTZ 2024: LOKOMOTIVE ODER BREMS?



Im Interview mit Dr. Ralf W. Schadowski, Vorstand im Bundesfachverb
und aktives Mitglied in der Gesellschaft für Datenschutz und Datensic

Dr. Ralf W. Schadowski ist eine herausragende Persönlichkeit im Bereich Datenschutz und Informationssicherheit, bringt dazu eine wirklich beeindruckende Palette von Qualifikationen und Erfahrungen mit und zeichnet als Geschäftsführer für die datenschutz- wie IT-sicherheitsrelevante Leitung und strategische Ausrichtung von Unternehmen verantwortlich. Er ist ein ISO/IEC 17024 zertifizierter und überwachter europäischer Datenschutzbeauftragter, was seine hohe Fachkompetenz in Datenschutzfragen unterstreicht. Zudem besitzt er die Zertifizierungen als ISO/IEC 27001 zertifizierter Lead Auditor und Implementer sowie als ISO/IEC 27701 zertifizierter Lead Implementer. Dies demonstriert seine Fähigkeit zur Implementierung von Informationssicherheits- und Datenschutz-Managementsystemen auf höchstem Niveau.

DATA BREMSKLOTZ?

Band der IT-Sachverständigen BISG e.V.
Sicherheit GDD e.V.

Dr. Schadowski ist nicht nur im Rahmen von Zertifizierungen und Audits aktiv, sondern auch als Fachgruppenleiter für Datenschutz und Vorstandsmitglied im renommierten Bundesfachverband der IT-Sachverständigen BISG e.V. Hier setzt er sich für die Förderung von IT-Sicherheits- sowie Datenschutz-Fachwissen und dementsprechenden bewährten Praktiken ein. Darüber hinaus engagiert sich der Experte in der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., einer angesehenen Datenschutz- und Datensicherheits-Organisation, wo er sein Wissen mit anderen Spezialisten teilt und in die Gestaltung von Datenschutzrichtlinien und -praktiken einbringt. Durch seine umfangreichen Kompetenzen ist

Dr. Schadowski Schlüsselfigur sowie Meinungsbildner in puncto Datenschutz und IT-Sicherheit in Deutschland. Und damit für uns der ideale Gesprächspartner, um zu erfahren, ob Datenschutz im kommenden Jahr insbesondere für den Mittelstand businessfördernd oder -hemmend wird.

DIGITAL FUTUREmag: Herr Schadowski, mit der Einführung der Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union wurde der Datenschutz in Deutschland sowie international weiter harmonisiert und gestärkt. Soweit die Theorie. Hat die DSGVO ihre Ziele erreicht?

Dr. Ralf W. Schadowski: Die DSGVO hat erreicht, dass viele Organisationen endlich mit der Umsetzung der Datenschutzerfordernisse begonnen, eine ganze Menge aber noch nicht einmal die grundlegenden Dinge im Datenschutz angepackt haben. Die Daten gehören dem Betroffenen, und die Einhaltung deren Grundrechte muss jede Organisation nachweisen können. Es ist unfassbar, was wir in den letzten 1.000 Audits teilweise feststellen mussten. Es wird Zeit, dass Verantwortliche bei Fahrlässigkeit endlich in die persönliche Haftung gehen müssen. Dann bewegt sich das auch. Auf der anderen Seite wird die DSGVO teils zu scharf umgesetzt und führt zur Innovationsbremse. Hier braucht es Augenmaß!

DIGITAL FUTUREmag: Wie kann der Datenschutz in Unternehmen effektiv in die Planung und Umsetzung digitaler Transformationsprojekte integriert werden, um Risiken zu minimieren?

Dr. Ralf W. Schadowski: Am Ende des Tages geht es doch um Kontrolle über Daten. Keine Organisation will Daten verlieren und an einen Pranger kommen. Die Anforderungen der DSGVO sollten verantwortliche Geschäftsführer und Vorstände als Leitplanken verstehen, nicht als Bürde. Dann hilft Datenschutz nicht nur personenbezogene, sondern jegliche Daten unter Kontrolle zu halten.

DIGITAL FUTUREmag: Welche bewährten Praktiken und Strategien empfehlen Sie Firmen, um die Datenschutzerfordernisse in einer sich ständig verändernden digitalen Umgebung zu erfüllen?

Dr. Ralf W. Schadowski: Die Datenschützer haben Werkzeuge wie zum Beispiel die Verzeichnisse nach Artikel 30 DSGVO, in der Organisationen nicht nur datenschutzrechtliche Pflichtdokumentation führen, sondern eine wertvolle Prozessdokumentation darstellen und jede Organisation stabilisieren. Bei Veränderungen, etwa bei der Einführung von Cloud-Technologien oder durch Systemveränderungen, ist so ein geordneter Ablauf zu Gunsten der Organisation sichergestellt.

DIGITAL FUTUREmag: Wie schaffen es Verantwortliche, dass sie die geltenden Datenschutzerfordernisse in verschiedenen Ländern und Regionen einhalten, insbesondere in Anbetracht der globalen Reichweite digitaler Geschäftsmodelle?

Dr. Ralf W. Schadowski: Oft fehlt es an einer IT-Prozess- und System-Dokumentation, weil interne Abteilungen überlastet sind und das nicht auch noch nebenher erledigen können. Hat man das "Bild der Prozess- und Systemlandschaft" einmal erstellt, ist es ein Leichtes, den Überblick zu behalten, bei jedem Verarbeitungsort und -weg die richtigen Maßnahmen einzuleiten sowie bei Änderungen anzupassen. Ordnung ist das halbe Leben. International treffen wir auf zahlreiche abweichende Regelungen und Normen, die über eine Matrix-Bewertung zu einem akzeptierten Unternehmens-Standard führen. So können globale Datenströme rechtskonform stattfinden.

DIGITAL FUTUREmag: Inwiefern kann Datenschutz als Wettbewerbsvorteil und Wegbereiter für innovative Geschäftsmodelle dienen, anstatt als Hindernis?

Dr. Ralf W. Schadowski: Wir bedienen aktuell 400 Organisationen in nahezu allen Branchen, regional bis global. Querbeet erhalten die Organisationen "Lieferantenaudits", man spricht von Supply Chain, ob nun DSGVO, NIS2, DORA, CER, et cetera. Besteht die Organisation das Audit nicht, verliert sie unmittelbar den Auftrag, Geld, Jobs und so weiter. Die Anforderungen sind nicht kompliziert, es fehlt an Aufmerksamkeit und Interesse, grundlegende Anforderungen an Datensicherheit umzusetzen. Einmal durchgeführt, sollten Organisationen den Reifegrad nach außen zeigen.

DIGITAL FUTUREmag: Wie kann eine proaktive Datenschutzstrategie dazu beitragen, das Risiko von Daten- und Datenschutzverletzungen zu minimieren sowie gleichzeitig das Vertrauen der Kunden zu erhöhen?

Dr. Ralf W. Schadowski: Organisationen sollten einen einfachen, leistbaren Implementierungs- und Auditplan erstellen und verwirklichen. Die Ergebnisse sollten den Geschäftspartnern unaufgefordert mitgeteilt werden. Das stärkt in heutigen Zeiten das Vertrauen nicht nur in Geschäftsbeziehungen, sondern auch in den Arbeitgeber!

DIGITAL FUTUREmag: Welche erfolgreichen Unternehmen gibt es, die den Datenschutz als integralen Strategiebestandteil nutzen, um das Customer Trust zu stärken und ihre Marktposition zu optimieren?

Dr. Ralf W. Schadowski: Ich darf keine Namen nennen. Es gibt zahlreiche Veröffentlichungen, die zeigen, welche



Unternehmen Daten verloren, erpresst wurden oder auch Ordnungsgelder erhielten. Jeder hat Zugriff. Lernen wir aus den Fehlern, die dort gemacht wurden und sorgen dafür, dass sich genau das nicht wiederholen kann. Mit einfachen Mitteln und gesundem Menschenverstand wären diese Organisationen nicht in die Schlagzeilen geraten.

DIGITAL FUTUREmag: Welche Tools und Technologien stehen Firmen zur Verfügung, um Datenschutz-Compliance zu erleichtern und gleichzeitig Geschäftswachstum zu fördern?

Dr. Ralf W. Schadowski: Je nach Branche und Größe einer Organisation können erfahrene Datenschutzbeauftragte mit Bordmitteln ein funktionierendes DSMS, also Datenschutz-Managementsystem, aufbauen und betreiben. Der Aufwand ist übersichtlich und stabilisiert die Resilienz der Abläufe. Fertige DSMS Tools in der Cloud geben Einsteigern eine Orientierung, aber benötigen zusätzliches Budget und führen zu Abhängigkeiten.

DIGITAL FUTUREmag: Wie können Entscheider sicherstellen, dass die ISO 27.001-Zertifizierung nicht nur ein bürokratischer Prozess ist, sondern tatsächlich dazu führt, die Informationssicherheit zu verbessern?

Dr. Ralf W. Schadowski: Als erfahrener ISO 27001 Senior Implementer und Auditor stelle ich fest, dass die meisten Organisationen im Rahmen der ISO 27001 erstmals systematisch über Risiko-Management und fundamentale IT-Sicherheitsprinzipien nachdenken. Das ist der eigentliche Gewinn für jede Organisation, die eine Zertifizierung anstrebt. Die nachfolgenden „internen Auditierungen“ helfen ihr, Bedrohungen aufmerksam wahrzunehmen und widerstandsfähiger zu sein.

DIGITAL FUTUREmag: Die Künstliche Intelligenz ist weltweit auf dem Vormarsch. Welche Rolle spielen neue Technologien wie diese oder das Internet der Dinge bei der Erhöhung der Datenschutzerfordernungen?

Dr. Ralf W. Schadowski: Die Einbindung von KI in tägliche Aufgaben ist faszinierend und beschleunigt richtig eingesetzt die Arbeit enorm. IT-affines Personal muss von der Geschäftsleitung in Delegation sensibilisiert werden für die richtige Anwendung, um den Verlust von geistigem Eigentum zu vermeiden. Unternehmen, die KI nicht evaluieren, werden ins Hintertreffen geraten.

DIGITAL FUTUREmag: Ich bin sicher, auf diese Frage haben Sie gewartet: Wie würden Sie insgesamt das

Thema Datenschutz in Bezug auf Digitalisierung und die Entwicklung unserer Wirtschaft beurteilen – als Lokomotive oder als Bremsklotz?

