DATENSCHUTZAKTUELL
JUL II
2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

SCHUTZ VOR CYBERCRIME: STÄRKEN SIE DIE ERSTE VERTEIDIGUNGSLINIE

Kein Datenschutz ist auch keine Lösung

Liebe Leserin, lieber Leser,

Datenschutz ist schon immer ein heiß diskutiertes und hoch umstrittenes Thema – vielleicht auch in Ihrem Unternehmen. Und auch in der Politik gibt es Stimmen, die als Maßnahme zum Bürokratieabbau den Datenschutz zurückfahren wollen.

Natürlich ließe sich manche gesetzliche Anforderung erheblich vereinfachen. Das werden Sie als Datenschutzbeauftragter sicher auch so sehen. Wichtig ist jedoch, dass Sie die Grundidee verteidigen. Nicht jeder soll mit personenbezogenen Daten machen dürfen, was er will. Schließlich hat jeder das Recht auf Schutz seiner Daten. Und dieses Recht muss erhalten bleiben.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz im Unternehmen pragmatisch umsetzen lässt.

Inhalt

Zu Ihrem Onlinebereich:
https://www.privacyxperts.de

Live-Talk:
https://t1p.de/live-talk

E-Mail-Beratung:
https://t1p.de/andreas-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Tomasz Zajda; Seite 1: Adobe Stock | PhotographyByMK

Erscheinungsweise: 36-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Erhalten Sie sich Ihre Erholung mit unserer Checkliste für einen guten Einstieg.

Zurück aus dem Urlaub: So klappt ein guter Wiedereinstieg

Wenn Sie in Urlaub waren und eine schöne Zeit hatten, fällt es Ihnen zurück am Arbeitsplatz vielleicht gar nicht so leicht, wieder in die Gänge zu kommen. Keine Sorge, das geht den meisten Menschen so. Damit Sie jedoch möglichst lange von Ihrer Erholung profitieren, sollten Sie die erste Arbeitswoche durchdacht angehen.

So schaffen Sie den Wiedereinstieg ganz relaxt

Gerade nach einer mehrwöchigen Auszeit kann der Wiedereinstieg schwerfallen. Umso wichtiger ist, dass Sie das Ganze planvoll und risikoorientiert angehen. Risikoorientiert vor allem deshalb, weil nicht alles so wichtig ist, dass es Ihrer vollen und sofortigen Aufmerksamkeit bedarf. Für die ersten Tage nach dem Urlaub finden Sie in der folgenden Checkliste 20 Erledigungen, sprich To-dos. Arbeiten Sie diese ab, können Sie sich sicher sein: Sie kommen langsam wieder auf Touren, Sie setzen die richtigen Schwerpunkte und der Stress hält sich in Grenzen.

Übrigens: Die 20 To-dos klingen nach ganz schön viel Arbeit für die ersten Tage. Doch wer sagt eigentlich, dass Sie alles in den ersten Tagen erledigen müssen? Eben. Nehmen Sie sich die Zeit, die Sie brauchen.

Denken Sie aber nicht nur an Ihre Arbeit

Das Leben besteht nicht nur aus Arbeit. Auch wenn es komisch klingt, das gilt erst recht für das Arbeitsleben. Nutzen Sie also die ersten Tage auch dafür, mit Kollegen ins Gespräch zu kommen. Treffen Sie sich auf einen Kaffee. Planen Sie dazu bewusst kurze Auszeiten ein. Zudem können Sie eine erste Besprechung im Team auch als freundliche Begrüßungsrunde ausgestalten. Beziehungen werden dadurch stärker. Und Sie bekommen ganz nebenbei viele „Updates" und den neuesten Flurfunk.

Checkliste: 20 To-dos für die ersten Arbeitstage nach dem Urlaub

	To-do	Achten Sie hierauf	Haken dran?
1.	Spontane Einfälle notieren	› Bevor Sie den Computer starten, sollten Sie sich ein Blatt nehmen und ein kurzes Brainstorming machen. › Notieren Sie sich alle Einfälle zu Fragen wie „Was muss ich diese Woche unbedingt erledigen?", „Mit wem muss ich schnellstens sprechen?". › Markieren Sie dann rot, was wichtig und dringend ist, gelb, was wichtig, aber nicht so eilig ist, und grün, was Zeit hat.	○ Ja ○ Nein
2.	Computer und IT auf aktuellen Stand bringen	› Waren Sie längere Zeit abwesend, sind eventuell einige (Sicherheits-)Updates fällig. Starten Sie diese unverzüglich. › Denken Sie auch an andere Geräte und Software. Auch die sollten auf neuestem Stand sein. › In der Zwischenzeit erledigen Sie andere To-dos aus der Liste.	○ Ja ○ Nein
3.	Post abholen und sortieren	› Statten Sie persönlich der Poststelle einen Besuch ab. Hier bekommen Sie nicht nur Ihre Post. Sie können auch erste Neuigkeiten in Erfahrung bringen. Zudem weiß man, dass Sie wieder da sind. › Öffnen Sie alle Post. Sortieren Sie mit Stapeln nach Wichtigkeit und Dringlichkeit.	○ Ja ○ Nein

