ARS Akademie

WISSEN MACHT ERFOLG

Themen-Special
Digitalisierung &
Cyber Security

Digitale Revolution als Innovationsmotor für Unternehmen

KI, AUTOMATISIERUNG, BIG DATA

BEREIT FÜR DIE DIGITALE REVOLUTION

Digitalisierung – ein Megatrend unserer Zeit. Vor allem in den letzten Jahren erfuhren viele Unternehmen einen „Crashkurs" in Sachen Digitalisierung. Home Office, virtuelle Kommunikation, hybride Meetings – was noch in weiter Ferne schien, ist jetzt Realität und in vielen Firmen Standard. Damit aus Digitalisierung eine digitale Revolution und damit ein Innovationsmotor wird, braucht es mehr. Automatisierte Produktions- & Geschäftsprozesse, digitale HR-Prozesse und die Erschließung neuer Geschäftsfelder sind nur der Anfang.

Der schmale Grat zwischen Chance und Risiko

Digitalisierung bringt zahlreiche Möglichkeiten mit sich und bietet für Unternehmen neue Lösungen im Umgang mit Kunden oder Produkten. Gleichzeitig werden die Wirtschaft und unsere Gesellschaft dadurch auch mit neuen Cyberbedrohungen und IT-Angriffsmaschen konfrontiert. Die Anzahl und die Komplexität von Cyberangriffen nimmt aktuell weltweit zu und wird durch den technischen Fortschritt in den nächsten Jahren eine noch größere Angriffsfläche bieten. Kurz: Eine erfolgreiche Digitalisierung ist eng mit der digitalen Sicherheit verbunden und das in Kombination mit der DSGVO-Konformität.

Cybersicherheit
Schneller als der Angreifer

Digitalisierung
Auf in eine neue Ära

Datenschutz
DSGVO-konform agieren

Beiträge, Checklisten & Seminare: Wir zeigen Ihnen, wie Sie aufstrebende Technologien sicher und effizient nutzen. Von strategischen Überlegungen, der technischen Umsetzung bis hin zum Monitoring und der Analyse: Unser Kursprogramm ebnet Ihnen den Weg in eine digitale Zukunft.

Wir freuen uns, Sie bald persönlich bei uns zu begrüßen.

Richard Melbinger, Geschäftsführer

Impressum: ARS Akademie, Seminar- und Kongress Veranstaltungs GmbH, Schallautzerstraße 4, 1010 Wien. Änderungen, Irrtümer, Satz- und Druckfehler vorbehalten. Es gelten die AGB der ARS Akademie: ars.at/agb. Aus Gründen der leichteren Lesbarkeit wird auf geschlechtsspezifische Formulierungen verzichtet. Imagefotos: © iStockphoto, Porträt Becker: © Schedl

Cyber Security: Schneller als der Angreifer

Digital unterwegs und trotzdem gut geschützt – ein Ziel vieler Unternehmen. Klingt für Sie unerreichbar? Mit der passenden Abwehrstrategie ist das kein Problem. Wir zeigen Ihnen, wie Sie Ihr Unternehmen vor Cyber-Angriffen schützen, Gefahren aus dem Netz erkennen und rechtzeitig die richtigen Maßnahmen setzen.

Grundlagen der IT-Security

31024

- Treffen Sie die richtigen Vorkehrungen für aktuelle Bedrohungsszenarien.
- Erfahren Sie alles zu Authentifikationsmethoden und sicheren Passwörtern.
- Besprechen Sie Aktuelles zu Tracking- und Funk-Technologien.

Cybercrime im Unternehmen

33116

- Minimieren Sie das Risiko für Cyberattacken im Unternehmen.
- Implementieren Sie effiziente Präventionsmaßnahmen.
- Besprechen Sie, wie Sie mit Lösegeldforderungen richtig umgehen.

IT-Recht in der Praxis

22184

- Erfahren Sie, wie Sie mit IT-Risiken rechtlich sicher umgehen.
- Sichern Sie sich aktuelles Know-how zu Outsourcing und Cloud Computing.
- Lernen Sie aus praktischen Use Cases der IT-Praxis.