Dr. Ralf W. Schadowski: Im Gegensatz zu vielen medialen Darstellungen ermöglicht ein mit Augenmaß angewendeter Datenschutz globale IT-Strategien unter Berücksichtigung unserer informationellen Selbstbestimmung. Das geht einfacher, als Nicht-Datenschützer sich das vorstellen können und wir seit langem beweisen. Datenschutz ist ein Werkzeug und keine Wissenschaft.

DIGITAL FUTUREmag: Ganz herzlichen Dank für Ihre Zeit und insbesondere auch für den Einblick in Ihre wichtigen Service-Angebote.



Dr. Ralf W. Schadowski

>> Bitte mit dicoo-App scannen

KONTAKT



Firma: ADDAG GmbH
Straße: Krefelder Strasse 121
PLZ und Ort: 52070 Aachen
Ansprechpartner: Dr. Ralf W. Schadowski
Telefon: +49 241-44688-20
Email: schadowski@addag.de
Website: <https://addag.de/>

Willkommen

in Europas neuem IT Cluster



Es ist Zeit Europas IT-Community neu zu denken.

Kannst Du Dir vorstellen, Teil eines großen und interaktiven Netzwerks zu sein, in dem Deine Meinung zählt, Du Unterstützung bei Deinen Herausforderungen erhältst und darüber hinaus Dein Unternehmen Sichtbarkeit und Anerkennung?

Wie wäre es, wenn es eine Community gäbe, die genau diese Kriterien für Dich erfüllt?

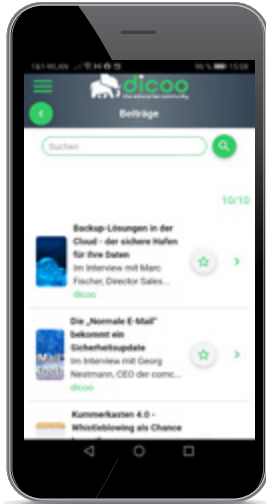
Die gute Nachricht: Diese Community entsteht gerade jetzt.

Das Silicon-Valley-Europe.com wartet auf Dich und Deine Expertise!

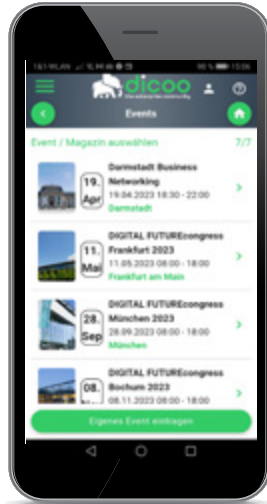
People • Events • Companies • Clubs Interviews • Videos • Podcasts • Jobs



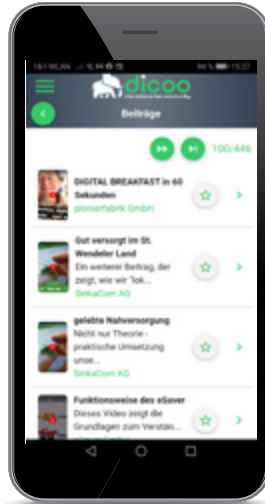
Home
Dein Überblick



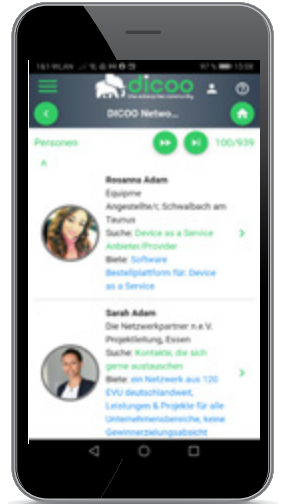
Interviews
Dein Input



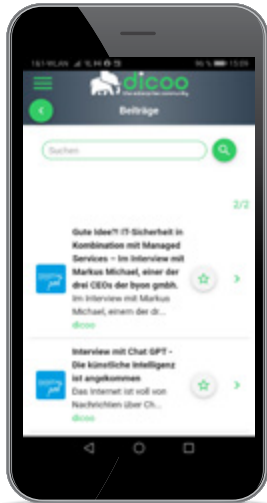
Eventübersicht
Alle Deine Events!



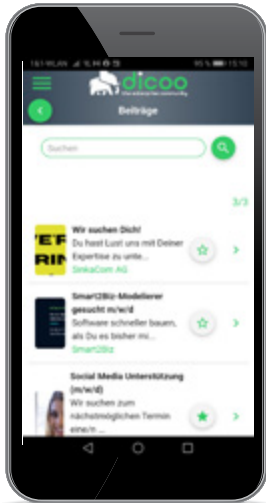
Videos
Deine Filme



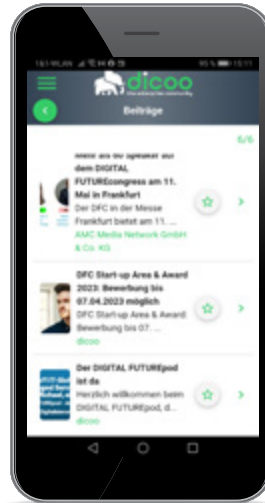
People
Dein Netzwerk



Podcasts
Dein Audiomarketing



Jobs
Deine offenen Stellen



News
Deine Neuigkeiten



Zuletzt besucht
Deine Historie

App-Store aufrufen und **dicoo-App** downloaden.



Android



iOS

DATENSCHUTZ FÜR KMU



AUFRÄUMEN MIT WEITVERBREITETEN MYTHEN

Im Interview mit Marc Oliver Giel von Datamog

Datamog | Datenschutz IT Recht wurde im Jahr 2017 von Rechtsanwalt Marc Oliver Giel ins Leben gerufen, um speziell kleinen und mittleren Unternehmen (KMUs) aus dem Bereich der Informationstechnologie eine kompetente Anlaufstelle in Bezug auf Datenschutz und Compliance-Anforderungen zu bieten.

Seine über 16 Jahre juristische Erfahrung und insbesondere Fach-Expertise im IT-Recht ermöglicht es Unternehmen, Datenschutzrichtlinien effizient und kostengünstig zu implementieren. Bei Datamog können Unternehmensverantwortliche eine Vielzahl von Datenschutzlösungen in Anspruch nehmen. Darunter Audits, Auftragsverarbeitungsverträge (AV-Verträge), Beratungsdienste, Erstellung von Datenschutzerklärungen, Datenschutz-Management-Systeme sowie Schulungen und mehr.



Gerade bei kleineren Firmen erhält das Thema Datenschutz häufig nicht die notwendige Aufmerksamkeit. Für Organisationen mit 20 oder mehr Mitarbeitern bietet Datamog die Möglichkeit eines externen betrieblichen Datenschutzbeauftragten, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Im Interview sprechen wir heute mit dem Experten insbesondere über gängige in der Businesswelt existierende Datenschutz-Behauptungen oder -Vermutungen, zu deren tatsächlichem Wahrheitsgehalt es einmal konkret aufzuklären gilt.

DIGITAL FUTUREmag: Herr Giel, welche weitverbreiteten Mythen gibt es bezüglich Datenschutz, die in der Öffentlichkeit und im Netz kursieren und warum halten sich diese zum Teil kuriosen Vorstellungen so lange?

Marc Oliver Giel: Ein Mythos kommt mir immer wieder unter, und zwar: Unternehmen mit weniger als 10 oder 20 Beschäftigten müssten im Datenschutz nichts machen. Dabei handelt es sich um „gefährliches Halbwissen“. Denn es gab früher mal die 10er-Regel, dass nur Unternehmen mit 10 oder mehr Beschäftigten einen Datenschutzbeauftragten bestellen müssen. Mit einer Gesetzesänderung im Jahre 2019 wurde die Schwelle auf 20 oder mehr Beschäftigte angehoben. Offenbar haben einige Geschäftsleitungen angenommen, der Datenschutzbeauftragte müsse sich um die Einhaltung von Datenschutz im Unternehmen kümmern und wenn ein solcher nicht bestellt werden muss, gibt es auch keine To-dos. Dies ist allerdings falsch. Auch wenn kein Datenschutzbeauftragter bestellt werden muss, hat sich die Geschäftsleitung selbst um die Umsetzung des Datenschutzes zu kümmern. Für Kleinunternehmen gibt es keine Gesetzesausnahme.

DIGITAL FUTUREmag: Welche praktischen Tipps haben Sie für Firmen mit weniger als 20 Leuten, um sich

dem Thema Datenschutz sinnvoll und vor allen Dingen professionell zu nähern?

Marc Oliver Giel: Ich sehe immer wieder, dass sich Geschäftsleitungen mit Vorlagen von Verbänden, aus dem Internet oder sogar von Mitbewerbern versorgen und annehmen, wenn auf dem Dokument ihr Firmenname stünde, wären alle Aufgaben erledigt. In vielen Fällen muss man als Experte aber feststellen: Es besteht meist gar kein Verständnis, welche Pflichten es überhaupt gibt und wie diese effektiv erfüllt werden können. Eine Auflistung an dieser Stelle würde den Rahmen des Beitrags sprengen. Daher ist mein Geheimtipp so einfach wie simpel: Lassen Sie sich von einem Datenschutzbeauftragten oder einem Rechtsanwalt mit Schwerpunkt Datenschutz individuell beraten. Schon nach ein bis zwei Stunden steht eine grobe To-do-Liste mit den 10 wichtigsten Aufgaben und die Geschäftsleitung versteht, warum was gemacht werden muss. Sie sagen Ihrem Facharbeiter, der mit Maschinen arbeitet, ja auch nicht: „Frag nicht warum, aber drück jeden Tag um 12 Uhr auf den blauen Knopf!“ Besser ist zu erklären, warum er das machen soll und welche Auswirkungen der blaue Knopf hat.

DIGITAL FUTUREmag: Weshalb ist es wichtig, dass B2B-Betreiber personenbezogene Daten achten und schützen müssen?

Marc Oliver Giel: Kess gesagt: Weil es im Gesetz steht. Aber im Ernst: Datenschutz ist kein bürokratischer Selbstzweck, sondern die Umsetzung des Rechts auf informationelle Selbstbestimmung. Die einfache Übersetzung dazu lautet: Jede Person soll selbst entscheiden dürfen, wie mit ihren Daten umgegangen werden muss. Wenn ein Unternehmen Datenschutz ernst nimmt, wertschätzt es gleichzeitig seine Kunden, Lieferanten, Geschäftspartner und vor allem seine Beschäftigten. Manche Datenschutzverstöße von Unternehmen lassen mich ratlos zurück: Wie kann man nur seine eigenen Mitarbeiter illegal per Video überwachen? Ich frage mich dann: Was nützt es dem einzelnen Mitarbeiter, wenn er einerseits über Mindestlohn vergütet wird, monatliche Tankgutscheine und betriebliche Altersvorsorge erhält, andererseits aber bei seiner täglichen Arbeit ausspioniert wird? Das ist grotesk!

