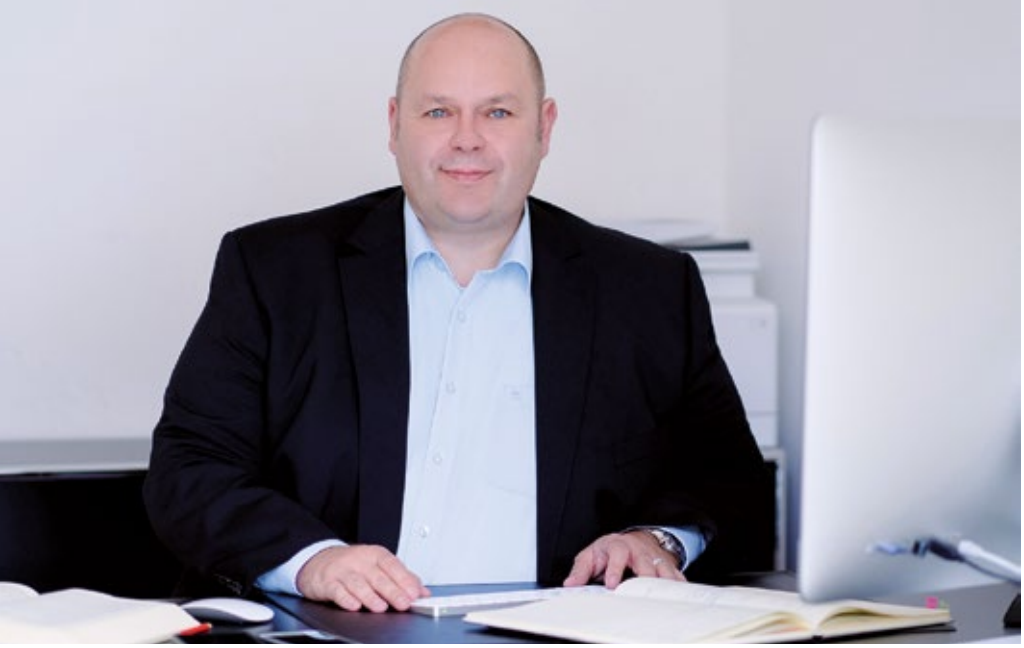
DATENSCHUTZAKTUELL
OKT I 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

AI GENERATED

ANIMIEREN SIE BESCHÄFTIGTE ZU DATENSCHUTZ IM HOMEOFFICE



Datenschutz ist eine Managementaufgabe

Liebe Leserin, lieber Leser,

vielleicht kennen Sie das: Geht es darum, dass Beschäftigte mit personenbezogenen Daten arbeiten, meint vielleicht mancher aus dem Management, dass Sie sich um alles kümmern würden. Schließlich sei das Ihr Job als Datenschutzbeauftragter. Diese Fehleinschätzung passiert manchmal aus Unkenntnis, manchmal jedoch auch mit Absicht. Allerdings sollten Sie sich weder mit dem einen noch dem anderen abfinden.

Machen Sie klar: Sie beraten im Datenschutz und kontrollieren diesen. Die Umsetzung ist Sache des Unternehmens – also hier des Managements. Ihnen kann man diese Verantwortung nicht übertragen.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

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

Inhalt

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

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

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

Impressum

PRIVACYXPERTS

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

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, 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: KI generiert; Seite 1: Adobe Stock | epixi-mages

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

Im Homeoffice sind Sie nicht präsent. Hier ist Awareness das Mittel der Wahl.

Animieren Sie Beschäftigte zu Datenschutz im Homeoffice

Vielleicht ist es in Ihrem Unternehmen wie in vielen anderen auch: Zumindest ab und an können die Beschäftigten aus dem Homeoffice arbeiten. Das ist nicht nur für Mitarbeiter praktisch. Es kann auch Kosten für das Unternehmen senken. Doch mit dem Homeoffice gehen auch Risiken einher, gerade im Datenschutz.

Keine Option: aus den Augen, aus dem Sinn

Als Datenschutzbeauftragter sollen Sie ein Auge darauf haben, dass bei Ihrem Unternehmen im Datenschutz alles passt. Das mag im Unternehmen vor Ort noch gut funktionieren. Schließlich gibt es hier Regeln und vieles wird technisch wie organisatorisch sichergestellt. Im Homeoffice kann das ganz anders aussehen. Doch die Risiken ignorieren sollten Sie keineswegs, auch wenn Sie vor Ort nicht nach dem Rechten schauen können. Hier ist Awareness das Mittel der Wahl. Sensibilisieren Sie für die Risiken. Das kann Ihnen beispielsweise mit einer E-Mail mit Selbstcheck gelingen.

Muster: Schreiben und Selbstcheck „Homeoffice“

Passt alles im Homeoffice? Machen Sie den Selbstcheck

Liebe Kolleginnen und Kollegen,

viele von uns arbeiten zumindest gelegentlich vom heimischen Arbeitsplatz aus. Und Sie werden bestimmt bestätigen: Im Großen und Ganzen funktioniert das richtig gut. Damit das auch weiterhin so bleibt, möchte ich Ihnen als Ihr Datenschutzbeauftragter etwas an die Hand geben: einen Selbstcheck. Mit diesem können Sie auf die Schnelle Ihr eigenes Homeoffice unter die Lupe nehmen. Schließlich muss auch im Homeoffice bei Datenschutz und Datensicherheit alles im grünen Bereich sein.

Darum ist Datenschutz für jeden von uns ein Thema

Tagtäglich arbeiten wir mit Informationen über oder zu Menschen. Da wären die Daten zu Kunden oder Geschäftspartnern, aber auch die zu Kollegen. Alle Betroffenen vertrauen darauf, dass unser Unternehmen und wir als Beschäftigte sorgfältig mit ihren Daten umgehen. Diese müssen sicher sein und dürfen nicht in falsche Hände geraten. Und dieser Gefahr müssen wir tagtäglich entgegenwirken. Jeder Einzelne ist dazu berufen, seinen Beitrag zu leisten.

Beim Homeoffice sind Sie besonders gefordert

Beim Arbeiten im Büro im Unternehmen gelten viele Regeln. Die müssen eingehalten werden. Nichts anderes gilt, wenn es um das Arbeiten in den eigenen vier Wänden geht. Zwar mag die Situation bei Ihnen zu Hause eine andere sein. Dennoch müssen Sie alles daransetzen, dass auch am heimischen Arbeitsplatz personenbezogene Daten angemessen geschützt sind. Schließlich ist klar: Das Arbeiten im Homeoffice darf etwa Cyberkriminellen nicht Tür und Tor öffnen.

