



AI GENERATED

NEUE MITARBEITER: SETZEN SIE AUF DIE FÜHRUNGSKRÄFTE

KNOW-HOW

Nutzen Sie Merkblätter,
um den Datenschutz vor-
wärtzubringen

4–5

DATENSCHUTZ- ORGANISATION

Finden Sie Verbündete im
Datenschutz

6



Onlinebereich:
<https://kurzlink.ch/privacy>



Live-Talk:
<https://kurzlink.ch/live-talk>



Expertenhotline:
<https://kurzlink.ch/kontakt-wuertz>



PRIVACYXPERTS



Drücken Sie kein Auge zu

Liebe Leserin, lieber Leser,

die Umsetzung des Datenschutzes kann mit einigem Aufwand und teils hohen Kosten verbunden sein. Kein Wunder, dass vielleicht der eine oder andere in Ihrem Unternehmen sich von Ihnen wünscht, dass Sie es mit den Anforderungen nicht so genau nehmen und einfach mal fünf gerade sein lassen.

Solchen Wünschen sollten Sie nie nachgeben! Einerseits kann Sie das persönlich in Teufels Küche bringen, wenn Sie absichtlich nicht so beraten, wie Sie es eigentlich müssten. Andererseits gewinnt das Unternehmen am Ende nichts. Gehen die Dinge im Datenschutz sogar schief, drohen heftiger Ärger und hohe Kosten.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredaktor

Ihr Experte für Datenschutz

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

Inhalt

Datenschutzorganisation

Neue Mitarbeiter: Setzen Sie auf die Führungskräfte

Seiten 1–2

Know-how

Kostenersparnis? So entzaubern Sie „Bring Your Own Device“

Seite 3

Awareness

Nutzen Sie Merkblätter, um den Datenschutz vorwärtszubringen

Seiten 4–5

Datenschutzorganisation

Mit diesen 5 Tipps finden Sie Verbündete im Datenschutz

Seite 6

Fragen an die Redaktion

Dürfen wir echte Kundendaten für Testzwecke einsetzen?

Seite 7

Müssen wir die Datenpanne der Arbeitnehmervertretung melden?

Seite 7

Urteil aus dem Ausland

E-Mail-Rechnungen müssen nicht verschlüsselt werden

Seite 8



Zu Ihrem Onlinebereich:
<https://kurzlink.ch/privacy>



Live-Talk:
<https://kurzlink.ch/live-talk>



Expertenhotline:
<https://kurzlink.ch/kontakt-wuertz>

Impressum



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, Michael Schrader, Bonn
V.i.S.d.P.: Michael Jodda (Adresse s. oben)
Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredaktor:
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: AI-generated; Seite 1: Adobe Stock |
contrastwerkstatt

Erscheinungsweise: 17-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Gerade neue Mitarbeiter müssen für den Datenschutz sensibilisiert werden.

Neue Mitarbeiter: Setzen Sie auf die Führungskräfte

Auch wenn Sie in Sachen Zeit und Budget aus dem Vollen schöpfen können, ist klar: Als Datenschutzberater können Sie sich nicht um alles kümmern und erst recht nicht jeden an die Hand nehmen. Das gilt unter Umständen gerade für neue Mitarbeiter. Doch den Datenschutz bei neuen Mitarbeitern zu vernachlässigen bringt Risiken mit sich. Und realisieren sich Risiken, ist der Ärger da.

Awareness braucht jeder Mitarbeiter, gerade die Neuen

Als Datenschutzberater stehen Sie unter Umständen vor folgendem Problem: Sie wollen sich um jeden neuen Mitarbeiter kümmern. Das ist jedoch schon zeitlich nicht machbar. Also müssen Sie das Problem pragmatisch angehen. Sie können eine Schulung für die neuen Mitarbeiter anbieten und auch ein Informationspaket zusammenstellen. Letzteres kann auch die Personalabteilung schon im Vorfeld des ersten Arbeitstags versenden, verbunden mit der Bitte, sich entsprechend einzulesen.

Neben der Schulung sollten Sie die Last in Sachen Awareness auf weitere Schultern verteilen. Schliesslich müssen Sie nicht alles selbst machen. Nehmen Sie die Vorgesetzten und Führungskräfte mit ins Boot, etwa mit einem Handlungsauftrag. Diese können in den ersten Arbeitstagen eines neuen Mitarbeiters viel für den Datenschutz tun, beispielsweise über wichtige Regelungen informieren oder Tipps zum richtigen Umgang mit Daten geben.

Das machen Sie mit Verweigerern

Auch wenn Sie einen guten Vorschlag machen, muss das noch lange nicht heissen, dass alle mitziehen. Stellen Sie fest, dass Vorgesetzte neuen Mitarbeitern nicht das nötige Wissen vermitteln wollen, etwa in einem Gespräch am ersten Arbeitstag, sollten Sie zunächst gute Argumente bringen. Überzeugen können Sie ggf. mit Folgendem: Es ist Teil der Aufgaben eines Vorgesetzten, Mitarbeiter zu führen. Geführt wird über Vorgaben und Anweisungen. So kann das Unternehmen bzw. der das Unternehmen und den Arbeitgeber vertretende Vorgesetzte Weisungen auch zum Umgang mit Personendaten erteilen. Das ergibt sich aus dem Weisungsrecht des Arbeitgebers nach Art. 321d des Obligationenrechts. Zudem sind gerade Führungskräfte besonders verpflichtet, Schaden vom Unternehmen abzuwenden. Und der kann drohen, wenn es unterlassen wird, neue Mitarbeiter mit relevanten Regelungen vertraut zu machen.



Muster: Information für Führungskräfte

Nehmen Sie Ihre neuen Mitarbeiter im Datenschutz an die Hand

Sehr geehrte Führungskraft,

ich wende mich heute mit einem wichtigen Anliegen an Sie. In den nächsten Wochen bekommen Sie ggf. neue Mitarbeiter oder Auszubildende. Bei diesen ist das Datenschutzwissen vielleicht nur in Ansätzen ausgeprägt. Damit diese den Gefahren und Risiken im Umgang mit Personendaten von Anfang an aus dem Weg gehen, sind Sie als Wissensvermittler und Vorbild gefragt.