DIGITAL FUTUREmag: Ist Datenschutz wirklich eine Lokomotive? Welche Vorteile bringt er für Kunden, Lieferanten, Geschäftspartner oder Mitarbeiter und wieso sollte man ihn nicht als bürokratische Schikane betrachten?

**Die IT-Personalgewinnungsplattform
für Ihr Unternehmen!**
powered by Silicon-Valley-Europe.com

 **provide-
recruit.eu**
european virtual recruiting event

24.-25.09.2024



www.provide-recruit.eu



Marc Oliver Giel: Um in Ihrem Bild der Lokomotive zu bleiben: Das technische Prinzip hinter einer Dampflok ist simpel. Die Bedienung aber gleichwohl nur etwas für erfahrene Personen. Ähnlich läuft es im Datenschutz. Der Kern des Datenschutzes ist glasklar: Der Schutz der informationellen Selbstbestimmung von uns Menschen. Eine vollständige Datenschutz-Compliance bedarf der Beratung durch Experten.

Mit anderen Worten: Datenschutz kann ein Bremsklotz sein, wenn man sich damit nicht auskennt und es in Eigenregie auf „Gut Glück“ versucht. Seien wir mal ehrlich: An einen Industrieroboter lassen wir doch auch nur top ausgebildete und erfahrene Mitarbeiter. Stellen Sie sich vor, die kaufmännische Geschäftsführung würde versuchen, einen solchen zu programmieren. An allen Ecken und Enden lagern wir Unternehmensaufgaben an Spezialisten (Unternehmensberater, Werbeagenturen, Rechtsanwälte, Steuerberater) aus. Warum nicht im Datenschutz?

Bereits letztes Jahr, also nur vier Jahre nach Beginn der Datenschutz-Grundverordnung (DSGVO), habe ich bei Mandanten erlebt, wie Datenschutz zu einem echten Wettbewerbsvorteil wird: Ein Lieferant machte die weitere Zusammenarbeit mit meinem Mandanten davon abhängig, dass ein Datenschutz-Audit erfolgreich durchlaufen wird. Es wurden Fragen gestellt und am Ende eine Bewertung vorgenommen. Unterschreitet die Bewertung eine gewisse Schwelle, gibt es keine weitere Zusammenarbeit. Mein Mandant hat zum Glück bestanden.

DIGITAL FUTUREmag: Welche Empfehlungen geben Sie KMUs, um den Datenschutz effektiv durchzuführen, und warum ist die Auswahl eines kompetenten Datenschutzbeauftragten von Bedeutung?

Marc Oliver Giel: Wurde in einem Unternehmen in Sachen Datenschutz noch gar nichts gemacht, gibt es eine sogenannte Aufbau- und eine Erhaltungsphase. In der Aufbauphase dominiert die Projektarbeit. Ich empfehle meinen Mandanten kleine Arbeitspakete, die in einer bestimmten Zeit umzusetzen sind. Danach gibt es das nächste Paket. So kommt man beständig voran, ohne den Betrieb lahmzulegen. In der Erhaltungsphase sind nur noch ein bis zwei Besprechungen pro Jahr nötig. Einen guten Datenschutzberater erkennen Sie daran, dass er Ihnen in kurzer Zeit eine To-do-Liste erstellt und mit Ihnen strukturiert umsetzt. Im Übrigen achte ich darauf, meine Mandanten nicht zu überfordern. Mein Motto lautet diesbezüglich: Lieber dauert die Aufbauphase etwas länger, als dass die Geschäftsleitung nicht versteht, worum es geht und was zu tun ist.

DIGITAL FUTUREmag: Welche Rolle spielt die Einwilligung von Personen in die Verarbeitung ihrer persönlichen Daten im Kontext des Datenschutzes? Wie sollten Unternehmen sie rechtmäßig einholen und verwalten?

Marc Oliver Giel: Leider wurde die Einwilligung zur Einführung der DSGVO im Jahre 2018 häufig als Allheilmittel missbraucht. Von überall kamen Zettel auch auf

mich zu mit den Worten „Das müssen Sie jetzt wegen dem neuen Datenschutz unterschreiben“. Aus fachlicher Sicht war das leider Quatsch, denn wenn ich beispielsweise bei einem Onlinehändler etwas bestelle, werden Name und Anschrift zwingend zur Belieferung benötigt. Da ist die Einholung einer Einwilligung grober Unfug. Wenn wirklich eine Einwilligung gebraucht wird, muss sie freiwillig abgegeben werden, sie muss informiert, nachweisbar und für einen bestimmten Zweck abgegeben und sie kann jederzeit widerrufen werden. Als Beispiel einer Newsletterbestellung lassen sich alle Voraussetzungen auch für Laien nachvollziehbar darstellen: Ich abonniere den Newsletter freiwillig, ich unterliege keinem Zwang. Die verlinkte Datenschutzerklärung informiert mich über den Zweck und welche Rechte mir zustehen. Über das Newslettersystem wird meine Anmeldung protokolliert, ist also nachweisbar. Und über den Abmeldelink in jedem Newsletter kann ich jederzeit „widersprechen“, mich also abmelden.

DIGITAL FUTUREmag: Wie können Unternehmen sicherstellen, dass sie bei der Datenerhebung und -verarbeitung die Grundsätze der Datensparsamkeit und Zweckbindung einhalten, um den Datenschutz zu gewährleisten?

Marc Oliver Giel: In Kontaktformularen und Anmeldebögen empfehle ich, die Pflichtangaben mit einem * zu kennzeichnen. Dadurch weiß die betroffene Person, was zwingend nötig ist und welche Daten, etwa die Handynummer, freiwillig mitgeteilt werden. Beim Einsatz von CRM-Systemen ist die Aufgabe etwas schwieriger. Früher kannte ich es, dass der Vertrieb hier gerne umfassende private Informationen zum Geschäftspartner oder Kunden hinterlegt. Solche Profilbildungen genügen in der Regel nicht mehr der Anforderung „Datensparsamkeit“ und sind aufzulösen.

Die Zweckbindung erreiche ich häufig durch den Einsatz separater Ablagen (bei analogen Systemen) oder separater Datenbanken (bei digitaler Verarbeitung). Beispiel: Die Daten aus einem Newslettersystem (Name, E-Mailadresse) darf ich nicht einfach in mein CRM- oder ERP- System kopieren. Stellen Sie sich einen großen Schrank mit vielen kleinen Schubladen vor. Jede Schublade steht für einen „Zweck“. Wenn Sie Daten in eine Schublade hineinstecken, dürfen Sie diese nicht später herausnehmen und in eine andere Schublade umsortieren. Das wäre ein Verstoß gegen die Zweckbindung. Wenn Sie die Daten in einer anderen Schublade zwingend benötigen, müssen diese dafür „erhoben“ werden. Deshalb sind Datenschutzerklärungen heute auch so lang und teilweise kompliziert. Denn dort

sollten sich alle diese „Zwecke“ wiederfinden.

Noch ein Beispiel: Wenn Sie das Geburtsdatum Ihrer Kunden erheben, um zu prüfen, ob diese volljährig sind, stecken Sie das Geburtsdatum gleichsam in die Schublade „Altersverifikation“. Wenn Sie später Kunden am Telefon identifizieren möchten und fragen, wie ihr Geburtsdatum lautet, ist das illegal. Denn die Identifizierung ist ein anderer Zweck, also eine andere Schublade und das Geburtsdatum darf eben nicht einfach umsorrtiert werden.

DIGITAL FUTUREmag: Inwiefern hat die zunehmende Digitalisierung und der Einsatz von Technologien wie Künstliche Intelligenz (KI) und Big Data Analytics die Herausforderungen im Datenschutz verändert? Welche Maßnahmen sind erforderlich, um damit Schritt zu halten?

Marc Oliver Giel: Klar ist: Der Datenschutz hinkt der technischen Entwicklung von KI-Systemen hinterher. Auf europäischer Ebene wird gerade eine KI-Verordnung vorbereitet. Diese enthält u.a. detaillierte Regelungen für sog. „Hochrisiko-KI-Systeme“. Auf nationaler Ebene wurden ganz aktuell zwei Hilfestellungen aus datenschutzrechtlicher Sicht veröffentlicht. Der Landesbeauftragte für Datenschutz Baden-Württemberg ist Herausgeber eines 32-seitigen Diskussionspapiers „Rechtsgrundlagen im Datenschutz beim Einsatz Künstlicher Intelligenz“. Der Hamburgische Beauftragte für Datenschutz brachte eine 5-seitige Checkliste zum Einsatz LLM-basierter Chatbots heraus. In Zukunft werden wohl noch weitere Veröffentlichungen folgen. Unternehmen, die KI-Systeme in ihrem Betrieb einsetzen möchten, sind gut beraten, solche Hilfestellungen zu nutzen.

Möchten Unternehmen mal „auf die Schnelle“ KI-Systeme ausprobieren, sollten sie auf die Übermittlung personenbezogener Daten verzichten.

In der Diskussion wird von mancher Seite vorgeschlagen, die KI-Nutzung so lange auszusetzen, bis der rechtliche aber auch der ethische Rahmen nachgezogen wurde. Allerdings besteht dagegen der berechtigte Einwand, in der Zwischenzeit den technologischen Anschluss zu verlieren. Mein pragmatischer Ansatz lautet daher: Bis Spezialregelungen kommen müssen alle bestehenden DSGVO-Vorschriften beim KI-Einsatz so vollständig wie irgend möglich eingehalten werden. Dazu können ebenfalls Datenschutzbeauftragte beraten.

Das Thema Big Data ist datenschutzrechtlich schon etwas älter und daher gereifter. In den wenigsten Fällen ist der Datenschutz der „Show-Stopper“. Mit anderen Worten: Für sehr viele Anwendungsfälle gibt es praktikable Lösungen.

DIGITAL FUTUREmag: Vielen Dank für das gemeinsame Aufräumen und Reinemachen in Sachen Datenschutz. Ich glaube, wir konnten hier einiges gemeinsam klären und etwas Licht ins Dunkel bringen.



