DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
Schweiz
AUG 2025

WENIGER HOMEOFFICE? GEBEN SIE DEN BESCHÄFTIGTEN DIESE TIPPS AN DIE HAND

Know-how muss nachhaltig sein

Liebe Leserin, lieber Leser,

als Datenschützer stehen Sie tagtäglich vor einer grossen Herausforderung: Man schildert Ihnen ein Problem oder stellt eine Frage und erhofft sich von Ihnen die Lösung bzw. die Antwort. Einfach nur eine Lösung oder Antwort zu präsentieren, erledigt zwar die betreffende Anfrage – allerdings ist das nicht unbedingt nachhaltig.

Besser ist es, wenn Sie Ihre Lösung oder Antwort verständlich erklären, also Know-how vermitteln. Damit erübrigt sich vielleicht manche zukünftige Frage. Schliesslich kann man das Erlernte anwenden. Und das ist auch insofern nachhaltig, weil es Ihre Ressourcen schont.

Viele Grüsse

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Inhalt

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

Online-Premiumbereich: premium.vnr.de/datenschutz-aktuell-schweiz

Bildnachweise:
Titel: Adobe Stock | drubig-photo
Seite 1: Adobe Stock | Thomas Söllner

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: Deinzer Grafik, Gartow
Druck: Warlich Druck Meckenheim GmbH, Meckenheim
Erscheinungsweise: 16-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Helfen Sie dabei, dass die Kollegen sich wieder im Büro zurechtzufinden.

Weniger Homeoffice? Geben Sie den Beschäftigten diese Tipps an die Hand

In vielen Unternehmen war in der Coronapandemie Homeoffice das Mittel der Wahl, um das Infektionsrisiko niedrig und das Unternehmen am Laufen zu halten. Doch inzwischen gibt es einen Trend in vielen Unternehmen. Und der heisst: zurück ins Büro. Egal, ob das Bummeln im Homeoffice unterbunden oder die Zusammenarbeit gefördert werden soll: Bei der Rückkehr ins Büro ist auch der Datenschutz wichtig.

Awareness muss nicht aufwendig sein

Damit es mit dem Schutz von Daten richtigläuft, müssen Sie vor allem eines in Angriff nehmen: Sie müssen die betreffenden Kollegen mit dem nötigen Wissen ausstatten. Doch auch die Sensibilität für richtiges Verhalten in bestimmten Situationen ist ein entscheidender Faktor für gelebten Datenschutz. Geht es für die Mitarbeiter „zurück ins Büro", können Sie beispielsweise eine Information verschicken. Die kann wie in folgendem Muster eine Checkliste enthalten. Oder Sie basteln aus dem Muster eine kurze Präsentation für eine Informationsveranstaltung. Auch das geht ruckzuck.

MUSTER: Checkliste „Zurück ins Büro – Rückkehr aus dem Homeoffice"

Liebe Kollegin, lieber Kollege,

wie Sie bereits wissen, hat die Unternehmensleitung unter Zustimmung des Betriebsrats entschieden, dass ab dem 1.8.2025 Homeoffice zwar weiterhin möglich sein wird. Um insbesondere die Zusammenarbeit und das Wirgefühl zu stärken, soll aber das Arbeiten im Büro wieder zum Standard werden. Gerade wenn Sie in erster Linie im Homeoffice gearbeitet haben, vielleicht auch schon einige Jahre, sollten Sie sich einige wichtige Tipps zu Herzen nehmen. Damit fällt es Ihnen nicht nur leichter, sich wieder im Büro zurechtzufinden. Sie tragen auch dazu bei, dass Sie Pannen & Co. im Datenschutz vermeiden.

Machen Sie jetzt den Selbstcheck
Steht bei Ihnen die Rückkehr an den Büroarbeitsplatz an, sollten Sie sich frühzeitig Gedanken zur zukünftigen Arbeitssituation und dem sich daraus ergebenden Handlungsbedarf machen.

Das ist wichtig	Achten Sie auf diese Punkte	Das trifft zu.
Über die Rahmenbedingungen am Arbeitsplatz weiss ich Bescheid.	› Klären Sie frühzeitig, welche Rahmenbedingungen zukünftig für Sie und Ihre persönliche Arbeitssituation gelten. Prüfen Sie dazu Regelungen und abteilungsspezifische Vorgaben. › Sprechen Sie mit dem Vorgesetzten, falls etwas aus Ihrer Sicht nicht passt oder unter Datenschutzaspekten zum Problem werden kann. Im Gespräch findet sich meist eine Lösung.	☐ Ja ☐ Nein
Ich setze Clean Desk und Clear Screen am Arbeitsplatz um.	› Achten Sie am Schreibtisch darauf, dass dort nichts Schützenswertes herumliegt, wenn Sie abwesend sind. Schliessen Sie alles Schützenswerte weg, was andere nichts angeht. Das umfasst nicht nur Akten und Unterlagen. Auch Notebook, Smartphone oder USB-Sticks sollten Sie auf geeignete Weise schützen. › Sperren Sie Ihren Computer, auch wenn Sie nur kurzfristig den Arbeitsplatz verlassen. Das klappt ganz einfach, indem Sie gleichzeitig die Windows-Taste und L drücken. So stellen Sie sicher, dass erstens niemand unter Ihrem Namen Schindluder treiben kann. Und zweitens können schützenswerte Informationen nicht in falsche Hände geraten.	☐ Ja ☐ Nein

