DATENSCHUTZAKTUELL Professional
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
MÄR I 2025

IM UNTERNEHMEN STEHT KURZARBEIT AN? DAS SOLLTEN SIE NUN AUF DEM RADAR HABEN

Kreativität lässt sich nicht erzwingen

Liebe Leserin, lieber Leser,

vielleicht geht es Ihnen manchmal wie vielen Autoren oder Journalisten: Sie wollen einen Artikel oder eine Präsentation erstellen. Kreativität ist also gefragt. Doch irgendwie ist es wie verhext: Selbst einfache Gedankengänge fallen Ihnen schwer und Sie bekommen keine geraden Sätze zustande. Irgendwie ist alles nur „Mist" an diesem Tag.

In solch einem Fall hilft meist nur eines: Belassen Sie es dabei und machen Sie Schluss, zumindest für diese Aufgabe und für den Augenblick. Quälen Sie sich nicht. Denn Kreativität lässt sich einfach nicht erzwingen. Starten Sie morgen einen neuen Versuch. Dann klappt es bestimmt.

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 pragmatisch umsetzen lässt.

Inhalt

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
www.privacyxperts.de/kontaktformular/

Bildnachweise:
Titel: Adobe Stock | CrazyCloud
Seite 1: Adobe Stock | DoodleDaze

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: Milena Eilers, 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, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Gelegenheit macht Diebe – sensibilisieren Sie die Kollegen dafür.

„World Backup Day" am 31.3.2025: Steigern Sie die Sensibilität für Back-ups

Wie jedes Jahr findet auch 2025 am 31.3. der „World Backup Day" statt. Das Sichern von wichtigen Daten ist über die Jahre immer wichtiger geworden. Dazu haben auch Cyberkriminelle beigetragen, die Daten stehlen, verschlüsseln und Lösegeld erpressen wollen. Wer dann ohne Back-up ist, hat ganz schlechte Karten. Nutzen Sie also den 31.3.2025, um die Sensibilität etwas zu steigern.

Sensibilisieren Sie im Handumdrehen

Awareness zu schaffen, kann ganz einfach sein. Als Aufhänger nutzen Sie den „World Backup Day" und schicken an Ihre Zielgruppe, etwa Führungskräfte, eine informative E-Mail. Dazu können Sie sich an nachfolgendem Muster orientieren. Kombinieren Sie das Ganze noch mit einer gemeinsam mit der IT-Abteilung angebotenen Sprechstunde, wird die Wirkung noch verstärkt. Denn meist ist klar: Setzen sich die Kollegen mit dem Thema auseinander, wird es Fragen geben.

MUSTER: Information zum Thema Back-up und Datensicherung

Liebe Kollegin, lieber Kollege,

aus der Betreffzeile wissen Sie, warum ich mich gerade heute an Sie wende. Genau, am heutigen 31.3.2025 ist „World Backup Day". Dieser „Gedenktag" soll für das wichtige Thema Datensicherung sensibilisieren. Denn ein Back-up von wichtigen Daten kann nicht nur im privaten Umfeld eine Art (Über-)Lebensversicherung sein, etwa wenn Daten (versehentlich) gelöscht oder von Cyberkriminellen zwecks Erpressung verschlüsselt wurden bzw. die Technik (z. B. Festplatte) den Geist aufgegeben hat. Setzen Sie sich also mit dem wichtigen Thema auseinander, und zwar für Ihren unmittelbaren Arbeitsbereich. Haben Sie ein Auge auf die Technik und die Daten, mit denen Sie arbeiten. Beugen Sie dem Datenverlust vor und sorgen Sie dafür, dass die unter technikaffinen Menschen gerne bemühte Weisheit „No backup, no mercy – keine Datensicherung, keine Gnade" sich nicht bewahrheitet.

Übrigens: Das Thema Datensicherung hat auch eine hohe Datenschutzrelevanz. So zählt das Sichern personenbezogener Daten zu den Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Dabei muss das Sichern selbst so erfolgen, dass dem Datenschutz entsprochen wird und beispielsweise unbefugter Zugriff ausgeschlossen ist.

Klären Sie für sich die folgenden Fragen:

Sind Daten dahingehend bewertet, ob und wenn ja für welchen Zeitraum auf sie verzichtet werden kann?
Das ist wichtig: Um eine passende Strategie für die Sicherung zu entwickeln, ist entscheidend, dass Sie objektiv bewerten, welcher Schutzbedarf und welche Verfügbarkeitsanforderungen bestehen. Geht es etwa um höchstsensible Informationen, kommt ggf. eine

MUSTER: Information zum Thema Back-up und Datensicherung (Fortsetzung)

Sicherung in der Cloud nicht in Betracht, selbst wenn die Daten dort verschlüsselt liegen würden. Auch hinsichtlich der Verfügbarkeit ist eine objektive und realistische Einschätzung unerlässlich. Machen Sie aus, welche maximale Ausfallzeit besteht, sprich die Zeit, in der Sie bzw. Ihr Bereich auf Technik, Software oder Daten verzichten können, ohne dass größerer Schaden entsteht. Bedenken Sie dabei, dass nicht nur das Sichern von Daten Zeit braucht. Auch das Wiederherstellen von Daten geht nicht von jetzt auf gleich.

Habe ich für mich und meinen Zuständigkeitsbereich festgelegt, für welche Daten eine Sicherung unerlässlich bzw. sinnvoll ist?
Das ist wichtig: Gerade wenn Sie eigene Technik oder Datenverarbeitungen verantworten, sollte es eine Festlegung geben, was wie für eine Weiterarbeit bereitzuhalten bzw. zu sichern ist. So können funktionierende Ersatzgeräte nötig sein, um bei einem Defekt weiterarbeiten zu können. Ähnlich ist es mit Software, Lizenzen und natürlich Datensicherungen.

Wurden spezifische Gefahren bewertet und Risiken daraus abgeleitet?
Das ist wichtig: Zunächst müssen Gefahren ausgemacht werden. Hier sollten Sie alles in Erwägung ziehen, auch das, was nicht passieren sollte. Wird etwa eine Datensicherung auf einer externen Festplatte gemacht, kann diese schnell nichts mehr bringen, wenn die Festplatte aus der Hand fällt. Auch eine schlecht funktionierende Software zur Datensicherung oder ein schwieriger Zugriff auf die Sicherung kann im Fall der Fälle zum Problem werden. Damit aus einer Gefahr ein Risiko wird, müssen Sie die Schadenshöhe und die Eintrittswahrscheinlichkeit abschätzen. Bei Ihrer Risikobewertung können Sie gerne die Unterstützung der Kollegen der IT-Abteilung anfordern.