Daher meine Bitte: Geben Sie direkt am Anfang der Beschäftigung die richtigen Hinweise und tragen Sie dazu bei, dass die neuen Mitarbeiter das nötige Wissen aufbauen. Warum das so wichtig ist? Sie leisten damit einen wichtigen Beitrag, dass auch neue Mitarbeiter Stolperfallen rechtzeitig erkennen und Risiken aus dem Weg gehen. Das erspart uns allen Ärger, Imageschäden und ggf. sogar hohe Bussgelder. Beherzigen Sie bitte folgende Tipps:

Tipp Nr. 1: Machen Sie die neuen Mitarbeiter mit dem Datenschutz vertraut

Heissen Sie nicht nur den neuen Mitarbeiter willkommen. Machen Sie den Datenschutz frühzeitig zum Teil der Einarbeitung. Sprechen Sie das Thema bereits am ersten Arbeitstag kurz an. Erläutern Sie wichtige Grundsätze. Falls noch nicht erfolgt, lassen Sie die Verpflichtungserklärung zur Wahrung des Datenschutzes unterzeichnen.

Tipp Nr. 2: Fordern Sie zur Vertraulichkeit auf

Dass Personendaten oder schützenswerte Informationen aus dem Unternehmen nicht jeden etwas angehen, versteht sich leider nicht unbedingt von selbst. Machen Sie klar, dass Informationen über Kunden oder Kollegen Unbefugte genauso wenig angehen wie Geschäftsgeheimnisse, Entwicklungs- oder Vertriebsinformationen. Internes muss immer vertraulich bleiben, und zwar auch gegenüber Verwandten, Freunden und Bekannten.

Tipp Nr. 3: Vermitteln Sie wichtige Regeln

Nehmen Sie sich ausreichend Zeit, um einen ersten Überblick über besonders wichtige Regeln zum Datenschutz im Unternehmen bzw. in Ihrer Abteilung zu vermitteln. Dazu zählt beispielsweise die interne „Richtlinie zum Umgang mit Personendaten“. Geben Sie dem neuen Mitarbeiter die entsprechenden Informationen und Regelungen an die Hand, etwa per E-Mail oder als Ausdruck. Bitten Sie zudem darum, dass sich der neue Mitarbeiter damit auseinandersetzt. Haken Sie nach einigen Tagen unbedingt nach, ob das tatsächlich passiert ist.

Tipp Nr. 4: Informieren Sie über wichtige Ansprechpartner

Um im Notfall auch schnell Hilfe holen zu können, sollte Ihr neuer Mitarbeiter nicht nur wissen, wie er Sie oder seinen Ansprechpartner in der Abteilung erreichen kann. Geben Sie zusätzlich auch Informationen zu weiteren wichtigen Ansprechpartnern im Unternehmen. Erklären Sie, wie man die IT-Hotline oder das Cybersecurity-Team erreichen kann. Das kann etwa bei Phishing-Fällen wichtig sein. Vermitteln Sie auch, wie man den Datenschutzberater kontaktieren kann.

Tipp Nr. 5: Klären Sie über den richtigen Umgang mit Daten und Technik am Arbeitsplatz auf

Datenschutz fängt schon am eigenen Arbeitsplatz an. Erklären Sie am besten vor Ort, worauf es ankommt. Dazu zählt beispielsweise, was mit dem Clean-Desk-Prinzip gemeint ist. Auch wie man einen Computer bei Abwesenheit sperrt, sollten Sie am Objekt vor Ort zeigen. Nicht jedermann ist mit der Tastenkombination „Windows + L“ vertraut.

Machen Sie zudem klar, dass eine Privatsnutzung der zur Verfügung gestellten Geräte, Software und KI-Lösungen nicht erlaubt ist. Auch der Einsatz eigener Geräte, Software oder KI-Lösungen für die Bearbeitung von Informationen des Unternehmens und für die Kontaktaufnahme zu Kollegen oder zu Kunden ist nicht erlaubt.

Tipp Nr. 6: Bieten Sie sich als Ansprechpartner bei Fragen an

Als Führungskraft sind Sie aus Sicht eines neuen Mitarbeiters eine Respektsperson und jemand, den man bei Fragen vielleicht eher nicht ansprechen will. Schliesslich will man es sich mit dem Vorgesetzten nicht verscherzen oder ein schlechtes Bild abgeben. Bieten Sie sich aktiv als Ansprechpartner an. Machen Sie klar, dass Ihre Tür für jeden Mitarbeiter offen ist und Sie gerne weiterhelfen. Gerade im Datenschutz kann das wichtig sein. Denn ungestellte oder unbeantwortete Fragen zum richtigen Umgang mit Daten bergen das Risiko, dass im Zweifel falsch gehandelt wird.

Tipp Nr. 7: Nehmen Sie die Angst vor dem Melden von Fehlern

Sorgen Sie für eine vertrauensvolle Zusammenarbeit und ein Klima der Offenheit. Niemand soll Angst haben, Fehler zuzugeben und sich an Sie als Vorgesetzten zu wenden. Machen Sie klar, dass Sie niemanden „einen Kopf kürzer machen“, nur weil er Ihnen von einem Missgeschick berichtet. Stellen Sie klar, dass es darum geht, möglichen Schaden einzudämmen und aus Fehlern zu lernen.

Tipp Nr. 8: Setzen Sie Datenschutz immer wieder auf die Agenda

Wissen zum Datenschutz vermitteln ist keine einmalige Sache. Binden Sie verschiedene Aspekte immer wieder in Meetings mit Ihrem Team ein. Besprechen Sie gemeinsam Rahmenbedingungen, Vorschläge zum Vorgehen oder gemachte Erfahrungen.

Tipp Nr. 9: Seien Sie immer Vorbild

Bedenken Sie stets: Ihre Mitarbeiter, gerade die neuen, orientieren sich an Ihnen. Deshalb ist wichtig, dass auch Sie selbst die geltenden Regeln zum Umgang mit Personendaten einhalten. Achten Sie stets die Vertraulichkeit, gerade bei Gesprächen oder Besprechungen. Denken Sie auch stets an das Clean-Desk-Prinzip. Umgehen Sie keine Regelungen oder Prozesse und nehmen Sie sich für Ihre Person keine Sonderbehandlung heraus.