Cyber- und Betrugsversicherung

21420

- Erfahren Sie, welche Sicherheitsmaßnahmen Ihr Unternehmen treffen sollte.
- Lernen Sie Versicherungslösungen zur Absicherung des Restrisikos kennen.
- Klären Sie, was die Vertrauensschadenversicherung als passende Ergänzung bietet.

Angriff ist die beste Verteidigung

Ihr Wissen wird zum Schutzschild.
Investieren Sie in ein IT-Training und wehren Sie Cyberbedrohungen ab.

ars.at/cybersecurity

CYBERCRIME: NEUE MASCHEN – ALTE FEHLER

Risikofaktoren im Unternehmen abwehren

Die Angriffsszenarien von Cyberkriminellen werden immer kreativer. Wir haben mit dem Datenschutzexperten Univ.-Lekt. Nicolas Nagel, LL.M., CIPP/E, CIPM, CIPT, FIP, CDPO, CIPP/C, CIPP/US gesprochen, wie sich das Bild von Cybercrime in den letzten Jahren geändert hat und mit welchen Strategien sich Unternehmen bestmöglich absichern.

Die Fälle häufen sich – auch in Österreich. Laut Bundeskriminalamt wurden hierzulande im vergangenen Jahr rund 46.100 Fälle von Cybercrime angezeigt. Die Dunkelziffer ist vermutlich höher. Oft wird Lösegeldforderungen nachgegeben, um gestohlene Daten zurückzubekommen, die sich später als Betrugsmasche entpuppen. Die Täter sind auf und davon, aber gesehen hat man sie ja sowieso nie. Einst und heute gegenübergestellt, hat sich die Welt der Cyberkriminalität stark gewandelt.

Waren es früher einzelne Personen, stecken heute global agierende Organisationen dahinter.

Langsame Internetverbindungen und eingeschränkte technische Möglichkeiten haben Cyberkriminalität vor 20 Jahren vielleicht noch erschwert. Heute hingegen sind den kriminellen Machenschaften aufgrund von KI und Krypto Assets kaum noch Grenzen gesetzt. Während Phishing Mails früher leicht zu erkennen waren, erscheinen sie heute so wahrheitsgetreu, dass ein falscher Klick schnell getan ist. Die Risikofaktoren stiegen täglich – auf allen Seiten. Ins Hacker-Visier rücken neben Privatpersonen immer mehr Unternehmen und Behörden, selbst vor Krankenhäusern und Vereinen machen die Täter nicht Halt. Tendenz weiter steigend. Diebstahl, Erpressung, Sabotage, Aktivismus oder Spionage – die Motive sind verschieden. So unterschiedlich die Beweggründe auch sind, so sind auch die Mittel und Wege, die dafür eingesetzt werden. Häufig kombinieren Täter auch Angriffsmuster miteinander, um möglichst schnell, effektiv und breit Schaden anzurichten. Ein unachtsamer Moment, ein falscher Klick und man tappt in die Falle: Die eigene Website ist nicht mehr erreichbar, Firmendaten wer-

den abgesaugt, der Online-Shop ist gesperrt, Social-Media-Kanäle werden mit Falschinformationen gefüttert oder ganze IT-Infrastrukturen lahmgelegt. Unser Datenschutzexperte und Spezialist zum Thema Cybercrime – Nicolas Nagel – sieht es am Wichtigsten in diesem Zusammenhang, sich nie zu sicher zu fühlen. „Heute stellt sich weniger die Frage, ob, sondern wann man zum Angriffsziel eines Hackers wird", fasst es der Experte kurz zusammen. Aus seiner Praxis weiß er, dass Kriminelle vor allem lukrative, mittelständische Unternehmen, die nicht aus der IT-Branche stammen, bevorzugen sowie schnell wachsende Firmen mit großen Mengen an Daten, aber auch Kleinstunternehmen, deren Fokus nicht auf Datensicherheit liegt. Warum? Diese sogenannten „low hanging fruits" bieten die Aussicht auf „schnelles Geld" bzw. massenweise Daten. Schwachstellen sieht er großteils in der fehlenden Außensicht der Unternehmen auf ihre eigene IT-Infrastruktur und damit einhergehende Risiken. Regelmäßige Penetrationstests bzw. externe Überprüfungen können nach seinen Erfahrungen hier eine Abhilfe bieten und Cybercrime abwehren.