4.	Rufumleitung und Abwesenheitsnotiz deaktivieren	› Schalten Sie die automatische Abwesenheitsnotiz aus und deaktivieren Sie eine eventuelle Rufumleitung. › Prüfen Sie zudem, ob Sprachnachrichten eingegangen sind. Ist etwas Wichtiges dabei, machen Sie gleich eine Notiz.	○ Ja ○ Nein
5.	Zeitblöcke im Kalender blockieren	› Reservieren Sie sich gerade in der ersten Arbeitswoche zwei bis drei Stunden täglich für das Aufarbeiten Ihrer Themen. › Geblockte Zeiten sind auch nützlich, wenn Sie kurzfristig Termine für wichtige Besprechungen oder Beratungen unterbringen müssen. › Sehen Sie auch zwischen den ersten neuen Terminen Zeiträume vor, um sich gut vorzubereiten bzw. den Termin nachzubereiten. Beides kann in den ersten Tagen nach dem Urlaub mehr Zeit brauchen.	○ Ja ○ Nein
6.	E-Mails systematisch sichten	› Überfliegen Sie zunächst alle während Ihrer Abwesenheit eingegangenen E-Mails. Bearbeiten Sie noch nichts. Löschen Sie aber diejenigen Mails, die offensichtlich „Müll" sind, etwa Werbung. › Sortieren Sie mittels passender Ordner, beispielsweise „Wichtig und dringend", „Wichtig, nicht dringend", „Später bearbeiten", „Zur Info". › In den Ordnern schauen Sie sich zunächst an, was an Sie persönlich adressiert wurde. Dann schauen Sie die E-Mails mit Verteilern als Empfänger an und zuletzt E-Mails, die Sie in Kopie erhalten haben.	○ Ja ○ Nein
7.	Mit der Urlaubsvertretung sprechen	› Schauen Sie persönlich bei der Vertretung vorbei. Besprechen Sie, was während Ihrer Abwesenheit passiert ist. › Denken Sie an ein kleines Dankeschön. Das ist nicht nur Wertschätzung. Sie sichern sich auch eine gute Chance, dass man Sie demnächst gerne wieder unterstützt.	○ Ja ○ Nein
8.	Sich bei der Unternehmensleitung zurückmelden	› Sagen Sie kurz Hallo, am besten persönlich. › Erfragen Sie, ob es in der Zwischenzeit Relevantes für Sie gab. › Klären Sie, ob man eine kurzfristige Rücksprache wünscht. Ist dem so, klären Sie, ob Sie etwas vorbereiten können.	○ Ja ○ Nein
9.	Wichtige Ansprechpartner kontaktieren	› Sprechen Sie beispielsweise mit IT-Leiter, Compliance Officer oder Betriebsrat. So bringen Sie auf die Schnelle wichtige Neuigkeiten in Erfahrung. › Denken Sie auch an Vertrauenspersonen. Diese können Ihnen wichtige Infos zu Inoffiziellem geben. Denn nicht alles, was wichtig ist, wird auch offiziell kommuniziert.	○ Ja ○ Nein
10.	Status laufender Projekte und neuer Verarbeitungen klären	› Besprechen Sie den Fortschritt bei aktuellen Projekten oder diesbezüglichen Beratungen Ihrerseits. › Bringen Sie in Erfahrung, inwieweit es Veränderungen gibt, etwa bei Zeitplänen oder der Ausrichtung von Projekten und Verarbeitungen.	○ Ja ○ Nein
11.	Stand bei Betroffenenanfragen prüfen	› Klären Sie, inwieweit offene Anfragen bearbeitet wurden. Lassen Sie sich berichten, inwiefern es Reaktionen von Betroffenen auf die Antwort Ihres Unternehmens gab. Eventuell besteht diesbezüglich Handlungsbedarf. › Schauen Sie auch, ob neue Anfragen hinzugekommen sind und ob Ihre Beratung erforderlich ist.	○ Ja ○ Nein
12.	Datenpannen und Vorfälle prüfen	› Fragen Sie konkret nach, etwa bei der IT-Abteilung. Eventuell passierte etwas, wovon Sie noch nichts wissen. Möglicherweise muss schnell gehandelt werden. › Kam es tatsächlich zu Pannen, sollten Sie ein Auge auf ggf. erforderliche Meldungen haben. Informieren Sie sich, was wann der Datenschutzaufsicht gemeldet wurde.	○ Ja ○ Nein
13.	Terminanfragen bewerten und bearbeiten	› Sagen Sie nicht vorschnell Termine zu, etwa nur weil diese schon länger angefragt wurden. Prüfen Sie zunächst die Wichtigkeit und Dringlichkeit. › Ist Ihnen nicht klar, worum es bei einem Termin gehen soll, klären Sie das kurz vor einer Teilnahmezusage.	○ Ja ○ Nein
14.	Offene Aufgaben anderer einfordern	› Prüfen Sie, was bei anderen offen war bzw. noch ist. › Hat man Ihnen etwas nicht zukommen lassen, fordern Sie das nach. › Denken Sie insbesondere an zugesagte Konzepte, Informationen oder Vertragsentwürfe.	○ Ja ○ Nein
15.	To-do- bzw. Offene-Punkte-Liste pflegen	› Nehmen Sie neue Themen auf, die Sie in den ersten Arbeitstagen ausgemacht haben. › Sortieren Sie ggf. die Prioritäten neu. › Streichen Sie Erledigtes nur durch und löschen Sie nichts aus der Liste. Es motiviert, wenn Sie sehen, was abgearbeitet wurde.	○ Ja ○ Nein
16.	Ideen aus dem Urlaub festhalten	› Hatten Sie im Urlaub Einfälle, sollten Sie diese festhalten. › Überführen Sie die relevanten Themen in Ihre Offene-Punkte-Liste.	○ Ja ○ Nein
17.	Rechtliche Entwicklungen sichten	› Schauen Sie, was sich fachlich oder rechtlich getan hat. › Klären Sie, über welche Aspekte Sie andere Personen informieren müssen.	○ Ja ○ Nein
18.	Schwerpunkte für die nächsten Wochen setzen bzw. anpassen	› Legen Sie fest, was Sie in den nächsten vier bis acht Wochen erledigt haben wollen. › Planen Sie realistisch und laden Sie sich nicht zu viel auf die Schultern. › Haben Sie auch ein Auge auf Ihre bisherige Jahresplanung. Ggf. sind hier Anpassungen erforderlich.	○ Ja ○ Nein
19.	Manöverkritik zur Abwesenheit durchführen	› Prüfen Sie kritisch, was während Ihrer Abwesenheit gut oder schlecht lief. › Definieren Sie Maßnahmen, damit Problematisches das nächste Mal besser läuft. › Sprechen Sie auch mit Fachabteilungen, inwieweit aus deren Sicht Verbesserungsbedarf besteht.	○ Ja ○ Nein
20.	Risikoorientiert in den Arbeitsalltag starten	› Setzen Sie bei all Ihren Aktivitäten Prioritäten. Verschieben Sie weniger Wichtiges nach hinten. › Lassen Sie sich nicht in Beratungen „quatschen", gerade am Telefon. Klären Sie kurz, worum es geht, geben Sie eine erste kurze Einschätzung und vereinbaren Sie einen Besprechungstermin.	○ Ja ○ Nein

Gute Frage: Wie sicher sind eigentlich Ihre Daten?