Marc Oliver Giel

KONTAKT



Firma: datamog
Straße: Lagerstraße 11a
PLZ Ort: 64807 Dieburg
Ansprechpartner: Marc Oliver Giel
Telefonnummer: +49 6071 4306 911
Email: mail@datamog.de
Web: <https://datamog.de/>

Die virtuelle Kongressmesse rund um die Digitalisierung in der öffentlichen Verwaltung

14.-15.11.2024
virtual

dikomm
zukunft digitale kommune



DER NUTZEN EINES AKT



DSC

BIETET VIELSEITIGE VO

Im Interview mit Ralf Kamnitzer,
einem sehr erfahrenen Datenschützer im Rhein-Main-Gebiet

Seit 25.05.2018, dem Einführungsdatum der neuen EU-Datenschutz-Grundverordnung (DSGVO), ist eine Menge passiert. Während viele Unternehmen mit diesem Thema noch hadern und es als die größte Wirtschaftsbremse oder Verhinderer von Innovationen ansehen, preisen andere den Datenschutz in Deutschland als die einzige richtige Lösung und Entscheidung. Die FürsprecherInnen fordern von der heimischen Wirtschaft und ihren Teilhabern, sich daran vollumfänglich zu beteiligen, sämtliche Geschäftsprozesse daraufhin zu überprüfen und den Datenschutz somit vollständig in das Unternehmen zu integrieren.

TIVEN DATENSCHUTZES

GVO

RTEILE



Um einen besseren Überblick zur Diskussion und interessierten EntscheiderInnen Handlungsempfehlungen für eine konforme Sicherung ihres betriebseigenen Know-hows zu geben, sprechen wir heute mit dem langjährigen Datenschutz-Experten Ralf Kamnitzer.

DIGITAL FUTUREmag: Herr Kamnitzer, seit der europaweiten Einführung der Datenschutz-Grundverordnung vor drei Jahren ist viel passiert. Warum ist Datenschutz überhaupt so wichtig geworden?

Ralf Kamnitzer: Das Interesse an persönlichen Informationen über das Leben und Wirken der Nachbarn ist für viele nach wie vor sehr interessant und erstrebenswert. Dies

beweisen polizeilich registrierte Straftaten-Zahlen im Umfeld von Cyberkriminalität hierzulande. Die neueste BKA-Statistik (aus 2023 für 2022) dokumentiert mit 136.865 Cyberangriffen einen weiteren Höhepunkt. Der vom Digitalverband BITKOM erstellte Wirtschaftsschutzbericht weist einen fast doppelt so hohen monetären Schaden aus gegenüber 2019, nämlich 203 Milliarden EURO.

Datenschutz ist keine neomodische Erfindung, sondern ein altes und heute noch praktiziertes Recht. Wir respektieren und halten uns an diese Rechte, ohne zu wissen, wieso und warum. Hier einige bekannte Klassiker: Der Eid des Hippokrates (Arztgeheimnis), Beichtgeheimnis (Kirche), Brief- und Postgeheimnis, teilweise noch das Bankengeheimnis. Diese gesetzlichen Datenschutznormen sind strafbewehrt. Ein Verstoß gegen diese Normen bewerten und ahnden die Gerichte unterschiedlich stark. Unser natürliches Leben wird bewusst oder unbewusst von

diesen (Verhaltens-)Regeln beeinflusst.

Am 13. Oktober 1970 trat das Hessische Datenschutzgesetz als erstes und ältestes Datenschutzgesetz der Welt für die öffentliche Verwaltung in Kraft. Darin wurde festgelegt, wie, wann und warum personenbezogene Daten verarbeitet werden. Dessen Ziel ist auch gegenwärtig noch, das Recht auf informationelle Selbstbestimmung (Urteil des BVerfG vom 15.12.1983) nicht zu verletzen.

Das spätere Bundesdatenschutzgesetz (BDSG), seit Januar 1978 aktiv, stellt die Grundlage für das aktuelle Recht, die Europäische Datenschutz-Grundverordnung von 2018 dar. Damit schuf man eine rechtliche Basis, nicht nur für die Bundesrepublik Deutschland, sondern europaweit.

DIGITAL FUTUREmag: Viele Unternehmen wissen nicht genau, wie sie den Datenschutz intern integrieren sollen. Welchen fachlichen Rat können Sie Firmen geben?

Ralf Kamnitzer: Der Datenschutz auf Basis der europäischen Datenschutz-Grundverordnung (DSGVO) gehört bei allen Unternehmen in den Bereich der Unternehmens-Compliance. Praktizierter Datenschutz ist für sämtliche Firmenverantwortliche zwingend. Heute werden die unterschiedlichsten Daten von Kunden, Mitarbeitenden, Praktikanten, Lieferanten und Dienstleistern erfasst, gespeichert und verarbeitet. Egal ob Solo-UnternehmerIn, KMU oder Konzern: Jeder ist verpflichtet, Rechenschaft abzulegen, wie er die gewonnenen bzw. überlassenen Informationen erfasst, speichert oder verarbeitet.

Damit dieser Prozess einer einheitlichen Form genügt, bietet derzeit die gesetzliche Norm (DSGVO) die notwendige Vorgabe.

Datenschutz ist kein Einmalprodukt, sondern lebt, wie alle anderen Compliance-Vorschriften, für das Unternehmen. Es gilt, die vorhandenen Arbeitsabläufe (Prozesse) Erfassen, Speichern und Verarbeiten von personenbezogenen Daten fortzuschreiben und den Realitäten anzupassen.

Entsprechend der gesetzlichen Norm müssen die einzelnen Arbeitsabläufe (Prozesse) in einer geregelten und dokumentierten Form festgehalten werden. Nachfolgend einige Beispiele: Erfassung von MitarbeiterInnen bei der Einstellung, Erfassung von Fehlzeiten, Durchführung von Weiterbildungsmaßnahmen, Umgang mit gegebenenfalls Videoüberwachung, Behandlung von Kundendaten, Geheimhaltungsverpflichtung von Mitarbeitenden und Dienstleistern.

Diese Arbeitsabläufe (Prozesse) sind überall bekannt. Nur durch die rechtliche Verpflichtung, Rechenschaft über das geschäftliche Treiben abzulegen, wird eine Dokumentation notwendig. Deshalb sollte man bei der Existenzgründung genauso viel Wert darauflegen wie bei der Erstellung des Business- oder Finanzplans. Je früher der Datenschutz mit einbezogen wird, desto leichter lässt sich die rechtliche Norm umsetzen. Die gemachte Erfahrung zeigt aber, dass langjährige MitarbeiterInnen ungern an neue Themen, wie Datenschutz im Unternehmen, heran gehen. Nach dem Motto: „Wir kennen doch unseren Laden...“.

Datenschutz verstehen mittlerweile schon viele Unternehmen als Marketing-Projekt und nutzen ihn. Denn: Viele KundInnen schauen bewusst nach, ob ein Anbieter oder Hersteller Datenschutz aktiv betreibt und vergeben entsprechend Aufträge.

DIGITAL FUTUREmag: Die Reglementierungen und Auflagen im Bereich Datenschutz sind für viele Unternehmen



eine Bürde - andere wiederum sehen die Vorteile darin.
Welchen weiteren Nutzen kann ein Unternehmen aus dem Projekt Datenschutz ziehen?

Ralf Kamnitzer: Der Nutzen eines aktiven Datenschutzes bietet vielseitige Vorteile. Die Auswirkungen sind sowohl im Innen- wie Außenverhältnis zu sehen und zu erkennen. Durch die Sensibilität der einzelnen Mitarbeitenden für diesen Aspekt lässt sich die Sicherheit im Unternehmen einerseits im Umgang untereinander und andererseits auch mit KundInnen/ Lieferanten neu definieren. Der aktive Datenschutz wird von jedem einzelnen MitarbeiterIn am Arbeitsplatz und für den Arbeitsplatz genutzt. Der aktive Datenschutz hilft, die Sicherheit in der Kommunikation und im jeweiligen Arbeitsablauf zu festigen.

Die Anwesenheit einer/eines Datenschutzbeauftragten kann hilfreich sein, um Spannungen zwischen Geschäftsführung, Belegschaft und Betriebsrat abzubauen. Die Aufgabe der Datenschutzbeauftragten besteht darin, das Unternehmen bei der Anwendung der datenschutzrechtlichen Normen zu beraten und zu unterstützen. Etwa bei der Nutzung von Internet und E-Mail-Verkehr oder der Ausgewogenheit bei der Aufgabenverteilung der Mitarbeitenden. Dabei ist nicht nur die Datenschutz-Grundverordnung zu beachten, sondern auch noch eine Vielzahl anderer Vorschriften, wie das Sozialgesetzbuch, das Grundgesetz, Abgabenordnung oder Luftverkehrsgesetz.

Die vorgeschriebene Dokumentation der einzelnen Arbeitsabläufe (Prozesse) kann dazu führen, eine Strukturveränderung sichtbar zu machen. Dadurch kann ein wirtschaftlicher Gewinn für das Unternehmen herauspringen (Kosteneinsparung). Hier sind die Datenschutzbeauftragten gleich noch UnternehmensberaterInnen. Ähnlich wie bei der Optimierung der Fertigungsprozesse in den letzten Jahrzehnten. Die gewachsenen Arbeitsabläufe werden jetzt auf den Prüfstand gestellt.

Ein weiteres großes Potenzial ergibt sich bei der Analyse der Arbeitsabläufe. Hier wird hinterfragt, wieso, weshalb und warum der Arbeitsprozess so läuft, wie er läuft. Gleichzeitig ist dadurch unter anderem zusätzlich überprüfbar, ob die Verteilung der Verantwortlichkeit der einzelnen MitarbeiterInnen noch mit der im Arbeitsvertrag beschriebenen übereinstimmt.

Ganz wichtig für das Unternehmen ist die Realisierung der Betroffenenrechte. Hier bedarf es oft, so die gemachte

Erfahrung, der Mithilfe durch die Beauftragten für den Datenschutz. Denn damit kann das Unternehmen einen positiven Eindruck hinterlassen. Ich denke in diesem Zusammenhang etwa an entsprechende Marketing-Maßnahmen.

Lassen Sie mich dies am Ende vielleicht noch kurz bemerken: Praktizierter Datenschutz und funktionierende IT-Sicherheit sind in meinen Augen integrale Bestandteile des Qualitätsmanagements. Außerdem hilft der Datenschutz bei der Optimierung der Geschäftsprozesse und ist zudem ein Schutzwall bzw. -schirm für das eigene Business. Denn abhanden gekommene Unternehmensinterna sind weder ersetzbar noch wiederzubeschaffen!

DIGITAL FUTUREmag: Vielen lieben Dank für Ihre transparenten Einblicke und Erläuterungen zu essentiellen betriebsrelevanten Security-Maßnahmen, die EntscheiderInnen dabei unterstützen, ihre geschäftlichen Ressourcen erfolversprechend zu nutzen.