Durch den rasanten technischen Fortschritt verändern sich auch die Tatwerkzeuge der Hacker. Ihre Wege sind schwer nachzuverfolgen. Durchschnittlich führt nur jede dritte Anzeige zu einer Aufklärung. Kurz: Ermittlungen laufen oft ins Leere. Nicolas Nagel beobachtet schon länger, dass Cyberkriminelle in ersten Ansätzen KI-basierte Technologien nutzen, um intelligente Malware zu entwickeln. Dabei sieht er für Unternehmen vor allem in der mit Hilfe von künstlicher Intelligenz erstellten polymorphen Schadsoftware potenzielle Gefahr. Diese Software kann den Code und die Angriffsmuster automatisch verändern und sich so bis zur Unkenntlichkeit tarnen. Deepfakes für die Stimmen- und Videokopie (z. B. der CEOs) sind bereits in der „Erprobung" und werden laut Nicolas Nagel auch in Zukunft weiterentwickelt und verstärkt auftreten.

Sie sehen, der Ideenvielfalt von Cyberkriminellen sind keine Grenzen gesetzt und die Vorgehensweisen werden in Zukunft noch gefinkelter. Hack-Roboter, die das Netz nach instabilen Systemen durchsuchen und selbstständig angreifen. Deepfakes, die eine Täuschung durch manipulierte Bild-, Ton- und Videoaufnahmen mit Hilfe von künstlicher Intelligenz einfacher machen. Gefälschte QR-Codes, die mit dem „Vertrauens-Trick" in Umlauf gebracht werden. Kurz, die Technik macht leider vieles möglich. Der Grundsatz: Awareness Know-how ist die beste Verteidigung. Führungskräfte von heute sind gefordert, Cyberrisiken richtig einzuschätzen und Mitarbeiter für IT-Risiken zu sensibilisieren. Die Prävention von Nutzerverschulden bei IT-Problemen sowie die Absicherung der Geschäftsprozesse durch umfassende Datensicherheit – das Bewusstsein für IT-Sicherheit wird in Zukunft noch stärker in den Mittelpunkt rücken.

Weiterbildung und speziell Awareness-Seminare bieten dafür die optimale Grundlage und sind ein wichtiger Bestandteil der IT-Sicherheitsstrategie eines Unternehmens.

> **Mittelfristig werden Quantencomputer die heutigen sicheren Verschlüsselungsalgorithmen gefährden und aller Voraussicht nach knacken.**
>
> *Nicolas Nagel*

In seinen zahlreichen Kursen teilt Nicolas Nagel seine Schulungsinhalte in die konkrete Wissensvermittlung und in spezielle Awareness-Sessions, welche auf ein bestimmtes Thema oder Entwicklungen aufmerksam machen. Eine klare Schulungsstruktur, abgestimmt auf die jeweilige Mitarbeiterrolle sieht er dabei als Erfolgsfaktor. Er selbst greift in seinen Kursen immer aktuelle Fälle aus dem Alltag auf, zeigt aber auch Klassiker: Wie man ein Passwort „knackt" und wie einfach dies eigentlich ist, wenn es die klassischen Fehler beinhaltet, oder wie man am Telefon sensible Daten erlangt, Stichwort „Phishing". Am Schluss bleibt uns nur zu sagen: Entscheiden Sie selbst, ob Ihre Mitarbeitenden eine IT-Sicherheitslücke sind oder als Verteidigungszentrum für Ihr Unternehmen agieren.

SEMINARTIPPS

Grundlagen der IT-Security	**31024**
Software – rechtliche Praxis	**10462**
Workshop: Alltagsfälle im Datenschutz üben & lösen	**31100**
Datenschutz Praxisseminar	**20807**

Digitalisierung: Auf in eine neue Ära

Was für viele Unternehmen vor einigen Jahren noch in weiter Ferne schien, ist jetzt Standard. Wie steht es um ihre digitale Transformation? Digitalisierung im HR-Management, in der Dokumentation, im Rechnungswesen oder im Projektmanagement: Die Möglichkeiten sind unendlich, um das volle Potenzial der digitalen Welt für sich zu entdecken.