Ist eine passende Datensicherungsmethode gefunden?
Das ist wichtig: Es gibt viele Möglichkeiten der Datensicherung. Alle haben Vor- und Nachteile. So ist eine Vollsicherung vollständig, aber das Sichern dauert sehr lange. Werden in der Folge nur noch Änderungen gesichert, geht das zwar schneller. Eventuell kann das aber zu Unvollständigkeiten führen. Auch wie und wo gesichert wird, hängt von den Umständen und Bedürfnissen in der konkreten Situation ab. So kann eine Sicherung in der Cloud eine Möglichkeit sein. Allerdings gibt es hier wiederum Risiken, die es bei lokalen und sicher aufbewahrten Datensicherungen eher nicht gibt, etwa das Risiko durch Cyberkriminelle. Klären Sie also mit der IT-Abteilung, was für Ihr Anwendungsszenario am besten passt. Hier wird man Ihnen auch Empfehlungen dazu geben, inwieweit Sicherungsmethoden kombiniert werden sollten. Außerdem können Sie sicher sein, dass die Datensicherungen zukunftssicher sind, sprich die Daten auch in Zukunft les- und wiederherstellbar sind.

Wurde ein Regelwerk für das Sichern von Daten erstellt, ist dieses aktuell und sind die Regeln allen relevanten Personen kommuniziert?
Das ist wichtig: Achten Sie darauf, dass klar geregelt ist, wer wie was machen muss, damit etwa Daten regelmäßig gesichert werden. Das ist vor allem wichtig, wenn die Sicherung nicht automatisch erfolgt. Doch Regeln aufschreiben allein reicht nicht. Sie müssen dafür sorgen, dass sie beispielsweise den zuständigen Mitarbeitern bekannt sind und dass man sie befolgt. Ggf. sind hier auch Kontrollen erforderlich, ob die Regelungen umgesetzt werden, ob sie noch passen bzw. ob Änderungen nötig sind.

Funktioniert die Datensicherung in der Praxis?
Das ist wichtig: Hier kann vor allem eines bedeutsam sein: Sicherungsprogramme erstellen meist einen Bericht zur erfolgten Sicherung. Wurden ggf. Verzeichnisse oder Dateien übersprungen oder gab es generelle Fehler, muss gehandelt werden. Schließlich passt etwas nicht. Und die Sache ignorieren geht nicht. Denn manche Daten sind eben nicht gesichert. Gerade auf die kann es im Fall der Fälle ankommen.

Außerdem ist wichtig: Der Zugriff auf gesicherte Daten bzw. die Wiederherstellung der Daten sollte ab und an probiert werden. Unter Umständen wird erst hier bemerkt, dass es irgendwo hakt. Lassen sich Sicherungen oder gesicherte Dateien später nicht öffnen, führt das zumindest zu erheblichem Aufwand bei der Problemlösung. Schlimmstenfalls sind die Daten verloren.

Wie werden die Datensicherungen vor unbefugtem Zugriff geschützt?
Das ist wichtig: Das ist gerade dann wichtig, wenn Daten in falsche Hände geraten können. Und das kann schneller passieren als gedacht. Wird etwa die externe Festplatte verloren, kann das auch datenschutzrechtlich zum Problem werden. Denn das kann einen meldepflichtigen Vorfall darstellen, worüber z. B. die Datenschutzaufsichtsbehörde binnen 72 Stunden zu informieren ist. Um dem und etwa auch einem unbefugten Zugriff auf gesicherte Daten in der Cloud vorzubeugen, müssen Sie auf Verschlüsselung setzen. Die muss dem Stand der Technik entsprechen. Lassen Sie sich dazu von der IT-Abteilung beraten. Übrigens: Beim Verschlüsseln steht und fällt die Sicherheit meist mit dem verwendeten Passwort. Achten Sie darauf, dass dieses möglichst komplex ist. Doch auch hier ist wichtig: Denken Sie daran, das sichere Passwort zu sichern.

Wie und wo werden die Datensicherungen gelagert?
Das ist wichtig: Auch das ist ein Thema, mit dem Sie sich eingehend auseinandersetzen müssen. Das vor allem dann, wenn Sie selbst die Datensicherung vornehmen, etwa auf einer externen Festplatte. So muss natürlich der Datenträger vor unbefugtem Zugriff geschützt sein und beispielsweise in einem Tresor, Raum oder sonstigen sicheren Behältnis aufbewahrt werden. Doch mindestens genauso wichtig ist, dass Sie typische Gefahren bedenken. Etwa Feuer und Wasser. Und es ist schlussendlich geboten, mehrere Sicherungskopien an unterschiedlichen Orten aufzubewahren. Das ist zwar mit Aufwand verbunden. Allerdings sinkt das Risiko, dass eine eigentlich vorhandene Sicherung unbrauchbar ist, weil etwa das bei einem Rohrbruch ausgetretene Wasser die Festplatte zerstört hat.

Sie haben Fragen zum Thema?
Besuchen Sie die gemeinsame Sprechstunde von IT-Abteilung und Datenschutzbeauftragtem, und zwar übermorgen von 15 bis 16 Uhr. Einladung folgt!

Einfachheit: Machen Sie das zu Ihrem Arbeitsmotto Nummer 1

Die Welt ist kompliziert: Das merkt jeder, egal, ob es um das Privat- oder Arbeitsleben, Politik und Wirtschaft oder die „Situation insgesamt und überhaupt" geht. Und gerade beim Schwerpunkt Ihrer Tätigkeit, dem Datenschutz, ist es nicht viel anders. Also ist wichtig, dass Sie die Dinge nicht noch komplizierter machen, als sie ohnehin schon sind. Setzen Sie auf diese drei Profi-Tipps:

Profi-Tipp 1: Achten Sie auf Ihre Sprache

Sprache ist entscheidend. Wollen Sie, dass sich der Datenschutz in die richtige Richtung entwickelt, müssen Sie viel reden und vermitteln. Insofern ist es für Ihren Erfolg von essenzieller Bedeutung, dass man Sie und Ihre Hinweise bzw. Empfehlungen versteht. Dazu müssen Sie sich sprachlich an dem orientieren, was Ihre Zielgruppe ausmacht.