Ralf Kamnitzer

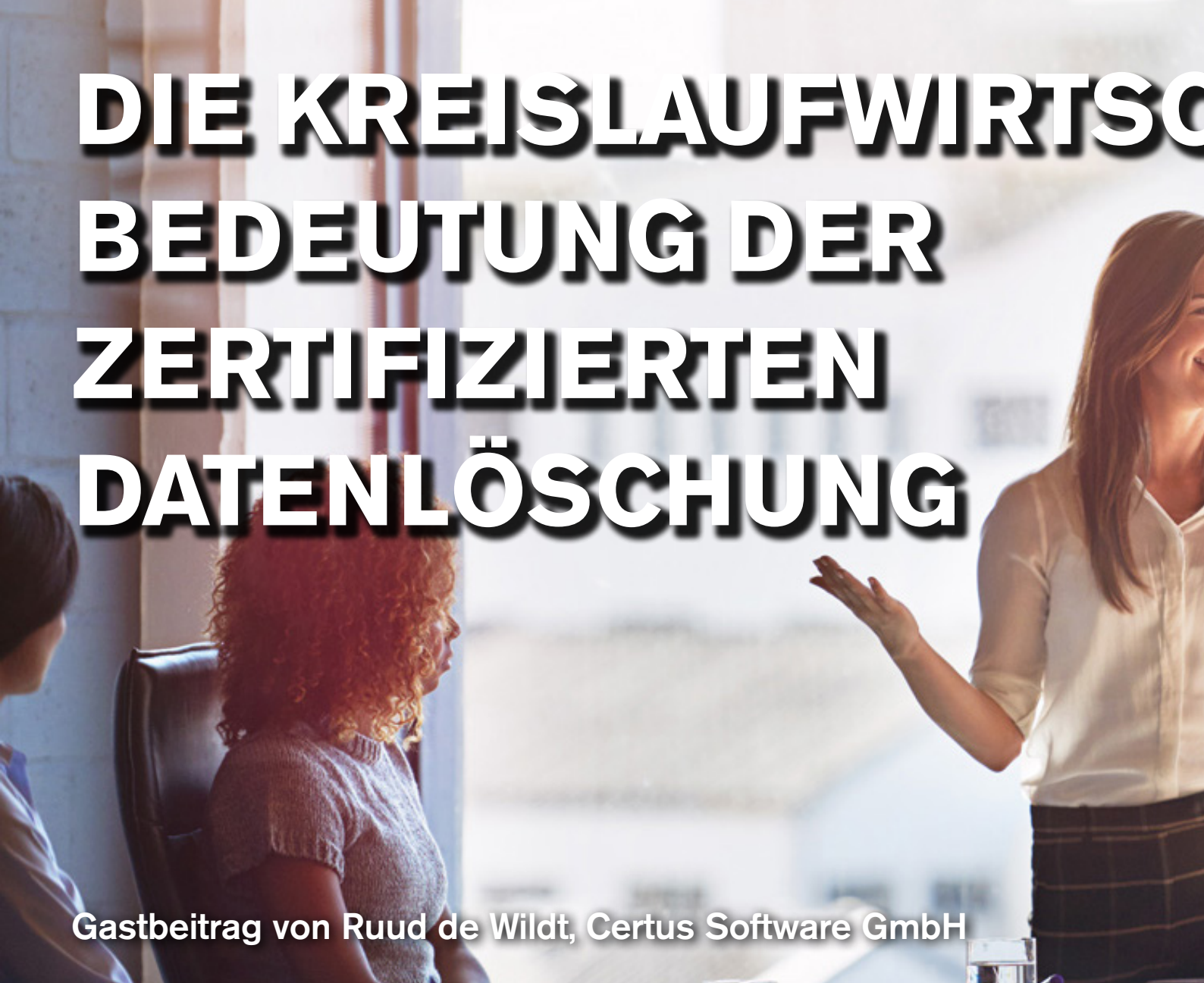
>> Bitte mit dicoo-App scannen

KONTAKT



Firma: Ralf Kamnitzer Key-Kom
Straße: Draiser Weg 4
PLZ Ort: 65346 Eltville
Ansprechpartner: Ralf Kamnitzer
Telefonnummer: +49 6123 605 681
Email: info@key-kom.de
Web: <https://www.key-kom.de>

DIE KREISLAUFWIRTSCHAFT BEDEUTUNG DER ZERTIFIZIERTEN DATENLÖSCHUNG



Gastbeitrag von Ruud de Wildt, Certus Software GmbH

Im heutigen digitalen Zeitalter kann die Bedeutung einer sicheren und vorschriftsmäßigen Datenlöschung gar nicht hoch genug eingeschätzt werden. Angesichts der zunehmenden Bedenken hinsichtlich des Datenschutzes müssen Unternehmen Maßnahmen ergreifen, um sicherzustellen, dass sensible Informationen sicher von elektronischen Geräten wie Smartphones, Tablets, Laptops, PCs, Speichersystemen, USB-Sticks, Servern usw. gelöscht werden, bevor sie die Arbeitsumgebung zur Entsorgung oder zum Recycling verlassen.

CHAFT UND DIE



Datenschutz als Teil des Kreislaufwirtschaftsprozesses für IT-Geräte

Einer der Schritte im Kreislaufprozess ist der Prozess der Rückführung von Produkten oder Materialien von ihrem endgültigen Bestimmungsort zu ihrem Ausgangspunkt aus verschiedenen Gründen, wie z.B. Rückgabe, End-of-Life, Reparatur oder Recycling. Als Teil dieses Prozesses müssen elektronische Geräte mit eingebautem Speicher sicher gelöscht werden, bevor sie die Arbeitsumgebung verlassen, um an den Verkäufer zurückgegeben, weiterverkauft oder dem Recycling zugeführt zu werden, vor allem, wenn die Datensicherheit für den Benutzer von großer Bedeutung ist, um Datenschutzverletzungen oder Verstöße gegen die Datenschutzbestimmungen zu verhindern.

Um ein Höchstmaß an Sicherheit im Kreislaufprozess zu gewährleisten, ist es wichtig, die Daten zu löschen, bevor ein Wirtschaftsgut die Arbeitsumgebung verlässt. Das bedeutet, dass der Datenlöschungsprozess an dem Ort stattfinden sollte, an dem die Geräte verwendet werden, und nicht an eine externe Einrichtung zur Löschung geschickt wird. Die wichtigsten Vorteile dieses Verfahrens sind:

Sicherheit: Das Löschen von Daten, bevor die Geräte die Arbeitsumgebung verlassen, gewährleistet, dass die Daten jederzeit unter der Kontrolle der Organisation bleiben. Dies verringert das Risiko von Datenverletzungen, die während des Transports zu oder an einem externen Standort auftreten können. Für jedes Gerät kann ein Datenlöschungszertifikat ausgestellt werden, bevor die Geräte physisch entfernt werden.

Effizienz: Die Löschung von Daten und eine eventuelle (optische und technische) Diagnose und Berichterstattung, bevor die Assets die Arbeitsumgebung verlassen, kann effizienter sein als die Löschung der Assets an einem externen Standort. Nach einer schnellen Verarbeitung in der Arbeitsumgebung können die Geräte direkt an ihren endgültigen Bestimmungsort versandt werden, wodurch die zusätzlichen Schritte für den Versand, das Be- und Entladen sowie das Ein- und Auspacken reduziert werden. Dadurch verkürzt sich die Durchlaufzeit des Logistikprozesses, was die Kundenzufriedenheit erhöht und die Kosten senkt.

Compliance: Das Löschen von Daten auf Assets, bevor diese die Arbeitsumgebung verlassen, kann Unternehmen dabei helfen, die Datenschutzbestimmungen einzuhalten. Durch die Löschung der Daten vor Ort behält das Unternehmen die 100-prozentige Kontrolle über den Datenlöschungsprozess, und die Daten werden in Übereinstimmung mit den einschlägigen Vorschriften wie NIST, GDPR usw. sicher gelöscht.

Zertifizierte Datenlöschung

Bei der Datenlöschung ist es wichtig, eine zertifizierte Datenlöschung zu verwenden, die den staatlichen Vorschriften wie DSGVO und dem Standard NIST 800-88 Revision 1 entspricht. Dadurch wird sichergestellt, dass der Löschvorgang ordnungsgemäß durchgeführt und dokumentiert wird, so dass eine dokumentierte Spur zu Prüfzwecken vorhanden ist.

Die Bezeichnung „zertifiziert“ kann auf Datenlöschsoftware angewandt werden, wenn sie einen anerkannten Zertifizierungsprozess erfolgreich durchlaufen hat und die

spezifischen Kriterien und Standards der zertifizierenden Organisation erfüllt.

Die spezifischen Anforderungen für die Zertifizierung können je nach der zertifizierenden Organisation und den von ihr befolgten Standards variieren. Zu den gängigen Zertifizierungen für Datenlöschsoftware gehören die Common Criteria-, ADISA- und NCSC-Zertifizierungen sowie die NATO-Akkreditierung, bei der Sicherheitsfunktionen bewertet werden, und Zertifizierungen im Zusammenhang mit Datenschutz und Datensicherheit, wie z. B. die von IEC oder NIST. Sobald die Software den Zertifizierungsprozess erfolgreich durchlaufen hat und eine offizielle Zertifizierung von der entsprechenden Organisation erhalten hat, kann sie als „zertifiziert“ gekennzeichnet werden, um anzuzeigen, dass sie die festgelegten Standards für die Datenlöschung erfüllt. Die Zertifizierung gibt den Anwendern die Gewissheit, dass die Software gründlich getestet und bewertet wurde, und vermittelt ein gewisses Vertrauen in ihre Wirksamkeit und Sicherheit.

Das Ergebnis ist, dass die Daten nach der sicheren Löschung nicht wiederhergestellt werden können. Als Beweis wird ein fälschungssicheres Löschzertifikat ausgestellt, das alle erforderlichen Nachweise enthält. Diese Zertifikate können verwendet werden, um die Einhaltung von Branchenvorschriften nachzuweisen und im Falle einer Prüfung oder eines Rechtsstreits als Beweis für die Sorgfaltspflicht zu dienen.

NIST-Konformität

Das National Institute of Standards and Technology (NIST) ist eine nicht-regulatorische Behörde des US-Handelsministeriums, die Normen und Richtlinien für

Digitalisierung & Transformation · Online-Marketing & Sales ·
Prozessoptimierung & Kommunikation · New Work / Recruiting ·
Cyber Security & Datensicherheit / IT-Recht

DFC

23. - 24.04.2024

**Die Online-Kongressmesse mit Strategie-
sowie Technologie-Best Practices rund um
Business-Digitalisierung**

DIGITALTM
FUTUREcongress
virtual

Der DIGITAL FUTUREcongress virtual richtet sich an Geschäftsführende und Führungskräfte deutschsprachiger mittelständischer Unternehmen.

www.virtual.digital-futurecongress.de



verschiedene Branchen entwickelt, darunter auch für die Cybersicherheit. Insbesondere hat das NIST eine Reihe von Richtlinien für die Datenlöschung entwickelt, die Anleitungen für die sichere Löschung von Daten aus elektronischen Geräten enthalten.