Das ist wichtig	Achten Sie auf diese Punkte	Das trifft zu.
Unbefugte können nicht bei mir auf dem Bildschirm mitlesen.	› Haben Sie ein Auge darauf, wer Ihnen über die Schulter schauen kann. Das ist ggf. ein Problem, wenn Sie mit Sensiblem oder Persönlichem arbeiten. Versuchen Sie, den Bildschirm bzw. Ihren Arbeitsplatz entsprechend auszurichten. › Beschaffen Sie sich ggf. eine abnehmbare Sichtschutzfolie für den Bildschirm. Diese macht es für Unbefugte nahezu unmöglich, von der Seite etwas auf Ihrem Bildschirm zu erkennen.	☐ Ja ☐ Nein
Vertrauliche Gespräche kann ich in geschützter Umgebung führen.	› Nicht alles, was Sie per Telefon oder in einem virtuellen Meeting besprechen, ist auch für die Ohren Dritter bestimmt. Bedenken Sie das stets, wenn Sie Gespräche führen. › Machen Sie sich mit der Situation vor Ort vertraut. Sind entsprechende Gespräche planbar, reservieren Sie sich einen Raum oder eine „Telefonzelle". Alternativ kann auch ein Tag im Homeoffice eine gute Lösung sein. Stimmen Sie sich mit Ihrem Vorgesetzten ab.	☐ Ja ☐ Nein
Ist es möglich, vertraulich zu drucken?	› Drucken Sie ganz normal, kann jeder am Drucker lesen, was Sie gedruckt haben. Eventuell kommt das Gedruckte sogar abhanden, wenn Sie nicht schnell am Drucker sein können. › Ist etwas sensibel, sollten Sie daher auf vertrauliches Drucken setzen. Erst mit Eingabe einer PIN am Drucker wird Ihr Druckauftrag bearbeitet, und zwar in Ihrem Beisein.	☐ Ja ☐ Nein
Ich kann Schützenswertes wegschliessen.	› Damit Clean Desk gut funktioniert, brauchen Sie entsprechende Aufbewahrungsmöglichkeiten. Das Schloss sollte auch wirklichen Schutz bieten und nicht nur Deko sein. Ziehen Sie Schlüssel immer ab. › Haben Sie ein Zahlenschloss, sollten Sie eine PIN wählen, die nicht leicht zu erraten ist, aber die Sie sich gut merken können.	☐ Ja ☐ Nein
Persönliches kann ich sicher aufbewahren.	› Denken Sie hier beispielsweise an die Geldbörse oder den Autoschlüssel. Auch die sollten Sie sicher verstauen können. › Haben Sie keine Möglichkeit, sprechen Sie mit Ihrem Vorgesetzten. Meist findet sich auch für Wechselarbeitsplätze eine gute Lösung, etwa durch abschliessbare Rollcontainer oder Trolleys.	☐ Ja ☐ Nein
Beim Desksharing beweise ich Datenschutzsensibilität.	› Haben Sie stets vor Augen, dass ein entsprechender Arbeitsplatz von einer Vielzahl von Kollegen genutzt werden kann, wenn Sie nicht vor Ort sind. Daher sollten Sie diesen bei Feierabend abräumen und alles Schützenswerte wegschliessen. › Belassen Sie nichts vor Ort, was für Langfinger interessant sein könnte. Jeder entsprechende Verlust ist ärgerlich und meist auch schmerzhaft.	☐ Ja ☐ Nein
Passwörter bewahre ich sicher auf.	› Passwörter müssen sicher sein. Das gilt nicht nur für deren Zusammensetzung, sondern auch für deren Aufbewahrung. Notizzettel oder ein Post-it unter der Tastatur gehen gar nicht. Auch ein Zettel in der unverschlossenen Schublade ist richtig schlecht. › Setzen Sie einen Passwortsafe ein. Diese Software wird Ihnen von der IT-Abteilung gerne zur Verfügung gestellt. Passwörter sind so sicher verwahrt. Vorteil ausserdem: Sie müssen sich nur ein Hauptpasswort merken.	☐ Ja ☐ Nein
Mobile Datenträger sind sicher verstaut.	› Idealerweise haben Sie für sich eine Übersicht, über welche Datenträger Sie verfügen. Bewahren Sie diese immer an derselben Stelle auf und legen Sie diese unverzüglich dorthin zurück, wenn sie nicht gebraucht werden. Das erleichtert es Ihnen, den Überblick zu behalten. › Beugen Sie Datenverlusten vor: Setzen Sie einerseits auf Verschlüsselung und denken Sie auch an ein Back-up.	☐ Ja ☐ Nein
Schützenswertes kann ich datenschutzkonform entsorgen.	› „Ausschuss" mit schützenswerten Informationen darf nicht in die Hände Unbefugter gelangen. Achten Sie daher auf eine sichere Entsorgung. Bei Unklarheiten besprechen Sie sich mit Ihrem Vorgesetzten. › Machen Sie sich mit der Situation vor Ort vertraut, insbesondere dem Standort der nächsten Datenschutztonne. Bringen Sie zu Entsorgendes unverzüglich direkt dorthin und sammeln Sie nichts am Arbeitsplatz.	☐ Ja ☐ Nein
Ich nutze keine private Technik und Software für dienstliche Zwecke.	› Dies kann neben Sicherheitsrisiken auch Lizenzprobleme mit sich bringen. Nutzen Sie stets nur diejenigen Lösungen, die Ihnen bereitgestellt werden. Diese sind geprüft und sicher. › Benötigen Sie etwas für Ihre Arbeit, sprechen Sie mit Ihrer Führungskraft bzw. mit der IT-Abteilung.	☐ Ja ☐ Nein
Ich nehme relevante Informations- und Schulungstermine wahr.	› Machen Sie sich mit dem vertraut, was für Ihre Arbeit wichtig ist. Das ist auch der Datenschutz. Nutzen Sie die im Intranet verfügbaren Selbstlernmedien oder nehmen Sie an Informationsveranstaltungen und Trainings teil. › Haben Sie Fragen zum Datenschutz oder zum situationsangemessenen richtigen Umgang mit Daten, kontaktieren Sie den Datenschutzberater, gern auch per Telefon.	☐ Ja ☐ Nein

Sie haben irgendwo ein Nein angekreuzt? Das zeigt Ihnen, dass es hier Verbesserungsbedarf gibt. Arbeiten Sie daran und setzen Sie die Hinweise um. Stimmen Sie sich ggf. mit Kollegen oder Ihrem Vorgesetzten ab, wie Sie der Anforderung besser gerecht werden können. Bei Fragen können Sie sich auch an mich wenden.

Ihr Datenschutzberater
Pit Schnass

Ein Meeting jagt das nächste? So machen Sie dem Problem den Garaus

Wer kennt das nicht: Der Arbeitstag ist in der heutigen Zeit meist ziemlich durchgetaktet. Da jagt ein Besprechungstermin den nächsten. Und ehe Sie sich versehen, gehen Sie unter. Schnell ist der Überblick verloren, und was wann wie besprochen wurde, können Sie sich kaum noch in Erinnerung rufen. Das kann frustrieren. Aber: Das Problem lässt sich lösen.

Sie brauchen Managementqualitäten

Jeder Datenschutzberater weiss: Um die Aufgaben, etwa das Beraten oder Kontrollieren des Datenschutzes, gut wahrnehmen zu können, braucht es viel fachliches Know-how. Doch das hilft Ihnen auch nur bedingt, wenn Sie das ganze Drumherum nicht im Griff haben. Das gilt auch für das Managen von Terminen und Meetings. Setzen Sie auf diese Tipps.