Also: Menschen fällt es im Allgemeinen schwer, langen Sätzen konzentriert zuzuhören. Je länger Ihr gesprochener Satz ist, desto höher ist die Wahrscheinlichkeit, dass man Ihnen nicht mehr folgen kann. Ihre Botschaft verpufft also irgendwo auf dem Weg vom Ohr ins Gehirn Ihrer Zuhörer.

Daher: Nur wenn Sie es mit Menschen zu tun haben, die Kompliziertes gewohnt sind, kann Ihre Wortwahl bzw. auch Ihr Satzbau etwas komplizierter ausfallen. Doch auch diesen Menschen tun Sie einen großen Gefallen, wenn Sie nicht zu sehr auf eine anspruchsvolle Bildungssprache setzen. Beherzigen Sie insbesondere folgende Grundsätze:

- **Kurze, einfache Sätze:** Je einfacher der Satzbau ist, desto besser. Denn einfache Sätze sind eingängiger und bleiben leichter hängen. Achten Sie darauf, dass immer klar ist, was Sie meinen und was Bezugspunkt einer Formulierung ist. Setzen Sie möglichst auf die Faustformel für verständliches Texten: Ein Gedanke – ein Satz.

- **Maximal ein Nebensatz:** Vermeiden Sie nach Möglichkeit komplizierte Nebensatzkonstruktionen. Die sind bei Texten für viele Menschen schon Horror genug. Doch beim gesprochenen Wort ist meist garantiert, dass Ihnen der eine oder andere Zuhörer nicht mehr folgen kann. Sagen Sie also Nebensätzen den Kampf an. Sind sie nicht vermeidbar, versuchen Sie, diese kurz zu halten.

- **Normales Sprechtempo:** Reden Sie so, dass man Ihnen gut folgen kann. Auch wenn etwa bei einer Präsentation die Zeit drängt, bringt es nichts, das Sprechtempo zu erhöhen. Damit sorgen Sie für Unmut bei den Zuhörern. Denn die können Ihnen nicht mehr folgen oder schalten geistig ab. Besser ist es, wenn Sie Themen verkürzt darstellen oder ganz ausklammern. Übrigens: Es ist auch besonders wichtig, dass Sie deutlich sprechen. Genuscheltes kommt bei niemandem an.

- **Keine Fachbegriffe, Abkürzungen oder Anglizismen:** Wenn Sie unter Datenschützern sind, dann können Sie natürlich mit in dieser Zielgruppe bekannten Fachbegriffen oder Abkürzungen um sich werfen. Denn hier wird man meist verstehen, was Sie mit DSGVO oder einem Transfer Impact Assessment meinen. Außerhalb einer solchen Zielgruppe sollten Sie lieber von Datenschutz-Grundverordnung sprechen. Auch das Transfer Impact Assessment bei einem Drittstaatentransfer wird für einen „Nicht-Spezialisten" vom Begriff her selbsterklärend, wenn Sie es als Abschätzung der Folgen eines Datenaustauschs bezeichnen. Und ein verständlicher Begriff bleibt garantiert leichter im Gedächtnis.

Profi-Tipp 2: Erklären Sie die Welt, aber einfach

Reden Sie von einem schwierigen Thema und fragt Ihre Zuhörerschaft nicht nach, heißt das nicht, dass man Sie verstanden hat. Nur wenige Menschen geben gern offen zu, etwas nicht verstanden zu haben. Meist will man sich nicht die Blöße geben, dass man zu den „Nichtwissenden" zählt. Beugen Sie dem vor, indem Sie kurz und knapp auch die Dinge erklären, die nicht „Allgemeinwissen" sind. Dabei geht es nicht darum, dass Sie in die Details gehen. Meist reicht eine grobe und im konkreten Fall passende Erklärung aus.

Außerdem ist wichtig: Erklären Sie die Dinge so, dass sie leicht nachvollziehbar sind. Das heißt in kleinen Häppchen, schrittweise und auf das Wesentliche konzentriert. Als Orientierung können Ihnen die Erklärstücke aus der „Sendung mit der Maus" dienen. Die Dinge einfach zu erklären, kann zwar für Sie manchmal eine Herausforderung sein. Doch die Arbeit wird belohnt, wenn Sie ein „Jetzt hab ich es endlich verstanden" hören.

Auch wenn es um das Umsetzen oder richtiges Vorgehen geht, ist Einfachheit entscheidend. Können Sie Vorgehensweisen zum Beispiel als verständliche Schritt-für-Schritt-Anleitung darstellen, fällt den betreffenden Personen die Umsetzung garantiert leichter. Zudem fördern Sie, dass man die Dinge auch tatsächlich angeht.

Profi-Tipp 3: „Erst Pflicht, dann Kür"

Dieser Redewendung sind Sie bestimmt schon oft begegnet und vielleicht orientieren Sie sich bereits daran. Denn sie beschreibt ein schlaues Vorgehen. Gemeint ist nämlich, dass zunächst die grundlegenden Aufgaben oder Anforderungen angegangen werden, sprich die Basics. Erst dann widmet man sich dem, was darauf aufbaut, bzw. nimmt die spezielleren Aufgaben oder Anforderungen in Angriff. Manchmal trifft es die Sache noch besser, wenn Sie sich am Schulnotensystem orientieren. Entscheidend ist zunächst zu bestehen und etwa im Zeugnis eine Vier zu erreichen. Natürlich ist es gut, besser zu sein. Doch die Eins mit Sternchen muss es nicht immer sein. Denn das erfordert meist erheblich größere Anstrengungen. So ist es auch im Datenschutz.