Übrigens: Gutes Vorbild sind Sie auch dadurch, dass Sie die geltenden Regeln umsetzen. Prüfen Sie beispielsweise regelmässig, ob vergebene Berechtigungen noch – Achtung, Wortspiel – ihre Berechtigung haben.

Tipp Nr. 10: Sie haben immer meine Unterstützung

Führungskraft, Vorgesetzter und Vorbild im Datenschutz zu sein kann ab und an eine ganz schöne Herausforderung darstellen. Doch Sie müssen nicht jede Herausforderung allein meistern oder das Rad neu erfinden. Geht es um Datenschutzrelevantes können Sie sich an mich wenden, Ihren Datenschutzberater. Ich stehe Ihnen mit Rat und Tat zur Seite. Und das natürlich ganz vertraulich.

Ich danke Ihnen für Ihre Unterstützung!

Ihr Hanns Solo
Datenschutzberater

Kostenersparnis? So entzaubern Sie „Bring Your Own Device“

Gerade wenn die Zeiten schwierig sind, wird in manchen Unternehmen jeder Stein umgedreht, um mögliche Einsparmöglichkeiten ausfindig zu machen. Und weil die IT-Kosten in vielen Unternehmen einen grossen Anteil am Gesamtbudget ausmachen, kommt man vielleicht auch bei Ihnen auf die Idee: Die Mitarbeiter könnten doch die privaten Geräte nutzen? Doch das ist keine gute Idee!

Das steckt hinter BYOD

Die Idee hinter „Bring Your Own Device“ (BYOD) ist schnell erklärt. Die Beschäftigten nutzen privat beschaffte IT, etwa Notebook und Smartphone, und zwar eben auch im Zusammenhang mit der Arbeit für Ihr Unternehmen. Auf den ersten Blick bringt die Idee viele Vorteile mit sich. Jeder nutzt das Gerät mit dem er am besten zurechtkommt. Das steigert die Zufriedenheit. Und Ihr Unternehmen muss nicht viel Geld für Geräte und Support ausgeben. Das macht der Mitarbeiter selbst. Doch was wie Werbeversprechen aus Hochglanzbroschüren daherkommt, steckt voller Risiken.

Ziehen Sie den Zahn schnellstens

Kommen Sie in die Situation, dass Sie als Datenschutzberater zu BYOD Stellung nehmen sollen, brauchen Sie nicht lange grübeln. Zeigen Sie die folgenden Risiken auf. Diese lassen sich meist nicht wirklich so minimieren, dass man sie hinnehmen könnte. Im Ergebnis muss es heissen: Finger weg von BYOD!

Risiko Nr. 1: BYOD ist selten ein Kostensenker

Meist wird nur Pi mal Daumen kalkuliert. Zwar sieht man die Kosten, die man sich für Geräte sparen könnte. Übersehen werden jedoch die Kosten, die unter Umständen durch BYOD sogar in die Höhe getrieben werden. Zu nennen sind hier Kosten für Support, für ein Device-Management oder Lizenzen. So muss der Support viele Gerätetypen und Modelle abdecken, etwa im Zusammenhang mit Sicherheitseinstellungen und Updates. Auch bei Software erhöht sich nicht nur der Betreuungsaufwand. Auch Lizenzkosten können steigen, wenn etwa Mengenrabatte nicht mehr greifen.

Risiko Nr. 2: Kontrollverlust

Ihr Unternehmen ist Verantwortlicher im Sinne des Bundesgesetzes über den Datenschutz. Um die Bearbeitung sicher zu machen, müssen angemessene Schutzmassnahmen ergriffen werden. Genau das kann mit BYOD zum Ding der Unmöglichkeit werden. Ihr Unternehmen bleibt für seine Bearbeitungen durch die Beschäftigten voll verantwortlich. Da ist es egal, ob die auf deren Geräten stattfindet. Die Kontrolle, was wie mit den Daten passiert, gibt es jedoch in die Hände der Beschäftigten. Meist ist das keine gute Idee.

Risiko Nr. 3: Freiwilligkeit kann zum Problem werden

Schon arbeitsrechtlich ist klar: Ihr Unternehmen muss den Beschäftigten einen funktionsfähigen Arbeitsplatz zur Verfügung

stellen. Das gilt auch für die Arbeitsmittel. Kein Arbeitnehmer muss diese mitbringen oder bereitstellen. Also geht BYOD nur freiwillig und auf Einwilligungsbasis. Gerade wenn Ihr Unternehmen auf Privatgeräten Software installieren oder darauf Zugriff nehmen will, braucht es die Einwilligung des Betroffenen. Und die ist im Beschäftigungsverhältnis immer problematisch. Ausserdem: Einwilligungen können ohne Weiteres widerrufen werden. Sagt ein Mitarbeiter Nein zu BYOD, muss Ihr Unternehmen Alternativlösungen haben. Und die werden dann aufwendig und teuer.

Risiko Nr. 4: Ärger mit Lizenzen

Nur weil Software funktioniert, darf sie noch lange nicht für Ihr Unternehmen genutzt werden. Privat beschaffte Software, Shareware oder Open-Source-Programme dürfen oft eben nur für nicht gewerbliche Zwecke eingesetzt werden. Das bedeutet, dass Ihr Unternehmen alle Lizenzen der auf den Privatgeräten eingesetzten Software prüfen muss. Macht es das nicht und wird dem Rechteinhaber ein Lizenzverstoss bekannt, wird es meist sehr teuer. Nachlizenzierungen oder Schadensersatzforderungen sprengen schnell jede Portokasse.

Risiko Nr. 5: Sicherheit ist Glückssache

Sie wissen als Datenschutzexperte: Um die Sicherheit bei der Bearbeitung von Personendaten zu gewährleisten, muss die eingesetzte Technik auf der Höhe der Zeit sein. Das gilt besonders für Betriebssysteme und Software. Doch wie will Ihr Unternehmen z. B. das unverzügliche Aktualisieren bei Privatgeräten sicherstellen? Passiert das nicht, haben Cyberkriminelle leichtes Spiel.