10 Minuten für mehr Sicherheit – machen Sie den Check

Nachfolgend finden Sie eine Liste mit Fragen für einen Selbstcheck. Damit können Sie die Datenschutzsituation im Homeoffice einschätzen. Dabei ist wichtig: Setzen Sie sich kritisch mit den Fragen und der Situation vor Ort auseinander. Müssen Sie bei einer Frage mit einem Nein antworten, ist das noch kein Beinbruch. Vielmehr ist es die Gelegenheit, dass Sie die Dinge optimieren. Brauchen Sie dafür Rat oder Unterstützung, können Sie sich an die IT-Hotline oder an mich wenden.

Danke fürs Mitmachen!

Ihr Tom Bola

Datenschutzbeauftragter

Machen Sie das bereits?	Darauf sollten Sie achten	Erfüllt bzw. umgesetzt?
Arbeitsumgebung		
Mein Arbeitsplatz ist so gewählt und eingerichtet, dass Unbefugte nicht den Bildschirm oder Unterlagen einsehen können?	› Bedenken Sie immer: Auch Partner, Kinder, Mitbewohner oder Gäste sind Unbefugte, unabhängig von Ihrem persönlichen Vertrauensverhältnis. Interna und personenbezogene Daten des Unternehmens gehen sie nichts an. › Richten Sie Ihren Arbeitsplatz so aus, dass eine Kenntnisnahme für Unbefugte ausgeschlossen ist.	○ Ja ○ Nein
Bei Telefonaten oder Videokonferenzen können Unbefugte nicht zuhören oder zuschauen?	› Achten Sie bei vertraulichen Gesprächen darauf, dass Türen und Fenster geschlossen sind. › Deaktivieren Sie smarte Geräte, die mithören und Vertrauliches anderswohin übertragen können.	○ Ja ○ Nein
Bin ich abwesend, sperre ich den Computer?	› Niemand soll mitlesen können, auch wenn Sie nur schnell mal um die Ecke müssen. › Mit „Windows-Taste und L" sperren Sie im Handumdrehen Ihren Computer.	○ Ja ○ Nein
Bei langer Abwesenheit bzw. bei Feierabend schließe ich Unterlagen, Notizen und Datenträger weg?	› Gehen Sie auf Nummer sicher: Ein leerer Tisch schützt vor großen Augen und vor Langfingern. › Nutzen Sie idealerweise eine abschließbare Ablage. Ziehen Sie den Schlüssel nach dem Abschließen ab.	○ Ja ○ Nein
Arbeitsmittel und Datenübertragung		
Mein Router ist ein aktuelles Modell, bei dem Firmware und Sicherheitsfeatures auf aktuellem Stand sind?	› Prüfen Sie, ob Ihr Gerät noch auf der Höhe der Zeit ist, am besten auf der Seite des Herstellers. › Installieren Sie Sicherheitsupdates und ändern Sie das aufgedruckte Standardpasswort.	○ Ja ○ Nein
Das WLAN ist nach aktuellem Stand verschlüsselt und mit einem starken Passwort gesichert?	› Setzen Sie mindestens auf den Standard WPA2 oder noch besser auf WPA3. › Ändern Sie das voreingestellte WLAN-Passwort des Herstellers. 18 Zeichen oder mehr sollten es schon sein. › Nutzen Sie für Dritte oder Gäste einen Gastzugang.	○ Ja ○ Nein
Angebotene Updates installiere ich unverzüglich auf dem Router und auf meinen dienstlichen Geräten?	› Mit jedem Sicherheitsupdate werden Lücken geschlossen. Und was geschlossen ist, kann niemand mehr ausnutzen. › Aktivieren Sie bei Ihrem Router das automatische Installieren von Updates. › Stehen Updates bei Notebook oder Smartphone an, installieren Sie diese ohne Verzug.	○ Ja ○ Nein
Für die Verbindung ins Unternehmensnetzwerk nutze ich nur die bereitgestellte VPN-Verbindung?	› Setzen Sie auf VPN, sprich das Virtual Private Network, ist der Datenaustausch mit dem Unternehmen verschlüsselt und sicher. › Umgehen Sie nie die VPN-Lösung. Andernfalls besteht das Risiko, dass Unbefugte mitlesen oder Hacker angreifen.	○ Ja ○ Nein
Ich nutze für meine Arbeit nur bereitgestellte Geräte und Software?	› Private und anderweitig genutzte Geräte oder Software bergen Sicherheitsrisiken. Die müssen vermieden werden. › Fehlt Ihnen ein Arbeitsmittel, sprechen Sie mit Ihrem Vorgesetzten bzw. der IT. › Überlassen Sie niemandem Ihre Geräte!	○ Ja ○ Nein
Zugangsdaten gebe ich nicht weiter und sind sicher verwahrt?	› Lassen Sie keine Passwörter offen herumliegen. Eine sichere Aufbewahrung ist ein Muss. › Am besten: Nutzen Sie den Passwortmanager auf Notebook und Smartphone.	○ Ja ○ Nein
Unterlagen und Daten		
Dienstliche Daten speichere ich zentral im Firmennetzwerk und nicht nur lokal auf dem Notebook?	› Sichern Sie Ihre Daten immer auf zentralen Servern. So sind sie gesichert und können im Bedarfsfall wiederhergestellt werden. › Arbeiten Sie nur vorübergehend mit lokalen Kopien. Denken Sie nach Abschluss der Arbeit an die Sicherung bzw. den Upload der Daten.	○ Ja ○ Nein
Unterlagen, Akten und Datenträger bewahre ich sicher auf?	› Nutzen Sie einen Schrank oder ein Fach, auf das andere keinen Zugriff haben. › Lassen Sie Unterlagen nicht offen herumliegen, wenn Unbefugte einen Blick darauf werfen könnten.	○ Ja ○ Nein
Für Ausdrucke oder Scans nutze ich keine privaten Accounts oder Geräte?	› Private Drucker und Multifunktionsgeräte sind tabu. Nutzen Sie die Geräte im Unternehmen. › Arbeiten Sie auch nicht mit „Workarounds". Auch das Weitersenden von Informationen zwecks besserer oder einfacherer Bearbeitung ist ein No-Go.	○ Ja ○ Nein
Unterlagen mit schützenswerten Informationen entsorge ich immer sicher?	› Sicher vernichten heißt hier: Verwahren Sie die Unterlagen und entsorgen Sie diese am nächsten Arbeitstag im Unternehmen in den Datenschutztonnen. › Lassen Sie sich die Nutzung eines Schredders freigeben. Der muss mindestens einen Partikelschnitt auf Sicherheitsstufe P-4 schaffen.	○ Ja ○ Nein
Richtiges Verhalten		
Bevor ich E-Mails und deren Anhänge öffne, prüfe ich diese kritisch?	› Nehmen Sie sich vor Phishing in Acht. Gehen Sie Cyberkriminellen nicht auf den Leim. › Eine Prüfung geht im Handumdrehen. Prüfen Sie den Absender, den Betreff, den Inhalt und Anhänge. Passt hier etwas nicht oder ist etwas verdächtig, sollten Sie haltmachen. Lassen Sie sich auch nicht unter Druck setzen. Auch bei echt wirkenden Nachrichten sollten Sie im Zweifel auf alternativem Weg beim echten Absender nachfragen.	○ Ja ○ Nein
Bei Verdachtsfällen oder Pannen weiß ich, was ich tun muss?	› Geht etwas schief oder haben Sie den Verdacht, dass Cyberkriminelle am Werk sind, dürfen Sie nicht abwarten. Informieren Sie unverzüglich die Kollegen der IT-Hotline oder den Datenschutzbeauftragten. › Sofortiges Melden ist wichtig, damit nicht größerer Schaden entsteht. Und niemand macht Sie einen Kopf kürzer.	○ Ja ○ Nein