Im Unternehmen steht Kurzarbeit an? Das sollten Sie nun auf dem Radar haben

Die Zeiten sind für viele Unternehmen schwieriger denn je. Egal, ob Konjunkturschwäche, Absatzprobleme oder Auftragseinbruch, bei vielen Unternehmen geht es jetzt ans Eingemachte. Ist das auch in Ihrem Unternehmen der Fall, will man vielleicht zunächst auf Kurzarbeit setzen. Das kann auch Relevanz für Sie als Datenschutzbeauftragten haben. So gehen Sie die Sache an:

Schritt 1: Klären Sie, was man vorhat

Geht es dem Unternehmen schlecht, zählt es zu den Pflichten der Unternehmensleitung, gegenzusteuern und passende Maßnahmen einzuleiten. Das muss nicht gleich die Reduzierung der Zahl der Mitarbeiter sein. Denn: Geht es dem Unternehmen wieder besser und sind gute Mitarbeiter nicht mehr an Bord, steht man vor dem nächsten großen Problem. Gute Mitarbeiter sucht nämlich nicht nur Ihr Unternehmen.

Besser ist es also, beispielsweise auf Kurzarbeit zu setzen, wenn die entsprechenden Voraussetzungen erfüllt sind. So muss der Arbeitsausfall auf wirtschaftliche Gründe (etwa Auftragsmangel, Lieferengpässe) oder ein unabwendbares Ereignis (z. B. Brand) zurückgehen. Steht Kurzarbeit im Raum, sollten Sie mit Blick auf den Datenschutz folgende Fragen klären:

- Welche Bereiche und Beschäftigten sind in welchem Umfang betroffen?
- Inwieweit hat der Arbeitsausfall bzw. die Kurzarbeit Datenschutzrelevanz?
- Bei welchen Verarbeitungen kann es zu Problemen kommen?
- Wie verändert sich die Risikosituation im Hinblick auf personenbezogene Daten?
- Inwieweit soll ich als Datenschutzbeauftragter betroffen sein?

Gute Frage: Wie steht es eigentlich mit Kurzarbeit beim Datenschutzbeauftragten?
Steht in Ihrem Unternehmen Kurzarbeit an, kann das zwar bedeuten, dass mehr oder weniger die gesamte Arbeit ruht. Auch als Datenschutzbeauftragter können Sie betroffen sein. Allerdings sollten Sie frühzeitig mit der Unternehmensleitung einige Dinge klären, wodurch die Entscheidung über Kurzarbeit in Ihrem konkreten Fall vielleicht doch noch einmal anders ausfallen kann. Erwähnen Sie beispielsweise Folgendes:

- Sind Sie Teilzeit-Datenschutzbeauftragter, sprich, nehmen Sie die Funktion neben einer anderen Tätigkeit wahr, ist die Einschränkung der anderen Tätigkeit zumindest unter Datenschutzaspekten unproblematisch.
- Für Vollzeit-Datenschutzbeauftragte bzw. generell im Hinblick auf die Funktion und die Wahrnehmung der Aufgaben eines Datenschutzbeauftragten sieht die Sache anders aus. Trifft Ihr Unternehmen die Pflicht zur Benennung eines Datenschutzbeauftragten, ändert sich an dieser Anforderung nichts, wenn es zu Kurzarbeit kommt. Ihr Unternehmen ist in jeglicher Hinsicht weiterhin Verantwortlicher für die von ihm betriebenen Verarbeitungen personenbezogener Daten und muss daher seinen Pflichten vollumfänglich erfüllen.
- Sie müssen Ihren Aufgaben nach Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO) auch dann nachkommen können, wenn beispielsweise in weiten Teilen des Unternehmens die Arbeit ruht. Das bedeutet insbesondere, dass Sie auch in Zeiten von Kurzarbeit für Fragen des Datenschutzes verfügbar und ansprechbar sein müssen.
- Das Unternehmen muss Sie auch während der Kurzarbeit in vollem Umfang bei der Erfüllung Ihrer Aufgaben unterstützen. Das kann bedeuten, dass Sie auch dann arbeiten können müssen, wenn etwa Büros geschlossen sind und Sie keinen Arbeitsplatz vor Ort haben. Insofern brauchen Sie eine entsprechende Ausstattung, um aus dem Homeoffice arbeiten zu können.
- Es bestehen für das Unternehmen viele Anforderungen, bei denen der Datenschutzbeauftragte eine Rolle spielt. So sind Sie bei allem frühzeitig einzubinden, was mit der Verarbeitung personenbezogener Daten zu tun hat. Genauso ist es bei der Datenschutz-Folgenabschätzung. Auch bei geltend gemachten Betroffenenrechten wird man Sie meist zurate ziehen müssen. Macht man das nicht und werden etwa Anfragen nicht bearbeitet, kann das Ärger mit Betroffenen und der Datenschutzaufsicht bedeuten. Auch ein Bußgeld ist drin.

Schritt 2: Schauen Sie, was Kollektivvereinbarungen bzw. Gesetze vorgeben

Kurzarbeit einfach arbeitgeberseitig anordnen ist meist nicht drin. Ist Ihr Unternehmen tarifgebunden, sollte Ihr Blick in Richtung Tarifverträge gehen. Diese können relevante Festlegungen zum Vorgehen und zur Umsetzung enthalten. Unter Umständen gibt es auch Betriebsvereinbarungen, die entsprechende und für Ihre Arbeit relevante Rahmenbedingungen setzen.

So können beispielsweise bestimmte Funktionen und Bereiche von Kurzarbeit ausgenommen sein. Auch Pflichten zur Dokumentation oder zur Arbeitszeiterfassung können größere Datenschutzrelevanz haben. Daneben sind auch gesetzliche Regelungen von Bedeutung. Steht Kurzarbeitergeld im Raum, müssen beispielsweise die Vorgaben des Sozialgesetzbuchs (SGB) III beachtet werden.

Schritt 3: Bringen Sie sich ein

Im Zusammenhang mit Kurzarbeit können auch viele Datenschutzfragen aufkommen. Etwa dazu, wie Arbeitszeiten dokumentiert werden müssen oder ob diese oder jene Verarbeitung zulässig ist.

Prinzipiell kann es auch zu „Kurzarbeit null“ kommen, sprich, die Arbeit fällt für die betreffenden Beschäftigten komplett aus. Hier kann Ihre Unterstützung gefragt sein, damit das „Herunterfahren“ auch unter Datenschutzaspekten gut funktioniert. Dazu können Sie beispielsweise die abgedruckte Checkliste für Führungskräfte und deren Bereiche zur Verfügung stellen.

