DATENSCHUTZAKTUELL

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

DEZ 2026

Schweiz



ANIMIEREN SIE BESCHÄFTIGTE ZU DATENSCHUTZ IM HOMEOFFICE

TRENDS & KI

Achten Sie bei Wissensdatenbanken auf diese Punkte 3

KNOW-HOW

Das ist zu prüfen, wenn der Chef das Unternehmen verlässt 4–5



Datenschutz ist eine Managementaufgabe

Liebe Leserin, lieber Leser,

vielleicht kennen Sie das: Geht es darum, dass Beschäftigte mit Personendaten arbeiten, meint vielleicht mancher aus dem Management, dass Sie sich um alles kümmern würden. Schliesslich sei das Ihr Job als Datenschutzberater. 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 Chefredaktor

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

Inhalt

Awareness
Animieren Sie Beschäftigte zu mehr Datenschutz im Homeoffice
Seiten 1–2

Trends & KI
Achten Sie bei Wissensdatenbanken auf diese Punkte
Seite 3

Know-how
Das ist zu prüfen, wenn der Chef das Unternehmen verlässt
Seiten 4–5

Datenschutzberater
So reagieren Sie auf Unqualifiziertes zum Datenschutz
Seite 6

Fragen an die Redaktion
Muss ich bei einem konsolidierten Tätigkeitsbericht mitmachen?
Seite 7

Was muss ich bei den Unterlagen für meinen Nachfolger beachten?
Seite 7

Urteil aus dem Ausland
SG Nürnberg: kein Ersatz hypothetischer Schäden
Seite 8

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

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

Expertenhotline:
https://kurzlink.ch/kontakt-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 Chefredaktor:
RA Andreas Würtz, Freiberg am Neckar

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

Erscheinungsweise: 17-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

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

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

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

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



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 Datenschutzberater 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 Datenschutzberater 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 Personendaten 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

Datenschutzberater

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 Personendaten 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 Datenschutzberater. › Sofortiges Melden ist wichtig, damit nicht grösserer Schaden entsteht. Und niemand macht Sie einen Kopf kürzer.	○ Ja ○ Nein

Achten Sie bei Wissensdatenbanken auf diese Punkte

Wissensdatenbanken sind vor allem für den Kundenservice ein wichtiges Werkzeug. Hat ein Kunde ein Problem, gab es genau dieses vielleicht schon öfters. Da ist die Lösung schnell gefunden, wenn man in einer Wissensdatenbank nach dem geschilderten Problem suchen kann. Beim Aufbau einer solchen Datenbank ist einiges zu beachten, gerade wenn auch noch KI ins Spiel kommt.

Wissensdatenbanken sind ein Datenschutzthema

Die in Wissensdatenbanken enthaltenen Lösungen gehen auf reale Fälle zurück und damit auf Kunden. Da gibt es Tickets, E-Mails, Uploads und andere kundenbezogene Informationen. Hier können viele Personendaten im Spiel sein. Doch an sich sind diese für einen „Lösungsvorschlag" in einer Wissensdatenbank nicht erforderlich. Also gibt es einiges zu tun, damit diese nicht zum Datenschutzproblem wird. Die beste Lösung: Alles, was einen Kunden identifizieren kann, sollte entfernt bzw. anonymisiert werden. Doch manchmal geht es nicht ohne Personenbezug.

Das hat es mit RAG-Systemen auf sich

Basierend auf einer Wissensdatenbank wagen immer mehr Unternehmen den nächsten Schritt: die Nutzung generativer KI in Verbindung mit Retrieval Augmented Generation (RAG). Ein RAG-System teilt beispielsweise grosse Textmengen aus einer Wissensdatenbank in Textabschnitte auf und überführt sie schliesslich in Zahlenreihen in eine Vektordatenbank. Wird dann über ein KI-Sprachmodell eine Frage des Servicemitarbeiters gestellt, werden die passenden Abschnitte in der Vektordatenbank gesucht. Aus dem Gefundenen wird dann eine Antwort erzeugt.