Künstliche Intelligenz: Essentials & Use Cases — 332117

KI ist mehr als ein Trend. KI ist die Zukunft. Sie wird unseren Berufsalltag prägen und wandeln. Sie ist in aller Munde und der treibende Motor hinter Innovationen in verschiedenen Branchen und Bereichen. Durch den Einsatz von KI-Technologien und -Ansätzen entstehen Potenziale. Für Unternehmen und Organisationen heißt das: Prozesse verbessern, neue Produkte und Dienstleistungen entwickeln und die Marktposition stärken. Dieses Seminar verschafft Ihnen einen theoretisch fundierten, aber vor allem auch praxisbezogenen Überblick zum Thema KI. Wir zeigen Ihnen, wie Sie bereits jetzt nach erfolgsversprechenden KI Use Cases suchen, die Ihnen den entscheidenden Wettbewerbsvorteil verschaffen.

DIGITALES KNOW-HOW ERWEITERN

Grundlagen der Telemedizin — 332111

Der Kontakt zwischen Arzt und Patient erfolgt immer öfter via Telefon oder Videocall. Das erscheint auf den ersten Blick mühelos, wirft aber rechtliche Fragen auf. Informieren Sie sich über die Rechtslage.

ESG-Daten Digitalisierung — 33182

ESG ist in aller Munde. Die Verfügbarkeit von verlässlichen ESG-Daten ist wichtig, um regulatorische Verpflichtungen zu erfüllen und die Chancen der Transformationsprozesse zu nutzen.

Basiswissen Digital Marketing — 30063

Touchpoints zu Kunden verlagern sich immer mehr in den digitalen Raum und verändern die Art, wie wir werben. Machen Sie sich mit den wichtigsten Tools und Konzepten vom Online Marketing vertraut.

DIGITALISIERUNG IST EIN HANDWERK

Dafür braucht es Visionen, Strategien & Fachkräfte

Digitalisieren oder nicht digitalisieren, das ist hier die Frage – und an dieser Frage scheitert es oft schon zu Beginn. Unternehmen kämpfen nicht nur mit der richtigen Definition und oft fehlender Strategie, sondern auch mit fehlenden Fachkräften. Christoph Becker, Geschäftsführer der ETC, gibt Anregungen zur Digitalisierung und wie man IT-Know-how aufbauen kann.

Woran fehlt es Ihrer Meinung nach bei der Digitalisierung? Es fehlt am Grundverständnis, was ist Digitalisierung und was nicht. Automatisierung von Arbeits- und Produktions-Prozessen kann sich mittlerweile jeder vorstellen. Aber ab wann spricht man von Digitalisierung? Bei der Digitalisierung helfen Daten und Algorithmen, Prozesse oder auch ganze Geschäftsmodelle zu verbessen. Aus meiner Sicht besteht die Gefahr, dass wir oft in der Phase der Automatisierung stecken bleiben.

Wie sollte man Digitalisierung angehen? Derzeit treibt die Digitalisierung entweder der CIO/CEO oder auch Covid. Jetzt ist es meiner Meinung nach an der Zeit, sich nicht von externen Faktoren treiben zu lassen, sondern aktiv das Steuer in die Hand zu nehmen. Digitalisierungsprojekte müssen Teil der Unternehmensstrategie sein und den damit verbundenen Stellenwert bekommen. Dabei sollte man sich zuerst fragen: Was haben wir im Unternehmen schon digitalisiert – es wird mehr sein als gedacht. Diese Erfahrungen können dann genutzt werden, um ein Minimum Viable Product – also einen ersten lauffähigen Prototypen – zu erstellen.

Welchen weiteren Aspekt sollte man berücksichtigen? Nicht nur in die Vergangenheit zu schauen, sondern auch den Blick in die Zukunft zu werfen. Wo liegen die Trends in der Branche? Wie könnte sich mein Geschäft weiterentwickeln? Wo könnte die Digitalisierung dabei hilfreich sein? Verbindet man die Vergangenheit (was habe ich bereits digitalisiert) mit der Zukunft, dann ist man fit für größere Themenstellungen.