Risiko Nr. 6: Unbefugte sind ein grosses Risiko

Privatgeräte werden unter Umständen auch von Familienangehörigen oder Freunden genutzt. Was diese mit dem Gerät anstellen oder welchen Cyberrisiken sie sich aussetzen, kann Ihr Unternehmen nicht steuern. Weiteres Problem: Unbefugte dürfen keinen Zugriff auf die Personendaten aus Ihrem Unternehmen haben. Auch das wäre eine meldepflichtige Datenpanne.

Risiko Nr. 7: Bestimmte Daten oder Personengruppen wären aussen vor

Auch bei BYOD müsste Ihr Unternehmen weiterhin für bestimmte Daten (etwa Gesundheitsdaten) bzw. Personengruppen Geräte und Software bereitstellen. Sensible Daten oder Informationen im Zusammenhang mit Beschäftigten haben nichts auf Privatgeräten verloren.



Nutzen Sie Merkblätter, um den Datenschutz vorwärtszubringen

Datenschutz im Unternehmen klappt dann am besten, wenn die Beschäftigten gut Bescheid wissen. Ist bekannt, worauf es ankommt, wird manches Datenschutzproblem erst gar nicht entstehen. Merkblätter können hier viel bringen. Und kommen auch Ihnen als Datenschutzberater zugute. Denn was Sie nicht beraten oder beantworten müssen, nimmt keine wertvolle Zeit in Anspruch.

Machen Sie sich das Leben leichter

Vielleicht denken Sie jetzt, dass Sie keine Zeit zum Erstellen von Merkblättern haben. Doch das sollten Sie sich zweimal überlegen. Denn: Viele, gerade oft gestellte Fragen können sich erübrigen, wenn Mitarbeiter sich diese selbst beantworten können. Insofern ist Ihre Zeit in die Erstellung von Merkblättern für die Kollegen gut investiert.

Setzen Sie auf das Prinzip „Hilfe zur Selbsthilfe“

Bedenken Sie stets: Nicht jeder traut sich, sich bei Fragen direkt an Sie zu wenden. Zwar sollte es hier keine Berührungsängste geben. Die Realität sieht manchmal etwas anders aus. Um auch „Schüchterne“ mit Wissen zu versorgen, sollten Sie dieser Zielgruppe ermöglichen, dass sie sich zunächst selbst hilft. Gerade wenn einem Fragen oder die eigene Unwissenheit peinlich sind, sind Merkblätter ein erster Anlaufpunkt für wichtige Informationen.

Beherzigen Sie diese Tipps

Einfach mal ein Merkblatt erstellen klingt nach einer Sache, die sich im Handumdrehen erledigen lässt. Ob Ihnen damit aber direkt der grosse Wurf gelingt, ist jedoch nicht ausgemacht. Gehen Sie lieber auf Nummer sicher. Wollen Sie Merkblätter erstellen, sollten Sie die folgenden Tipps umsetzen:

Tipp Nr. 1: Ermitteln Sie den Bedarf und sammeln Sie Themen

Am besten starten Sie zunächst mit einem Brainstorming. Notieren Sie, welche Fragen Ihnen immer wieder gestellt werden. Schreiben Sie Ihre Einfälle zur Frage „Was klappt oft nicht oder geht schief?“ auf. Überlegen Sie zudem, bei welchen Themen Sie immer wieder viel Beratungsaufwand haben.

Tipp Nr. 2: Setzen Sie Prioritäten

Priorisieren Sie vor allem unter den Aspekten „Wichtig und dringend“ oder „Was bringt mir die grösste Arbeitserleichterung?“. Schliesslich müssen Sie zum Start nicht alle Merkblätter zur Verfügung stellen. Es ist schlauer, wenn Sie diese nach und nach veröffentlichen. Das erhöht den Effekt des „Neuen“ und macht die Beschäftigten neugierig.

Überprüfen Sie immer wieder Ihre Priorisierung. Unter Umständen stellen Sie zwischendurch fest, dass ein zunächst weniger wichtiges Thema nun doch erheblich an Relevanz gewonnen hat.

Tipp Nr. 3: Machen Sie sich Synergien zunutze

Sprechen Sie frühzeitig mit zwei Abteilungen, nämlich der IT- und der Personalabteilung. Klären Sie ab, inwieweit es dort Materialien oder Merkblätter gibt, auf denen Sie aufsetzen können. Eventuell können Sie auch Vorlagen nutzen. Denn klar ist: Warum das Rad neu erfinden, wenn es schon vorhanden ist?

Tipp Nr. 4: Sprechen Sie mit dem Marketing

Dieses Gespräch ist wichtig, weil Sie sich unter Umständen viel Arbeit sparen können. Eventuell kann man Ihnen Designvorlagen zur Verfügung stellen, die Sie nur noch befüllen müssen. Das ist gerade dann wichtig, wenn Sie mit Office- oder Layout-Programmen nicht so vertraut sind. Schliesslich ist wichtig: Auch Merkblätter sollten optisch etwas hermachen. Haben Sie grosses Glück, übernimmt man die eine oder andere Arbeit für Sie. Und das schafft wieder Freiräume für Sie, um andere Dinge zu erledigen.

Tipp Nr. 5: Beschränken Sie sich bei Inhalten auf das Wesentliche

Bedenken Sie: Ein Merkblatt soll einen schnellen Überblick über das Wesentliche geben. Es ist gerade keine „Gebrauchsanleitung“ und kein Leitfaden, der alle Aspekte abdecken soll. Daher: Setzen Sie sich eine Obergrenze. Beschränken Sie sich auf ein Blatt Papier, sprich Vorder- und Rückseite im Format DIN A4. Wählen Sie zudem eine gut lesbare Schrift in angemessener Grösse, etwa Arial, Schriftgrösse 11.

Schon aus Platzgründen müssen Sie sich nun auf das Wesentliche beschränken. Versuchen Sie dennoch, bei allen Merkblättern eine einheitliche Struktur durchzuhalten. Dabei können Sie drei bis fünf Schwerpunkte setzen. Ein Merkblatt zum Thema Phishing könnten Sie folgendermassen strukturieren:

- › Was Sie zu Phishing wissen sollten
- › Beachten Sie unbedingt
- › So handeln Sie richtig
- › Weitere Infos (Regelungen, Links)
- › Kontakt und Ansprechpartner bei Vorfällen

Tipp Nr. 6: Fokussieren Sie sich auf die Zielgruppe

Je nach Zielgruppe sollten Sie besonders die Vorbildung, den Wissensstand und -bedarf der betreffenden Kollegen berücksichtigen. Gehen Sie regelmässig davon aus, dass Sie keine Datenschutzprofis vor sich haben. Verzichteten Sie also auf typische Formulierungen oder Abkürzungen, die nur Datenschutzspezialisten verstehen.