Kurzarbeitergeld: Das sollten Sie dazu wissen

Kommt es zu Arbeitsausfall bei Beschäftigten, geht das im Regelfall auch mit Gehaltseinbußen einher. Ist mindestens ein Drittel der Beschäftigten in einem Betrieb von einem Entgeltausfall von über 10 % betroffen, kann Kurzarbeitergeld bezahlt werden. Das Unternehmen berechnet und zahlt das Kurzarbeitergeld an den Beschäftigten aus. Das sind 60 % des entfallenen Nettoentgelts; hat der Beschäftigte ein Kind, sind es 67 %.

Nach Beantragung bei der Bundesagentur für Arbeit erhält das Unternehmen eine entsprechende Erstattung.

Für die Beantragung bzw. für die Abrechnung des Kurzarbeitergelds gegenüber der Bundesagentur für Arbeit müssen auch personenbezogene Angaben gemacht werden, so z. B. in der „Abrechnungsliste für Kurzarbeitergeld“, welche Teil des Leistungsantrags ist. Aufzunehmen sind hier verschiedene Informationen zum jeweiligen Beschäftigten, etwa Name, Versicherungsnummer, Entgelt- und Steuerinformationen.

Hinsichtlich der Rechtsgrundlage für eine Datenübermittlung brauchen Sie sich hier nicht lange den Kopf zu zerbrechen. Einerseits ist die Verarbeitung erforderlich, um das Beschäftigungsverhältnis (§ 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz) bzw. ein Vertragsverhältnis mit dem Betroffenen (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO) durchzuführen. Andererseits ist die entsprechende Verarbeitung erforderlich, um arbeitgeberseitig ein gesetzliches Recht wahrzunehmen und Kurzarbeit bzw. Kurzarbeitergeld zu beantragen. Insofern greift als Rechtsgrundlage Art. 6 Abs. 1 Buchst. c DSGVO in Verbindung mit §§ 95 ff., 317, 319 f., 394 SGB III.

KURZCHECK: 7 Aktivitäten zur Vorbereitung auf Kurzarbeit

Aktivität	Hintergrund	Erledigt?
Risiken und To-dos identifizieren	› Überlegen Sie, was für die Zeit der Kurzarbeit in Ihrem Bereich wichtig ist bzw. was zum Problem werden kann. › Leiten Sie Aktivitäten für Ihr Team und sich selbst ab, terminieren Sie diese und achten Sie auf die rechtzeitige Umsetzung.	☐ Ja ☐ Nein
Stellvertreter arbeitsfähig machen	› Müssen einige Arbeiten von anderen weitergeführt werden, müssen diese sich in Ihrem Thema zurechtfinden. Dazu müssen Sie diese mit Informationen versorgen. Ideal sind ein schriftliches und mündliches Briefing. › Statten Sie den Stellvertreter mit den nötigen Berechtigungen aus, damit er die Aufgaben auch tatsächlich erledigen kann.	☐ Ja ☐ Nein
E-Mail-Postfach vorbereiten	› Eventuell gehen in Ihrem Postfach Nachrichten ein, um die sich jemand auch bei Ihrer Abwesenheit kümmern muss. Verweisen Sie den Absender einer E-Mail in einer Abwesenheitsnotiz auf den richtigen Ansprechpartner. Alternativ können Sie beispielsweise dem Vertreter lesenden Zugriff auf Ihr Postfach gewähren. › Räumen Sie einen Zugriff auf Ihr Postfach ein, sollten Sie dieses vorab aufräumen. Entfernen Sie Privates und alles, was Ihren Vertreter nichts angeht. Informieren Sie ggf. Kommunikationspartner über die Situation.	☐ Ja ☐ Nein
Clean Desk umsetzen	› Machen Sie reinen Tisch, bevor Sie in die Auszeit gehen. An Ihrem Arbeitsplatz sollte nichts mehr für Unbefugte zugänglich sein, was wertvoll ist oder unter Datenschutz- oder Vertraulichkeitsaspekten schützenswert ist. Schließen Sie also Notebook und Unterlagen mit personenbezogenen Daten weg. › Werfen Sie auch einen Blick auf Ihr Umfeld. Haben Kollegen etwas vergessen wegzuräumen, sollten Sie das erledigen und die Kollegen informieren.	☐ Ja ☐ Nein
Back-up durchführen	› Passieren kann immer etwas. Machen Sie sicherheitshalber noch ein Back-up, damit es zu keinem größeren Datenverlust kommen kann. Denn dieser wäre nicht nur ärgerlich. Er verursacht viel Frust und Arbeit. Auch kann die Sache meldepflichtig sein. › Haben Sie Fragen zur Umsetzung, sprechen Sie mit der IT-Abteilung. Diese hilft bei Auswahl der Methode und der praktischen Umsetzung.	☐ Ja ☐ Nein
Passwörter managen	› Arbeiten Sie längere Zeit nicht, können selbst die Passwörter in Vergessenheit geraten, bei denen Sie das nie denken würden. Daher: Sichern Sie Passwörter in einem Passwortmanager. › Prüfen Sie in diesem Zusammenhang, inwieweit Passwörter sicher sind und nicht mehrfach verwendet werden.	☐ Ja ☐ Nein
Kontaktaufnahme im Notfall ermöglichen	› Sprechen Sie mit weiterarbeitenden Kollegen, wie man Sie im Notfall erreichen kann. So können Sie ab und an etwa auf Ihrem dienstlichen Smartphone nachschauen bzw. Nachrichten abhören. › Hinterlegen Sie beispielsweise bei einer Vertrauensperson Kontaktdaten in einem verschlossenen Umschlag. Instruieren Sie die Person, wer in welchem Fall die Daten erhalten darf. Teilen Sie relevanten Mitarbeitern mit, wo Informationen verfügbar sind.	☐ Ja ☐ Nein

Künstliche Intelligenz und Datenschutz: Setzen Sie auf die Grundsätze

Künstliche Intelligenz, kurz KI, dürfte auch 2025 in vielen Unternehmen das Thema Nummer eins sein. Schließlich erhofft man sich davon bessere Angebote und Produkte, mehr Effizienz oder mehr Umsatz. Und ab und an werden im Zusammenhang mit KI auch personenbezogene Daten eine Rolle spielen. Ganz klar: Das ist dann auch Ihr Thema.