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. So kann jeder Mitarbeiter das Gerät nutzen, mit dem er am besten zurechtkommt. Das steigert die Zufriedenheit. Und Ihr Unternehmen muss nicht viel Geld für Geräte, Management und Support ausgeben. Das macht der Mitarbeiter selbst. Ihr Unternehmen spart richtig viel Geld. Doch was wie Werbeversprechen aus Hochglanzbroschüren daherkommt, steckt voller Risiken.

Ziehen Sie den Zahn schnellstens

Kommen Sie in die Situation, dass Sie als Datenschutzbeauftragter 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 der Datenschutz-Grundverordnung. Um die Verarbeitung sicher zu machen, müssen angemessene Schutzmaßnahmen ergriffen werden. Genau das kann mit BYOD zum Ding der Unmöglichkeit werden. Ihr Unternehmen bleibt für seine Verarbeitungen 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 Verarbeitung personenbezogener Daten 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 personenbezogenen Daten 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 (z. B. Betriebsrat) Geräte und Software bereitstellen. Sensible Daten oder Informationen im Zusammenhang mit Beschäftigten haben nichts auf Privatgeräten verloren.

Das ist zu prüfen, wenn der Chef das Unternehmen verlässt

Gerade in schwierigen Zeiten wie jetzt kann es schnell passieren, dass es an der Führungsspitze des Unternehmens zu Veränderungen kommt. Solche Wechsel bei der Geschäftsführung erfolgen meist einvernehmlich. Manchmal geht man auch im Streit auseinander. Doch egal wie: Mit dem Wechsel müssen schnell Änderungen vorgenommen werden. Und die haben große Datenschutzrelevanz.

Berechtigungen & Co. müssen auf den Prüfstand

Schützenswerte Daten, etwa personenbezogene Informationen oder Geschäftsgeheimnisse, dürfen nicht in falsche Hände geraten. Das kann jedoch schnell passieren, wenn Beschäftigte das Unternehmen verlassen. Dementsprechend müssen auch risikoangemessene technische und organisatorische Schutzmaßnahmen ergriffen werden. Art. 32 Datenschutz-Grundverordnung (DSGVO) macht es notwendig, dass etwa auch bei einem Wechsel oder Austritt in der Geschäftsleitung die nötigen Maßnahmen umgesetzt werden. Das bedeutet insbesondere, dass Berechtigungen entzogen und der Zugriff auf Daten eingeschränkt werden.

Setzen Sie auf die folgende Checkliste

Wechsel oder Austritte in der Führungsetage passieren manchmal von jetzt auf gleich. Dann sind auch Sie als Datenschutzbeauftragter gefragt. Schließlich muss vieles bedacht werden, wenn aus einem heute noch Befugten morgen schon ein Unbefugter im Hinblick auf Informationen Ihres Unternehmens wird. Setzen Sie dann auf die folgende Checkliste.

Ziehen Sie sich nicht jeden Schuh an

Beherzigen Sie stets: Ihren Fokus müssen Sie als Datenschutzbeauftragter in erster Linie auf den Datenschutz und den Umgang mit personenbezogenen Daten richten. Bei einem Wechsel in der Geschäftsführung oder im oberen Management können auch andere Themen von großer Bedeutung sein. So müssen ggf. auch Anpassungen bei Vertretungs- oder Zeichnungsberechtigungen, im Handelsregister oder im Impressum der Webseite vorgenommen werden. Überlassen Sie diese Themen am besten den zuständigen Kollegen, etwa aus der Rechtsabteilung. Allerdings können Sie auf den Handlungsbedarf hinweisen, damit nichts unbeachtet bleibt, gerade wenn es etwas drunter und drüber gehen sollte.