CHECKLISTE: Meetings schlau managen

Praxistipp	Das können Sie machen	Das mache ich?
Vor dem Meeting		
Bereiten Sie den Tag strukturiert vor.	› Werfen Sie morgens einen Blick in Ihren Kalender. Prüfen Sie, welche Meetings besonders wichtig sind oder bei welchen Sie eine besondere Rolle spielen, etwa weil Sie eingeladen haben. › Entscheiden Sie, welche Termine Prio A haben und einer strategischen Vorbereitung bedürfen. Notieren Sie beispielsweise relevante Aspekte oder Fragen.	☐ Ja ☐ Nein
Planen Sie Puffer ein.	› Müssen Sie Termine an unterschiedlichen Orten wahrnehmen, braucht es seine Zeit, um von A nach B zu kommen. Planen Sie Wegezeiten ein. › Puffer sind auch wichtig, um sich vor einem wichtigen Termin zu sammeln und auf das Thema, das Ziel oder die Teilnehmer einzustellen.	☐ Ja ☐ Nein
Blockieren Sie sich Zeiten für das Reflektieren und die Nachbereitung.	› Oft ist es unerlässlich, dass Sie Termine nachbereiten oder im Zusammenhang mit dem Termin etwas erledigen. Dafür brauchen Sie Zeit. Reservieren Sie sich diese im Kalender. › Sinnvoll kann es sein, dass Sie nach dem Termin mit anderen Teilnehmern sprechen. Das kann nötig sein, um Dinge zu klären oder ein gemeinsames Verständnis zu finden.	☐ Ja ☐ Nein
Legen Sie sich alles zurecht, was Sie für Notizen brauchen.	› Ein Notizblock mit Stift ist immer noch das beste Mittel, um im Termin mitzuschreiben. › Natürlich können Sie auch auf digitale Lösungen setzen. Haben Sie hier jedoch immer auf dem Radar: Aktivieren Sie unbedingt das automatische Speichern. Denken Sie auch daran, dass Sie ggf. den Akku laden müssen.	☐ Ja ☐ Nein
Im Meeting		
Stimmen Sie direkt das Ziel des Termins ab.	› Wenn nicht ohnehin schon klar, sollten Sie kurz klären, warum es den Termin gibt und was das Ziel des Termins ist. › Begrenzen Sie das Besprechungsthema so, dass es zeitlich passt. Geht das nicht, sollte frühzeitig ein Folgetermin festgelegt werden.	☐ Ja ☐ Nein
Kündigen Sie am Anfang an, wenn Sie früher oder pünktlich rausmüssen.	› Haben Sie einen wichtigen Folgetermin, sollten Sie vorab ankündigen, dass Sie nicht bis zum Terminende dabei sein können. › Wenn Sie das Meeting verlassen, verabschieden Sie sich kurz.	☐ Ja ☐ Nein
Schreiben Sie aktiv mit.	› Notieren Sie alles Wesentliche. Besonders wichtig sind Statements oder Entscheidungen. Notieren Sie auch, wer was gesagt hat. › Stellen Sie Fragen, sollten Sie auch diese gemeinsam mit den Antworten notieren.	☐ Ja ☐ Nein
Erstellen Sie ein gemeinsames Ergebnisprotokoll.	› Unter Umständen nehmen alle ein Meeting anders wahr. Daher kann es sinnvoll sein, wenn schon im Termin ein Ergebnisprotokoll erstellt wird. › Gibt es Entscheidungen oder müssen Aufgaben übernommen werden, sollten Sie darauf achten, dass Verantwortliche und Erledigungstermine klar benannt sind.	☐ Ja ☐ Nein
Nach dem Meeting		
Ergänzen Sie Ihre Notizen.	› Eventuell wollten Sie manches nicht im Termin notieren, weil die Nachbarn mitlesen könnten. Holen Sie solche Notizen unverzüglich nach. › Notieren Sie auch Eindrücke zum Termin. Das kann Ihnen helfen, auch nach einigen Tagen die Situation besser einzuordnen.	☐ Ja ☐ Nein
Reflektieren Sie den Termin.	› Überlegen Sie, was Sie aus dem Termin mitnehmen. Das geht insbesondere in Richtung Inhalte, Effizienz und Nutzen. › Hatten Sie eine tragende Rolle, sollten Sie überlegen, was gut lief und was nicht. Schauen Sie, welche Schlüsse Sie für zukünftige Termine ziehen können.	☐ Ja ☐ Nein

Schärfen Sie bei Ihren Führungskräften das Bewusstsein für diese Cyberrisiken

Als Profi im Datenschutz wissen Sie: Mitunter die grössten Gefahren und Risiken drohen inzwischen wohl jedem Unternehmen aus Richtung Cybercrime. Egal, ob Hacker oder Erpresser, die Cyberkriminellen machen vor keinem Unternehmen halt, egal wie gross oder egal wie (un)bedeutend. Damit Risiken sich nicht realisieren, kommt es auf Sensibilität an, gerade bei Führungskräften.

Darum sollten Sie die Führungskräfte wachrütteln

Führungskräfte haben viel um die Ohren: Da wären nicht nur Ziele, die zu erreichen sind. Auch das Führen der Mitarbeiter kann eine grosse Herausforderung sein. Kein Wunder, dass man sich dann vielleicht weniger Gedanken um Sicherheitsrisiken für die Daten des Unternehmens macht. Doch darauf vertrauen, dass schon nichts passieren wird, ist keine gute Idee. Informieren Sie die Führungskräfte beispielsweise in einer informativen E-Mail über die wichtigsten Cybercrime-Risiken. Die entsprechenden Gefahren lauern auf jeden, eben auch auf Führungskräfte. Orientieren Sie sich an diesem Muster:

MUSTER: Führungskräfte-Info „7 Cyberrisiken“

Liebe Kollegin,
lieber Kollege,

Daten sind für unser Unternehmen von unschätzbarem Wert. Und was macht man mit Schätzen? Genau, man muss sie gut schützen. So ist es auch mit den Daten im Unternehmen, egal, ob es Personendaten sind oder nicht.

Als Führungskräfte sind Sie nicht nur dafür verantwortlich, Ihre Mitarbeiter anzuleiten und gemeinsam zum Erfolg des Unternehmens beizutragen. Sie haben es auch in der Hand, dass unser Datenschatz angemessen geschützt ist. Dazu ist es wichtig, dass Sie über Gefahren und Risiken Bescheid wissen. Denn dann können Sie einerseits Ihre Mitarbeiter passend informieren und sensibilisieren. Andererseits erkennen Sie schneller, ob etwas zum Problem werden kann.

Denn meist ist im Fall der Fälle besonders entscheidend: Es muss schnell gehandelt werden, um grösseren Schaden zu vermeiden. Genau das muss Ziel von uns allen sein. Denn jeder Schaden für das Unternehmen ist auch ein Schaden für die Beschäftigten und uns alle.

Diese Gefahren und Risiken sollten Sie auf dem Radar haben und Ihre Mitarbeiter entsprechend informieren:

Risiko 1: Phishing
Das ist die Gefahr: Cyberkriminelle versenden gefälschte E-Mails oder Nachrichten (z. B. SMS), die vorgaukeln, von vertrauenswürdigen Quellen zu stammen. Das Ziel: Es sollen vom Empfänger sensible Informationen preisgegeben werden, etwa Anmeldeinformationen oder Passwörter. Meist will man die ergaunerten Informationen nutzen, um Schadsoftware zu platzieren oder eine Zahlung an die Kriminellen zu veranlassen.