Sie wissen nur zu gut: Weil Datenschutz nicht jedermanns Lieblingsthema ist und manche Ihrer Forderungen infrage gestellt werden, müssen Sie das Vorbild schlechthin im Datenschutz sein. Damit niemand sagen kann, dass Sie Wasser predigen, aber Wein trinken, müssen Sie auch in Ihrem Arbeitsumfeld streng auf Datenschutz und Datensicherheit achten.

Schauen Sie einmal bei sich genauer hin

Als Datenschutzbeauftragter müssen Sie personenbezogene Daten verarbeiten, um Ihre Aufgaben wahrnehmen zu können. Dieses Verarbeiten lässt sich auf Ihre Aufgabenerfüllung aus Art. 39 Datenschutz-Grundverordnung (DSGVO) stützen. Zudem erfüllen Sie und Ihr Unternehmen eine gesetzliche Verpflichtung (Art. 6 Abs. 1 Satz 1 Buchst. c DSGVO). Doch auch bei der Datensicherheit nach Art. 32 DSGVO muss alles passen. Um einmal zu prüfen, wie es denn um die Sicherheit bei Ihnen steht, können Sie auf die folgende Checkliste setzen. Machen Sie Verbesserungspotenzial aus und gehen Sie die Optimierung zeitnah an.

Checkliste: Datensicherheitsmaßnahmen für den Datenschutzbeauftragten

Frage zur Umsetzung bzw. Handhabung	Darauf kommt es an	Geprüft und in Ordnung?
Die Risiken für Daten in meinem Verantwortungsbereich sind analysiert?	› Analysieren und bewerten Sie Gefahren sowie Schwachstellen in Ihrem Bereich (z. B. zu Verlust, Diebstahl oder unbefugtem Zugriff). › Bewerten Sie die Risiken auf Basis von möglichem Schaden und Eintrittswahrscheinlichkeit.	○ Ja ○ Nein
Angemessene Schutzmaßnahmen sind abgeleitet und umgesetzt?	› Wählen Sie Maßnahmen insbesondere danach aus, wie einem Risiko am besten begegnet und dieses auf ein vertretbares Niveau reduziert wird. › Achten Sie auf Risikoorientierung. Es kommt nicht unbedingt auf das Teuerste oder Modernste an. Eine Maßnahme muss zum Risiko passen.	○ Ja ○ Nein
Ich nutze eine eigene, separate Datenablage für meine Arbeit als Datenschutzbeauftragter?	› Gerade wenn Sie neben einer anderen Tätigkeit Datenschutzbeauftragter sind, müssen Sie auf eine getrennte Datenhaltung achten. › Auch Kollegen können Unbefugte sein. Insofern dürfen diese keinen Zugriff auf Ihre Daten haben.	○ Ja ○ Nein
Clean Desk und Clear Screen halte ich konsequent ein?	› Lassen Sie bei Abwesenheit Schützenswertes nicht offen herumliegen. › Sperren Sie Ihren Computer bei längerer Abwesenheit. › Schließen Sie Schränke und Bürotür bei Abwesenheit ab.	○ Ja ○ Nein
Nicht mehr erforderliche Daten lösche ich bzw. diese werden von mir anonymisiert?	› Auch als Datenschutzbeauftragter müssen Sie personenbezogene Daten bei Vorliegen der Voraussetzungen (Art. 17 DSGVO) löschen. › Beachten Sie geltende Aufbewahrungspflichten. › Bei Mustern oder Beispielen setzen Sie auf das Anonymisieren. Entfernen Sie jeden Personenbezug.	○ Ja ○ Nein
Ich habe einen Überblick über alle Datenträger und Speichermedien?	› Erstellen und führen Sie eine Inventarliste über Computer, Smartphones und Speichersticks. › Bewahren Sie Datenträger sicher an geschützten Orten, z. B. verschließbarer Schrank oder Rollcontainer. Vermerken Sie die Aufbewahrungsorte in der Liste.	○ Ja ○ Nein
Unterlagen kann ich sicher und datenschutzkonform entsorgen?	› Ihre sensiblen Informationen dürfen nicht in falsche Hände geraten. › Wollen Sie einen Schredder nutzen, sollte dieser der Sicherheitsstufe P5 entsprechen.	○ Ja ○ Nein
Alle alten bzw. defekten Geräte werden datenschutzkonform entsorgt?	› Setzen Sie hier unbedingt auf sichere Löschmethoden, beispielsweise das Überschreiben des Datenträgers. › Beim Einsatz von Löschsoftware sollten Sie ein Löschprotokoll aufbewahren. › Ist eine Löschung nicht mehr möglich, muss der Datenträger bzw. das Gerät zerstört werden.	○ Ja ○ Nein
Berechtigungen habe ich auf das erforderliche Maß begrenzt?	› Setzen Sie das Minimalprinzip bzw. das „Need-to-know-Prinzip" um. › Achten Sie auch darauf, dass nicht zu viele Administratoren Zugriff auf Ihre Daten haben. › Werfen Sie auch einen Blick auf Ihre Berechtigungen. Was nicht benötigt wird, lassen Sie löschen.	○ Ja ○ Nein
Ich führe regelmäßig Datensicherungen (Back-ups) durch?	› Orientieren Sie sich bei der Häufigkeit an der Kritikalität der Daten. › Führen Sie die Sicherung eigenhändig durch, planen Sie dafür Regeltermine im Kalender ein. › Nutzen Sie Verschlüsselung. › Probieren Sie aus, ob Sie auf gesicherte Daten wirklich zugreifen können.	○ Ja ○ Nein
Meine Passwörter sind gut und werden sicher verwahrt?	› Setzen Sie für jeden Account auf individuelle und komplexe Passwörter. › Nutzen Sie Mehr-Faktor-Authentifizierung oder Passkeys, gerade bei sensiblen Systemen. › Legen Sie Ihre Passwörter in einem Passwortmanager ab.	○ Ja ○ Nein
Ich setze bei Schützenswertem im Bedarfsfall auf Verschlüsselung?	› Wenn Sie mit Daten unterwegs sind oder wenn Sie besonders Sensibles auf Reisen schicken (z. B. per E-Mail), ist eine Verschlüsselung unerlässlich. › Setzen Sie auf eine aktuelle Verschlüsselung und ein gutes Verschlüsselungspasswort.	○ Ja ○ Nein

Schutz vor Cybercrime: Stärken Sie die erste Verteidigungslinie

Cyberkriminelle haben es auf Ihr Unternehmen abgesehen. Und weil niemand ausschließen kann, dass dem so ist, muss vorgesorgt werden. Schließlich sollen sich Cyberkriminelle am besten an Ihrem Unternehmen die Zähne ausbeißen. Damit das gelingt, kommt es entscheidend auf die Beschäftigten an.