Tipp Nr. 7: Gestalten Sie die Sache ansprechend

Vermeiden Sie Textwüsten. Arbeiten Sie unbedingt mit Zwischenüberschriften oder Aufzählungen. Auch Schritt-für-Schritt-Anleitungen können eine grosse Hilfestellung sein. Um das Lesen zu erleichtern, sollten Sie nicht nur eine ausreichend grosse und gut lesbare Schriftart wählen. Arbeiten Sie ggf. auch mit Spalten. Denn das erleichtert dem Auge das Erfassen des Textes.

Tipp Nr. 8: Machen Sie den Nutzwert-Check

Nur weil Sie ein Merkblatt perfekt finden, muss das den Nutzern noch lange nicht so gehen. Daher: Machen Sie unbedingt den Check vor der Veröffentlichung. Bitten Sie einige spätere Nutzer um kritische Durchsicht. Auch Kollegen aus anderen Abteilungen, z. B. IT-Abteilung, können einen kritischen Blick auf Ihr Merkblatt werfen. So stellen Sie sicher, dass die Sache wirklich rund ist und Sie nach Veröffentlichung nicht gleich ein Update hinterherschieken müssen.

Tipp Nr. 9: Wählen Sie die passende Veröffentlichungsform

Haben Sie eine Intranetseite, sollten Sie dort eine entsprechende Rubrik aufmachen. Halten Sie dort die Merkblätter als PDF bereit.

Probieren Sie immer aus, ob der Download und das Ausdrucken der Merkblätter funktionieren. Um einen entsprechenden Test sollten Sie auch einen Kollegen bitten. So ist sicher, dass alles auch für andere klappt.

Tipp Nr. 10: Informieren Sie geschickt über die Merkblätter

Hier sollten Sie gut überlegen, wie Sie Ihre Merkblätter geschickt in Szene setzen. Haben Sie bereits mehrere Merkblätter, sollten Sie diese nicht alle auf einmal veröffentlichen. Stellen Sie diese beispielsweise im Abstand von zwei bis vier Wochen bereit. Informieren Sie über das neue Merkblatt per E-Mail. Das bringt mehrere Vorteile mit sich: Sie können jedes Mal das Interesse auf den Datenschutz lenken. Zudem erhöhen Sie die Chance, dass sich die Empfänger auch tatsächlich mit Ihrem Thema bzw. dem jeweiligen Merkblatt beschäftigen.

Keine Ideen? Wie wäre es mit diesen Merkblättern?

Vielleicht fragen Sie sich: Über was könnte ich denn informieren oder zu welchen Themen könnte ich ein Merkblatt zur Verfügung stellen? Schauen Sie sich die Vorschläge in der folgenden Checkliste an. Greifen Sie sich einige Vorschläge heraus und setzen Sie diese in den nächsten Monaten um.

Checkliste: Themen für Ihre Merkblätter als Datenschutzberater

Thema, Schwerpunkt	Hintergrund	Umsetzen?
Datenschutzbasics für neue Mitarbeiter	- Stellen Sie die wichtigsten Punkte für neue Mitarbeiter zusammen. - Denken Sie auch an nützliche Links zu Regelungen oder Standards und Kontaktdaten wichtiger Ansprechpartner.	☐ Ja ☐ Nein
Datenschutz am Arbeitsplatz	- Fassen Sie die zu beachtenden Regeln zusammen. Clean Desk und das Sperren des Computers bei Abwesenheit müssen enthalten sein. - Erläutern Sie auch, worauf es bei vertraulichen Gesprächen ankommt.	☐ Ja ☐ Nein
Datenschutz in Homeoffice und auf Reisen	- Auch wenn dieselben Regeln wie im Büro gelten: Geben Sie einen Überblick, was zu beachten ist. - Denken Sie auch an das Entsorgen von Unterlagen. Das geht nicht über den Papiermüll.	☐ Ja ☐ Nein
Schutz vor Phishing & Co.	- Erklären Sie, wie man entsprechende Angriffe erkennt. - Geben Sie Tipps, wie man sich richtig verhält und was im Fall der Fälle zu tun ist.	☐ Ja ☐ Nein
Richtiges Verhalten bei Datenpannen	- Ursachen für Datenpannen kann es viele geben. Immer gilt: schnell und richtig reagieren. - Geben Sie die entsprechenden Schritte vor. Nennen Sie wichtige Ansprechpartner.	☐ Ja ☐ Nein
Einsatz von IT-Dienstleistern	- Auch hier muss viel beachtet werden, gerade im Datenschutz. - Meist ist nicht nur Auftragsbearbeitung ein wichtiges Thema.	☐ Ja ☐ Nein
Wichtige To-dos bei neuen Bearbeitungen	- Nicht jedem ist klar, dass hier auch der Datenschutz eine Rolle spielt und Sie einzubeziehen sind. - Geben Sie einen kurzen Leitfaden an die Hand.	☐ Ja ☐ Nein
Datenschutzfreundliche Nutzung von KI	- Erklären Sie, was Personendaten sind. Und die sollten bei der Nutzung von KI am besten nicht zum Einsatz kommen. - Geben Sie Tipps zur zulässigen bzw. datensparsamen Nutzung von KI.	☐ Ja ☐ Nein
Umgang mit den Rechten der betroffenen Personen	- Hier gibt es viele Regeln zu beachten. Stellen Sie unbedingt die bei Ihnen geltenden Prozesse vor. Dann geht in Sachen Erfüllung der Rechte nichts schief. - Klären Sie auf, wer einzubinden ist, etwa Sie als Datenschutzberater.	☐ Ja ☐ Nein
Praxistipps: Passwörter und Verschlüsselung	- Hierbei handelt es sich um wichtige Schutzmassnahmen, bei denen viel vom Nutzer abhängt. - Erläutern Sie, worauf es ankommt. Dazu zählt auch das sichere Aufbewahren von Passwörtern, etwa in Passwortmanagern.	☐ Ja ☐ Nein
Datenschutz für Führungskräfte	- Klären Sie einerseits über Besonderheiten zum Umgang mit Beschäftigtendaten auf. - Andererseits sollten Sie die Verantwortung für den Datenschutz verdeutlichen.	☐ Ja ☐ Nein
Umgang mit Fotos und Videos	- Hier wird oft viel falsch gemacht. Geben Sie Tipps, was beim Anfertigen und Veröffentlichen von Fotos und Videos zu beachten ist. - Machen Sie deutlich, dass es oft nur mit Einwilligung geht. Hier gelten besondere Anforderungen.	☐ Ja ☐ Nein
Datenschutzgerechtes Entsorgen	- Setzen Sie hier vor allem einen Schwerpunkt auf das Löschen von Daten und das Entsorgen von elektronischen Datenträgern. Daten dürfen nicht wiederherstellbar sein. - Erklären Sie auch, worauf es beim Entsorgen von Unterlagen ankommt.	☐ Ja ☐ Nein