Darauf sollten Sie achten: Oft gibt es eine unpassende oder unpersönliche Ansprache wie „Lieber Kunde“. Die Formulierungen sind unüblich und ggf. kommen auch Fehler bei Rechtschreibung und Satzbau vor. Es wird Druck aufgebaut, mit einem Übel gedroht und zu schnellem bzw. heimlichem Handeln aufgefordert. Auch wenn die E-Mails den Anschein erwecken, echt zu sein, stimmt oft etwas mit der Absender-E-Mail-Adresse nicht. Es werden häufig Buchstaben vertauscht, das Original imitiert oder Zahlen anstatt von Buchstaben verwendet.

Risiko 2: Quishing (QR-Code-Phishing)
Das ist die Gefahr: QR-Codes werden manipuliert, etwa mit Aufklebern überklebt. Das Ziel: Die Nutzer bemerken die Fälschung nicht und landen auf einer gefälschten bzw. schadhaften Webseite. Dort geben sie sensible Anmeldeinformationen ein oder veranlassen direkt Zahlungen auf die Konten von Kriminellen.

Darauf sollten Sie achten: Bei QR-Codes sollten Sie immer Vorsicht walten lassen. Prüfen Sie etwa an Parkautomaten, ob es sich um einen Originalaufkleber handelt oder ob dieser überklebt wurde. Wird nach dem Erfassen der Link angezeigt, sollten Sie diesen genau unter die Lupe nehmen. Im Zweifel sollte die betreffende Webseite durch Eingabe der offiziellen Adresse aufgerufen werden, ggf. nach Suche über eine Suchmaschine.

Risiko 3: Whaling
Das ist die Gefahr: Dabei handelt es sich um speziell auf Führungskräfte ausgerichtete Angriffe von Kriminellen. Meist erfolgen diese Angriffe per E-Mail. Das Ziel: Man will direkt an die „dicken Fische“, um besonders wertvolle Informationen zu erhalten oder Zahlungen von grösseren Summen zu veranlassen.

Darauf sollten Sie achten: Auch hier wird meist dringender Handlungsbedarf vorgetäuscht. Zudem nutzt man gerne das Hierarchiegefüge aus, indem etwa vorgegaukelt wird, dass die E-Mail von einer wichtigen Person im Unternehmen kommt und nur der Adressat ins Vertrauen gezogen wird. Achten Sie also besonders darauf, ob die Forderung zum Üblichen passt. Insbesondere sollten Sie hellhörig werden,

wenn ungewöhnliche Vorgehensweisen eingefordert werden oder übliche Prozesse umgangen werden sollen. Solche Anfragen sollten Sie stets kritisch sehen, mit Vorgesetzten oder anderen Führungskräften besprechen oder mit demjenigen abklären, der die Forderung angeblich gestellt hat. Natürlich nutzen Sie zur Kontaktaufnahme nur die Kontaktdaten aus unserem internen Adressbuch. Suchen Sie die Kontaktdaten aktiv heraus.

Risiko 4: Spear-Phishing
Das ist die Gefahr: Hierbei handelt es sich um gezielte Phishing-Attacken, bei denen konkrete Informationen über den Empfänger genutzt werden, etwa zu Tätigkeit oder Aufgaben. Das Ziel: Es soll Vertrauen aufgebaut oder die Hilfsbereitschaft des Empfängers ausgenutzt werden.

Darauf sollten Sie achten: Solche E-Mails sind oft stark mit Informationen auf den Empfänger ausgerichtet. Es drängt sich oft die Frage auf: „Hä, warum schreibt der das?" Achten Sie darauf, ob der Inhalt zum Üblichen passt. Erhalten Sie von einem Abteilungsleiterkollegen die Bitte, eine Datei zu öffnen, obwohl das noch nie der Fall war, sollte Sie das stutzig machen. Das erst recht, wenn die Kommunikationsform unüblich ist. Auch eine Bitte per SMS ist verdächtig, wenn bisher immer per E-Mail kommuniziert wurde. Machen Sie in solchen Fällen immer den Gegencheck, bevor Sie ggf. dem Geforderten nachkommen. Rufen Sie beispielsweise den angeblichen Absender an, natürlich unter der im Adressbuch enthaltenen Telefonnummer.

Risiko 5: Business E-Mail Compromise (BEC) und E-Mail-Account Compromise (EAC)
Das ist die Gefahr: Bei BEC kompromittieren die Kriminellen zunächst echte geschäftliche E-Mail-Kommunikation. So werden etwa echte E-Mails abgefangen und enthaltene Informationen bzw. Anhänge verändert bzw. ausgetauscht. Das Ziel: Der Adressat gibt sensible Informationen preis oder veranlasst Zahlungen. Beim EAC haben die Kriminellen die betreffenden E-Mail-Konten gekapert und verschicken „echte E-Mails" von den an sich echten Accounts. Inzwischen häufen sich jedoch auch die Fälle, in denen Kriminelle die Vorgehensweise auf Briefpost übertragen und echte geschäftliche Kommunikation durch gefälschte ersetzen. Dabei werden gestohlene Originalbriefe eingescannt. Der Inhalt (z. B. Beträge, Bankverbindung) wird am Computer manipuliert und wieder ausgedruckt. Die perfekte Täuschung, die allenfalls bei genauem Hinsehen und nur mit Mitdenken auffällt.

Darauf sollten Sie achten: Setzen Sie auf Ihre Erfahrung und Erwartung. Weicht etwas vom Üblichen ab, sollten Sie stets besondere Vorsicht walten lassen. Das ist gerade dann angebracht, wenn sich Kommunikationsmuster oder -wege ändern oder aus heiterem Himmel Zahlungsdaten aktualisiert werden sollen. Gerade wenn sich die Bankverbindung ändert bzw. nicht mehr zur bisherigen passt, ist eine Bestätigung durch den Geschäftspartner unerlässlich. Wählen Sie dafür die Ihnen bekannten Kontaktdaten und nutzen Sie keinesfalls diejenigen, die in der E-Mail oder auf dem Brief angegeben sind. Setzen Sie im Zweifel auch immer auf das Vieraugenprinzip bzw. holen Sie sich eine zweite Meinung ein, etwa von Kollegen.

Risiko 6: Social Engineering
Das ist die Gefahr: Die Kriminellen setzen auf manipulative Vorgehensweisen, um den Angesprochenen oder Adressaten zur Preisgabe von vertraulichen Informationen zu bewegen. Gern wird versucht, über angeblich gemeinsame Freunde oder Interessen eine Vertrauensbasis zu schaffen. Doch auch geschickt platzierte Komplimente oder ein Appell an die Hilfsbereitschaft sollen die Zurückhaltung überwinden.