Sensibilisieren Sie die Mitarbeiter

Ihr Unternehmen kann noch so viel in technische Schutzmaßnahmen investieren. Alles ist für die Katz, wenn ein Beschäftigter unbedacht einen E-Mail-Anhang mit Schadcode öffnet. Um dem vorzubeugen, ist entscheidend, dass die Beschäftigten wissen, worauf es ankommt. Um das nötige Wissen zu vermitteln und richtiges Handeln zu fördern, können Sie z. B. eine Awareness-E-Mail verschicken.

Muster: Awareness-E-Mail zu den Maschen von Cyberkriminellen

Betreff: So haben Cyberkriminelle bei Ihnen keine Chance

Liebe Kolleginnen und Kollegen.

bestimmt ist auch Ihnen bewusst: Cyberkriminalität ist schon lange keine Randerscheinung mehr. Inzwischen ist Internetkriminalität mitten im Leben angekommen. Und die Machenschaften von Cyberkriminellen stellen für Sie wie auch für unser Unternehmen ein großes Risiko dar, und zwar nicht nur wirtschaftlich, sondern auch was den Datenschutz angeht. Geraten schützenswerte Informationen, etwa personenbezogene Daten oder Geschäftsgeheimnisse, in die Hände von Cyberkriminellen, ist gewaltiger Ärger vorprogrammiert. Seien Sie sich sicher: Cyberkriminelle haben es nicht nur auf große Konzerne abgesehen. Auch unser Unternehmen steht als mittelständisches Unternehmen im Fokus. Denn Cyberkriminelle hoffen, dass bei kleineren Unternehmen die Schutzmaßnahmen weniger hoch und die Sensibilität der Beschäftigten eher gering sind.

Es fängt meist harmlos an

Die meisten erfolgreichen Angriffe von Cyberkriminellen beginnen mit einer E-Mail, einem Anruf, einer Messenger-Nachricht oder einer SMS. Hinzu kommt, dass der Empfänger nicht genau hinschaut, nicht nachdenkt oder im falschen Moment unaufmerksam ist. Schnell kann es dann passiert sein. Da bringen auch die besten technischen Lösungen wie Firewall oder Virenscanner kaum noch etwas, wenn den Cyberkriminellen Tür und Tor geöffnet wird.

Cyberkriminelle sind keine Anfänger

E-Mails mit vielen Schreibfehlern, die leicht als Phishing zu erkennen waren, kommen nun weniger oft vor. Inzwischen gehen Cyberkriminelle hochprofessionell vor. Sie nutzen KI, etwa um perfekte E-Mail-Fälschungen herzustellen. Deepfakes werden erzeugt, um die Stimme des Chefs oder Videos für die Onlinekonferenz zu klonen. Zudem recherchieren sie Informationen in sozialen Netzwerken oder sammeln diese auf Webseiten.

Sie sind die wichtigste Verteidigungslinie

Egal, wo Sie arbeiten und auf welcher Hierarchiestufe Sie tätig sind: Jeder kann ins Fadenkreuz der Cyberkriminellen geraten. Dabei darf es nicht zu einem unbedachten Klick, einer achtlosen Weitergabe von Anmeldeinformationen oder einer übereilten Überweisung kommen. Damit Sie Cyberkriminellen nicht auf den Leim gehen, ist es wichtig, dass Sie insbesondere die folgenden fünf Maschen kennen.

Masche Nr. 1: Phishing per E-Mail

Was passiert? Bei Ihnen landet eine E-Mail im Postfach, die scheinbar von einem vertrauenswürdigen und ggf. auch bekannten Absender kommt. Das kann etwa eine Bank, eine Behörde, ein Paketdienst oder eine Servicenachricht von einem sozialen Netzwerk sein. Auch kann die Mail scheinbar von einem Kollegen, Vorgesetzten oder Geschäftspartner stammen. Ziel des Ganzen: Geschickt will man Sie dazu bringen, dass Sie schnell handeln, nicht nachdenken und etwa auf einen Link klicken. Der führt Sie auf eine täuschend echt aussehende Webseite. Dort sollen Sie Anmeldedaten eingeben oder eine Datei öffnen. Die eingegebenen Daten werden dann missbraucht. Die Datei enthält Schadsoftware.

Woran erkennen Sie es? Typischerweise gibt es noch eine unpersönliche oder unpassende Anrede. Zudem wird Handlungsdruck erzeugt, etwa mit einer „letzten Mahnung", einer „Kontosperrung" oder einem „Strafverfahren" gedroht. Manchmal gibt es noch Rechtschreibfehler, auch wenn diese in Phishing-E-Mails dank KI weniger werden. Enthalten sind oft Links zu einer Webseite, bei der erst auf den zweiten Blick auffällt, dass sie nicht das „Original" ist. Beigefügt sind gerne auch Anhänge, z. B. Rechnungen oder Angebote etwa als .docx-, xlsx- oder Zip-Datei.

Masche Nr. 2: Voice Phishing (Vishing)

Was passiert? Sie erhalten einen Anruf. Am anderen Ende der Leitung ist eine freundliche Person. In perfektem Deutsch gibt sie sich als Mitarbeiter der IT-Hotline oder des Supports unseres Unternehmens oder von Microsoft & Co. aus. Manchmal gibt man auch vor, Mitarbeiter einer

Behörde, einer Bank oder eines Geschäftspartners zu sein. Der Anrufer schildert ein Problem, etwa einen Sicherheitsvorfall, ein technisches Problem oder eine verdächtige Zahlung. Und genau Sie – nur Sie – können dabei helfen, das Problem zu lösen. Sie sollen etwa eine Wartungssitzung mit Zugriff auf Ihren Computer erlauben, Passwörter preisgeben oder von einer Webseite ein Update herunterladen. Letzteres enthält natürlich Schadcode. Woran erkennen Sie es? Werden Sie bei unangekündigten Anrufen von angeblichen IT-Spezialisten, Support-Mitarbeitern oder Behördenvertretern immer stutzig. Diese rufen in der Regel nie unaufgefordert an. Druck wird aufgebaut und Sie sollen sofort handeln. Zudem fordert man Sie auf, eine Webseite aufzurufen, einen Zugriff zu erlauben oder einen zugesendeten Anhang zu öffnen. Alternativ sollen Sie Anmeldeinformationen mitteilen. Auch werden mit KI geklonte vertraute Stimmen genutzt, um Sie in die Falle zu locken.