Die KI-VO spielt für Sie kaum eine Rolle

Mit der EU-Verordnung 2024/1689, der KI-Verordnung (kurz KI-VO), werden die Rahmenbedingungen zur Gestaltung und zum Einsatz von KI geregelt. Allerdings ist in der KI-VO nichts zum Thema Datenschutz enthalten. Woran das liegt? Ganz einfach, der EU-Gesetzgeber hat aus seiner Sicht bereits alles Relevante in der Datenschutz-Grundverordnung (DSGVO) geregelt. Dementsprechend finden Sie in Art. 2 Abs. 7 KI-VO und Erwägungsgrund 10 zur KI-VO die Festlegung, dass die DSGVO in Sachen Umgang mit personenbezogenen Daten unberührt bleibt. Also muss die DSGVO vorrangig angewendet werden.

Geben Sie Orientierung mit den Datenschutz-Grundsätzen

Werden Sie gefragt, was in Sachen KI und Datenschutz zu beachten ist, fangen Sie am besten bei den Basics an. Dabei können Sie die folgende Übersicht als Spickzettel nutzen:

ÜBERSICHT: Datenschutz-Grundsätze gemäß Art. 5 Abs. 1 DSGVO

Grundsatz	Ihre Erläuterung
Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 Buchst. a DSGVO)	› Im Prinzip gilt immer: Die Verarbeitung von personenbezogenen Daten ist nur erlaubt, wenn eine entsprechende Rechtsgrundlage für die Verwendung der Daten besteht. Dabei ist KI meist eher als eine Verarbeitungstechnologie anzusehen, bei der auf Basis eines Modells statistische Schlüsse gezogen werden. › Für das Verarbeiten personenbezogener Daten kommen insbesondere in Betracht: ○ Einwilligungen ○ Verträge oder vorvertragliche Maßnahmen mit dem Betroffenen ○ überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten
Transparenz, Treu und Glauben (Art. 5 Abs. 1 Buchst. a DSGVO)	› Zwar kennt auch die KI-VO Transparenzpflichten, etwa in Art. 50 KI-VO. Die haben jedoch nichts mit dem Transparenzgebot der DSGVO zu tun. › Dieses zielt darauf ab, dass die betroffene Person über das informiert sein muss, was mit ihren personenbezogenen Daten passiert. Denn nur dann ist sie in der Lage, ihre Betroffenenrechte (z. B. Auskunft, Berichtigung, Löschung) geltend zu machen. Die erforderliche Transparenz wird unter anderem durch die Informationspflichten gemäß Art. 12 ff. DSGVO erfüllt. › „Treu und Glauben" meint nicht den im deutschen Zivilrecht verankerten gleichnamigen Grundsatz. Europarechtlich interpretiert ist damit vielmehr „faires Verhalten" und „Waffengleichheit" gemeint.
Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)	› Der Zweck muss schon vor der Beschaffung der Daten festgelegt, eindeutig und rechtmäßig sein. Eine Weiterverarbeitung zu anderen Zwecken ist nur bei Vorliegen bestimmter Voraussetzung erlaubt. › Verarbeitungen personenbezogener Daten ohne konkreten Zweck sind unzulässig. Das gilt auch im Zusammenhang mit KI.
Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO)	› Gemeint ist: so wenig wie möglich und nur so viel wie unbedingt nötig. › Die betreffenden personenbezogenen Daten müssen dem Zweck angemessen und zur Erreichung des Zwecks erforderlich sein. › Mehr Daten oder diese auf Vorrat sammeln ist auch im Hinblick auf KI datenschutzrechtlich nicht machbar.
Richtigkeit der Datenverarbeitung (Art. 5 Abs. 1 Buchst. d DSGVO)	› Egal, ob personenbezogene Daten konventionell oder mit KI verarbeitet werden: Sie müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. › Sind die vorhandenen personenbezogenen Daten unrichtig, müssen die Daten unverzüglich berichtigt (Art. 16 DSGVO) oder unverzüglich gelöscht werden (vgl. Art. 17 Abs. 1 Buchst. d DSGVO). › Eine KI-Lösung muss ggf. überwacht werden, um falsche oder fantasierte Ergebnisse (Halluzinationen) zu erkennen.
Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO)	› Personenbezogene Daten unterliegen der Pflicht zur Löschung. Da macht es keinen Unterschied, ob KI zum Einsatz kommt. Die relevanten Aspekte ergeben sich aus Art. 17 DSGVO. › Besonders wichtig: Ist der Zweck der Verarbeitung erreicht, muss gelöscht werden. Nur wenn Aufbewahrungspflichten bestehen, etwa aus Gesetzen, dürfen die Daten weiterhin verarbeitet werden. › Werden Daten z. B. für KI-Trainingszwecke benötigt, sollten diese anonymisiert werden, um sie unproblematisch verwenden zu können.
Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO)	› Die Verarbeitung personenbezogener Daten muss sicher sein, auch wenn KI eingesetzt wird. Hierzu sind risikoangemessene technische und organisatorische Maßnahmen erforderlich. › Die Details zu angemessenen Schutzmaßnahmen ergeben sich aus Art. 32 DSGVO.

Datenschutzkonzept des Betriebsrats: Muss ich das abnehmen?

FRAGE: Bei uns gibt es einen Betriebsrat. Dieser ist sehr auf seine Unabhängigkeit und Eigenständigkeit bedacht. Nun hat der Betriebsrat ein Datenschutzkonzept erarbeitet und beschlossen. Darin legt er fest, welche Verarbeitungen es gibt und wie schutzwürdig die betreffenden personenbezogenen Daten sind. Außerdem ist geregelt, welche Schutzmaßnahmen umgesetzt werden müssen und welche Regeln die Mitglieder des Betriebsrats bei der Wahrnehmung ihrer Aufgaben zu beachten haben. Dieses umfassende Konzept hat man nun mir vorgelegt. Ich soll das Datenschutzkonzept abnehmen und die dadurch erzielte Datenschutzkonformität bestätigen. Daher meine Frage: Muss ich als Datenschutzbeauftragter wirklich eine Abnahme bzw. Bestätigung vornehmen?