Darauf sollten Sie achten: Gibt es ungewöhnliche Anfragen oder will man Sie näher kennenlernen, sollten Sie hellhörig werden. Gerade wenn man Sie über Ihren Job oder das Unternehmen ausfragt, sollten Sie nicht zu auskunftsfreudig sein. Nicht selten wird auch hier Druck aufgebaut, eine Notlage vorgetäuscht oder dringende Hilfe eingefordert. Geben Sie keine schützenswerten Informationen heraus, auch wenn das aus Ihrer Sicht unproblematisch ist. Auch das sind Interna, die Fremde nichts angehen. Und vielleicht ist das nur der Einstieg, um Sie zu erpressen und wirklich Sensibles zu fordern.

Risiko 7: Ausnutzung von Schwachstellen
Das ist die Gefahr: Kriminelle setzen immer wieder darauf, dass ihre Opfer Software installieren oder nutzen, die Sicherheitslücken aufweist. Diese werden dann als Einfallstor genutzt, um etwa weitere Schadprogramme einzuschleusen, Daten abzugreifen oder mittels Ransomware zwecks Lösegelderpressung zu verschlüsseln.

Darauf sollten Sie achten: Nutzen Sie nur Software und entsprechende Quellen, die von der IT-Abteilung freigegeben ist. Brauchen Sie andere Lösungen, installieren Sie diese nicht auf eigene Faust, sondern stimmen das mit der IT-Abteilung ab. Halten Sie Ihre Geräte und Software immer auf dem aktuellen Stand. Bereitgestellte Aktualisierungen installieren Sie unverzüglich. Stellen Sie bei Computer & Co. ungewöhnliche Aktivitäten fest, reagiert dieser ungewöhnlich langsam oder können Sie nicht mehr auf Daten zugreifen, sprechen Sie sofort die Kollegen der IT-Abteilung an. Stellen Sie ausserdem sicher, dass Ihre Daten bzw. solche in Ihrer Verantwortung regelmässig gesichert werden. Ein Back-up kann entscheidend sein, um im Fall der Fälle weiterarbeiten zu können. Im Fall der Fälle haben Kriminelle ein Druckmittel weniger zur Verfügung.

Immens wichtig: Bleiben Sie wachsam!
Bei allen vorgenannten Risiken gibt es zahlreiche Varianten und Spielarten. Seien Sie also stets auf der Hut. Informieren Sie ausserdem Ihre Mitarbeiter. Denn auch hier haben Sie es als Führungskraft in der Hand, dass diese vor Risiken gewarnt sind und Kriminellen nicht auf den Leim gehen.

Sie haben Fragen oder brauchen Unterstützung? Kein Problem! Melden Sie sich bei mir. Als Datenschutzberaterin unterstütze ich Sie gern, beispielsweise beim Sensibilisieren Ihrer Mitarbeiter bei einer Abteilungsbesprechung.

Ihre Datenschutzberaterin
Mira Belle

„Blöde Fragen“? Mit diesen 7 Tipps reagieren Sie richtig

Egal, ob Sie in einem Beratungsgespräch stecken oder eine Schulung durchführen, es kann Ihnen immer passieren, dass Ihre Gesprächspartner Fragen stellen. Das ist natürlich gut, weil man mehr wissen will. Doch vielleicht sind Sie mit Fragen konfrontiert, die Sie schon unzählige Male beantwortet haben oder denen Sie nur das Etikett „dumme Frage“ verpassen wollen. Hier heisst es: Professionell bleiben!

Sie haben es in der Hand, wie „professionell“ man Sie wahrnimmt

Als Datenschutzberater bekleiden Sie eine verantwortungsvolle und herausgehobene Position im Unternehmen. Dabei ist nicht nur wichtig, dass Sie es fachlich draufhaben. Sie müssen auch Profi im Zwischenmenschlichen sein. Und gerade in diesem Bereich können Sie sich schnell auf dünnem Eis bewegen. Dass es dazu nicht kommt, liegt ganz bei Ihnen. Auch bei „blöden“ Fragen können Sie professionell mit Stil und Respekt reagieren. Das gelingt Ihnen mit links, indem Sie die folgenden sieben Tipps beherzigen:

Tipp 1: Keine Frage ist ohne Berechtigung

Dass man Sie fragt, passiert nicht einfach so. Meist steckt dahinter die Motivation des Fragenden, etwas verstehen zu wollen. Und selbst hinter aus Ihrer Sicht banalen oder „blöden“ Fragen kann ein tieferes Anliegen stecken. So beispielsweise dass man endlich Klarheit haben oder endlich etwas richtig machen will. Um das Motiv besser zu verstehen, sollten Sie genau zuhören, am besten aktiv. Das kann jeder. Dazu wiederholen Sie in eigenen Worten, was Sie vom Sachverhalt bzw. von der Frage verstanden haben. Fragen Sie aktiv nach, ob Sie die Frage so richtig verstanden haben. Damit zeigen Sie, dass Sie das Anliegen des Fragenden und natürlich ihn selbst ernst nehmen.

Tipp 2: Vermeiden Sie alles Abschätzige

Auch wenn die Frage noch so banal ist: Verkneifen Sie sich jedes laute Lachen, Grinsen oder sonstiges abschätzige Verhalten. Erst recht ein „Scheibenwischer“ vor dem Kopf oder ein gezeigter Vogel sorgen allenfalls für einige Lacher bei anderen Teilnehmern. Doch darauf können Sie verzichten. Denn mit Herabwürdigungen disqualifizieren Sie sich immer als professioneller Gesprächspartner, und zwar bei mehr Menschen, als Sie denken. Zudem zerstören Sie die Basis für einen offenen und vertrauensvollen Austausch. Und gerade das brauchen Sie für Ihre Arbeit als Datenschutzberater.

Tipp 3: Setzen Sie auf eine freundliche und wertschätzende Kommunikation

Das klingt schwieriger, als es in der Praxis wirklich ist. Achten Sie darauf, dass Sie Ihre Antworten immer mit einem freundlichen Einstieg beginnen. Starten Sie beispielsweise mit einem „Das ist eine gute Frage“ oder „Ich freue mich, dass Sie dieses Thema ansprechen“. Damit signalisieren Sie dem Fragenden, dass Sie ihn ernst nehmen. Und selbst bei einer noch so banalen Frage wird er gegenüber anderen Teilnehmern nicht blossgestellt. Im Übrigen gewinnen Sie mit solchen Einstiegen etwas Zeit, um sich die passende und situationsangemessene Antwort zurechtzulegen.