Nachhaltigkeit

Die zertifizierte Datenlöschung ist ein entscheidender Schritt, wenn es um die Wiederverwendung von IT-Geräten geht, da die zurückgelassenen Daten Risiken bergen. Sobald die Datenschutzbestimmungen erfüllt sind, können IT-Geräte sicher und zuverlässig wiederverwendet werden. Dies führt zu Kosteneinsparungen, reduziert den Elektroschrott, trägt zur Nachhaltigkeit bei und schont wertvolle Ressourcen.

Fazit

Die Verwendung einer zertifizierten Datenlöschung, die den staatlichen Vorschriften wie DSGVO und dem Standard NIST 800-88 Revision 1 entspricht, hat mehrere Vorteile für die Circular IT-Branche. Erstens verringert sie das Risiko von Datenschutzverletzungen und Verstößen gegen Vorschriften, die zu erheblichen finanziellen und rufschädigenden Schäden führen können. Zweitens stellt die Norm sicher, dass Unternehmen die Datenschutzbestimmungen einhalten, was das Vertrauen und die Loyalität der Kunden stärken kann. Und schließlich bietet er einen dokumentierten Nachweis des Löschvorgangs, der für Prüfungszwecke nützlich sein kann.

CERTUS LÖSCHT DATEN. DAUERHAFT.



Ruud de Wildt

>> Bitte mit dicoo-App scannen

KONTAKT



Firma: Certus Software GmbH
 Straße: Karl-Nolan-Str. 3
 PLZ und Ort: 86157 Augsburg
 Ansprechpartner: Ruud de Wildt
 Telefon: +49 821 650688 0
 Email: ruud@certus.software
 Website: <https://www.certus.software>



Bis zum 17. Dezember 2023 müssen alle Unternehmen mit mehr als 50 Mitarbeitenden (gezählt wird die Kopfzahl, nicht die Kapazität) das Gesetz zum Schutz der Hinweisgeber (Hinweisgeberschutzgesetz – HinSchG) umgesetzt haben. Viele der betroffenen Firmen sind noch mitten in der Planungsphase oder machen sich sogar jetzt erst Gedanken, wie man das sinnvoll gestalten kann. Für die Realisierung sollten sie allerdings ausreichend Zeit mitbringen.

Die einfachste Lösung ist die Nutzung eines digitalen Systems, das die gesetzlichen Anforderungen des Hinweisgeberschutzgesetzes ebenso erfüllt wie die Anforderungen an die IT-Sicherheit.

WISSELBLOWINGGESETZ FÜR DIE ZIELGERADEN:

JETZT KOMMT DAS HINWEISGEBERSCHUTZGESETZ FÜR KLEINE UNTERNEHMEN!

Ein Gastbeitrag von Astrid Meyer-Krumenacker, Rechtsanwältin

Allerdings ist es mit dem Installieren einer Softwarelösung alleine nicht getan. Die Anforderungen des Hinweisgeberschutzgesetzes sind vollständig umzusetzen, sonst drohen Bußgelder. Die Mitarbeitenden, die die Meldestelle für das Hinweisgebersystem betreuen sollen (die sogenannten „betrauten Personen“), benötigen nach § 15 Absatz 2 HinSchG einen Fachkundenachweis. Die Mitspracherechte des Betriebsrates nach § 87 Absatz 1 BetrVG sind zu berücksichtigen, oft besteht der Betriebsrat auf einer Betriebsvereinbarung.

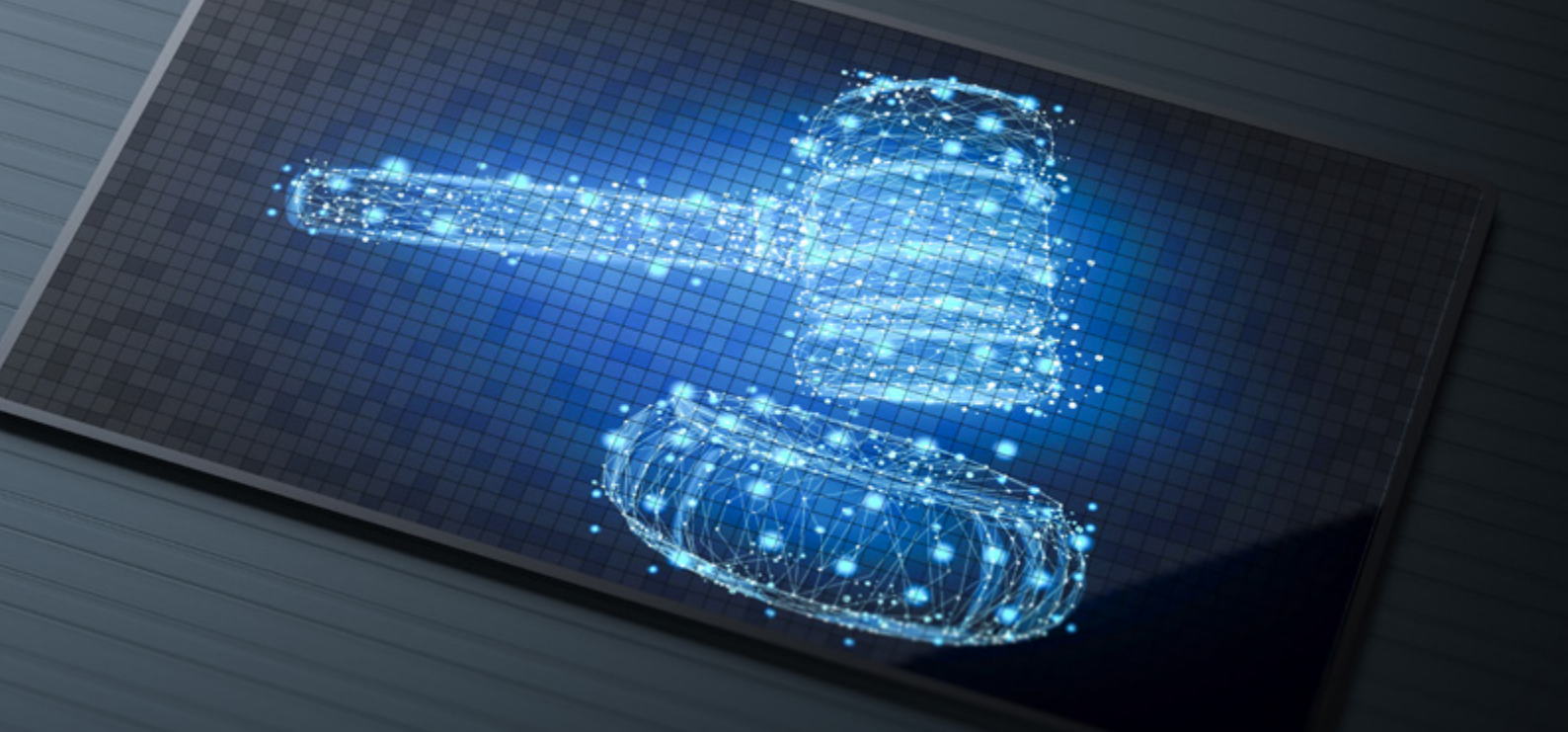
Eine sehr wichtige Rolle spielt auch der Datenschutz. DSGVO und BDSG sind bei der Einführung eines Hinweisgebersystems ebenso zu beachten wie die

Anforderungen aus dem Hinweisgeberschutzgesetz. Jede Meldung enthält personenbezogene Daten, mit denen sorgfältig umzugehen ist. Gelangen Informationen über ein angebliches Fehlverhalten an die Öffentlichkeit, kann dies gravierende Folgen für die betroffene Person haben. Deshalb sollte man zum Beispiel für ein Hinweisgebersystem eine Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO durchführen.

Zweifellos ist es mit Aufwand verbunden, ein solches System zu installieren. Lohnt sich dieser Aufwand?

Nach meiner Einschätzung ja.

Das Hinweisgebersystem markiert einen ganz wesentlichen Baustein eines Compliance Management-Systems und des betrieblichen Risikomanagements. Hat man dieses System ordentlich eingeführt und die Mitarbeitenden informiert, welches Fehlverhalten zu



melden ist – nämlich Verstöße, die strafbar sind oder bestimmte Ordnungswidrigkeiten, die dem Schutz von Leben und Gesundheit der Bürger sowie dem Schutz der Rechte von Beschäftigten dienen – stellt es ein optimales Frühwarnsystem dar. Es ist einfach angenehmer, durch eine E-Mail im digitalen System von einem Problem zu erfahren, als durch die Strafverfolgungsbehörden.

In der Regel werden Diebstähle, Betrug, Korruption und Sachbeschädigungen gemeldet. Voraussetzung ist außerdem, dass dieses Fehlverhalten einen Bezug zur beruflichen Tätigkeit hat. Diese Meldungen führen üblicherweise zu Personalmaßnahmen gegenüber denjenigen, die Fehlverhalten begangen haben. Möglicherweise erfolgen auch eine Strafanzeige und eine Klage auf Schadensersatz. Ursache für das Fehlverhalten sind aber meistens mangelhafte Prozesse und Kontrollen, manchmal auch fehlende Unterweisungen oder Schulungen.

Wer also aus einem Hinweisgebersystem den größtmöglichen Nutzen ziehen will, darf bei der Ahndung des Fehlverhaltens nicht aufhören, sondern muss weiterdenken. Insbesondere sollte man sich immer folgende Frage stellen: „Warum konnte dieses Fehlverhalten erfolgreich durchgeführt werden?“. Nach jeder Meldung sind deshalb die relevanten Prozesse zu überprüfen und gegebenenfalls zu optimieren. Vielleicht sind auch Schulungen zu einzelnen Themen notwendig, etwa wenn das Fehlverhalten ein Korruptionsfall war.

Wird das Hinweisgebersystem auf diese Weise genutzt, kann es einen erheblichen Beitrag zur Optimierung der

Managementsysteme und Verbesserung der gesamten Organisation leisten.