Für die Digitalisierung braucht es auch Fachkräfte: Wie viele IT-Kräfte fehlen derzeit in Österreich? In der IT fehlen aktuell rd. 24.000 Fachkräfte. Dieser Mangel ist die größte Hürde bei der Digitalisierung. Bereits 39 % der Unternehmen haben dadurch Umsatzeinbußen. Mittlerweile ist jeder Job ein digitaler Job, setzt also in irgendeiner Form digitale Grundkompetenzen voraus. Das DSB (digital skills barometer) von fit4internet weist für die Gesamtbevölkerung aber nur eine digitale Fitness von 41,6 % aus.

In welchen IT-Bereichen spürt man diesen FK-Mangel besonders? Der IT-Fachkräftemangel betrifft alle Wirtschaftszweige. Seit einigen Jahren sind mehr ITler in non IT-Unternehmen angestellt als in IT-Unternehmen. So hat jedes zweite Unternehmen in Österreich eigene IT-Mitarbeiter*innen. Die IT-Kompetenz fehlt also an allen Ecken und Enden.

Was können Unternehmen proaktiv gegen den FK-Mangel tun? Die aspire Education hat ein 2-Phasen-Modell entwickelt, um a) die Skills zu erheben und b) Wissen aufzubauen. In Phase 1, dem Job Screening, werden IT-Fähigkeiten gecheckt und mit dem DigCERT von fit4internet zertifiziert. Danach werden Weiterbildungen und Jobrollen empfohlen. Nun wissen die Firmen, was der Status quo ist und in welche (potenzielle) Mitarbeiter*innen man investieren kann. Die Phase 2, das Job-Matching, funktioniert wie eine Dating-Plattform: Bewerber*innen und Unternehmen finden anhand ihrer Merkmale zusammen und wenn notwendig, kann anschließend der Skills-Gap für die geforderte Jobrolle geschlossen werden.

Mehr dazu finden Sie auf **aspire-education.com**

CHRISTOPH BECKER ist seit 1995 EDV-Trainer in der Erwachsenenbildung und seither in unterschiedlichen Management-Positionen tätig. Seit 2014 ist er Geschäftsführer bei **ETC – Enterprise Training Center GmbH.**

Im aspire Education Management-Team, dem größten privaten Bildungsanbieter im DACH Raum, hat er seit 2019 die Querschnittsverantwortung für Learning Services und Cross-Selling.

DIGITALISIERUNG IM HUMAN RESSOURCE

Datenschutz im Arbeitsverhältnis — 10011

- Verarbeiten Sie Arbeitnehmerdaten DSGVO-konform.
- Erheben & verwahren Sie Daten von Bewerbern rechtssicher.
- Lernen Sie die Rolle des Betriebsrates und seine Befugnisse kennen.

Employer Branding in Zeiten des „War for Talents“ — 33104

- Verstehen Sie den strategischen Prozess hinter Employer Branding.
- Positionieren Sie Ihr Unternehmen als attraktiven Arbeitgeber.
- Lernen Sie Social Media als Instrument des Employer Brandings kennen.

Tagung Personalverrechnung & Digitalisierung — 11746

- Besprechen Sie die Automatisierungs-Trends in der Lohnverrechnung.
- Holen Sie sich wertvolle Tipps für den Digitalisierungsprozess.
- Erfahren Sie, wie Sie neue Mitarbeiter trotz Fachkräftemangel gewinnen.

DIGITALISIERUNG IM BANKING & FINANCE

Digital Operational Resilience Act — 332197

- Verstehen Sie die Anforderungen an die digitale Betriebsstabilität.
- Klären Sie den regulatorischen Rahmen & die Hintergründe von DORA.
- Erfahren Sie mehr zu Anwendungsbereichen & Regelungsinhalten.

Regulierung von Krypto-Assets — 31107

- Diskutieren Sie den schmalen Grat zwischen Ökonomie und Ökologie.
- Erhalten Sie eine Einführung in die Blockchain-Technologie.
- Besprechen Sie die Grundzüge der EU-Verordnung zu Krypto-Assets.

Digital Accounting — 22168

- Optimieren Sie Rechnungswesen mit digitalen Technologien & Tools.
- Sichern Sie sich einen detaillierten Überblick über die Digitalisierung im Rechnungswesen.
- Besprechen Sie die Trends bis 2025: Blockchain und Artificial Intelligence (AI).