Mit diesen 5 Tipps finden Sie Verbündete im Datenschutz

Vielleicht kennen Sie das: Anscheinend sind Sie als Datenschutzberater der Einzige im Unternehmen, dem am Thema Datenschutz etwas liegt. Doch auch wenn Sie sich im Stich gelassen fühlen, ist das kein Zustand, den Sie hinnehmen und akzeptieren sollten. Im Gegenteil: Sie können viel dafür tun, damit Ihr Einzelkämpferdasein ein Ende hat.

Ändern Sie Ihr Mindset

Ihr Mindset zu Ihrer Situation, sprich Ihre innere Haltung, sollten Sie als Erstes anpassen. Sagen Sie sich nicht, dass Sie alles allein stemmen müssen. Im Gegenteil: Sie sind als Datenschutzberater nur Teil des Ganzen. Sie beraten und unterstützen bei der Schulung und Anwendung (Art. 10 Abs. 2 Bundesgesetz über den Datenschutz – DSG). Entscheiden müssen Sie nichts und erst recht nichts umsetzen. Das ist Sache des Verantwortlichen, wie sich aus Art. 7 Abs. 1 DSG ergibt. Daraus ergibt sich auch Ihr Hebel: Andere brauchen Sie, um ihrer Verantwortung im Datenschutz gerecht zu werden.

Verbündete finden ist kein Hexenwerk

Von nichts kommt nichts – damit Ihr Einzelkämpferdasein bald ein Ende hat, können Sie auf diese Tipps setzen:

Tipp Nr. 1: Machen Sie zunächst ein Brainstorming

Nehmen Sie sich Zeit und ein grosses Blatt Papier. Überlegen Sie sich relevante Fragen, die Sie sich selbst stellen. Mit ausreichend Zeit zum Nachdenken notieren Sie sich alles, was Ihnen zum jeweiligen Aspekt einfällt. Dabei ist wichtig: Denken Sie auch an Aspekte, die Sie und Ihre Tätigkeit kritisch hinterfragen. Schauen Sie dann im nächsten Schritt, was von Ihren Einfällen besondere Relevanz hat und wie Sie die Sache angehen oder die Situation verbessern können. Impulsfragen können beispielsweise sein:

- Warum habe ich den Eindruck, Einzelkämpfer zu sein?
- Wie werde ich von anderen wahrgenommen?
- Was muss sich bzw. was muss ich ändern?
- Wer verfolgt ähnliche Ziele im Unternehmen wie ich?
- Wer kann mit bei der Erreichung meiner Ziele helfen?

Tipp Nr. 2: Kontaktieren Sie Partner

Auch hier kann ein Brainstorming sinnvoll sein. Denn unter Umständen ist Ihnen nicht klar, wer alles als Partner infrage kommt. Denn nicht alle sind auf den ersten Blick naheliegend. Typischerweise in Betracht kommen Abteilungen und Kollegen, die viel mit Personendaten zu tun haben. So sollten Sie unbedingt die IT-Abteilung auf Ihrer Liste haben. Diese muss nämlich nicht einfach nur (Personen-) Daten bearbeiten. Sie hat auch ein grosses Interesse an IT-Sicherheit. Die entsprechenden Massnahmen sind auch oft im Interesse des Datenschutzes, sprich im Hinblick auf den Schutz der Bearbeitung nach Art. 8 DSG.

Denken Sie aber auch an andere Kontrollorgane im Unternehmen. Gibt es etwa einen Compliance Officer oder eine Unternehmens-

revision, verfolgt man auch dort das gleiche Grundinteresse wie Sie: Gesetze und interne Vorschriften müssen eingehalten werden, und zwar ohne Ausnahme. Daneben kann auch die Rechtsabteilung wichtige Partner für Sie bereithalten.

Gehen Sie auf diese Stellen aktiv zu. Vereinbaren Sie Termine zum persönlichen Kennenlernen bzw. zum Austausch. In aller Regel stellt sich dann schnell heraus, wo man gemeinsame Sache machen kann. Das gilt gerade für gemeinsame Aktivitäten, etwa Prüfungen oder Awarenessmassnahmen.

Tipp Nr. 3: Vermarkten Sie den Datenschutz positiv

Achten Sie immer darauf, dass Sie die Dinge positiv darstellen. Selbst wenn bei einer Beratung herauskommt, dass das Ange-dachte datenschutzrechtlich nicht zulässig ist, können Sie aufzeigen, wie man es doch noch hinkommt. Nimmt man Sie als Möglichmacher, sprich Enabler, wahr, sind Sie ein gern gesehener Gesprächspartner und Berater im Datenschutz.

Daneben sollten Sie stets darauf achten, dass Sie den Nutzen des Datenschutzes herausstellen. Natürlich kosten Schutzmassnahmen Geld. Doch das ist gut investiert, wenn dadurch noch grösserer finanzieller Schaden vermieden wird.

Tipp Nr. 4: Bieten und nehmen Sie Hilfe an

Sie kennen die Weisheit „Eine Hand wäscht die andere“? Die sollten Sie aber nicht negativ verstehen. Vielmehr geht es um „Hilfst du mir, dann helfe ich dir“. Unterstützen Sie einerseits die Kollegen im Datenschutz durch gute Tipps. Stehen Sie zudem mit Rat und Tat zur Seite. Geben Sie Hilfestellung, wo immer das möglich ist.

