



NEUE MITARBEITER: SETZEN SIE AUF DIE FÜHRUNGSKRÄFTE

KNOW-HOW

Nutzen Sie Merkblätter,
um den Datenschutz
vorwärtszubringen

4–5

DATENSCHUTZBEAUF- TRAGTER

Sie sind garantiert
qualifiziert! Aber können
Sie das belegen?

6



Onlinebereich:
<https://www.privacyxperts.de>



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



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

Datenschutzorganisation

Neue Mitarbeiter: Setzen Sie auf die Führungskräfte

Seiten 1–2

Schauen Sie bei der Datenverfügbarkeit genauer hin

Seiten 3

Know-how

Nutzen Sie Merkblätter, um den Datenschutz vorwärtszubringen

Seiten 4–5

Datenschutzbeauftragter

Sie sind garantiert qualifiziert! Aber können Sie das belegen?

Seite 6

Fragen an die Redaktion

Braucht unser Newsletter eigene Datenschutzhinweise?

Seite 7

Ist eine etwas zu lange Videoaufzeichnung vertretbar?

Seite 7

Recht

E-Mail-Rechnungen müssen nicht verschlüsselt werden

Seite 8



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



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



E-Mail-Beratung:
<https://t1p.de/andreas-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 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 | Daniel Ernst; Seite 1: Adobe
Stock | contrastwerkstatt
Erscheinungsweise: 36-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 Datenschutzbeauftragter 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 Datenschutzbeauftragter 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 personenbezogenen Daten erteilen. Das ergibt sich aus dem Weisungsrecht des Arbeitgebers nach § 106 Gewerbeordnung. 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 personenbezogenen Daten 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 personenbezogene Daten 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 personenbezogenen Daten“. 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 Datenschutzbeauftragten 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 Verarbeitung 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 personenbezogenen Daten 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 Datenschutzbeauftragten. Ich stehe Ihnen mit Rat und Tat zur Seite. Und das natürlich ganz vertraulich.

Ich danke Ihnen für Ihre Unterstützung!

Ihr Hanns Solo

Datenschutzbeauftragter

Schauen Sie bei der Datenverfügbarkeit genauer hin

Daten sind der Treibstoff für den Motor Ihres Unternehmens. Doch wenn Daten nicht mehr verfügbar sind, passiert das Gleiche wie bei einem Verbrennungsmotor: Erst kommt es zum Stottern und dann bleibt er stehen. Umso wichtiger ist für Ihr Unternehmen, dass es dafür sorgt, dass (personenbezogene) Daten stets verfügbar sind.

Verfügbarkeit dient der Sicherheit der Verarbeitung

Schauen Sie in Art. 32 Abs. 1 Datenschutz-Grundverordnung (DSGVO), finden Sie dort die Sicherheitsziele. Eines ist, dass Ihr Unternehmen dafür sorgen muss, dass personenbezogene Daten verfügbar sind, um diese bei einem physischen oder technischen

Zwischenfall schnell wiederherzustellen. Typisch sind hier ausreichend dimensionierte Technik, Redundanzsysteme und Datenspiegelungen in RAID-Systemen. Doch gerade kleinere Unternehmen werden vor allem auf Back-ups setzen. Wie es um die Datenverfügbarkeit in Ihrem Unternehmen steht, können Sie in einem Beratungsgespräch herausfinden. Setzen Sie auf diese Checkliste:

Checkliste: Wichtige Aspekte bei Datenverfügbarkeit und Back-up



Aspekt	Darauf kommt es an	In Ordnung?
Inwieweit sind personenbezogene Daten betroffen?	➤ Geht es auch um personenbezogene Daten, greifen insbesondere die Vorgaben der DSGVO. ➤ Besonders relevant sind die Festlegungen des Art. 32 DSGVO. Zu den Schutzziele zählt auch das Sicherstellen der Verfügbarkeit von personenbezogenen Daten.	☐ Ja ☐ Nein
Gibt es einen Überblick bzw. eine Bewertung dazu, welche Daten wie verfügbar sein müssen?	➤ Eine solche Bewertung ist unerlässlich. Schließlich ist sie Ausgangspunkt für alles Weitere, etwa zu Datenspiegelungen und Back-ups, zu Wiederherstellungsprozessen oder tolerablen Ausfall- bzw. Wiederherstellungszeiten. ➤ Nicht alle Daten sind gleich sicherungswürdig. Klar ist jedoch: Je verfügbarer Daten sein müssen, desto mehr Aufwand muss bezüglich Redundanzsystemen oder Back-ups getrieben werden.	☐ Ja ☐ Nein
Welche Prozesse greifen, wenn Daten nicht verfügbar sind?	➤ Es sollte klare Vorgaben geben, wie etwa Notfallpläne, Prozessbeschreibungen und Checklisten. ➤ Hinterfragen Sie, inwieweit das Funktionieren der Festlegungen getestet wurde. Nur wenn das passiert ist, ist wahrscheinlich, dass alles auch im Fall der Fälle klappt.	☐ Ja ☐ Nein
Gibt es eine Risikoanalyse?	➤ Insbesondere die Schutzmaßnahmen nach Art 32 DSGVO müssen risikoangemessen sein. ➤ Grundlegendes Vorgehen: Gefahren identifizieren, möglichen Schaden und Eintrittswahrscheinlichkeit abschätzen, Risiken bewerten und mit geeigneten Maßnahmen behandeln.	☐ Ja ☐ Nein
Inwieweit gibt es Datenspiegelungen und Redundanzsysteme?	➤ Gerade wenn es um Hochverfügbarkeit geht, können Datenwiederherstellungen aus Back-ups zu lange dauern. Unter Umständen sind Datenspiegelungen oder Redundanzsysteme die bessere Wahl. ➤ Klären Sie auch den Aspekt der Verfügbarkeit bzw. der Möglichkeit zur Weiterarbeit an einem anderen Standort. Brennt der Hauptstandort ab, ist hier auch eine Weiterarbeit unmöglich.	☐ Ja ☐ Nein
Welche Daten werden auf welche Weise gesichert?	➤ Lassen Sie sich das Vorgehen erläutern. So muss klar werden, welche Daten in welchen Abständen, wie und auf welchen Medien gesichert werden. ➤ Abgedeckt sein sollten auch Betriebssysteme, Software, Datenbanken und Server. ➤ Achten Sie darauf, dass das Ihnen Erläuterte auch zu den Festlegungen in einem Sicherheitskonzept oder Betriebshandbuch passt. ➤ Prüfen Sie zudem: Entsprechen das Vorgehen und die eingesetzten Methoden dem Stand der Technik?	☐ Ja ☐ Nein
Wo werden die gesicherten Daten aufbewahrt?	➤ Besprechen Sie die physische Aufbewahrung von Sicherungen. In einem Gebäude sollte das in unterschiedlichen Brandabschnitten erfolgen. ➤ Bedenken Sie aber auch andere Gefahren, wie Naturereignisse oder einen Wasserschaden. ➤ Haben Sie zudem ein Auge darauf, dass unbefugter Zugriff ausgeschlossen sein muss.	☐ Ja ☐ Nein
Werden bei automatisierten Sicherungen Protokolle ausgewertet?	➤ Automatische Sicherungen bringen den Vorteil, dass nicht vergessen wird, sie durchzuführen. Allerdings kann es dennoch zu Fehlern oder Abbrüchen kommen. ➤ Bringen Sie in Erfahrung, wer wann welche Checks durchführt.	☐ Ja ☐ Nein
Sind Datensicherungen vor Schadprogrammen geschützt?	➤ Die beste Sicherung bringt nichts, wenn Schadprogramme auch dort aktiv werden können. ➤ Klären Sie, wie das verhindert wird, etwa durch eine Trennung der Datenverbindungen.	☐ Ja ☐ Nein
Sind Dienstleister datenschutzkonform eingebunden?	➤ Setzt Ihr Unternehmen auf Services von anderen Unternehmen, etwa Cloud-Angebote, muss ggf. einiges zum Datenschutz bedacht werden. ➤ Häufig liegt eine Auftragsverarbeitung vor, die zu regeln ist. Ist der Anbieter in einem Drittstaat ansässig, kommen die Anforderungen aus Kapitel V der DSGVO hinzu.	☐ Ja ☐ Nein
Wie geht man mit Betroffenenanfragen um?	➤ Legen Sie hier vor allem den Fokus auf das Recht auf Löschung. Grundsätzlich greift das auch bei Datensicherungen. ➤ Lassen Sie sich das Vorgehen erklären. Wird in einer Sicherung nicht gelöscht, muss das zumindest bei der Datenwiederherstellung erfolgen.	☐ Ja ☐ Nein