Masche Nr. 3: Der Chef-Trick (CEO-Fraud)

Was passiert? Sie erhalten vom Chef eine E-Mail oder einen Anruf. Doch das ist schon der Trick. Das stimmt natürlich nicht. Man gaukelt Ihnen nur vor, dass der Geschäftsführer Sie, ja gerade Sie, ins Vertrauen zieht. Es geht regelmäßig um eine ganz eilige und streng vertrauliche Aktion, etwa einen noch geheimen Unternehmenszukauf. Nur Sie können dafür sorgen, dass nichts schiefgeht. Dazu sollen Sie ganz dringend eine Überweisung tätigen oder sensible Informationen weitergeben. Meist sollen Sie dabei auf bestehende Anweisungen oder Prozesse keine Rücksicht nehmen. Doch alles ist erstunken und erlogen.

Woran erkennen Sie es? Die Sache ist immer höchst eilig und absolut geheim. Nur Sie dürfen von der Sache wissen, auch wenn das gar nicht zu Ihrer Tätigkeit passt oder in Ihrer Entscheidungskompetenz liegt. Zudem wird Druck aufgebaut. Machen Sie nicht das Geforderte, soll großer Schaden entstehen. Vorgeschriebene Prozesse oder etablierte Checks (z. B. Vier-Augen-Prinzip") sollen Sie ignorieren. E-Mail-Adressen weichen kaum erkennbar von der echten Adresse ab. Mit Deepfakes erzeugte Stimmen klingen zwar vertraut, aber irgendwie passt etwas nicht.

Masche Nr. 4: Schocknachrichten

Was passiert? Sie erhalten einen Anruf oder eine Sprachnachricht, etwa per Messenger. Der Inhalt erscheint dramatisch. Ein Kollege ist verunglückt oder wurde wegen einer erheblichen Straftat ins Gefängnis gesteckt. Oder es ist von einer Abmahnung, einem Ermittlungsverfahren bzw. einem drohenden Bußgeldbescheid gegen das Unternehmen die Rede. Nur mit schnellem Handeln kann das Schlimme noch abgewendet werden. Das Ziel: Sie sollen in dieser Schrecksituation unbedacht handeln und etwa Geld überweisen, sensible Informationen preisgeben oder einen Link anklicken.

Woran erkennen Sie es? Die Botschaft soll Sie schockieren. Dazu setzt man auf Angst, Sorge Pflichtgefühl oder Schuldgefühle. Es wird Druck aufgebaut und Sie müssen schnell handeln, um Schaden abzuwenden. Nur Sie sind in der Lage, das Unheil abzuwenden. Sie werden aufgefordert, die Sache geheim zu halten. Meist sollen Zahlungen in einer Form erfolgen, die unüblich ist, etwa als Auslandsüberweisung oder in Kryptowährung.

Masche Nr. 5: „Der Enkeltrick" im Unternehmen

Was passiert? Ältere Menschen werden gerne über den Tisch gezogen, weil sich der angeblich in Not geratene Enkel meldet und dringend Hilfe braucht. Aus Verbundenheit, Pflichtgefühl und Hilfsbereitschaft werden dann oft Geldbeträge an den „falschen Enkel" gegeben, eben die Kriminellen. Das funktioniert auch im Unternehmen. Es meldet sich etwa ein Kollege, der dringend Ihre Hilfe braucht. Sie sollen ihm bestimmte Dateien zur Verfügung stellen. Allerdings kann das auch am Eingang zum Gebäude passieren, wenn angeblich die Zutrittskarte vergessen wurde.

Woran erkennen Sie es? An sich wirken die Anfragen harmlos, das Ziel ist jedoch meist, dass Sie Daten herausgeben oder den Zugang gestatten. Die Person ist Ihnen eigentlich unbekannt. Gerne kommt es auch zu „Namedropping", sprich, man bezieht sich auf andere Stellen oder bekannte Personen wie z. B. „Herr Meier, unser Geschäftsführer, schickt mich". Um Vertrauen zu schaffen, kommt man ins Plaudern oder es regnet Komplimente.

So verhalten Sie sich richtig

Damit all diese Maschen ins Leere gehen, ist entscheidend, dass Sie sich richtig verhalten. Machen Sie Folgendes:

- **Bevor Sie handeln: zweimal nachdenken.** Zeitdruck ist ein wichtiger Erfolgsfaktor für Cyberkriminelle. Nehmen Sie sich immer die Zeit, um die nächsten Schritte gut zu überlegen.
- **Machen Sie nicht das, was in einer verdächtigen Situation gefordert wird.** Klicken Sie nicht auf Links, geben Sie nichts Sensibles preis und öffnen Sie keine Anhänge.
- **Weichen Sie nie von geltenden Regeln und Prozessen ab.** Gerade das Vier-Augen-Prinzip, Freigabeprozesse und Sicherheitsregeln gelten immer und ausnahmslos.
- **Nehmen Sie Ihr Bauchgefühl ernst.** Kommt Ihnen etwas seltsam vor, dann trifft das in den meisten Fällen tatsächlich zu.
- **Halten Sie im Zweifel immer Rücksprache.** Fragen Sie Kollegen, Vorgesetzte oder andere relevante Stellen im Unternehmen. Auch können Sie den Datenschutzbeauftragten ansprechen.
- **Bestätigen Sie die Echtheit über bekannte Wege:** Nutzen Sie nie Links oder Kontaktinformationen aus der E-Mail. Setzen Sie auf unser Firmenadressbuch oder offizielle Quellen.

Und wenn trotzdem etwas schiefgeht?