ANTWORT: Es ist schon mal eine sehr gute Sache, dass sich der Betriebsrat dem Thema Datenschutz verschrieben hat und seine Verantwortung ernst nimmt. Denn: Selbst wenn das Unternehmen nach außen hin auch für die Verarbeitungen personenbezogener Daten des Betriebsrats verantwortlich ist, kann der Betriebsrat nicht nach Belieben schalten und walten. Denn für ihn gelten die Rahmenbedingungen der Datenschutz-Grundverordnung (DSGVO), was sich gerade aus § 79a Betriebsverfassungsgesetz ergibt. Das bedeutet insbesondere, dass auch für diese Interessenvertretung der Arbeitnehmer einige wichtige Rahmenbedingungen umzusetzen sind. Zu nennen sind insbesondere:

- **Grundsätze der Verarbeitung personenbezogener Daten:** Diese müssen auch bei jeder Verarbeitung im Zusammenhang mit der Wahrnehmung der Aufgaben des Betriebsrats beachtet werden.
- **Rechtsgrundlagen:** Die sind zwingend erforderlich, damit eine Verarbeitung personenbezogener Daten zulässig ist.
- **Sicherheit:** Jede Verarbeitung muss sicher sein. Insofern muss auch der Betriebsrat für seine Verarbeitungen risikoangemessene Schutzmaßnahmen ergreifen (Art. 32 DSGVO). Die Maßnahmen können technischer und organisatorischer Natur sein. Sie sind beispielsweise in einem Konzept festzulegen und auch in der Praxis umzusetzen.
- **Maßnahmen zur Gewährleistung der DSGVO:** Generell müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, um sicherzustellen und nachweisen zu können, dass eine Verarbeitung im Einklang mit der DSGVO steht (Art. 24 Abs. 1 DSGVO).

Erläutern Sie freundlich, was Sache ist

Ein Konzept ist eine gute Sache. Und Sie sollten sich dieses auch anschauen und im Bedarfsfall Verbesserungsvorschläge machen. Mehr können Sie als Datenschutzbeauftragter jedoch nicht machen. Erläutern Sie dazu Folgendes:

- Zu Ihren Aufgaben als Datenschutzbeauftragter zählt es nach Art. 39 Abs. 1 DSGVO, dass Sie das Unternehmen und dessen Beschäftigte zu allen Fragen des Datenschutzes beraten. Sie können also beim Finden von Lösungen unterstützen. Sie schreiben jedoch keine Lösungen vor.
- Sie sind keine Genehmigungsinstanz und geben nichts frei. Über die Verarbeitungen entscheidet derjenige, der Verantwortlicher ist, also der über Ob und Wie einer Verarbeitung bestimmt. Das kann auch das Betriebsratsgremium sein.

Was Sie empfehlen, orientiert sich an Ihrer unabhängigen Einschätzung der Situation, der geltenden Rahmenbedingungen und der konkret anzuwendenden Vorgaben. Aufgaben und Entscheidungen des Verantwortlichen können Sie nicht übernehmen, da dies zu Interessenkonflikten führen würde. Zu diesen darf es nicht kommen.

Verliert ein altes Ausbildungszertifikat mit der Zeit an Bedeutung?

FRAGE: Ich plane aktuell meine Weiterbildung für 2025. Vor einigen Jahren habe ich eine Ausbildung zum zertifizierten Datenschutzbeauftragten gemacht. Nach einer Prüfung habe ich auch ein Zertifikat erhalten, das meine Qualifikation bestätigt. Diesbezüglich frage ich mich: Verliert eine solche Zertifizierung nicht an Bedeutung, je länger die Ausbildung zurückliegt?

ANTWORT: Prinzipiell liegen Sie richtig mit Ihrer Einschätzung. Haben Sie eine Ausbildung mit einer Prüfung und einem Zertifikat abgeschlossen, wird damit ein bestimmter Wissensstand zum Zeitpunkt der Prüfung dokumentiert. Allerdings ist klar: Liegt die Ausbildung schon längere Zeit zurück, dürfte manches, was heutzutage im Datenschutz relevant ist, noch kein Thema gewesen sein. Das liegt einfach daran, dass sich die Datenschutzwelt fortlaufend ändert. Dazu tragen beispielsweise neue Technologien, Regelungen oder Rechtsprechung bei. Zwar ist ein altes Zertifikat nicht wertlos, weil es Ihnen z. B. Grundlagenwissen im Datenschutz bestätigt. Allerdings müssen Sie auf dieser Basis aufbauen und sich fortlaufend weiterbilden. Bei der Wahl Ihrer Weiterbildungsmaßnahmen sollten Sie darauf achten, dass Sie Teilnahmebestätigungen oder Zertifikate erhalten. So können Sie leichter belegen, dass Sie Ihr Know-how aktuell halten.

ArbG Duisburg: Unzulässige E-Mail über Mitarbeiter kann 10.000 € kosten

Gibt es Streit zwischen Chef und Mitarbeiter, fliegen manchmal auch per E-Mail die Fetzen. Wird jedoch mehr offenbart als zulässig, kann das für den Versender richtig teuer werden. Das zeigt ein Urteil des Arbeitsgerichts (ArbG) Duisburg vom 26.9.2024 (Az. 3 Ca 77/24).

Der Sachverhalt

Ein Mann, der spätere Kläger, war bei einem Verband für Luftsportvereine beschäftigt und leitete dort den Bereich Training. Dieser Verband vertrat die Interessen von 177 Luftsportvereinen und damit von rund 10.000 Vereinsmitgliedern. Dem Verband stand zum betreffenden Zeitpunkt eine Frau als Präsidentin vor, die spätere Beklagte. Geleitet wurde der Verband von einem Präsidium.

Streit führt zu problematischen E-Mails

Im Mai 2022 begann ein Streit zwischen Kläger und Beklagter zur Führung des Verbandspräsidiums und einem bestimmten Geschäftsführer. Nachdem der Kläger seit Mai 2022 mehrfach und ab November 2022 dauerhaft krank war, kam es im Mai 2023 zu einer Mail des Klägers an 24 Personen, darunter die Beklagte, das Verbandspräsidium und der betreffende Geschäftsführer. In der E-Mail erläuterte der Kläger seine gesundheitliche Situation und die Ursachen für seine Arbeitsunfähigkeit.