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 Datenschutzbeauftragtem 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 Datenschutzbeauftragter

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 Auftragsverarbeitung ein wichtiges Thema.	☐ Ja ☐ Nein
Wichtige To-dos bei neuen Verarbeitungen	› 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 personenbezogene Daten 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 Betroffenenrechten	› 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 Datenschutzbeauftragter.	☐ 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



Sie sind garantiert qualifiziert! Aber können Sie das belegen?

Datenschutz ist kein Thema, das man sich mal eben anlesen kann. Gerade für die Aufgaben des Datenschutzbeauftragten braucht es vor allem Qualifikation und Know-how. Doch einfach mal behaupten, dass man qualifiziert sei, kann im Einzelfall nicht ausreichen, etwa wenn die Aufsichtsbehörde nachfragt. Gut, wenn Sie dann eine Übersicht aus der Schublade ziehen können.

Das fordert die DSGVO

Braucht ein Verantwortlicher einen Datenschutzbeauftragten, etwa weil die Voraussetzungen nach Art. 37 Abs. 1 Datenschutz-Grundverordnung (DSGVO) oder nach § 38 Bundesdatenschutzgesetz (BDSG) erfüllt sind, gilt: Das kann nicht einfach jeder Beschäftigte machen, der nicht bei drei auf den Bäumen ist.

Der Verantwortliche muss bei der Auswahl Folgendes beachten:

- › berufliche Qualifikation,
- › Fachwissen in Datenschutzrecht und Datenschutzpraxis,
- › Fähigkeit zur Erfüllung der Aufgaben nach Art. 39 Abs. 1 DSGVO.

Jemand mit der nötigen Qualifikation zum Datenschutzbeauftragten zu benennen dient aber nicht nur dazu, den gesetzlichen Anforderungen gerecht zu werden. Das ist auch Teil der Risikoversorge Ihres Unternehmens.

Ihre Qualifikation sollte belegbar sein

Zwar gibt es nach der DSGVO keine speziellen Festlegungen, wonach Ihre Qualifikation nachweisbar sein müssen. Das kann schnell anders sein, wenn Ihr Unternehmen auditiert wird und der Auditor Ihre Qualifikation genauer unter die Lupe nimmt.

Dokumentieren Sie im eigenen Interesse

Dass es sinnvoll ist, für sich Buch zu führen, liegt auf der Hand. Schließlich ist eine gute Dokumentation in Ihrem eigenen Interesse. So können Sie gegenüber der Unternehmensleitung demonstrieren, dass Sie hoch qualifiziert und spezialisiert sind.

Das kann hilfreich sein, wenn es einmal um die Frage geht, ob Ihr Unternehmen Sie als Datenschutzbeauftragten noch braucht, etwa wenn die deutschen Benennungspflichten nach § 38 Abs. 1 BDSG entfallen.

Daneben beugen Sie dem Vergessen vor. Denn Sie bauen tagtäglich Wissen und praktische Erfahrungen bei den Beteiligten auf, etwa wenn Sie zu einer komplexen Verarbeitung beraten. Auch was Sie sich selbst aneignen, ist Wissen, das Sie sich selbst bestätigen können.

Gehen Sie pragmatisch vor

Um Ihre Qualifikation und Ihr Wissen zu dokumentieren, sollten Sie wie folgt vorgehen:

Sammeln Sie Nachweise

- › Warten Sie nicht zu lange mit dem Dokumentieren. Am besten dokumentieren Sie den Wissenserwerb direkt nach Abschluss einer Aktivität.
- › Nehmen Sie an Veranstaltungen teil, bewahren Sie Teilnahmebestätigungen, Zertifikate und ggf. auch Rechnungen auf.
- › Bietet der Veranstalter keinen Nachweis von sich aus an, können Sie um die Ausstellung einer Teilnahmebestätigung bitten. Machen Sie das zeitnah.
- › Existiert keine Teilnahmebestätigung, etwa bei kostenlosen Webinaren, sichern Sie sich die Einladung bzw. die Veranstaltungsinformationen oder bereitgestellte Unterlagen.