Checkliste: Wichtige Datenschutzaspekte beim Geschäftsführerwechsel

Aspekt	Das sollten Sie beachten	Umgesetzt?
Allgemeines		
Ist ein Datum bzw. ein Zeitpunkt für das Ausscheiden bzw. den Wechsel festgelegt?	› Gerade wenn man plötzlich oder im Streit getrennte Wege geht, müssen relevante Punkte schnellstens umgesetzt werden. Insbesondere muss unterbunden werden, dass Daten abfließen oder vernichtet werden. › Klären Sie mit der Personalabteilung bzw. anderen zuständigen Stellen im Unternehmen, wann die „Stunde null" ist.	○ Ja ○ Nein
Gibt es einen kleinen Personenkreis, der relevante Vorbereitungen oder Maßnahmen trifft?	› Mahnen Sie die Einhaltung des Minimalprinzips bzw. des Need-to-know-Prinzips an. Denn generell gilt: Je weniger von der Sache wissen, desto kleiner ist das Risiko, dass Informationen geleakt werden. › Betrachten Sie unbedingt die funktionalen Aspekte, und zwar über Hierarchiegrenzen hinweg. Unter Umständen müssen auch Administratoren auf unterer Ebene eingebunden sein.	○ Ja ○ Nein
Ist geklärt, welche Funktionen, Rollen und Berechtigungen die betreffende Person hatte?	› Achten Sie darauf, dass es einen vollständigen Überblick über diese Aspekte gibt. Nur so wird sichergestellt, dass keine Umsetzungslücke und damit auch Risiken für den Datenschutz und für Geschäftsgeheimnisse entstehen. › Denken Sie nicht nur an systemgenerierte Übersichten. Auch das Gespräch mit wichtigen Kontaktpersonen bzw. mit der Assistenz kann Unbekanntes zutage fördern.	○ Ja ○ Nein
Sind andere wichtige relevante Stellen im oder außerhalb des Unternehmens eingebunden?	› Kommt es zu einem Wechsel an oberster Stelle, hat dies auch große Auswirkungen auf andere Themenbereiche, etwa im Bereich Gesellschafts- und Handelsrecht. Das heißt, z. B. Vollmachten und Zeichnungsberechtigungen müssen angepasst werden. › Klären Sie, inwieweit etwa die Rechtsabteilung und der Compliance Officer eingebunden sind. Ggf. sind auch externe Berater oder Kanzleien zu informieren, etwa im Rahmen von Ermittlungen.	○ Ja ○ Nein
Sind die Beteiligten zur Vertraulichkeit bzw. Geheimhaltung verpflichtet?	› Vertrauen Sie hier nicht auf mündliche Zusagen oder die Aussage, dass sich das doch von selbst verstehe. › Prüfen Sie zumindest stichprobenhaft, ob entsprechende Verpflichtungen existieren, am besten schwarz auf weiß.	○ Ja ○ Nein
Wer trifft relevante Entscheidung bezüglich einzuleitender Maßnahmen?	› Diese Information kann auch für Sie wichtig sein, denn nur so wissen Sie, wen Sie beraten müssen. › Gerade beim Geschäftsführerwechsel, kommt es auch zu einem Austausch des Kopfes des Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO.	○ Ja ○ Nein

Läuft alles nach dem festgelegten Offboarding-Prozess?	› Auch wenn aufgrund einer besonderen Situation besondere Maßnahmen erforderlich sind, sollten die Verantwortlichen den Standardprozess einhalten. Das bewahrt davor, dass sie etwas vergessen oder übersehen. › Haben Sie vor allem ein Auge auf die datenschutzrelevanten Prüfpunkte beim Offboarding. Prüfen Sie zudem, inwieweit eine Checkliste auf der Höhe der Zeit ist. Neue Themen, z. B. die Sperrung des Zugangs zu Onlinespeichern, dürfen nicht fehlen.	○ Ja ○ Nein
Berechtigungen		
Haben Administratoren alle zugeordneten Benutzerkonten deaktiviert?	› Achten Sie darauf, dass zunächst alle Single-sign-on-Konten deaktiviert werden. Dann ist der Zugriff auf zugeordnete Systeme ebenfalls deaktiviert. Auch sollten aktive Sitzungen gezielt beendet werden. › Ein Deaktivieren von Konten reicht zunächst aus, über das Löschen wird später entschieden. Ein sofortiges bzw. unbedachtes Löschen kann viel Schaden anrichten, etwa wenn es um Beweismittel geht oder wenn personenbezogene Daten unbefugt gelöscht werden.	○ Ja ○ Nein
Hat die IT-Abteilung Fernzugriffe unterbunden und Berechtigungen eingeschränkt oder deaktiviert?	› Solche Zugänge dürfen nicht übersehen werden. Ansonsten können Daten weiter aus der Ferne abgerufen werden. › Die Deaktivierung sollte mit sofortiger Wirkung erfolgen, um die vollständige Kontrolle über die im Zugriff liegenden Daten zu erhalten.	○ Ja ○ Nein
Wurde der Zugriff auf externe Systeme oder Datenspeicher (z. B. Cloud) gestoppt?	› Unter Umständen hatte die betreffende Person auch Zugriff auf Fremdsysteme. Diese Zugriffe sollten unverzüglich entzogen werden. › Eventuell müssen Dritte gebeten werden, einen Account in deren System zu sperren. Auch hier sollte bei der entsprechenden Anfrage das Need-to-know-Prinzip umgesetzt werden.	○ Ja ○ Nein
Wurden Prozesse und Genehmigungsberechtigungen angepasst?	› Gerade Geschäftsführer oder das obere Management verfügen über weitreichende Verfügungsbefugnisse. Diese müssen beschränkt werden. › Binden Sie hier andere relevante Stellen mit ein, etwa auch das Finanzcontrolling, wenn es um die Freigabe von Zahlungen geht.	○ Ja ○ Nein
Geräte, Datenträger und Unterlagen		
Hat die ausscheidende Person alle technischen Arbeitsmittel und Unterlagen zurückgegeben?	› Idealerweise wird hier auf eine Inventarliste gesetzt. Gegen diese kann geprüft werden, ob alles zurückgegeben wurde. › Geräte und Unterlagen im Homeoffice dürfen nicht vergessen werden. › Ggf. müssen andere Stellen eingebunden werden, um Geräte oder Unterlagen vor Ort abzuholen. Zu langes Warten kann hier zum Problem werden.	○ Ja ○ Nein
Hat die IT-Abteilung Kommunikationsmöglichkeiten deaktiviert bzw. umgeleitet?	› Das gilt nicht nur für das E-Mail-Postfach. Auch Mobilfunk, Messenger- oder Social-Media-Accounts sollten gesperrt werden. › Bei einer Umleitung muss geprüft werden, ob dies unter Datenschutz- und Transparenzaspekten vertretbar ist.	○ Ja ○ Nein
Haben die zuständigen Stellen festgelegt, ob eine Löschung der Geräte bzw. Datenträger erfolgen darf?	› Unter Umständen haben die Geräte Bedeutung für rechtliche Auseinandersetzungen. Ein unbedachtes Löschen wäre schlecht. › Am besten wird für die Geräte oder Datenträger konkret festgelegt, wer wann über eine Löschung entscheidet.	○ Ja ○ Nein
Zutritt und physische Sicherheit		
Hat die betreffende Person alle Zutrittsmittel zurückgegeben?	› Das sind vor allem (General-)Schlüssel oder Codekarten. Zu denken ist aber auch an Schlüssel für Schließfächer oder Archivräume außerhalb. › Am besten wird gegen eine Inventarliste geprüft. Für Fehlendes müssen Maßnahmen festgelegt werden. › Relevante Berechtigungen zu Zutritt oder Zufahrt sollten systemseitig gesperrt werden.	○ Ja ○ Nein
Ist der Empfang bzw. Werkschutz informiert und instruiert?	› Klare Anweisungen sind unerlässlich, damit etwa der frühere Geschäftsführer nicht einfach durchgewunken wird. › Geregelt sein sollte das Verhalten in bestimmten Situationen.	○ Ja ○ Nein
Information und Transparenz		
Werden die Beschäftigten zeitnah und einheitlich informiert?	› Es sollte kurz und knapp informiert werden, wer das Unternehmen zu welchem Datum verlässt. Das Need-to-know-Prinzip muss gewahrt werden. › Achten Sie darauf, dass eine Information alle Beschäftigten erreicht.	○ Ja ○ Nein
Sind besonders betroffene interne oder externe Stellen gesondert informiert und instruiert worden?	› Unter Umständen sind bestimmte Personen oder Stellen gesondert zu informieren und brauchen auch mehr Informationen, etwa zum richtigen Verhalten. › Auch wichtige externe Kontaktpersonen sind ggf. unverzüglich über einen Wechsel zu informieren.	○ Ja ○ Nein
Dokumentation		
Sind die getroffenen Entscheidungen und veranlassten Maßnahmen schriftlich festgehalten?	› Nachvollziehbarkeit ist ein Muss. Dies gerade, wenn Datenschutzrelevanz besteht. Denken Sie hier insbesondere an die Ihrem Unternehmen obliegende Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO. › Achten Sie auf eine umfassende Dokumentation. Entscheidend ist: Wer hat was wann wie entschieden bzw. umgesetzt? Auch Begründungen sind festzuhalten.	○ Ja ○ Nein
Wurden datenschutzrelevante Aktivitäten geprüft und das Ergebnis dokumentiert?	› Gerade beim (kurzfristigen) Austritt oder Wechsel von Führungspersonen kann viel mit Datenschutzbezug zu prüfen sein. Die Prüfung, die Begründung und das Ergebnis sollten festgehalten werden. › Wichtig ist auch: Ihre Beratung als Datenschutzbeauftragter muss dokumentiert werden.	○ Ja ○ Nein