Checkliste: Wichtige Aspekte bei Wissensdatenbanken

Aspekt	Das ist wichtig	Geklärt?
Wissensdatenbank		
Ist der Zweck der Datenbank konkret festgelegt?	Der Zweck ist ein wichtiges Kriterium für die datenschutzrechtliche Zulässigkeit. Einziger Zweck sollte die „Nutzung als Lösungshilfe" sein.	○ Ja ○ Nein
Weisen die Inhalte Personenbezug auf?	Personenbezug kann im Hinblick auf Kunden und Mitarbeiter bestehen. Schauen Sie sich die Daten an.	○ Ja ○ Nein
Liegt eine Rechtsgrundlage vor?	Lassen Sie sich erläutern, worauf man die Bearbeitung von Personendaten stützt.	○ Ja ○ Nein
Ist der Grundsatz der Datenminimierung umgesetzt?	Nur Erforderliches darf bearbeitet werden. Bewerten Sie das im Hinblick auf den verfolgten Zweck.	○ Ja ○ Nein
Wurden Daten wo immer möglich anonymisiert?	Lassen sich Fälle komplett anonymisieren, ist der Datenschutz kein Problem.	○ Ja ○ Nein
Können Rechte betroffener Personen umgesetzt werden?	Sind Personendaten enthalten, können betroffene Personen auch Rechte geltend machen. Die muss Ihr Unternehmen umsetzen können.	○ Ja ○ Nein
KI und RAG-System		
Ist der Einsatzzweck klar festgelegt?	Das Gesamtsystem sollte nur ein Hilfsmittel für den Kundenservice sein und nicht für den direkten Kundenkontakt (z. B. als Chatbot) verwendet werden.	○ Ja ○ Nein
Wurde das Sprachmodell sorgfältig ausgewählt?	Das sollte mit den enthaltenen Informationen und der Sprache gut zurechtkommen. Hin-und-Her-Übersetzungen können Fehler und Kontrollaufwände verursachen.	○ Ja ○ Nein
Erfolgt der Betrieb auf eigenen Servern?	Das ist ideal. Geht das nicht, muss bei der Bearbeitung von Personendaten meist eine Vereinbarung zur Auftragsbearbeitung geschlossen werden. Denken Sie hier auch an Drittstaatentransfer nach Art. 16 Bundesgesetz über den Datenschutz (DSG).	○ Ja ○ Nein
Fliessen personenbezogene Informationen in die Vektordatenbank ein?	Am besten wird das vermieden. Die Umsetzung von Rechten betroffener Personen, z. B. Löschung, kann ansonsten aufwendig und teuer werden.	○ Ja ○ Nein
Wurde eine ggf. erforderliche Folgenabschätzung durchgeführt?	Gerade beim Einsatz von KI kann eine Datenschutz-Folgenabschätzung erforderlich sein. Ist diese nicht nötig, sollte auch das dokumentiert werden.	○ Ja ○ Nein
Ausserdem bei Wissensdatenbank, KI und RAG-System zu bedenken		
Passen die technischen und organisatorischen Schutzmassnahmen?	Denken Sie hier auch an Berechtigungen. Nur wer Zugriff für seine Arbeit braucht, sollte diesen auch haben.	○ Ja ○ Nein
Gibt es Regelungen und Dokumentationen?	Klare Regeln fördern richtiges Verhalten. Schauen Sie sich Regelungen und Dokumentation an. Ist wirklich alles Wichtige abgedeckt?	○ Ja ○ Nein
Sind die Nutzer in Sachen KI geschult?	Das ist zwar nicht gesetzlich vorgeschrieben, aber eine Schulung ist auf jeden Fall sinnvoll. Wissen schadet nicht.	○ Ja ○ Nein
Erfolgt die Dokumentation im Verzeichnis von Bearbeitungstätigkeiten?	Achten Sie darauf, dass die entsprechenden Angaben in das Verzeichnis aufgenommen werden.	○ Ja ○ Nein

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 Personendaten 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. 8 Bundesgesetz über den Datenschutz (DSG) 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 Datenschutzbeater 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 Datenschutzberater in erster Linie auf den Datenschutz und den Umgang mit Personendaten 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. 5 Buchst. j DSG.	○ 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 Personendaten 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 Berücksichtigung der Grundsätze aus Art. 6 DSG. › Achten Sie auf eine umfassende Dokumentation. Entscheidend ist: Wer hat was wann wie entschieden bzw. umgesetzt? Auch Begründungen sollten Sie festhalten.	○ 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 Datenschutzberater sollten Sie dokumentieren.	○ Ja ○ Nein