Tipp 4: Formulieren Sie Ihre Antwort einfach und verständlich

Eines ist klar: Als Datenschutzprofi können Sie so manchen mit Fachbegriffen und komplexen Erläuterungen in Grund und Boden reden. Doch das sollte nie Ihr Ziel sein, auch wenn Sie nervende Fragen bekommen. Vermeiden Sie unnötige Fachbegriffe. Erklären Sie alles Relevante mit einfachen Worten, und zwar so, dass es auch ein Laie versteht. Orientieren Sie sich gedanklich einfach an der leichten Verständlichkeit aus den Erklärstücken der „Sendung mit der Maus“. Und bedenken Sie stets: Wird etwas verstanden, wird es leichter verinnerlicht und eben auch umgesetzt.

Tipp 5: Geduld und Empathie sind ein Muss

Auch wenn es Ihnen vielleicht ab und an schwerfällt: Üben Sie sich in Geduld. Nicht jeder kennt sich mit der Materie so gut aus wie Sie. Insofern liegt es in der Natur der Sache, dass auch einfache Dinge unbekannt sind oder dass Sie manches immer wieder aufs Neue erklären müssen. Versetzen Sie sich gedanklich in die Situation des Fragenden. Der hat ggf. ganz andere Wissens- oder Tätigkeitsschwerpunkte, sodass es eigentlich kaum Berührungspunkte zum Datenschutz gibt.

Tipp 6: Erklären Sie die Dinge praxisnah

Oft werden Sie bei einer Antwort etwas erklären müssen. Damit der Groschen fällt, sollten Sie zu abstrakte Antworten vermeiden. Viel besser ist es, wenn Sie Ihre Erklärungen mit konkreten Beispielen ergänzen, idealerweise aus dem Arbeitsalltag des Fragenden. Damit zeigen Sie nicht nur, wie Theorie und Praxis zusammenhängen. Sie fördern mit guten und positiven Beispielen, dass man diese nachahmt.

Tipp 7: Machen Sie manche Frage überflüssig

Versuchen Sie auszumachen, warum eine Frage gestellt wurde. Manchmal liegt es einfach nur daran, dass der Fragende bei seiner Suche nach einer Antwort gerade keine solche gefunden hat. Häufen sich bestimmte einfache oder „blöde“ Fragen, sollten Sie darüber nachdenken, wie Sie proaktiv die Antworten liefern können. Das kann beispielsweise eine Liste mit häufig gestellten Fragen sein, die Sie im Intranet veröffentlichen. Eine solche Liste kann auch Teil des Materials sein, das Sie beispielsweise neuen Mitarbeitern oder bei Schulungen zur Verfügung stellen.

Analyse von Reisekosten: Worauf sollte ich hinweisen?

FRAGE: In unserem Unternehmen gibt es viele Aussendienstmitarbeiter. Dementsprechend entstehen hohe Kosten für Fahrzeugmieten, Tickets, Hotels und Verpflegung. Um hier einen besseren Überblick zu bekommen und vor allem auch Einsparpotenziale zu erkennen, will die zuständige Abteilung Auswertungen fahren. Weil es ja nicht nur um Daten zu Reisen an sich geht, sondern meist wohl auch ein Personenbezug besteht, hat man mich als Datenschutzberater um Hinweise gebeten. Worauf sollte ich in diesem Zusammenhang hinweisen?

ANTWORT: Zunächst sollten Sie mit den Kollegen ins Gespräch kommen. Schliesslich ist unerlässlich, dass Sie genau in Erfahrung bringen, was man vorhat und was Sache ist. Laden Sie am besten zu einem Termin ein. Klären Sie Fragen wie beispielsweise folgende:

- Welches Ziel hat man vor Augen bzw. was wird mit der Bearbeitung bezweckt?
- Welche Informationen sollen bearbeitet werden?
- Inwieweit ist eine personenbezogene Bearbeitung erforderlich?
- Woher stammen die Daten?
- Welche Auswertungen soll es konkret geben?
- Auf welcher Rechtsgrundlage soll eine Bearbeitung von Personendaten stattfinden?

Stellen Sie auf diese Punkte ab

Sicher ist: Das Vorhaben hat wohl Datenschutzrelevanz. Allerdings können Sie schon in einem ersten Gespräch auf einige Punkte hinweisen, die für eine erfolgreiche Umsetzung des Vorhabens entscheidend sein dürften:

› Idealerweise geht es ohne Personenbezug
Hinterfragen Sie, inwieweit es für den verfolgten Zweck überhaupt erforderlich ist, Personendaten zu bearbeiten. Unter Umständen reichen auch aggregierte Informationen aus, etwa Gesamtsummen für bestimmte Kostenarten. Eventuell kann es schon ausreichen, wenn man auf Kostenstellenebene auswertet. Allerdings kann es hier auch schnell zum Personenbezug kommen. Ist nur eine oder sind nur wenig reisende Personen auf einer Kostenstelle, kann es schnell passieren, dass man doch Personenbezug bei den Daten annehmen muss.

› Pseudonym ist besser als personenbezogen
Unter Umständen reicht es aus, wenn Personendaten pseudonymisiert bearbeitet werden. Auch das wäre datenschutzfreundlicher. Sollen beispielsweise missbräuchliche Abrechnungen aufgedeckt werden, kann dies zunächst pseudonymisiert erfolgen, sprich, ein Personenbezug wäre erst in einem weiteren Schritt herstellbar, wenn etwa ein Pseudonym anhand einer Referenztabelle wieder einem Mitarbeiter zugeordnet wird.

› Grundsätze der Bearbeitung müssen eingehalten werden
So muss beispielsweise die Rechtmässigkeit sichergestellt werden, sprich, es bedarf für die Bearbeitung einer Rechtsgrundlage. Wahrscheinlich wird man dies eher nicht auf die Erfüllung eines Vertrags mit dem Betroffenen (z. B. Arbeitsvertrag), also Art. 31 Abs. 2 Buchst. a Bundesgesetz über den Datenschutz (DSG), stützen können, weil hierfür eine Analyse nicht erforderlich sein dürfte. Allerdings kommt auch die Bearbeitung auf Basis eines überwiegenden berechtigten Interesses in Betracht (Art. 31 Abs. 1 DSG).

Geht es um Personendaten, die für einen anderen Zweck erhoben wurden, kommt keine zweckändernde Weiterbearbeitung in Betracht. Das ergibt sich aus Art 6 Abs. 3 DSG. Danach dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden. Die Daten dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

Auch die anderen Grundprinzipien sind von Relevanz. So z. B. die Verhältnismässigkeit. Danach müssen die Personendaten dem Zweck angemessen und erheblich sein sowie auf das für die Zwecke der Bearbeitung notwendige Mass beschränkt werden (Art. 6 Abs. 2 DSG).