Digitales Controlling, Big Data & Business Intelligenc — 21518

- Erfahren Sie, wie Sie digitale Werkzeuge im Controlling sicher integrieren.
- Lernen Sie einfache Tools für Planung, Analyse und Reporting kennen.
- Diskutieren Sie, wie Sie im Controlling die Potenziale von Big Data ausschöpfen.

Datenschutz: DSGVO-konform agieren

Qualitativ hochwertige Daten sind das A und O jeder erfolgreichen Verkaufstätigkeit. Aber während Sie Daten anreichern, werden auch die Anforderungen an die rechtskonforme Verarbeitung und Ablage immer größer. Kurz: Der Grat zwischen Daten und Schutz ist schmal. Um das zu vereinbaren, ist ein solides Grundwissen im Bereich Datenschutzrecht gefragt.

Ausbildung zum Datenschutzbeauftragten

10013

Die Aufgaben des Datenschutzbeauftragten sind vielseitig. Neben der Beratung und Überwachung von datenschutzrechtlichen Vorgaben erfordert es auch an sozialer Kompetenz, um Mitarbeiter zu schulen und nachhaltig zu sensibilisieren. In 6 Tagen vermitteln Ihnen unsere langjährigen Datenschutz-Experten die aktuellsten gesetzlichen Rahmenbedingungen zur EU-Datenschutz-Grundverordnung (DSGVO) und dem Datenschutzrecht in Österreich. Sie erfahren, welche Vorkehrungen aus Sicht des Marketings und des HR-Bereichs getroffen werden müssen und was organisatorisch zu beachten ist, um datenschutzkonform agieren zu können. Tipps und Tricks aus der Praxis erleichtern Ihnen die anschließende Umsetzung in Ihrem Unternehmen.

CERTIFIED BY AUSTRIAN STANDARDS

Nach der Ausbildung können Sie

- die Aufgaben des Datenschutzbeauftragten gem. Art. 39 DSGVO sicher wahrnehmen,
- Ihr Unternehmen DSGVO-konform beraten und mit Rat zur Seite stehen,
- bei der Umsetzung von datenschutzrechtlichen Anforderungen unterstützen,
- Mitarbeiter für datenschutzrechtliche Verhaltensweisen sensibilisieren,
- als Anlaufstelle für die Aufsichtsbehörde Ihr Unternehmen kompetent vertreten.

Die Module der Ausbildung

- Grundlagen des Datenschutzrechts — 10016
- Datenschutzrechtliche Pflichten & Behördenverfahren — 11278
- IT-Sicherheitsmanagementsystem & Notfallplan — 22143
- Das Unternehmen im Internet — 11639
- Datenschutz & Direktmarketing — 10014
- Verwendung von Mitarbeiterdaten — 10015

Die DSGVO ist Geschichte

Lassen Sie sich keine Märchen erzählen.
Investieren Sie in Weiterbildung und behalten Sie damit den Durchblick im Datenschutzrecht.

ars.at/datenschutzrecht

CHECK YOUR DATA – KNOW THE FACTS

Sie wollen alles? Sie bekommen alles: Daten, Schutz und Sicherheit. Checken Sie jetzt, ob Ihr Unternehmen DSGVO-konform aufgestellt ist. Mit unseren Datenschutz-Facts behalten Sie den Überblick, wo es noch Weiterbildungsbedarf erfordert und wie Sie nachhaltig Wissenslücken schließen.

Fact 1: Sie brauchen Support – Wir bilden ihn aus

Der Bereich Datenschutz ist komplex. Aber die gute Nachricht ist: Sie müssen sich nicht allein durch den Daten-Dschungel kämpfen. Lassen Sie einen Mitarbeiter zum Datenschutzbeauftragten ausbilden, der die Lage rechtlich im Blick behält.

Unser Tipp: Ausbildung zum zertifizierten Datenschutzbeauftragten **10013**

Fact 2: Wissen schützt vor Daten-Pannen

Und auch vor Datenschutzverstößen. Deswegen zahlt es sich aus, sich für den Umgang mit personenbezogenen Daten zu sensibilisieren. Sie haben keine Zeit für eine 6-tägige Ausbildung? Kein Problem, dafür gibt es unser Einführungsseminar.