Notieren Sie jeden Wissensaufbau

- › Halten Sie fest, wenn Sie sich etwa im Zusammenhang mit Beratungen mit bestimmten Themen besonders intensiv auseinandergesetzt haben.
- › Schreiben Sie nicht nur auf, mit was Sie sich beschäftigt haben. Schätzen Sie zudem den zeitlichen Umfang Ihrer Weiterbildung.
- › Auch Soft Skills können Sie dokumentieren. Die sind auch wichtig, um die Aufgaben des Datenschutzbeauftragten gut wahrnehmen zu können.
- › Nutzen Sie beispielsweise eine Tabelle und listen Sie alle relevanten Aktivitäten auf.

Beispiel: Dokumentation Ihrer Qualifikation



Datum	Maßnahme	Schwerpunkte	Art	Dauer	Nachweis?
17.8.2026	Update Datenschutzrecht	› aktuelle rechtliche Entwicklungen im Datenschutz › aktuelle Rechtsprechung	Externe Weiterbildung	8 h	Teilnahmezertifikat
26.8.2026	Teilnahme Redaktionssprechstunde live, „Datenschutz aktuell“	› Audits › Teilnehmerfragen	Webkonferenz	1 h	Terminankündigung
7.9. bis 9.9.2026	Rechtsrecherche Auftragsverarbeitung	› Pflichten für Auftragsverarbeiter › Zulässigkeit von Klickverträgen	Selbststudium	4 h	Eigenbestätigung

Braucht unser Newsletter eigene Datenschutzhinweise?

FRAGE: Kürzlich hat sich ein Betroffener bei uns wegen unseres E-Mail-Newsletters beschwert. Wir würden gegen den Datenschutz verstoßen, weil der Newsletter keine Informationen zum Datenschutz enthält. In diesem Zusammenhang fragen wir uns: Braucht unser E-Mail-Newsletter tatsächlich eigene Datenschutzhinweise?

ANTWORT: Egal, ob Ihr Unternehmen die Registrierung für den Newsletter auf der Webseite, in einem Onlineshop oder in einer Smartphone-App anbietet. In der Regel zielt dies auf die Verarbeitung personenbezogener Daten ab, etwa der E-Mail-Adresse und des Namens des Empfängers.

Bei der Erhebung muss informiert werden

Will Ihr Unternehmen personenbezogene Daten verarbeiten, muss es für die erforderliche Transparenz sorgen. Werden die personenbezogenen Daten beim Betroffenen erhoben, müssen die Informationen nach Art. 13 Datenschutz-Grundverordnung (DSGVO) mitgeteilt werden. Und nun kommt das Entscheidende: Die Informationen müssen zum Zeitpunkt der Erhebung der Daten gegeben werden. Der Betroffene muss also vorab wissen können, was mit seinen personenbezogenen Daten passiert. Dadurch wird er in die Lage versetzt, sich für oder gegen eine Verarbeitung seiner Daten zu entscheiden.

Einmalige Information reicht aus

Die DSGVO sieht keine mehrmalige Information des Betroffenen vor. Es reicht die Information zum Zeitpunkt der Erhebung aus. Das hat für Ihren Fall zur Folge, dass bei der Registrierung für den Newsletter die Möglichkeit zur Kenntnisnahme der relevanten Informationen gegeben werden muss. Dazu kann beispielsweise ein Link zu den Datenschutzhinweisen gesetzt werden. Über diesen werden dem Betroffenen die nötigen Informationen bereitgestellt.

Im Ergebnis besteht also keine Pflicht, im Newsletter selbst Datenschutzhinweise zu integrieren. Allerdings kann es aus pragmatischen Gründen sinnvoll sein, neben einer Abmeldemöglichkeit auch einen Link zu den Datenschutzhinweisen Ihres Unternehmens aufzunehmen. Eventuell kommt es dann gar nicht zu Anfragen von Betroffenen, weil sie den Umgang mit den personenbezogenen Daten jederzeit über die Datenschutzhinweise nachvollziehen können.

Ist eine etwas zu lange Videoaufzeichnung vertretbar?