Doch auch ausserhalb des Datenschutzes sollten Sie auf gegenseitige Hilfe setzen. Bestimmt haben Sie Know-how, was anderen im Unternehmen nutzt. Können Sie jemandem unter die Arme greifen, wird er sich revanchieren. Bietet man Ihnen Hilfe an, sollten Sie diese auch annehmen.

Tipp Nr. 5: Steigern Sie Ihren Bekanntheitswert

Unterschätzen Sie nicht, was Sympathie ausmachen und bewegen kann. Doch Sympathie baut sich nicht von selbst auf. Einerseits ist wichtig, dass Ihre Kollegen ein positives Bild von Ihnen haben. Andererseits ist unerlässlich, dass Sie den Kollegen die Chance geben, Sie kennenzulernen. Daher ist wichtig: Nehmen Sie jede Gelegenheit wahr, um mit den Kollegen ins Gespräch zu kommen. Lassen Sie nichts aus, wo man sich in lockerer Runde kennenlernen kann.

Dürfen wir echte Kundendaten für Testzwecke einsetzen?

FRAGE: Das neue Kundenmanagementsystem soll ausgiebig getestet werden, bevor es zum Einsatz kommt. Dazu will man Echtdaten verwenden, etwa Kundendatensätze. Wie schätzen Sie das ein? Dürfen wir tatsächlich Echtdaten für Testzwecke verwenden?

ANTWORT: Geht es um das Bearbeiten von Personendaten, müssen bei jeder Bearbeitung die Grundsätze der Bearbeitung aus Art. 6 Bundesgesetz über den Datenschutz (DSG) umgesetzt werden. In diesem Zusammenhang gilt insbesondere:

- **Rechtsgrundlage ist erforderlich:** Will Ihr Unternehmen Personendaten bearbeiten, braucht es eine Bearbeitungserlaubnis, sprich eine Rechtsgrundlage. Diese Voraussetzung ergibt sich aus Art. 6 Abs. 1 und 31 DSG. Typisch ist etwa die Bearbeitung zur Durchführung eines Vertrags, auf Basis eines überwiegenden berechtigten Interesses oder auf Grundlage einer wirksamen Einwilligung des Betroffenen.
- **Zwecke sind nichts Beliebiges:** Schon bei der Beschaffung muss der Zweck festgelegt sein. Zudem muss er für die betroffene Person erkennbar sein. Die weitere Bearbeitung der Daten muss mit diesem Zweck vereinbar sein (Art. 6 Abs. 3 DSG). Eine Zweckänderung ist nicht generell ausgeschlossen. Das DSG enthält jedoch keinen Kriterienkatalog zur Kompatibilitätsprüfung. Bei privaten Unternehmen braucht eine unvereinbare Zweckänderung einen Rechtfertigungsgrund nach Art. 31 DSG: die Einwilligung der Betroffenen, ein überwiegendes privates oder öffentliches Interesse oder Gesetz.

Zweckänderung in Ihrem Fall problematisch

In Ihrem Fall sollen Echtdaten, sprich Personendaten von realen Kunden, für Testzwecke verwendet werden. Der Zweck der ursprünglichen Bearbeitung bestand in der Anbahnung bzw. Durch-

führung der Kunden- und Vertragsbeziehung mit der betreffenden Person. Dieser Zweck dürfte so auch den Betroffenen mitgeteilt worden sein. Von einer Verwendung der Daten für den weiteren Zweck „Test eines Kundensystems“ war bestimmt nie die Rede. Zudem erwartet auch kein Betroffener, wenn er etwa einen Kauf tätigt, dass seine Personendaten für Testzwecke verwendet werden.

Anonymisieren ist denkbar

Zwar könnten Sie daran denken, die Echtdaten zu anonymisieren, damit Sie so nicht mehr auf eine konkrete Person beziehbare Daten für Testzwecke zu erhalten. Doch oft steckt beim Anonymisieren der Teufel im Detail. Es muss nämlich sichergestellt sein, dass keine Verbindung zu einer bestimmten oder bestimmbar natürlichen Person mehr möglich ist. Übrigens: Das Entfernen oder Verändern des Namens oder einer Kundennummer reicht in der Regel nicht aus. Der Bezug lässt sich meist auch aus dem Kontext herstellen, etwa zu Bestellungen oder zur Korrespondenz mit dem Kunden.

Im Ergebnis können wirksam anonymisierte Kundendaten für Testzwecke verwendet werden; sie fallen nicht mehr unter das DSG. Die Anonymisierung selbst muss jedoch datenschutzkonform erfolgen. Aufwand und Kosten können hoch sein. Besser kann es daher sein, beim Anbieter des Systems um Testdatensätze fiktiver Personen zu bitten. Auch diese können um Besonderheiten Ihres Unternehmens ergänzt werden.

Wer muss die Datenpanne der Arbeitnehmervertretung melden?

FRAGE: Die Arbeitnehmervertretung hat eine E-Mail mit sensiblem Inhalt an den falschen Empfänger geschickt. Das ist passiert, weil man im E-Mail-Programm die automatische Vervollständigung der E-Mail-Adresse nutzte. Wer muss diese Panne dem EDÖB melden?

ANTWORT: Prüfen Sie zunächst, ob es sich überhaupt um einen meldepflichtigen Vorgang handelt. Kommen Sie dabei zum Ergebnis, dass kein hohes Risiko für die betroffene Person, kann ggf. eine Meldung unterbleiben.

Kommen Sie jedoch zu dem Schluss, dass im konkreten Fall ein hohes Risiko besteht, ist eine Meldung ggf. unumgänglich. Prüfen Sie dazu die Ausführungen des EDÖB als Datenschutzaufsichts-

behörde. Dieser gibt Hilfestellung bei der Bewertung der Meldepflichtigkeit.

Das Unternehmen als Verantwortlicher ist meldepflichtig, egal wer die Panne verursacht hat. Die Arbeitnehmervertretung ist Teil des Unternehmens, zu dem sie eben gehört. Das Unternehmen verantwortet auch die Bearbeitungen der Arbeitnehmervertretung, die sie zur Wahrnehmung seiner Aufgaben vornimmt.