Beratungs-Abo im Datenschutz: Kann man dem Schnäppchen trauen?

FRAGE: Ein externer Datenschutzberater bietet unserem Unternehmen ein günstiges Beratungs-Abo an. Er garantiert, dass es dank seiner Beratung zu keinen Verstössen mehr kommen soll. Was meinen Sie: Kann man dem Schnäppchen trauen?

ANTWORT: In der Tat ist bei Angeboten immer höchste Vorsicht geboten, wenn diese viel zu gut sind, um wahr zu sein. So dürfte es auch hier sein. Die Versprechen sollten Sie eher in die Rubrik „Marketing“ stecken, denn wirklich „garantiert“ dürfte nichts sein. So haftet etwa Ihr Unternehmen für Verstösse seiner Mitarbeiter und nicht ein Berater. Ob man sich dann bei diesem schadlos halten kann, steht auf einem anderen Blatt. Und wahrscheinlich dürfte es im Kleingedruckten einige Punkte geben, mit der eine Haftung bzw. eine Garantie weitgehend eingeschränkt wird.

OLG Stuttgart: Mitarbeiter für eigenmächtige Datenbearbeitung verantwortlich

Ihr Unternehmen bearbeiten Personendaten nicht selbst. Es sind vielmehr die Beschäftigten, die entsprechend agieren. Doch ist ein Mitarbeiter haftbar, wenn er Personendaten eigenmächtig für eigene Zwecke bearbeitet? Auf jeden Fall, meint das deutsche Oberlandesgericht (OLG) Stuttgart in einem Beschluss vom 25.2.2025 (Az. 2 ORbs 16 Ss 336/24).

Das führte zum Gerichtsverfahren

Ein Mann, der spätere Beschwerdeführer, war verbeamteter Polizist in einer Dienststelle in Baden-Württemberg. In der Nacht des 2.3.2021 griff der Polizist von einem Dienstrechner auf dem Polizeirevier auf eine polizeiliche Datenbank zu. Hier rief er Informationen über einen ehemaligen Kollegen ab, der wegen einer Straftat in Untersuchungshaft sass. Für die Abfrage gab es jedoch keine dienstliche Veranlassung. Bemerkt wurde die unbefugte Abfrage, nachdem Datenbankprotokolle zu den Abrufen ausgewertet wurden. Zu diesen Auswertungen kam es, nachdem ein WhatsApp-Chat mit Informationen zum in Untersuchungshaft sitzenden Kollegen bekannt wurde. Insofern kam es zum Verdacht, dass Polizeibeamte unbefugt Daten aus dem Informationssystem der Polizei abgerufen hatten.

Bussgeld wegen eigenmächtiger Bearbeitung

Nachdem auch der Landesbeauftragte für den Datenschutz von der Sache erfuhr, verhängte er gegen den Mann ein Bussgeld wegen einer unrechtmässigen Bearbeitung personenbezogener Daten. Dieses Bussgeld wollte der Mann nicht akzeptieren, weil er seiner Auffassung nach nicht für die Bearbeitung verantwortlich war. Also war das Amtsgericht Stuttgart zur Entscheidung über die Sache berufen.

Doch dort konnte der Polizist mit seinen Argumenten nicht überzeugen. Insbesondere ging das Gericht davon aus, dass er einerseits die Daten abgerufen hatte, weil in der besagten Nacht hierfür seine Nutzerkennung verwendet wurde. Andererseits sah das Gericht den Mann in der Verantwortung für die unrechtmässige Bearbeitung personenbezogener Daten. Nach Ansicht des Gerichts hatte die Datenschutzaufsichtsbehörde zu Recht das Verhalten mit einem Bussgeld belegt. Also verurteilte das Amtsgericht den Mann wegen der unrechtmässigen Bearbeitung personenbezogener Daten zu einer Geldbusse in Höhe von 1.500 € (Urteil vom 22.11.2023, Az. 31 OWi 315 Js 18340/23). Doch diese Entscheidung wollte der Mann nicht hinnehmen. Also musste sich das OLG im Rahmen einer Rechtsbeschwerde mit der Sache auseinandersetzen.

So entschied das OLG

Aus Sicht des Gerichts ist die Rechtsbeschwerde unbegründet. Das Amtsgericht hat den Mann zu Recht wegen der vorsätzlichen Ordnungswidrigkeit des rechtswidrigen Bearbeitens personenbezogener Daten zu einer Geldbusse von 1.500 € verurteilt. Der Abruf der Daten durch den Polizisten stellt eine rechtswidrige Bearbeitung im Sinn von Art. 4 Nr. 2 Datenschutz-Grundverordnung (DSGVO) dar. Zudem ist der Polizist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO anzusehen. Insofern hat das Amtsgericht den Mann zutreffend wegen einer vorsätzlich rechtswidrigen Bearbeitung nach Art. 83 Abs. 1, 2, 5 Buchst. a DSGVO verurteilt.

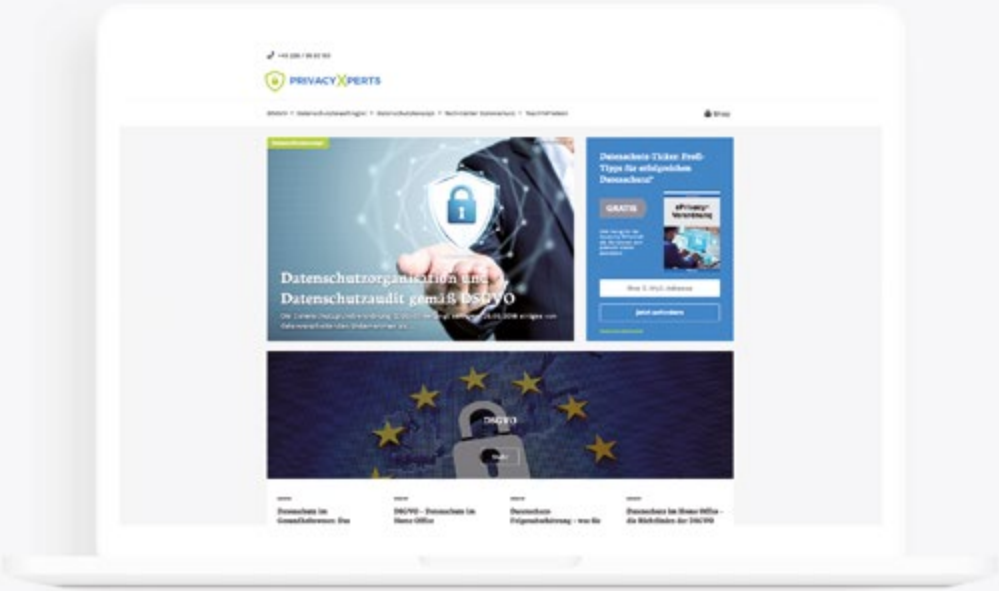
Dass der Polizist selbst als Verantwortlicher anzusehen ist, ergibt sich insbesondere daraus, dass der Datenschutzverstoss bewusst und gewollt aus dienstfremden Gründen erfolgt ist. Darin ist an sich auch kein Weisungsverstoss zu sehen. Vielmehr hat der Polizist überhaupt nicht betrieblich bzw. behördlich veranlasst gehandelt. Bei einem solchen Mitarbeiterexzess entzieht sich der Mitarbeiter der Leitung und Aufsicht seiner Vorgesetzten. Er begründet eine eigenständige Entscheidungsmacht bezüglich der Zwecke und Mittel der Bearbeitung. Dabei steht ausser Frage, dass es im konkreten Fall zu einer Bearbeitung gekommen ist. Es reicht das blosse Abfragen von Daten aus.