10 Tipps für Ihre gute Beziehung zum Betriebsrat

Vielleicht ist seit dem Frühjahr auch in Ihrem Unternehmen ein neuer Betriebsrat in Amt und Würden. Doch womöglich gab es bislang noch keine Gelegenheit, sich kennenzulernen oder auszutauschen. Das sollten Sie schnellstens nachholen. Schließlich sind Sie als Datenschutzbeauftragter auch für den Betriebsrat und dessen Verarbeitungen personenbezogener Daten zuständig.

Beherzigen Sie einige einfache Tipps

Klar ist: Eine gute Beziehung entsteht nicht von selbst. Gehen Sie die Sache geschickt an, indem Sie diese Tipps umsetzen:

Tipp Nr. 1: Starten Sie mit einem Gespräch

Warten Sie nicht, bis es zu einem Vorfall kommt oder Sie und der Betriebsrat in einer schwierigen Situation aufeinandertreffen. Unter Umständen steht dann die weitere Beziehung unter einem schlechten Stern. Besser ist, wenn Sie schnellstens die Initiative ergreifen. Versuchen Sie, einen persönlichen Kennenlerntermin zu arrangieren, und zwar mit dem ganzen Gremium. Geben Sie einem Termin vor Ort den Vorrang vor einem virtuellen Meeting. Sie bekommen so einen viel besseren Eindruck vom Betriebsrat und etwa der Situation vor Ort.

Tipp Nr. 2: Nehmen Sie den Betriebsrat ernst

Der Betriebsrat ist ein eigenständiges Gremium. Er ist unabhängig und in erster Linie Interessenvertretung der Arbeitnehmer. Im Rahmen seiner Aufgaben hat er viele Gestaltungsmöglichkeiten. Begegnen Sie daher dem Betriebsrat mit Respekt und auf Augenhöhe. Auch wenn Sie der Profi im Datenschutz sind, sollten Sie das nie nach außen zeigen und schon gar nicht den Betriebsrat spüren lassen. Im Gegenteil: Zurückhaltung ist angeraten und oft hilfreich.

Tipp Nr. 3: Lassen Sie keine Zweifel an Ihrer Rolle

Vertrauensbildend kann sein, dass Sie frühzeitig deutlich machen, welche Rolle Sie spielen. Sie sind nicht der verlängerte Arm des Arbeitgebers. Sie sind unabhängiger Berater in Datenschutzfragen und kontrollieren die Einhaltung des Datenschutzes im Unternehmen. Sie sind weisungsfrei und unabhängig in der Wahrnehmung Ihrer Aufgaben.

Tipp Nr. 4: Füllen Sie die Begriffe Vertraulichkeit und Vertrauen mit Leben

Basis für eine gute Zusammenarbeit sind Vertrauen und absolute Vertraulichkeit. Was man Ihnen anvertraut, das bleibt bei Ihnen. Dazu sind Sie sogar gesetzlich verpflichtet. Zudem sollten Sie dafür werben, dass man Ihnen Vertrauen schenken kann. Im Gegensatz zu vielen anderen Beschäftigten können Sie fachlich unabhängig agieren. Insofern brauchen Sie auch niemandem im Unternehmen Rechenschaft ablegen.

Tipp Nr. 5: Respektieren Sie die Autonomie des Betriebsrats

Zwar gehört der Betriebsrat zum Unternehmen. Allerdings ist er weitgehend autonom. Er kann sich selbst organisieren und sogar den Datenschutz für sich organisieren. Mischen Sie sich also nie in Entscheidungen des Betriebsrats ein. Sehen Sie etwas kritisch, führen Sie dazu eine Diskussion mit dem Betriebsrat. Das geht auch freundlich, sachlich und konstruktiv.