E-Mail-Rechnungen müssen nicht verschlüsselt werden

Die Datenschutz-Grundverordnung (DSGVO) fordert von Verantwortlichen, dass sie angemessene Schutzmassnahmen zur Gewährleistung der Sicherheit ergreifen. Doch geht das so weit, dass man generell auch E-Mails mit Rechnungen verschlüsseln muss? Nein, meint das Landgericht (LG) Karlsruhe in Deutschland in einem Urteil vom 20.5.2026 (Az. 8 O 266/25).

Das führte zum Rechtsstreit

Ein Ehepaar, die späteren Kläger, beauftragte einen Bekannten damit, bei einem Unternehmen, dem späteren Beklagten, Goldbarren zu kaufen. Der Wert der Barren lag bei rund 109.000 €. Der Bekannte einigte sich mit dem Unternehmen auf den Kauf. Danach gab er eine E-Mail-Adresse der Kläger an, an die die Rechnungen geschickt werden sollten.

Nun passierte Folgendes: Das Ehepaar erhielt tatsächlich mehrere Rechnungen, anscheinend vom Händler. Allerdings waren diese manipuliert. Die Kontodaten für die Überweisung des Geldes waren verändert worden. Das Ehepaar überwies das Geld und informierte das Unternehmen. Das bedankte sich. Allerdings konnte es keinen Zahlungseingang auf seinem Konto feststellen. Also lieferte es die Goldbarren nicht.

Ehepaar fordert echte Rechnungen an

Das Ehepaar meldete sich dann per E-Mail beim Unternehmen. Es teilte mit, dass man die Polizei eingeschaltet hätte. Wahrscheinlich hätten Kriminelle die Rechnung abgegriffen und manipuliert. Zudem baten sie um Originalrechnungen, die per Post an ihre in der E-Mail mitgeteilte Anschrift geschickt werden sollten. Diese Rechnungen enthielten die richtige Bankverbindung des Unternehmens bei einer Sparkasse.

Wer tatsächlicher Absender der E-Mails mit den manipulierten Rechnungen war, blieb insgesamt unklar, zumal auch das Ehepaar nicht mehr die ganze E-Mail mit den Angaben des E-Mail-Headers vorlegen konnte.

Kläger sehen keinen Fehler bei sich

Das Ehepaar beauftragte einen Anwalt. Und der klagte vor dem LG. Aus Klägersicht hätten die Kläger nichts falsch gemacht. Die Rechnungen seien unauffällig gewesen. Dass eine Manipulation erfolgt sei, müsse sich das Unternehmen zurechnen lassen. Dieses hätte die entsprechenden Rechnungen nur verschlüsselt verschicken dürfen. Also forderte der Anwalt die Lieferung der Barren. Hilfsweise forderte er Schadensersatz – in Höhe der falsch getätigten Zahlung. Das LG sah weder die Voraussetzungen für das eine noch das andere gegeben. Es wies die Klage des Ehepaars ab.

So entschied das Gericht

Für das Gericht besteht für das Ehepaar kein Anspruch auf Lieferung der gekauften Goldbarren. Auch besteht kein Anspruch auf Schadensersatz wegen der Überweisung auf das falsche Konto.

Mit der Zahlung auf das falsche Konto ist keine Erfüllung der Zahlungspflicht eingetreten. Insofern ist das Ehepaar weiterhin zur Zahlung des Kaufpreises verpflichtet. Dass das Unternehmen die Manipulation der Rechnungen zu vertreten hat, stellt nur eine unbelegte Behauptung der Kläger dar. Insbesondere konnten diese nicht die vollständige E-Mail mitsamt E-Mail-Header vorlegen. Insofern konnten die Kläger nicht konkret darlegen, wer Absender der E-Mail war.

Es gibt keinen Schadensersatz

Ein solcher Anspruch ergibt sich gerade nicht aus der Verletzung einer kaufvertraglichen Nebenpflicht. Dazu hätten die Kläger darlegen und beweisen müssen, dass das Unternehmen eine Pflicht verletzt hätte. Eine Pflicht, Rechnungen per Ende-zu-Ende-Verschlüsselung zu verschicken, besteht gerade nicht. Insbesondere hätten die Kläger im Vorfeld des Kaufs gerade nicht zu erkennen gegeben, dass sie eine entsprechende Sicherheitserwartung hätten.

Art. 82 DSGVO greift nicht

Es besteht kein entsprechender Schadensersatzanspruch. Hierfür hätte es einen Verstoß gegen die DSGVO, das Vorliegen eines Schadens sowie einen Ursachenzusammenhang zwischen beidem geben müssen.

Schon am Verstoß bestehen Zweifel. Es wurden nämlich nicht die Daten der Kläger verändert, sondern die des Unternehmens. Bei diesen Daten handelt es sich auch nicht um personenbezogene Daten. Im Übrigen hat das Unternehmen keine Pflichten verletzt. Eine Ende-zu-Ende-Verschlüsselung ist nach der DSGVO nicht vorgeschrieben. Im Übrigen entspricht sie auch nicht den Sicherheitsanforderungen des Geschäftsverkehrs beim E-Mail-Versand von Rechnungen. Erst recht spielt ein Rechnungsbetrag keine Rolle.

§

Diesen Schluss können Sie ziehen

Auch in der Schweiz besteht keine generelle Pflicht, Rechnungen per E-Mail mit Ende-zu-Ende-Verschlüsselung zu versenden. Ihr Unternehmen muss nach Art. 8 DSG eine dem Risiko angemessene Datensicherheit gewährleisten. Massgeblich sind Inhalt einer E-Mail und mögliche Schäden. Auch vereinbarte Sicherheitsanforderungen spielen eine Rolle. Je nach Sensibilität der Daten und Risiko können deshalb weitergehende Schutzmassnahmen erforderlich sein.

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

Erstellt für Schweizer Datenschutzberater
und für alle mit Aufgaben im Datenschutz
in der Schweiz von:



Telefon: +49 2 28 95 50 150

Fax: +49 2 28 36 96 480

E-Mail: kundendienst@privacyxperts.de

Internet: kurzlink.ch/privacy

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

Vorschau:

Neue Mitarbeiter:
Setzen Sie auf die Führungskräfte
Nutzen Sie Merkblätter,
um den Datenschutz vorwärtszubringen