Ein Hinweisgebersystem wird aber nur dann erfolgreich sein, wenn die Mitarbeitenden es akzeptieren. Dazu ist es notwendig, dass sie verstehen, welches Fehlverhalten gemeldet werden soll und wie die Meldung durchzuführen ist. Außerdem müssen sie ihrem Management vertrauen, dass die Meldungen wirklich vertraulich behandelt werden. Insbesondere darf der Name des Hinweisgebenden nicht ohne Rechtsgrund die Meldestelle „verlassen“. Das bedeutendste Werkzeug zur Erreichung dieses Zieles ist die Kommunikation, wozu bei Einführung des Systems die Erstellung eines Kommunikationskonzepts absolut Sinn macht. Die Mitarbeitenden benötigen sachliche, gut verständliche Informationen zu dem Zweck und der Nutzung des Systems. Es sollte auch ausdrücklich darauf hingewiesen werden, dass Denunziantentum nicht erwünscht ist und der Denunziant auch nach dem Hinweisgeberschutzgesetz nicht geschützt wird. Ein Denunziant kann nach dem Hinweisgeberschutzgesetz sogar mit einem Bußgeld belegt werden und sich gegenüber dem Geschädigten schadensersatzpflichtig machen.

Wenn Sie das Hinweisgeberschutzgesetz umsetzen müssen, machen Sie es richtig und nutzen Sie die Potentiale eines digitalen Hinweisgebersystems für Ihr Risikomanagement und/oder Compliance Management-System. Dann wird sich der Aufwand lohnen.

Link zum Quick-Check Hinweisgebersystem:
<https://www.amk-law.de/hinweisgebersystem/>

Über die Autorin

Astrid Meyer-Krumenacker ist Rechtsanwältin in München. Sie verfügt über langjährige Managementenerfahrung in verschiedenen Funktionen, unter anderem als Abteilungsleiterin Recht und Versicherungen, Recht und Personal sowie als Compliance Officer. Für einen süddeutschen Verlag ist sie als Autorin zu dem Thema Lieferkettensorgfaltspflichtengesetz tätig.

Als erfahrene Problemlöserin unterstützt sie Mittelständler durch die Einführung von Hinweisgebersystemen, Compliance Management-Systemen und der Umsetzung der Anforderungen aus dem Lieferkettengesetz dabei, ihren unternehmerischen Erfolg zu sichern und eigene Risiken zu minimieren.

Sie bietet Online-Seminare und Workshops zu verschiedenen Aspekten aus den Bereichen Compliance, Korruptionsvermeidung, Hinweisgebersysteme und Lieferkettensorgfaltspflichten an.

www.amk-law.de



Astrid Meyer-Krumenacker

>> Bitte mit dicoo-App scannen

KONTAKT



Firma: Rechts- und Compliance - Beratung
Straße: Gottfried-Böhm-Ring 29
PLZ und Ort: 81369 München
Ansprechpartner: Astrid Meyer-Krumenacker
Telefon: +49 89-7855375
Email: astrid.meyer-krumenacker@t-online.de
Website: <https://www.amk-law.de>

1000° E-PAPER

Wandeln Sie Ihre Magazine, Kataloge und Geschäftsberichte in wenigen Schritten in ein interaktives ePaper um.



Mit Blättereffekt, interaktivem Inhaltsverzeichnis, stufenlosem Zoom und Volltextsuche.



Unterstützt Ihre Inhalte mit Videos, Bildergalerien und Links.



Optimiert für mobile Endgeräte.



Hosting auf eigenen Servern oder in unserer Cloud.



10% Rabatt
Promocode:
digitalfuture21
bis 31.12.2023

Jetzt PDF hochladen

und 30 Tage lang kostenlos testen
unter www.1000grad-epaper.de

+49 341 963 82 63

kontakt@1000grad-epaper.de



IDENT

WE

Gastbeitrag von Dipl.-Chem.oec. Stephanie Ta, Business Development

Das Thema Datenschutz ist in aller Munde, doch oft wird die Sicherheit, Pflege und die Aufbewahrung von Identitätsdaten im Internet singularär betrachtet und gehandhabt. Warum Sie jetzt mit ganzheitlichen Lösungen auf das richtige Pferd setzen, erfahren Sie in dem Impulsbeitrag von Stephanie Ta.

IDENTITÄTSDATEN IM CYBERRAUM WARUM JEDE ANWENDUNG EIN IAM BRAUCHT

ment Manager / Prokuristin, Syntlogo GmbH

Die Gründe für den geänderten Bedarf liegen teilweise viele Jahre zurück. Insgesamt kann man vier große Veränderungen ausmachen, die den notwendigen Schutz von Identitätsdaten zum festen Bestandteil von Digitalisierungsaufgaben macht:

Veränderung Nr. 1:

Die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung, kurz DSGVO, erweist EU-Bürgern mehr Rechte hinsichtlich der Erhebung, Prozessierung und Speicherung ihrer Identitätsdaten. Das in seinen Ursprüngen größtenteils auf deutscher Gesetzgebung basierende EU-Recht fordert von Unternehmen eine besondere

Sorgfaltspflicht im Umgang mit den sensiblen Daten, wenn sie im EU-Raum agieren.

Veränderung Nr. 2:

Ursprünglich verwalteten Unternehmen Identitätsdaten ihrer Mitarbeiter über die Personalabteilung. Die IT steuerte den Zugriff auf Unternehmensressourcen in internen Umgebungen. Mit der Zeit öffnete sich die Anwendungslandschaft für externe Nutzer, wie z.B. Kunden, Lieferanten oder Partner. Diese beiden Welten funktionierten fast immer unabhängig voneinander, teilweise jetzt noch. Mittlerweile kreuzen sich diese Wege, d.h. eine Anwendung soll gewappnet sein für die Mitarbeiter, aber auch zur Verwaltung externer Nutzer. Und es kamen ganz neue Fälle dazu, wie z.B. digitale Bürgerservices, Onlineservices für Organisationen oder für Verbände. Die Bedingung hier, dass solche Services überhaupt digital funktionieren, ist die Integration der Prozesse und die Anbindung über moderne Standardschnittstellen und -protokolle, wie REST API, SCIM, OpenID Connect, SAML 2, ...

Veränderung Nr. 3:

Der dritte ausschlaggebende Punkt ist der starke Anstieg der Nutzung von Cloud- und browserbasierten Anwendungen; dieser entsteht zum einen durch die Online-Nutzung innovativer Produkte und Dienstleistungen sowie durch das Outsourcen von Services, die nicht zum Kern-Know-How des Anbieters gehören. Zum anderen, wie in Punkt 2 beschrieben, die Verlagerung von Anwendungen in den öffentlich zugänglichen Internetraum, um mobiles Arbeiten oder den Zugriff für externe Nutzer schnell und leicht zu ermöglichen.

Veränderung Nr. 4:

Die Konsolidierung digital angebotener Produktportfolios für Kunden, die mit nur wenigen Klicks verschiedene Leistungen online buchen können, erbringt mittlerweile einen starken Wettbewerbsvorteil. Die dadurch entstehenden Potentiale liegen nicht nur in der Vereinfachung der Registrierung von Nutzern, sondern auch im Cross- und Up-Selling. Das ist so, weil ein Unternehmen die gesamte User-Journey damit kundenorientiert abbilden kann und so gute Chancen auf mehr Geschäft bildet. Es gibt mehrere Anwendungen, aber nur einen Nutzer mit seiner Identität.

Mitunter könnte man diese Liste munter fortführen: Veränderungen wie der breite Einsatz von Microservices, die Einbindung neuer Anwendungen von oder für Kunden oder Partnern im gesamten, digitalen Unternehmens-Ecosystem oder der Trend in der Softwarearchitektur monolithische Anwendungen aufzubrechen, führen letztendlich dazu, dass es sinnvoll ist mit einem eigenständigen System zur Identitätsverwaltung Nutzer und ihre Berechtigungen datenschutzkonform zu administrieren.

Das Bedürfnis der Nutzer nach Komfort, Sicherheit ihrer Daten und Schnelligkeit in den Interaktionsprozessen mit dem Online-Service bestimmt letztendlich, ob ein Geschäftsmodell erfolgreich ist oder ob ein Abbruch der Geschäftsverbindung angedacht wird. Im B2C-Bereich ist das besonders ausgeprägt.

Der erste Interaktionsprozess in Verbindung mit dem Beginn der Nutzung eines digitalen Angebotes oder Service ist die Registrierung.

Der Account-Life-Cycle startet mit einer Registrierung

Um den Nutzer in den Mittelpunkt zu stellen, beginnen wir mit der Idee des „Digitalen Prozesses zur Erstellung und der Pflege seiner Identitätsdaten“. Im allerersten Schritt generiert der Nutzer einen Account. Dieser Schritt beginnt mit einer Registrierung, gefolgt von dem Consent Management, worunter auch die Zustimmung zur Datenschutzerklärung und ggf. weiteren Konditionen fällt. Der nächste Schritt ist die Datenerhebung zum Zwecke der Anwendung. Daraufhin gibt es verschiedene Berechtigungen, d.h. je nach Autorisierung erlangt ein Nutzer einige wenige, andere oder sensible Zugriffsrechte, je nach seiner Rolle in dieser Anwendung. Damit ist es nicht zu Ende, denn Daten bleiben in der Regel nicht statisch, sondern durch Datenupdates entstehen Aufgaben im Bereich Housekeeping. Zu guter Letzt kann ein Nutzer laut DSGVO die Löschung seines Kontos oder die Portierung seiner Daten verlangen bis auf den Aspekt der Aufbewahrung von Daten nach steuerlichen oder rechtlichen Vorgaben.

Schneller zum Ziel mit einem konsolidierten Service

Jede Anwendung hat von Beginn an dieser User-Journey die gleichen Aufgaben, um den Nutzer zum Ziel zu leiten. Nur je nach Anwendung sind die Einzelberechtigungen von System zu System unterschiedlich und für jeden Nutzer individuell. Trotzdem macht es Sinn alle vorgelagerten Prozesse, die für jeden Service gleich sind, durch ein zentrales System, ein Identity- und Access Management-System (IAM-System) durchführen zu lassen. In diesem Zusammenhang übernimmt ein IAM-System viele Aufgaben mit gleichbleibender Sicherheit und Qualität, unabhängig davon, wie es die angeschlossene Anwendung erledigen würde:

- Darstellung aller vertraglichen Konditionen sowie des Datenschutzes und Einholung der initialen Zustimmung dafür
- Authentifizierung, d.h. Prüfung der digitalen Anmeldeberechtigung
- Erweiterte Authentifizierung, wie adaptiv, mit Multifaktor, passwortlos, über Identity Provider, Social Logins, ...



Um den Nutzer in den Mittelpunkt zu stellen, beginnen wir mit der Idee des „Digitalen Prozesses zur Erstellung und der Pflege seiner Identitätsdaten“.