Fehler können jedem passieren. Doch auch dann sollten Sie das Richtige tun: Warten Sie nicht lange und melden Sie die Sache sofort der IT-Abteilung bzw. dem Datenschutzbeauftragten. Wird nämlich schnell gehandelt, kann Schlimmeres verhindern helfen. Melden Sie sich gerne auch bei erfolglosen Angriffsversuchen. Bleiben Sie auf der Hut!

Wir zählen auf Sie! Ihr Datenschutzbeauftragter

Heinz Elmann

USB-Sticks: Beugen Sie mit 10 Regeln Datenpannen vor

Meist sind sie das Mittel der Wahl, wenn Daten transportiert oder von einer Person zu einer anderen weitergegeben werden sollen. Die Rede ist von mobilen Datenträgern, wie z. B. USB-Sticks, Speicherkarten oder externen Festplatten. Was so praktisch ist, birgt aber auch so manches Datenschutzrisiko. Schärfen Sie also die Sinne der Mitarbeiter.

So gut wie alle Mitarbeiter wollen im Job nichts falsch machen. Denn Fehler sorgen regelmäßig für Stress und Ärger. Und den will sich jeder vom Hals halten. Doch USB-Sticks & Co. bringen Risiken mit sich, die hier und da aus Unkenntnis oder im Eifer des Gefechts außer Acht gelassen werden. Dem können Sie vorbeugen. Machen Sie den Mitarbeitern den richtigen Umgang mit Datenträgern leichter. Sorgen Sie dafür, dass bei der Ausgabe des Datenträgers durch die IT-Abteilung auch ein Merkblatt ausgehändigt wird.

Merkblatt: 10 goldene Sicherheitsregelung für USB-Sticks & Co.

Liebe Kollegin, lieber Kollege,

Sie haben heute von der IT-Abteilung einen externen Datenträger erhalten, beispielsweise einen USB-Stick oder eine Festplatte. So praktisch diese kleinen Datenträger sind: Umso größer sind die Risiken, etwa durch Verlust oder Diebstahl des Datenträgers. Auch können sie Schadprogramme einschleppen. Damit nichts schiefgeht, müssen Sie die folgenden zehn goldenen Regeln beachten:

1. Verwenden Sie nur den vom Unternehmen bereitgestellten Datenträger

Für dienstliche Zwecke verwenden Sie bitte nur den von der IT-Abteilung erhaltenen Datenträger. Nutzen Sie ihn nicht für Privates, etwa um Dateien zu übertragen. Das kann Risiken bergen, etwa für das Einschleppen von Viren oder Schadprogrammen über Privatgeräte.

2. Ohne Wenn und Aber: Setzen Sie auf Verschlüsselung

Verschlüsselung ist beim Transport von Daten eine zwingende Maßnahme. Ist der Datenträger nicht hardwareverschlüsselt, nutzen Sie etwa die bordeigene Verschlüsselung BitLocker von Microsoft Windows. Einzelne Dateien können Sie mit einem starken Passwort vor unbefugtem Zugriff schützen. Für mehrere Dateien können Sie auch eine verschlüsselte Zip-Datei erstellen.

3. Achten Sie auf ein starkes Passwort

Dieses sollte mindestens zwölf Zeichen umfassen und aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Nutzen Sie ein individuelles Passwort, das Sie nicht anderswo verwenden. Halten Sie das Passwort nicht auf einem Zettel fest, denn auch den können Sie verlieren oder er kann mit dem Datenträger geklaut werden. Besser ist ein Passwortmanager.

4. Besonders Schützenswertes müssen Sie mehr schützen

Müssen Sie besonders sensible oder schützenswerte Daten transportieren, setzen Sie am besten auf mehrere Schutzmaßnahmen. Lassen Sie sich von der IT-Abteilung einen hardwareverschlüsselten Datenträger geben. Verschlüsseln Sie zusätzlich die darauf befindlichen Daten. Vergeben Sie hier unterschiedliche Passwörter.

5. Nutzen Sie den Datenträger nicht als Dateiablage

Ein solcher Datenträger ist nur für den Transport bzw. den Austausch von Dateien gedacht und das eben nur temporär. Dateien legen Sie dort ab, wo sie hingehören. Das sind die zentral gemanagten Dateiablagen Ihrer Abteilung.

6. Löschen Sie den Datenträger regelmäßig, und zwar sicher

Räumen Sie den Datenträger nach der Nutzung auf. Löschen Sie beispielsweise alte Angebote. Achten Sie beim Löschen darauf, dass die Daten nicht nur im Papierkorb landen. „Schreddern" Sie die Daten digital. Die entsprechende Funktion finden Sie über das Kontextmenü im Dateiexplorer. Ein Rechtsklick auf die Datei genügt.

7. Bewahren Sie den Datenträger immer sicher auf

Tragen Sie den Datenträger nach Möglichkeit immer bei sich. Lassen Sie ihn nicht offen herumliegen. Schließlich gilt: Gelegenheit macht Diebe. Auch im Hotel sollten Sie allen „Gelegenheiten" vorbeugen. Schließen Sie den Datenträger sicher weg, etwa im Tresor.

8. Geben Sie den Datenträger nicht an Dritte weiter

Am besten ist, wenn Sie den Datenträger nie aus der Hand geben bzw. aus den Augen lassen. Auch „nette Menschen" können Böses im Schilde führen. Für das Kopieren unsichtbarer Schadprogramme reichen wenige Sekunden aus.

9. Prüfen Sie Erhaltenes auf Herz und Nieren

Nutzen Sie den Datenträger, um von anderen Personen Daten zu übertragen, sollten Sie direkt beim Anstecken des Datenträgers den Virenscanner für einen Check der Dateien nutzen. Das geht ruckzuck und Sie reduzieren das Schadensrisiko erheblich.

10. Pannen & Co. müssen Sie unbedingt melden

Haben Sie den Datenträger verloren oder wurde er gestohlen, gilt: Melden Sie das sofort bei der IT-Abteilung und beim Datenschutzbeauftragten. Hier müssen schnell Maßnahmen eingeleitet werden, um mögliche Schäden abzuwenden.

Gilt mein Kündigungsschutz bei weniger Mitarbeitern?