Tipp Nr. 6: Erst verstehen, dann bewerten

Beim Betriebsrat gibt es viele Verarbeitungen personenbezogener Daten. Manches mutet aus Ihrer Sicht seltsam oder falsch an. Doch heben Sie nicht gleich den Finger. Lassen Sie sich erklären, warum dieses oder jenes so ist. Bewerten Sie die Sache dann aus Ihrer Sicht und geben Sie Hinweise, was optimiert werden sollte.

Tipp Nr. 7: Beraten geht vor Kontrollieren

Vermeiden Sie, dass man Sie als Sheriff wahrnimmt. Zwar sollen Sie die Einhaltung des Datenschutzes kontrollieren, eben auch beim Betriebsrat. Allerdings macht hier der Ton die Musik. Auch Kontrollen können das Beraten im Fokus haben.

Tipp Nr. 8: Erleichtern Sie die Kontaktaufnahme

Wichtig ist, dass der Betriebsrat oder auch einzelne Mitglieder leicht mit Ihnen in Kontakt treten können. Erklären Sie, wo man Sie findet und wie man Sie auf direktem Weg erreichen kann. Dabei ist wichtig: Stellen Sie sicher, dass Sie gut und schnell erreichbar sind bzw. schnell reagieren können. E-Mails, die ewig unbeantwortet bleiben, sind der Killer für eine gute Zusammenarbeit.

Tipp Nr. 9: Halten Sie den Kontakt

Etablieren Sie nach Möglichkeit regelmäßige Austauschtermine. Zeigen Sie sich auch auf Betriebsversammlungen. Das ist einerseits Ihr gutes Recht als Arbeitnehmer. Andererseits zeigen Sie Interesse an relevanten Themen sowie an der Arbeit des Betriebsrats.

Tipp Nr. 10: Objektivität und Unabhängigkeit zählen

Lassen Sie sich nie vor den Karren spannen, weder den des Arbeitgebers noch den des Betriebsrats. Vermeiden Sie, dass man Sie irgendeinem Lager zurechnet. Sie sind in erster Linie den Betroffenen bzw. dem Datenschutz verpflichtet. Also sollten Sie die Dinge möglichst sachlich und objektiv betrachten.

Was müssen wir bei einer verspäteten Auskunft tun?

FRAGE: Ein Kunde hat sich beim Kundenservice per Brief gemeldet. Er machte mit dem Schreiben sein Recht auf Auskunft und Kopie geltend. Leider klappte intern die Weiterleitung nicht so richtig. Die Folge: Das Schreiben irrte intern herum. Die Erledigungsfrist aus Art. 12 Abs. 3 Datenschutz-Grundverordnung (DSGVO) war da schon um. Wir wollen schnell die Informationen bereitstellen, auch wenn wir schon über die Frist hinaus sind. Daneben fragen wir uns: Was müssen wir in Zusammenhang mit der verspäteten Auskunft tun? Droht uns etwa Ärger mit der Datenschutzaufsicht?

ANTWORT: Art 12 Abs. 3 DSGVO legt fest, dass unter anderem eine Auskunft nach Art. 15 DSGVO unverzüglich erfolgen muss. Die Bereitstellung der Informationen muss in jedem Fall innerhalb eines Monats nach Eingang des Antrags erfolgen. Nur bei komplexen Fällen oder vielen Anträgen kann eine Verlängerung der Frist um zwei weitere Monate erfolgen. Allerdings muss der Betroffene über die Fristverlängerung binnen eines Monats informiert werden. Das ist jedoch in Ihrem Fall nicht mehr möglich, da die Monatsfrist schon überschritten ist.

Auskunft schnell erteilen

Ihr Unternehmen sollte die Auskunft schnellstmöglich geben, um nicht noch mehr in Verzug zu geraten. Um einer eventuellen Verärgerung beim Betroffenen entgegenzuwirken, sollte Ihr Unternehmen sich für die Verzögerung entschuldigen. Erklären Sie, dass es aus organisatorischen Gründen etwas länger gedauert hat. Noch wirksamer kann es sein, wenn Ihr Unternehmen einen kleinen Gutschein für den Onlineshop beifügt. Denn das kann einen Kunden bzw. Betroffenen ggf. davon abhalten, sich bei der Datenschutzaufsichtsbehörde zu beschweren.

Die Sache kann Folgen haben

Allerdings muss das nicht unbedingt der Fall sein. So wäre es denkbar, dass die Aufsichtsbehörde nach einer Beschwerde aktiv wird. Möglich wäre in diesem Zusammenhang ein Bußgeld. Auch lässt sich nicht ausschließen, dass ein Betroffener Schadensersatz geltend macht. Hier können Sie nur zu einem raten: abwarten und Tee trinken. Unter Umständen ist die Sache dann für Ihr Unternehmen erledigt.

Folgeaktivitäten sind ein Muss

Zwar besteht an sich keine Meldepflicht gegenüber der Datenschutzaufsichtsbehörde nach Art. 33 DSGVO. Schließlich liegt nur ein Verstoß gegen die Anforderungen zu den Betroffenenrechten vor. Das stellt keine Verletzung der Sicherheit dar. Dennoch muss Ihr Unternehmen aktiv werden. So sollten unverzüglich die Prozesse überprüft werden und relevante Beschäftigte geschult bzw. eindringlich sensibilisiert werden. Schließlich sollte sich eine Verzögerung bei der Weiterleitung bzw. Bearbeitung einer Betroffenenanfrage nicht wiederholen.

Was muss ich bei den Unterlagen für meinen Nachfolger beachten?

FRAGE: Ich bin Datenschutzbeauftragter und gehe demnächst in Rente. Was muss ich bezüglich meiner Unterlagen beachten, welche ich meinem Nachfolger zur Verfügung stellen will, etwa Beratungsdokumente, Beschwerden oder Musterschreiben?

ANTWORT: Sichten Sie zunächst, was Sie alles aufbewahren. Denken Sie hier nicht nur an Digitales, etwa E-Mails und Dateien. Haben Sie auch ein Auge auf Unterlagen in Papierform. Prüfen Sie dann, was aus Ihrer Sicht für die Arbeit Ihres Nachfolgers von Relevanz ist. Hierzu kann es sinnvoll sein, auch die Wünsche und Bedürfnisse des Nachfolgers zu kennen. Fragen Sie ihn einfach.