FRAGE: Ich betreue ein kleines Unternehmen. Weil es schon Diebstähle im Ladengeschäft gab, kommt dort eine Videoüberwachung zum Einsatz. Die ist schon etwas betagt. Auf den Datenspeicher passen Bilddaten für ca. vier Tage. Ist der Speicher voll, werden die ältesten Aufnahmen überschrieben. Von den Aufsichtsbehörden wird eine Aufzeichnungsdauer von 72 Stunden, sprich drei Tage, meist problemlos akzeptiert. Die alte Anlage speichert also eigentlich etwas zu lange. Ist das dennoch irgendwie vertretbar?

ANTWORT: Unter Umständen wird von der zuständigen Aufsichtsbehörde auch eine viertägige Speicherdauer akzeptiert bzw. toleriert. Will man hier auf der sicheren Seite sein, kann sich die Nachfrage bei der Aufsichtsbehörde lohnen.

Grundsätzlich müssen diejenigen technischen und organisatorischen Maßnahmen ergriffen werden, damit eine Verarbeitung im Einklang mit der Datenschutz-Grundverordnung steht (Art. 24 Abs. 1 DSGVO). In Betracht zu ziehen sind solche Maßnahmen, die entweder für eine kürzere Speicherdauer sorgen oder eine erhöhte Beeinträchtigung des Persönlichkeitsrechts auf andere Weise kompensieren. Denken Sie also beispielsweise an folgende Möglichkeiten:

- Eine Festplatte kann ggf. durch eine kleinere Festplatte ersetzt werden, sodass schlichtweg weniger gespeichert werden kann.
- Eventuell lassen sich in der genutzten Software Parameter so ändern, dass die Festplatte schneller voll ist, etwa weil Daten weniger komprimiert werden. Ggf. lässt sich die Speicherdauer auch generell reduzieren.
- Organisatorisch kommen strenge Zugriffsbeschränkungen in Betracht, sodass ein Zugriff auf die Daten nur bei Vorliegen bestimmter Voraussetzungen möglich ist. Zudem kann das Unternehmen auch ein manuelles Löschen in Erwägung ziehen. Letzteres muss jedoch auch tatsächlich passieren. Stellen Sie das sicher.

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 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 Sicherheitserwartungen des Geschäftsverkehrs beim E-Mail-Versand von Rechnungen. Erst recht spielt ein Rechnungsbetrag keine Rolle.

§

Diesen Schluss können Sie ziehen

Es gibt keine generelle Pflicht, E-Mails mit Rechnungen mit Ende-zu-Ende-Verschlüsselung zu verschicken. Grundsätzlich muss ein Verantwortlicher, etwa Ihr Unternehmen, nur risikoangemessene Schutzmaßnahmen ergreifen. Im Übrigen sind die Sicherheitserwartungen im Rechts- bzw. Geschäftsverkehr von Bedeutung. Hier hatten weder die Kläger besondere Erwartungen mitgeteilt, noch gibt es die allgemeine Erwartung, dass Rechnungen verschlüsselt verschickt werden.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!

Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter www.privacyxperts.de/shop

**IT- & INFORMATIONSSICHERHEIT UPDATE**

Ihr digitaler Praxisratgeber für mehr Schutz Ihrer betrieblichen Informationen

Schnelles Filtern der News, die Sie brauchen

Aus Fehlern anderer lernen

Praxisnahe (Video-)Anleitungen

Audit-Prüflisten

Schulungsmaterial

Interpretation der Gesetze und Richtlinien

Darum sollten Sie nicht auf das IT- & Informationssicherheit Update verzichten:

- Erhalten Sie alle 2 Wochen News, Praxistipps und Rechtsempfehlungen
- Sicherheitsmaßnahmen messbar machen, dank interaktiver Checklisten
- Arbeitshilfen im Onlinebereich sparen Zeit bei Schulungen, Richtlinien & Co.

Testen Sie das E-Magazin für mehr IT- und Informationssicherheit 1 Monat GRATIS





Innovatives e-Magazin

Cyber-Resilienz

Neu: Mit eigenen Themen

<http://bit.ly/IT-Info-Update>



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:

Kennen Sie sich mit Art. 37 DSGVO aus?

So gelingt guter Datenschutz am Empfang