FRAGE: Ich bin Datenschutzbeauftragter eines Unternehmens mit rund 100 Mitarbeitern, davon mehr als 60 Mitarbeiter in der Produktion. Das Unternehmen soll in eine Unternehmensgruppe aufgeteilt werden. In dem einen Unternehmen sind mit 18 Mitarbeitern Verwaltung und Vertrieb gebündelt und im anderen Unternehmen die Produktion mit wenig Verarbeitungen personenbezogener Daten. Ich frage mich: Verliere ich den besonderen Kündigungsschutz?

ANTWORT: Ob weiterhin die Pflicht für einen Datenschutzbeauftragten besteht, hängt etwa von folgenden Faktoren ab:

- **Die Mitarbeiterzahl:** § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) schreibt einen Datenschutzbeauftragten vor, wenn mindestens 20 Personen ständig automatisiert personenbezogener Daten verarbeiten. Wird die Personenzahl unterschritten, entfällt auch die Benennungspflicht.
- **Bestimmte Verarbeitungen:** § 38 Abs. 1 Satz 2 BDSG sieht bestimmte Verarbeitungen vor, die zur Benennungspflicht führen, ohne dass es auf eine Beschäftigtenzahl ankommt.
- **Generelle Pflicht nach Art. 37 Datenschutz-Grundverordnung (DSGVO):** Die Benennungspflicht greift, wenn die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung sensibler Daten (Art. 9 DSGVO) besteht. Auch wenn der Fokus auf einer umfangreichen regelmäßige Überwachung von Betroffenen liegt, ist ein Datenschutzbeauftragter nötig.

Kein Kündigungsschutz für „Freiwillige"

Besteht keine gesetzliche Verpflichtung, einen Datenschutzbeauftragten zu benennen, ist ein Unternehmen nicht daran gehindert, dennoch einen Datenschutzbeauftragten zu haben. Das kann sinnvoll sein, etwa um den Datenschutz professionell anzugehen oder unter dem Aspekt der positiven Außenwirkung.

Jedoch greifen bei freiwillig benannten Datenschutzbeauftragten nicht die in DSGVO & Co. vorgesehenen Rechte und Pflichten. Denn die gelten nur, wenn ein Datenschutzbeauftragter verpflichtend zu benennen ist. Als „Freiwilliger" können Sie sich auf die Unterstützungspflicht oder Weisungsfreiheit genauso wenig berufen wie auf den in §§ 38 Abs. 2, 6 Abs. 4 BDSG verankerten besonderen Kündigungsschutz. § 6 Abs. 4 BDSG gilt nach § 38 Abs. 2 BDSG nämlich nur, wenn eine Benennung verpflichtend ist.

Kündigungsschutz entfällt nicht sofort

Entfallen die Voraussetzungen zur Benennungspflicht für das Unternehmen, etwa bei Absinken der Personenzahl, endet auch die Tätigkeit des „Pflicht-Datenschutzbeauftragten". Gemäß §§ 38 Abs. 2, 6 Abs. 4 Satz 3 BDSG ist eine Kündigung des Arbeitsverhältnisses innerhalb eines Jahres nach Ende der Tätigkeit als Datenschutzbeauftragter unzulässig, wenn nicht ein wichtiger Grund zur fristlosen Kündigung berechtigt.

Wie kann ich meinen Chef zum Kauf eines neuen Schredders bewegen?

FRAGE: Bei meinem sehr sparsamen Chef habe ich einen „historischen" Aktenvernichter entdeckt. Den will er weiter nutzen, auch wenn dieser nur einen relativ breiten „Spaghettischnitt" beherrscht. Wie kann ich ihn von einer Neuanschaffung überzeugen?

ANTWORT: Argumentieren Sie zunächst mit dem Datenschutz bzw. rechtlichen Pflichten. Damit personenbezogene Daten nicht von Unbefugten zur Kenntnis genommen werden können, müssen risikoangemessene Schutzmaßnahmen ergriffen werden (Art. 32 Datenschutz-Grundverordnung). Daher muss auch bei einem Schredder dessen Funktion zum Schutzbedarf passen. Schon bei normalen personenbezogenen Daten wäre ein Schredder mit „Spaghettischnitt" nicht risikoangemessen. Eine so geschredderte Seite lässt sich relativ leicht wieder zusammensetzen. Streifenschnitt entspricht meist der Sicherheitsstufe 1 und ist ungeeignet. Geraten Daten so in falsche Hände, kann das zu viel Ärger und zu einem Bußgeld führen. Empfehlen Sie die Anschaffung eines Schredders, der Mikroschnitt (Sicherheitsstufe 5) beherrscht, sodass ein Zusammensetzen von Seiten praktisch unmöglich ist.

Argumentieren Sie mit der Steuer

Überzeugend kann ggf. auch folgendes Argument sein: Ein Schredder kann in der Regel als geringwertiges Wirtschaftsgut im Jahr der Anschaffung komplett als Betriebsausgabe abgesetzt werden. Insofern ist der „Schmerz" der Kosten geringer. Dem Datenschutz erweist Ihr Chef jedoch einen großen Dienst.

VG Düsseldorf: Betroffener hat keinen Anspruch auf Bußgeld

Als Profi wissen Sie: Bei sensiblen Informationen müssen die Schutzmaßnahmen höher ausfallen. Gerade wenn es um die Übermittlung solcher Daten per E-Mail geht, stellt sich schnell die Frage, ob etwa eine Transportverschlüsselung zwischen den Servern ausreicht. In einem konkreten Fall äußerte sich nun das Verwaltungsgericht (VG) Düsseldorf zu dieser Frage (Urteil vom 2.4.2026, Az. 29 K 7351/23).

Das ging dem Rechtsstreit voraus

Ein Mann, der spätere Kläger, ging gegen die für ein Busunternehmen zuständige Datenschutzaufsichtsbehörde, der späteren Beklagten, vor. Diese hätte auf seine Beschwerde nicht angemessen reagiert.

Zur Beschwerde kam es am 28.6.2022 aus folgendem Grund: Der Mann war Gefahren für Leib und Leben ausgesetzt, sodass es im Melderegister eine Sperre gab und etwa die Auskunft zu seiner Wohnanschrift eingeschränkt war. Als der Mann am 20.1.2022 mit seinem Pkw unterwegs war, ereignete sich ein Unfall mit einem Bus. Dieser streifte den Pkw des Mannes und setzte die Fahrt fort, ohne dass es zu einer Unfallaufnahme kam. Der Mann schaltete die Polizei ein. Die ermittelte den Busfahrer. Diesem übergab der Mann einen Zettel mit Namen und Anschrift.