So reagieren Sie auf Unqualifiziertes zum Datenschutz

Früher oder später macht jeder Datenschützer Bekanntschaft damit. Die Rede ist von unqualifizierten oder populistischen Aussagen gegen den Datenschutz. Weil Sie im Unternehmen für viele der personifizierte Datenschutz sind, ist es kein Wunder, dass man Ihnen diese an den Kopf wirft. Die Vorwürfe brauchen Sie jedoch nicht schlucken. Drehen Sie einfach den Spiess um.

So reagieren Sie kompetent

Idealerweise beschäftigen Sie sich frühzeitig mit unqualifizierten Aussagen. Dann sind Sie nicht baff, wenn man Ihnen tatsächlich einmal etwas Unqualifiziertes um die Ohren haut. Überlegen Sie, wie Sie darauf reagieren und wie Sie die Aussagen entkräften können. Denn bei genauerem Überlegen lassen sich die Aussagen ganz schnell entkräften. Das zeigen Ihnen auch die folgenden Beispiele:

Die Aussage: „Der Datenschutz bremst unsere meisten Vorhaben und Pläne nur aus"

So gehen Sie damit um: Machen Sie klar: Meist trifft das nicht zu. Es handelt sich um gesetzliche Vorgaben, die schon frühzeitig in die Planung einzubeziehen sind. Verzögerungen werden nur als „Bremsen" empfunden, weil nachträglich Prüfungen, Bewertungen oder Anpassungen vorgenommen werden müssen. Manchmal müssen auch zunächst nicht bedachte Risiken behandelt oder Vereinbarungen mit Anbietern oder Dienstleister geschlossen werden. Das alles geht nicht von jetzt auf gleich.

Die Aussage: „Das machen doch alle so"

So gehen Sie damit um: Lassen Sie dieses Statement einfach so stehen. Denn meist stimmt nichts an der Aussage. Fragen Sie konkret nach, wer denn „alle" sein sollen. Fordern Sie Namen von anderen Unternehmen. Zudem sind die Fälle meist nicht identisch, sodass sich ganz andere Konstellationen im Datenschutz ergeben können.

Die Aussage: „Der Anbieter sagt, alles sei datenschutzkonform"

So gehen Sie damit um: Werten Sie das als ein positives Zeichen, dass der Anbieter sich anscheinend um den Datenschutz bemüht. Hinterfragen Sie jedoch, was konkret mit der Aussage gemeint ist, etwa die Ausgestaltung eines Services, die Festlegungen in einer Vereinbarung oder die Umsetzung im konkreten Fall Ihres Unternehmens. Im Übrigen können Sie feststellen: Unter Umständen handelt es sich nur um eine etwas überzeichnete Marketingaussage. Die hilft Ihrem Unternehmen nicht viel. Schliesslich ist und bleibt es für die Bearbeitung Personendaten verantwortlich.

Die Aussage: „Können Sie das nicht einfach freigeben?"

So gehen Sie damit um: Stellen Sie klar, welche Rolle und Funktion Sie haben. Sie sind der unabhängige Berater in Datenschutzfragen. Sie geben Empfehlungen, sie segnen nichts ab und geben nichts frei. Die Umsetzungsverantwortung und damit auch die unternehmerischen Entscheidungen im Zusammenhang mit einer Bearbeitung liegen beim Verantwortlichen, sprich der Unternehmensleitung.

Die Aussage: „Wir haben schon so viel Geld investiert. Wir können das nicht mehr ändern"

So gehen Sie damit um: Verdeutlichen Sie: Kam es zu Fehlentscheidungen oder vorschnellen Investitionen, ist das noch lange keine Rechtfertigung, um die geltenden gesetzlichen Anforderungen zu ignorieren. Empfehlen Sie, dass man Sie zukünftig frühzeitig einbindet, damit kostenträchtige Fehlentscheidungen vermieden werden.