Unser Tipp: Grundlagen des Datenschutzrechts **10016**

Fact 3: Die Fakten müssen regelmäßig gecheckt werden

IT und Recht entwickeln sich ständig weiter. Es ist daher nur naheliegend, dass sich auch der Status Quo in Windeseile ändert. Regelmäßige Updates, um wieder auf den neuesten Stand der Dinge zu kommen, sind daher essenziell.

Unser Tipp: Tagung Datenschutz **20398**

Fact 4: Denken Sie global – Datenschutz kennt keine Grenzen

Globalisierung prägt den Arbeitsalltag und hat neue Märkte erschlossen. Rechtliche Grundlagen unterscheiden sich von Land zu Land – vor allem außerhalb der EU. Informieren Sie sich, was das für den Datenaustausch über die Grenzen bedeutet.

Unser Tipp: Datentransfer in Drittländer **31126**

Fact 5: Praxis ist die Krönung des Wissens

Zwischen Theorie und Praxis liegen oft Welten. Im Fall Datenschutz können diese Welten teuer werden – eine Datenschutzpanne ist schnell passiert. Mit gekonnter Weitsicht und praktischer Erfahrung meistern Sie jeden Datenschutzfall.

Unser Tipp: Praxisseminar Datenschutz – Kompakt **21389**

Fact 6: Risky Business ist nur ein Filmtitel

Risiko bedeutet für manche vielleicht einen willkommenen Nervenkitzel, aber beim Thema Datenschutz sollten Risiken immer richtig bewertet werden. Whitelist – Blacklist – No-List: Beugen Sie unschöne Überraschungen vor und vermeiden Sie teure Folgen.

Unser Tipp: Data Breach & Datenschutz-Folgenabschätzung **22149**

Datenschutz: DSGVO-konform agieren

Tagung Datenschutz

20398

Die Digitalisierung hat in vielen Unternehmensbereichen zu technologischen, wirtschaftlichen und sozialen Veränderungen geführt. Dazu gesellen sich gesetzliche Änderung, wie die Whistleblowing-RL oder der EU-Rechtsrahmen für Künstliche Intelligenz, die im Datenschutz neue Fragen aufwerfen. Mit der Tagung bieten wir Ihnen die optimale Plattform für Wissensupdate und Erfahrungsaustausch. Unsere Datenschutzexperten präsentieren Ihnen die neuesten Entwicklungen, Leitlinien, Empfehlungen, bewährte Verfahren und berichten über die Standpunkte der Aufsichtsbehörde.

Buzzword Datenschutz

Verpassen Sie keinen Trend und keine Entwicklung rund um das Thema.

Backup Weiterbildung

Mit einem Datenschutz Update vermeiden Sie ungewollte Pannen.

Cookies & Kuchen

Zwischen Impulsvorträgen & Networking sorgen wir für Nervennahrung.

WISSEN PRAKTISCH VERMITTELT

Praxisseminar Datenschutz – Intensiv

20807

- Besprechen Sie den Aufbau eines Datenschutz-Managements-Systems (DMS).
- Erfahren Sie, wie Sie Fotos & Videos richtig verwenden und verarbeiten.
- Diskutieren Sie die Grundzüge des internationalen Datenverkehres.

Datenschutzverträge – Recht & Praxis

31111

- Kennen Sie die Verantwortlichkeiten im Sinne der DSGVO.
- Entscheiden Sie im Joint Controllership über die sichere Datenverarbeitung.
- Freuen Sie sich auf den Workshop zu den wichtigsten Vertragsklauseln.

Workshop Alltagsfälle im Datenschutz

31100

- Lernen Sie ein schematisches & standardisiertes Prüfungsverfahren kennen.
- Prüfen Sie richtig im Sinne der DSGVO und des DSG.
- Sichern Sie sich Übungsbeispiele für alltägliche Datenschutzfallen.

DIE ZUKUNFT IST DIGITAL.

Erschließen Sie neue Wege
und nutzen Sie
ungeahntes Potenzial.

ars.at/datenschutzrecht

Jeffrey Müller-Büchse
Bildungsberater
jeffrey.mueller-buechse@ars.at | +43 1 713 80 24-38

Nähere Informationen finden Sie unter: **ars.at/datenschutzrecht**

ARS Akademie