Über seinen Anwalt nahm der Mann Kontakt zum Busunternehmen auf. Er ließ mitteilen, dass bei ihm schutzwürdige Interessen vorlägen. Insofern müssten bei einer Verarbeitung seiner Daten besondere Schutzmaßnahmen ergriffen werden. Über seine Versicherung sei ihm bekannt geworden, dass E-Mails mit seinen Daten ohne Ende-zu-Ende-Verschlüsselung vom Busunternehmen an dessen Versicherung geschickt wurden. Zudem forderte der Mann am 12.4.2022 Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) vom Busunternehmen.

Aufsicht fordert Informationen

Am 30.9.2022 meldete sich die Aufsichtsbehörde beim Busunternehmen. Sie forderte bestimmte Informationen, um den Sachverhalt prüfen zu können. Zudem bat sie darum, das Auskunftsbegehren zu erfüllen. Das Busunternehmen beantwortete die Anfrage der Behörde. Es wies darauf hin, dass man ein berechtigtes Interesse gehabt hätte, den Schadensfall der Versicherung unverzüglich per E-Mail zu melden. Die Mails wären direkt gelöscht worden. Die Auskunft habe man nicht erteilen können, weil man den Betroffenen mit Vor- und Nachname nicht ausreichend identifizieren konnte.

Behörde antwortet Betroffenem

Der Mann erhielt eine Stellungnahme der Aufsichtsbehörde. Diese sah auch ein berechtigtes Interesse des Busunternehmens für die Schadensabwicklung per E-Mail. Es hätte keine erhöhten Risiken gegeben, sodass die Transportverschlüsselung der E-Mail-Server ausreichend gewesen wäre. Das vor allem, weil in den E-Mails nur der Name genannt wurde und die Privatadresse fehlte. Der Mann wollte das so nicht hinnehmen. Er klagte vor dem VG Düsseldorf. Das jedoch nur mit sehr geringem Erfolg.

So entschied das Gericht

Der Bescheid der Datenschutzaufsichtsbehörde ist weitgehend rechtmäßig. Aber den möglichen Datenschutzverstoß durch die verspätete Auskunft muss die Aufsichtsbehörde neu prüfen und ihr Ermessen bezüglich ihrer Maßnahmen fehlerfrei ausüben.

Ende-zu-Ende-Verschlüsselung nicht erforderlich

Die Verarbeitung der Daten des Klägers durch das Busunternehmen war auf Basis von Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO zulässig. Die Übermittlung des Namens zur Schadensabwicklung lag im berechtigten Interesse des Unternehmens. Auch in Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten liegt kein Verstoß vor. Die Verwendung der Transportverschlüsselung zwischen den E-Mail-Servern war im konkreten Fall risikoangemessen, zumal in den E-Mails nur sein Name enthalten war, der an sich nicht geheim und auch über das Internet frei zugänglich ist. Ein Bezug zur Privatadresse lässt sich nicht herstellen. Aufgrund des nicht erhöhten Risikos war auch keine Datenschutz-Folgenabschätzung erforderlich.

Kein Anspruch auf Bußgeld

Es gab keinen Datenschutzverstoß. Also besteht auch kein Anspruch auf entsprechende Anordnungen der Aufsichtsbehörde, etwa zur Beschränkung der Verarbeitung der Daten des Klägers durch das Busunternehmen oder hinsichtlich einer Pflicht zur Ende-zu-Ende-Verschlüsselung.

Die verspätete Auskunft stellt zwar einen Datenschutzverstoß dar. Allerdings kann der Kläger diesbezüglich nicht die Verhängung eines Bußgelds fordern. Er hat nur den Anspruch auf ermessensfehlerfreie Entscheidung über mögliche Abhilfemaßnahmen. Dieses Ermessen hatte die Aufsichtsbehörde nicht ordnungsgemäß ausgeübt, was nun nachzuholen ist.

§

Das können Sie folgern

Betroffene haben keinen Anspruch auf bestimmte Schutzmaßnahmen. Nur risikoangemessene Maßnahmen sind erforderlich. Beim Versand von E-Mails mit „normalen" Daten kann eine Transportverschlüsselung ausreichen.

Datenschutz aktuell Live Talk: Gratis-Webinar

Austausch, Aktualität, fachliche Tiefe für alle mit Aufgaben im Datenschutz

am letzten Freitag jeden Monats

um 16:30 Uhr 60 Minuten

Moderator & Fachexperte
Andreas Würtz

Warum am Live Talk teilnehmen?

Neue Leitlinien, geplante Gesetzesänderungen, behördliche Anforderungen und praxisnahe Umsetzungsfragen stellen Datenschutzverantwortliche regelmäßig vor neue Herausforderungen. Oft bleiben dabei konkrete Fragen offen – oder es fehlt die Gelegenheit, Themen direkt mit einem Experten zu besprechen.

Der **Datenschutz aktuell Live Talk** ist aufgrund seines digitalen Formats bequem von überall erreichbar. Im Mittelpunkt steht ein **vertraulicher, fachlicher Austausch** zu aktuellen Schwerpunktthemen aus Datenschutzrecht und Datenschutzpraxis.

Die Veranstaltung wird **nicht aufgezeichnet.** So entsteht ein geschützter Rahmen, in dem auch sensible Fragestellungen offen angesprochen werden können. Sie entscheiden selbst, wie aktiv Sie teilnehmen möchten: **Bringen Sie Ihre Fragen ein oder hören Sie einfach zu** – ganz nach Ihrem Bedarf und ganz wie Sie mögen.

Der Live Talk ist bewusst kein klassisches Webinar mit Frontalvortrag, sondern ein dialogorientiertes Format, das auf Austausch, Aktualität und fachliche Tiefe setzt.

Ich freue mich auf Ihre Teilnahme!

Ihr Moderator & Fachexperte Andreas Würtz
Rechtsanwalt | Datenschutzexperte
Chefredakteur des Fachratgebers „Datenschutz aktuell“

Jetzt zum nächsten Live-Talk anmelden:

t1p.de/live-talk

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn

Vorschau:

Möglicher Datenabfluss: So reagieren Sie richtig

Audits: Vermeiden Sie diese Patzer