Bei allem, was ohne Personenbezug ist, sind eine weitere Aufbewahrung bzw. Weitergabe und Nutzung unproblematisch. Allerdings kann es sinnvoll sein, Veraltetes und nicht mehr Relevantes zu löschen, um eine bessere Übersichtlichkeit zu erreichen. Bei Personenbezogenem sollten Sie genauer hinschauen. Beschwerden oder Schreiben, die sich an konkrete Personen richten, haben unter Umständen noch Relevanz. Grundsätzlich können Sie sich an einer Frist von drei Jahren orientieren, die beginnt, wenn ein Vorgang vollständig abgeschlossen ist.

Ist die Frist um und gab es auch keine rechtliche Auseinandersetzung, kann es sich anbieten, Unterlagen zu anonymisieren, etwa um diese als Muster weiterhin nutzen zu können. Bei Papierunterlagen ist es sinnvoll, diese einzuscannen und personenbezogene Informationen zu schwärzen.

SG Nürnberg: kein Ersatz hypothetischer Schäden

Hackerangriffe sind eine schlimme Sache, und zwar für Betroffene und das gehackte Unternehmen gleichermaßen. Gegenmaßnahmen zur Eindämmung von Schäden zu treffen ist aufwendig. Doch unter Umständen droht auch von anderer Seite Ärger: Betroffene, die Schadensersatz fordern. Das geht aber nicht so leicht, wie ein Urteil des Sozialgerichts (SG) Nürnberg vom 10.6.2026 (Az. S 5 SF 65/24 DS) zeigt.

Das führte zum Rechtsstreit

Ein 2018 geborenes Mädchen, die spätere durch die Mutter vertretene Klägerin, war bei einer Krankenkasse, eine der späteren Beklagten, versichert. Das Mädchen nahm an einem Bonusprogramm der Krankenkasse teil. Durch Aktivitäten konnten Bonuspunkte gesammelt werden, die zu Bonuszahlungen führten. Für das Programm nutzte die Krankenkasse eine App. Für deren Betrieb bediente sich die Kasse eines Auftragsverarbeiters, der später ebenfalls zu den Beklagten des Mädchens zählte. Eine Vereinbarung zur Auftragsverarbeitung war geschlossen. Schutzmaßnahmen waren konkret vereinbart. Der Auftragsverarbeiter setzte auf Software eines US-amerikanischen Unternehmens.

Hacker nutzen Zero-Day-Exploit aus

Nachdem Hacker schon mehrere Jahre versucht hatten, die Software des amerikanischen Unternehmens anzugreifen, gelang ihnen dies am 31.5.2023. Sie nutzten dazu eine bis dahin unbekannte Sicherheitslücke (sogenannten Zero-Day-Exploit). Dabei gelang es ihnen, sich Zugriff auf die auf den Servern gespeicherten Daten zu verschaffen, darunter auch Daten zur Klägerin. Betroffene Daten waren Vorname, Name, Krankenversicherungsnummer, Prämienbetrag sowie die IBAN. Letztere betraf jedoch das Konto der Mutter. Gesundheitsdaten waren keine betroffen.

Der Hackerangriff zielte nicht nur auf die Krankenkasse. Die Sicherheitslücke wurde bei rund 2.500 Unternehmen weltweit ausgenutzt. Als der Angriff bemerkt wurde, handelte der Softwarehersteller umgehend. Schon am 1.6.2023 wurde ein Sicherheitspatch bereitgestellt, um die Lücke zu schließen. Der Auftragsverarbeiter installierte das Update umgehend und informierte am 16.6.2023 die Krankenkasse über den Vorfall. Diese veröffentlichte zum Vorfall eine Pressemitteilung und informierte auch die Eltern als gesetzliche Vertreter der Klägerin.

Klägerin fordert 3.000 € Schmerzensgeld

Über ihren Anwalt forderte die Klägerin von der Krankenkasse die Zahlung eines Schmerzensgelds in Höhe von mindestens 3.000 €. Gestützt wurde die Forderung auf den Ersatzanspruch aus Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Die Krankenkasse hätte ihr obliegende Pflichten im Zusammenhang mit Art. 32 DSGVO missachtet. Insbesondere hätte sie nicht die nötigen Schutzmaßnahmen umgesetzt bzw. den Auftragsverarbeiter nicht angemessen beaufsichtigt. Durch den Diebstahl der Daten sei es bei der Klägerin zu einem anhaltenden Kontrollverlust über sensible Daten gekommen, was auch zu einer belastenden Ungewissheit über einen Missbrauch der Daten geführt hätte. Die Krankenkasse lehnte die Forderung ab. Also klagte das Mädchen, vertreten durch ihre Mutter, vor dem SG Nürnberg. Doch das Gericht wies die Forderungen zurück.

So entschied das Gericht

Es besteht kein Anspruch auf Schadensersatz, weder gegen die Krankenkasse als Verantwortliche noch gegen deren Auftragsverarbeiter. Die Voraussetzungen des Art. 82 Abs. 1 DSGVO sind nicht erfüllt.

Die DSGVO gewährt keinen absoluten Schutz personenbezogener Daten. Vielmehr wurde mit der DSGVO ein Risikomanagementsystem eingeführt, das auch in Art. 32 DSGVO zum Ausdruck kommt. Dem Verantwortlichen wird lediglich vorgegeben, durch technische und organisatorische Maßnahmen Verletzungen des Schutzes personenbezogener Daten so weit wie möglich zu verhindern. Kommt es zu einer Offenlegung personenbezogener Daten, etwa durch einen Hackerangriff, lässt sich daraus nicht schließen, dass die ergriffenen Schutzmaßnahmen des Verantwortlichen nicht geeignet waren.

Vorliegend konnte die Krankenkasse darlegen, dass die eingesetzte Software zum Zeitpunkt des Angriffs angemessen sicher war.

Kein immaterieller Schaden entstanden

Das Gericht erkennt keinen immateriellen Schaden. Die vorgebrachten Befürchtungen der Klägerin sind nicht begründet. So hat die zum Zeitpunkt des Vorfalls fünfjährige Klägerin nach Ausführungen des Vaters keine Kenntnis vom Vorfall. Zudem war das Bankkonto der Mutter betroffen und nicht das der Klägerin. Auch fehlen Anhaltspunkte, dass Daten zur Klägerin im Darknet aufgetaucht sind. Dies vor allem, weil es den Hackern um das Erpressen der betroffenen Unternehmen ging. Im Übrigen reicht das bloße Behaupten von Missbrauchsbefürchtungen nicht aus. Negative Folgen müssen nachgewiesen werden.