§

Das bedeutet die Entscheidung für Ihre Arbeit

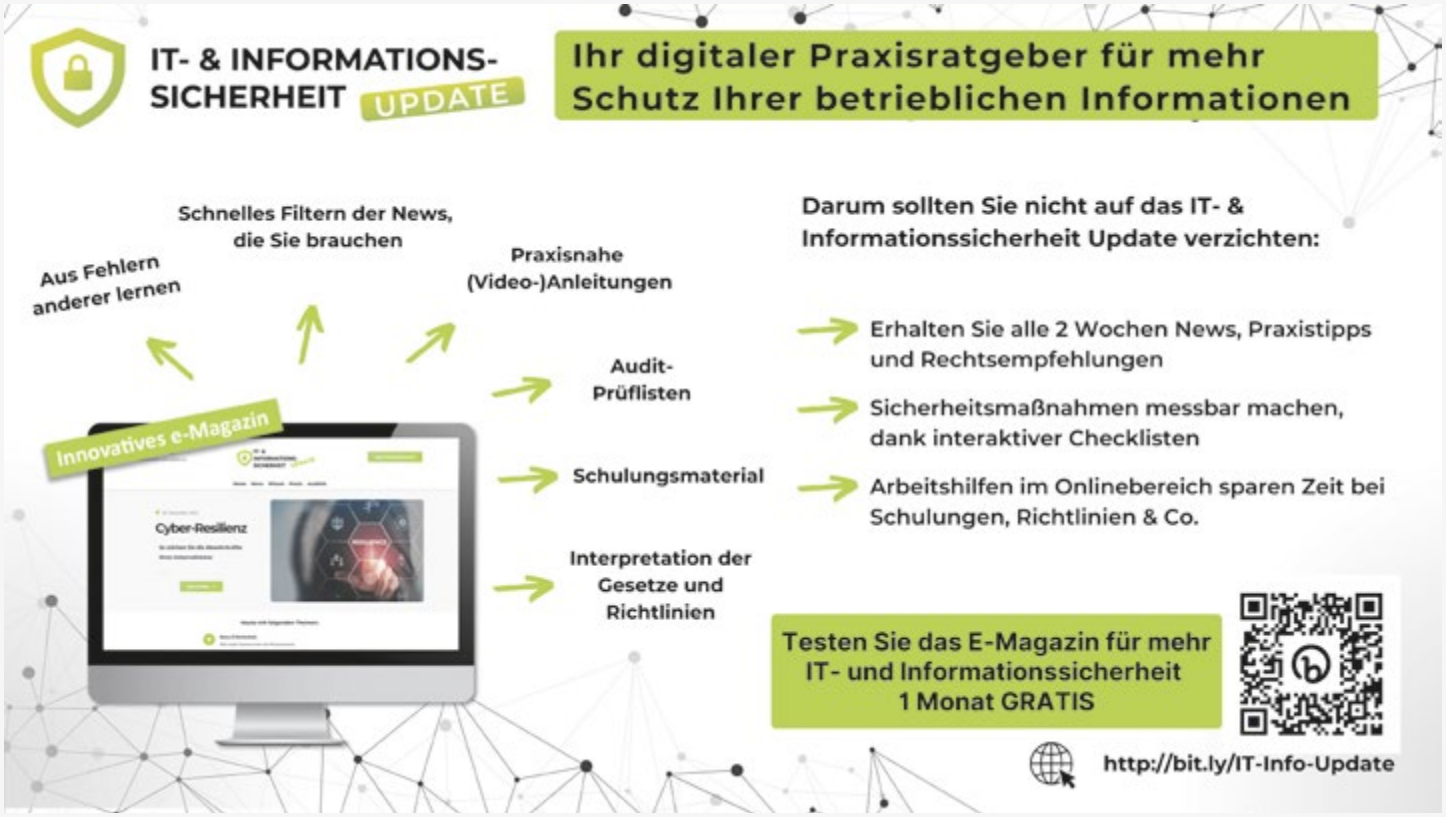
- Die Entscheidung ist bestens geeignet, um beispielsweise im Rahmen einer Schulung für den sorgsamen Umgang mit Personendaten zu sensibilisieren. Machen Sie deutlich, dass es kein Grund ist, Personendaten beispielsweise einfach nur interessehalber abzurufen oder anzuschauen. Das kann nach hinten losgehen. Insbesondere ist das kein Kavaliersdelikt.
- Gibt es für eine eigenmächtige Bearbeitung eines Beschäftigten keine aufgabenbezogene Veranlassung, kann ein Mitarbeiter selbst zum Verantwortlichen werden. Dazu bedarf es nicht immer ausdrücklicher Weisungen oder konkret ausgesprochener Verbote. Wird eigenmächtig über Zwecke und Mittel entschieden, ist man Verantwortlicher und unterliegt den Anforderungen und Pflichten der Datenschutzgesetze Das bedeutet auch im Umkehrschluss: Dem Unternehmen kann der Verstoss des Mitarbeiters nicht zugerechnet werden. Es haftet also nicht.
- Sie können gerade Administratoren auf die Problematik „Mitarbeiterexzess“ hinweisen. Das Bearbeiten von Personendaten über das dienstlich erforderliche Mass hinaus kann ernsthafte Konsequenzen haben. So wie in diesem Fall kann es zu einem Bussgeld führen, wenn der EDÖB von einem Verstoss erfährt, etwa durch einen Betroffenen. Und natürlich kann ein solcher ggf. gravierender Pflichtverstoss arbeitsrechtliche Konsequenzen nach sich ziehen, und zwar schlimmstenfalls bis hin zur Kündigung.

„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



Vorschau:

Ihr Urlaub ist vorbei? Das sind Ihre To-dos für die erste Arbeitswoche
Bezüglich des Supportendes von Windows 10 heisst es jetzt: „Gas geben“

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 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
Deutschland