- Monitoring von Logs (Login-Versuche, Änderungen an Berechtigungen, ...)
- Abfrage notwendiger Nutzerdaten und Synchronisierung aller Daten mit den angeschlossenen und dafür relevanten Systemen
- Autorisierung, d.h. Abfrage, Prüfung, Vergabe/Entzug und Auditierung der Berechtigungen eines Nutzers
- Einholung der Zustimmung zu veränderten Vertrags- oder Datenschutzbestimmungen ...

Diese und viele weitere Aufgaben übernimmt ein IAM-System für alle angeschlossenen Anwendungen, auch als zentrale Stelle für den Datenschutz aller Nutzer. Liefere das nicht über eine Zentrale, so würde man mit Datensilos arbeiten, die nicht mehr datenschutzkonform sind. Und wer möchte heute noch das Rad neu erfinden?

Die zentrale Datenschutzstelle – eine wichtige IAM-Aufgabe

Applikationen sind manchmal gezwungen persönliche Daten lokal zu speichern, z.B. Kontodaten; wenn ein Benutzerkonto gelöscht wird, müssen auch alle diese Daten gelöscht werden. Ein IAM-System fungiert hier als Drehscheibe zwischen dem Nutzer und den angeschlossenen Anwendungen, indem es sie informiert, dass sie diese Nutzerdaten löschen oder archivieren sollen, entsprechend

den gesetzlichen Vorgaben.

Ungelöschte Accounts stellen eine Cybergefahr dar

Ein Betreiber soll die Daten seiner Nutzer nicht länger speichern als notwendig. Dieser Teil des Minimalprinzips ist Bestandteil der DSGVO. Werden Benutzerkonten nicht rechtzeitig gelöscht, man spricht von „Orphaned Accounts“, so besteht die Gefahr der Account-Übernahme und eines Datenverlusts oder -diebstahls. Ein IAM-System ist hier der Aufpasser, denn bei nicht-genutzten Konten prüft es nach einer bestimmten Zeit, wie lange der Nutzer nicht mehr aktiv war. Und kann über seine Mail-Engine Hinweis-E-Mails versenden, dass der Account bald gelöscht wird, falls der Nutzer weiterhin passiv bleibt.

Data Breach Protection – Datenschutz auf höchster Ebene

Bei besonders schützenswerten Daten sind Betreiber von Onlineservices dazu verpflichtet die Änderungen an den Daten in einem Audit Log zu dokumentieren bzw. diese zu monitoren. Der ganze Aufwand wird unternommen, damit niemand Unberechtigtes auf diese Daten zugreifen und sie manipulieren kann.

Datenschutz-Pflichten - nicht immer einfach umsetzen

Aus Sicht des Betreibers oder Owners der Anwendungen sind das alles Pflichten oder notwendige Bedingungen, die er erfüllen sollte, um nicht nur im Datenschutz alles richtig zu machen. Sondern damit begibt er sich gleichzeitig in die Lage die Abwicklung von Prozessen für alle Nutzer schneller zu gestalten. Und erarbeitet sich dadurch einen Wettbewerbsvorteil.

Grundsätzlich sind GDPR-Anforderungen für Betreiber von Online-Services komplex. Zudem sind große Investitionen notwendig, um die entsprechende Compliance zu gewährleisten. Daher macht es Sinn den Online-Datenschutz für die gesamte Organisation zentralisiert bereitzustellen. Schön ist, dass zwei Vorteile als Nebeneffekt dabei herauspringen:

1. Die Reduktion der Kosten für die Implementierung neuer Anwendungen und ...
2. der komfortable Umgang für die Benutzer, der meist zu höheren Conversion Rates führt

Das ist der aktuelle Stand, wie Sie Datenschutz mit Hilfe von Identity & Access Management erfolgreich umsetzen können.

In den nächsten Jahren gelten neue Cyberregeln, auch beim Datenschutz

Einen wissenswerten Ausblick auf die Regulatorik in den nächsten Jahren, u.a. zum Thema Datenschutz konnte ich bei einem Meetup Cybersecurity in Stuttgart gewinnen. Dort referierten die beiden Rechtsanwälte Frau Münch und Dr. Klinger zum Umgang mit den neuen Cyber-Regeln. So sieht z.B. das NIS 2-Umsetzungs-Gesetz eine persönliche Haftung der Geschäftsführer und entsprechende Sanktionen vor, wenn Hacker sensible Daten durch einen Cybervorfall entwendet haben oder es durch einen Cyberangriff zu einem Datenverlust gekommen ist. Der Entwurf des neuen Cyber Resilience Act verpflichtet alle Hersteller und Inverkehrbringer von Produkten mit digitalen Elementen in der EU neben einer CE-Kennzeichnung zu bestimmten Maßnahmen hinsichtlich der Cybersicherheit, wie z.B. die Sicherstellung der Vertraulichkeit von Daten durch Verschlüsselung oder Datenminimierung. Softwareproduzenten sind bald im Bereich der Produkthaftung durch die Product Liability Directive betroffen. Diese und einiges mehr an Regularien werden auf den europäischen Markt niederprasseln, um die Rechte von Verbrauchern und geschädigten Unternehmen zu verbessern. Insbesondere der Entwurf zum AI Act und der AI Liability Directive neben einer neuen Maschinenverordnung – alles mit Bezug auf die Cybersicherheit, werden aktuell heiß diskutiert und für Unruhe sorgen.

Da ist es doch gut, wenn man jetzt seine Schäfchen, gemeint sind natürlich sensible Identitätsdaten, ins Trockene bringt und sich keiner Schwachstelle oder Inkonsistenz im Datenschutz aussetzt.



Stephanie Ta

>> Bitte mit DICOO-App scannen

KONTAKT



Firma: Syntlogo GmbH
Straße: Kurze Gasse 2
PLZ und Ort: 71063 Sindelfingen
Ansprechpartner: Stephanie Ta
Telefon: +49 6841 81 81 089
Email: stephanie.ta@syntlogo.de
Website: www.syntlogo.de

Weitere Infos zu IAM & DSGVO auf:
<https://login-master.com/dsgvo>

Quellen:

<https://www.e-recht24.de/dsg/12706-nutzerregistrierung.html>

„Um sich im Web für Dienste oder Portale anzumelden, müssen User in der Regel eine Nutzerregistrierung vornehmen. Das kann in der Praxis die Anmeldung für einen Onlineshop, ein Forum oder ein Dienstleistungsportal sein.“

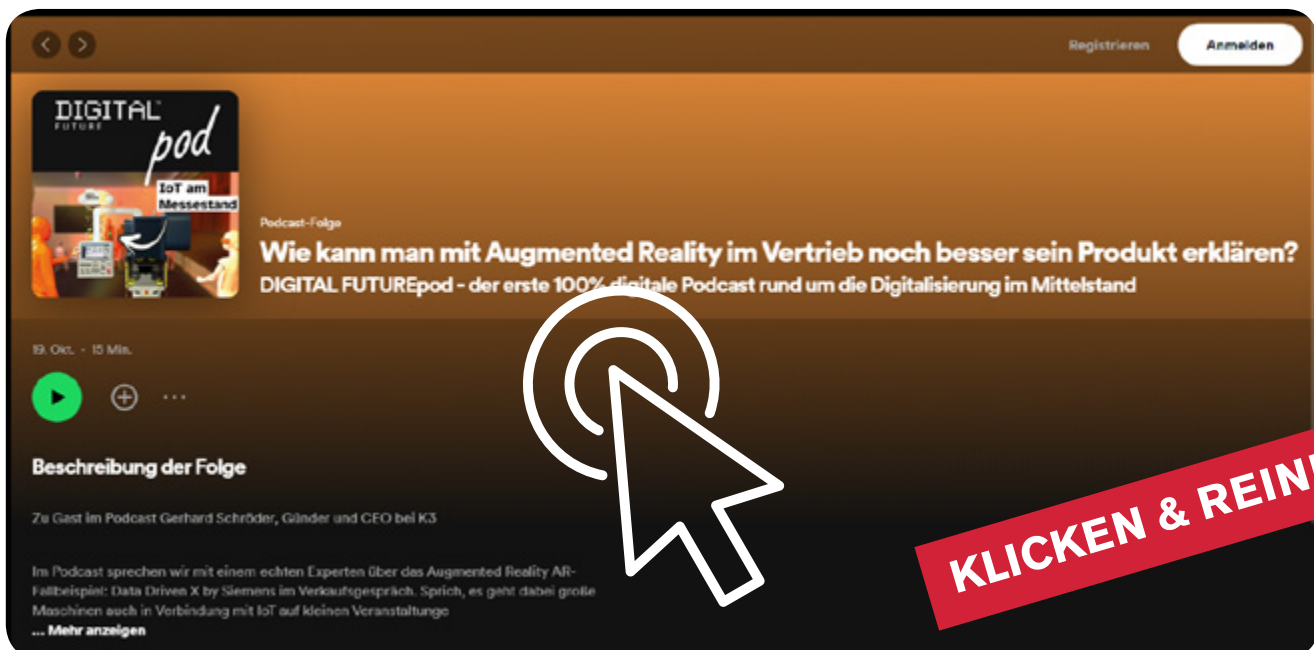
Meetup Cybersecurity Stuttgart am 20.11.2023 bei HEUKING KÜHN
LÜER WOJTEK
www.heuking.de

Erfahren Sie Neues aus der DIGITAL FUTUREworld! Jetzt Podcast anhören.

... für die umfassende, praxisnahe Digitalisierung in
Mittelstand und Großunternehmen

In regelmäßigen Abständen veröffentlichen wir ein
Interview mit Ihnen, einen aktuellen Bericht Ihres
Unternehmens oder Neuigkeiten rund um Ihre
Erfolgsgeschichten mit Best Practice-Beispielen.

Jetzt mehr erfahren



KLICKEN & REINHÖREN

Die europäische virtuelle
IT-Tech-Conference
powered by Silicon-Valley-Europe.com

 **provide-
tech.eu**
european virtual tech conference

03.-04.07.2024



www.provide-tech.eu

DIE NEUEN MEDIADATEN

**2024
SIND DA**



>> Bitte mit dicoo-App scannen

KONTAKT



AMC MEDIA NETWORK GmbH & Co. KG
Otto-Hesse-Straße 19 - T9
64293 Darmstadt
Michael Mattis
+49 6151 - 957577 -0
michael.mattis@amc-media-network.de
www.amc-media-network.de

DON'T MISS ME

DIGITAL
FUTURE
mag



KONTAKT



NEXT TIME!

DOKUMENTENMANAGEMENT