Die Aussage: „Sie hätten schon viel früher sagen müssen, dass das so nicht umsetzbar ist"

So gehen Sie damit um: Gerade wenn schon viel Zeit und Geld in eine Bearbeitung investiert wurden, kann es ärgerlich sein, wenn sich erst spät herausstellt, dass die Sache nicht machbar ist. Verdeutlichen Sie hier, dass Ihre Einschätzung nicht auf bösem Wissen basiert. Vielmehr liegt es meist an der Komplexität der Materie bzw. an sich erst spät herausstellenden wichtigen Einflussfaktoren. Soweit möglich: Machen Sie Vorschläge, wie man dem Ziel möglichst nahekommen kann, ohne mit dem Datenschutz in Konflikt zu geraten.

Die Aussage: „Wir brauchen heute noch grünes Licht. Ansonsten müssen wir alles stoppen"

So gehen Sie damit um: Stellen Sie klar, dass eine qualifizierte und fundierte Einschätzung ihre Zeit braucht. Mit einer vorschnellen oder oberflächlichen Prüfung Ihrerseits ist niemandem gedient. Ob etwa ein Roll-out gestoppt wird, weil Ihre Einschätzung noch nicht vorliegt, entscheiden nicht Sie. Das ist eine unternehmerische Entscheidung. Bitten Sie darum, dass man Sie zukünftig rechtzeitig einbindet, damit ein Startdatum nicht gefährdet ist.

Die Aussage: „Wir machen das jetzt. Um den Datenschutzkram kümmern wir uns später"

So gehen Sie damit um: Zeigen Sie auf, dass ein solches Vorgehen geradezu fahrlässig ist. Vor Beginn einer Bearbeitung muss alles Erforderliche umgesetzt sein. Zum Start einer Bearbeitung muss alles passen. Ein gestuftes Vorgehen nach dem Motto „Wir starten und ziehen dann das Nötige nach" kennen weder das Bundesgesetz über den Datenschutz noch die dazugehörige Verordnung. Datenschutzverstösse müssen von Anfang an vermieden werden.

Die Aussage: „Sie sorgen dafür, dass im Datenschutz alles passt"

So gehen Sie damit um: Stellen Sie klar, dass Sie gerade nicht der Umsetzer sind. Sie beraten und kontrollieren. Auch geben Sie gerne Hilfestellung. Das Umsetzen ist jedoch allein Sache des Unternehmens.

Muss ich bei einem konsolidierten Tätigkeitsbericht mitmachen?

FRAGE: Bei unserem Unternehmen gibt es regelmässige Tätigkeitsberichte, etwa der Beauftragten für Compliance und Arbeitssicherheit. Auch ich als Datenschutzberater habe bislang einen eigenen Tätigkeitsbericht zum Ende des Jahres erstellt. Die Geschäftsführung fordert nun erstmalig einen konsolidierten Bericht, in dem alle Tätigkeitsberichte einheitlich dargestellt werden. Auch sollen Schlüsselthemen vorgegeben sein, die jeder Beauftragte auf das Jahr bezogen darstellen soll. Muss ich als Datenschutzberater bei einem konsolidierten Bericht mitmachen und mich mit den Kollegen abstimmen?

ANTWORT: Für betriebliche Datenschutzberater gibt es keine gesetzliche Pflicht zur Erstellung eines Tätigkeitsberichts. Dass Ihre Geschäftsführung einen Bericht einfordert, kann insbesondere folgende Gründe haben:

- **Risikomanagement:** Ihr Unternehmen muss Risikovorsorge treffen und bestehende Risiken aktiv managen, etwa zum Schutz von personenbezogenen Daten. Unter Umständen ist ein Tätigkeitsbericht eine wichtige Säule, um darauf basierend die Risiken effektiv zu steuern.
- **Informationsinteresse:** Auch wenn Sie Datenschutzberater sind, sind Sie zugleich Arbeitnehmer. Ein Arbeitgeber kann von einem Arbeitnehmer fordern, dass er einen Überblick darüber gibt, was er in seiner Arbeitszeit macht. Die entsprechenden Vorschrift Art. 321d Abs. 1 im Obligationenrecht ist eindeutig formuliert. Der Arbeitgeber darf Ihnen Weisungen erteilen und damit auch einen Tätigkeitsbericht anfordern. Das vor allem dann, wenn Sie keine Dinge offenbaren, die Ihrer Pflicht zur Vertraulichkeit unterliegen.