§

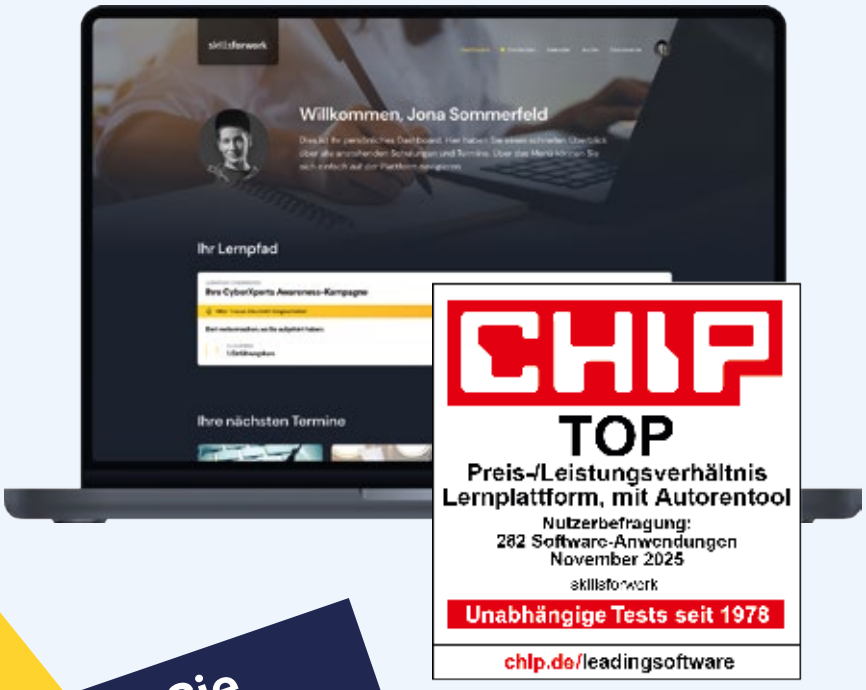
Das können Sie aus dem Urteil folgern

Ein Hackerangriff führt nicht automatisch dazu, dass Betroffene Schadensersatz vom Verantwortlichen fordern können. Hierzu braucht es mehr, etwa dass gebotene angemessene Schutzmaßnahmen unterlassen wurden. Zudem muss tatsächlich ein Schaden entstanden sein.

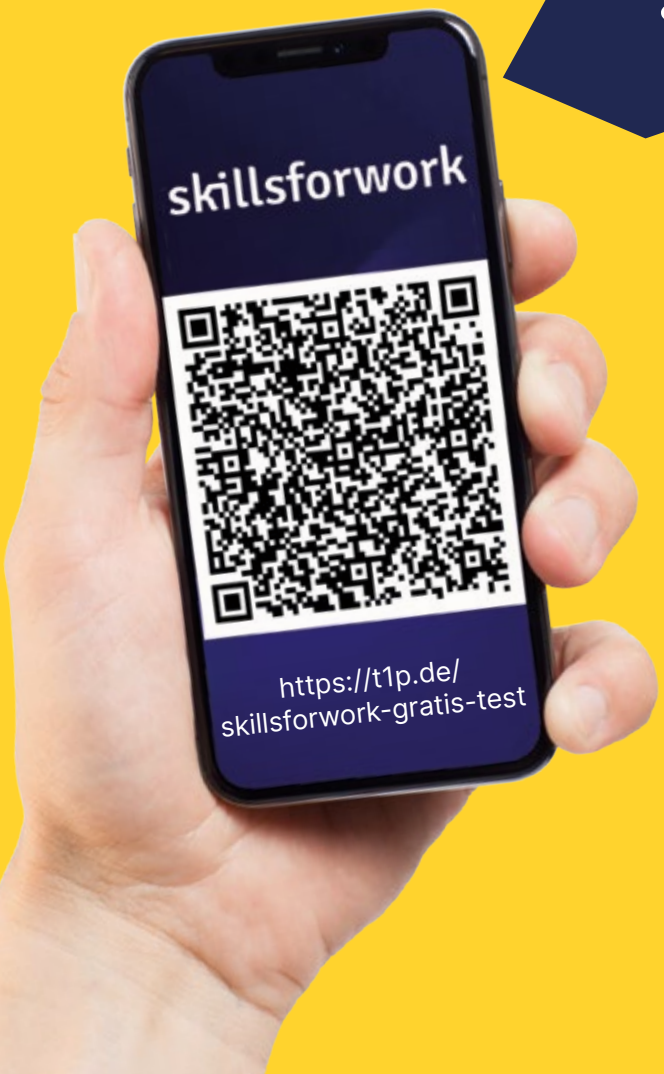
Die digitale Lösung für Ihre Pflichtschulungen

Arbeitssicherheit & Datenschutz

Schützen Sie Ihr Unternehmen vor Datenskandalen, hohen Strafzahlungen und Arbeitsunfällen, indem Sie geprüfte Schulungsunterlagen für Präsenz-, Online- oder E-Learning-Einheiten nutzen, den Lernfortschritt über kompakte Dashboards auf Mitarbeiter- oder Gruppenebene überwachen und Schulungen standortübergreifend zentral verwalten.



Testen Sie skillsforwork kostenlos



Compliance & ESG

Mit jährlich aktualisierbaren, individuell anpassbaren E-Learnings zu Compliance-, ESG- & KI-Compliance-Themen sensibilisieren Sie Ihre Mitarbeitenden wirksam durch alltagsnahe, interaktive Lerninhalte und sichern zugleich eine lückenlose Dokumentation des Lernfortschritts.

Cyber Security

Wirksame Awareness-Schulungen und individuell anpassbaren Phishing-Simulationen sensibilisieren Ihre Mitarbeitenden nachhaltig, während monatliche Reports Ihnen jederzeit einen klaren Überblick über das Sicherheitslevel Ihres Unternehmens geben.

skillsforwork

PRIVACYXPERTS

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

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

Vorschau:

In diesen Fällen ist Verschlüsselung ein Muss

Daten für den Betriebsrat? So können Sie prüfen