Konsolidierter Bericht grundsätzlich kein Problem

Dem Wunsch der Geschäftsführung nach einem konsolidierten und einheitlichen Bericht sollten Sie sich nicht verweigern. Das kann der Unternehmensleitung helfen, ein Gesamtbild zu erhalten. Schliesslich ist der Datenschutz nur ein Compliance-Thema unter vielen. Achten Sie bei der Abstimmung mit den Kollegen darauf, dass Ihre Vorstellungen von einem Bericht ausreichend berücksichtigt werden.

Klappt das nicht oder haben Sie vielleicht nicht genügend Platz, um alles Wichtige zu vermitteln, können Sie Folgendes machen: Sie nutzen den konsolidierten Bericht als Basis und geben eine Management Summary zum Stand der Dinge im Datenschutz. Im Bericht können Sie jedoch auf ausführliche Informationen in einem ergänzenden Bericht verweisen.

Reicht Ihnen der Verweis nicht aus, können Sie den Entscheidungsträgern einen ergänzenden Bericht auch per E-Mail zukommen lassen.

Was muss ich bei den Unterlagen für meinen Nachfolger beachten?

FRAGE: Ich bin Datenschutzberater und gehe demnächst in Pension. 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. Am einfachsten und auch am kollegialsten ist es, wenn Sie Ihren Nachfolger einfach fragen.

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 Personendaten 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. Auf diese Unterlagen sollten Sie ihren Nachfolger gesondert hinweisen.

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 Informationen, die sich auf konkrete Personen beziehen, 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) aus der deutschen Stadt 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.

§

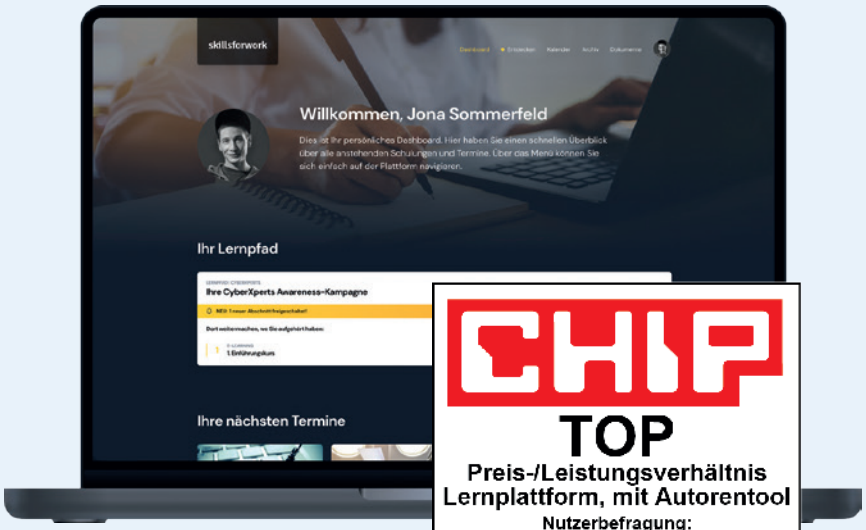
Das können Sie aus dem Urteil folgern

Ein Hackerangriff führt auch in der Schweiz nicht automatisch dazu, dass Schadensersatz vom Verantwortlichen eingefordert werden kann. Dafür braucht es etwas mehr. Die wichtigste Voraussetzung ist, dass tatsächlich ein Schaden entstanden ist.

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.



CHIP
TOP
Preis-/Leistungsverhältnis
Lernplattform, mit Autorentool
Nutzerbefragung:
282 Software-Anwendungen
November 2025
skillsforwork
Unabhängige Tests seit 1978
chip.de/leadingsoftware

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

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

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: kurzlink.ch/privacy

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

Vorschau:

Minimieren Sie die Risiken beim KI-Einsatz im Unternehmen

Kein Hexenwerk: So erstellen Sie Ihren Tätigkeitsbericht 2026