Präsidentin informiert Verbandsmitglieder

Ohne einen entsprechenden Präsidiumsbeschluss versandte die Verbandspräsidentin eine E-Mail an die rund 10.000 Verbandsmitglieder. Darin informierte sie, dass sich der Kläger im Krankenstand befinde. Auch hätte er haltlose Vorwürfe gegen den Geschäftsführer und die Beklagte in die Welt gesetzt. Man hätte mit dem Kläger in einen konstruktiven Dialog treten wollen, um eine vertrauensvolle Zusammenarbeit zu ermöglichen. Die Anstrengungen wären jedoch erfolglos geblieben. In der Folge hätte man dem Kläger das Arbeitsverhältnis gekündigt.

Kläger wird mit unangenehmen Fragen konfrontiert

Die arbeitsrechtliche Kündigung des Klägers wurde schließlich zurückgenommen. Die Beklagte wurde als Präsidentin abgewählt und verließ den Verband. Allerdings hatten die E-Mails der früheren Präsidentin für den Kläger negative Folgen. Seine Wahrnehmung: Er würde regelmäßig auf die in den E-Mails erwähnten Vorgänge angesprochen bzw. müsse diese erläutern und richtigstellen. Sein Name wäre negativ belastet. Die mit den E-Mails einhergehende Veröffentlichung sensibler Gesundheitsdaten hätten den Eindruck vermittelt, dass er krankfeiere und den Verband schädige. Im Übrigen war die per E-Mail erfolgte Veröffentlichung der sensiblen Daten ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO). Also verklagte er die ehemalige Präsidentin des Verbands auf Ersatz des immateriellen Schadens, und zwar in Höhe von mindestens 17.000 €.

So entschied das ArbG

Nach Ansicht des Gerichts besteht ein Anspruch auf Ersatz des immateriellen Schadens nach Art. 82 Abs. 1 DSGVO, allerdings nur im Umfang von 10.000 €.

Der für den Ersatzanspruch erforderliche Verstoß gegen die DSGVO liegt vor, und zwar gegen Art. 5 Abs. 1 Buchst. a DSGVO. Danach müssen personenbezogene Daten auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden. Die versendeten E-Mails der Beklagten, die auch Informationen zum Gesundheitszustand des Klägers enthielten, sind eine solche Verarbeitung. Diese war rechtswidrig. Es lag keine Rechtsgrundlage für die Verarbeitung vor. So fehlte es insbesondere an einer Einwilligung des Klägers. Diese kann auch nicht daraus geschlossen werden, dass der Kläger selbst eine E-Mail an einen ausgewählten Personenkreis schickte. Auch die anderen Rechtfertigungsgründe aus Art. 6 Abs. 1 Satz 1 Buchst. b bis f DSGVO greifen nicht.

Daneben ist auch ein Verstoß gegen Art. 9 Abs. 1 DSGVO gegeben. Als Gesundheitsdaten gelten auch Informationen zum früheren, gegenwärtigen und künftigen Gesundheitszustand. Ein Bezug zu einer Krankheit ist nicht erforderlich. Das Verarbeiten von Gesundheitsdaten ist verboten, wenn nicht die Ausnahmen nach Art. 9 Abs. 2 DSGVO greifen. Vorliegend waren die Ausnahmen nicht einschlägig, insbesondere fehlte die Einwilligung des Klägers.

Gericht sieht immateriellen Schaden

Durch die E-Mails hat der Kläger auch einen immateriellen Schaden erlitten. Dieser ergibt sich daraus, dass rund 10.000 Mitglieder des Verbands von seiner gesundheitlichen Situation erfahren haben. Dies führte dazu, dass er auch in seiner Freizeit auf die Vorgänge angesprochen wurde. Zugleich wurden sein Ruf und seine Reputation beschädigt.

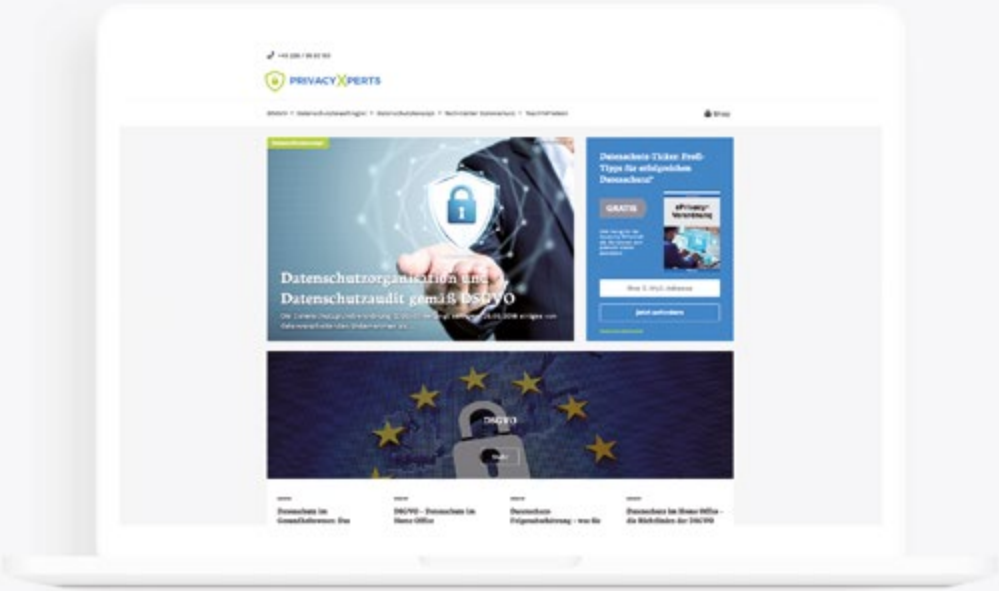
Die DSGVO misst dem Schadensersatz eine Ausgleichs- und keine Straffunktion bei. Für das Gericht ist daher ein Schadensersatz in Höhe von 10.000 € angemessen. Entscheidend hierfür war das Ausmaß der Beeinträchtigung, und zwar die Möglichkeit zur Kenntnisnahme besonders sensibler Daten durch rund 10.000 Empfänger der unzulässigen E-Mails.

§

Das können Sie aus dem Urteil folgern

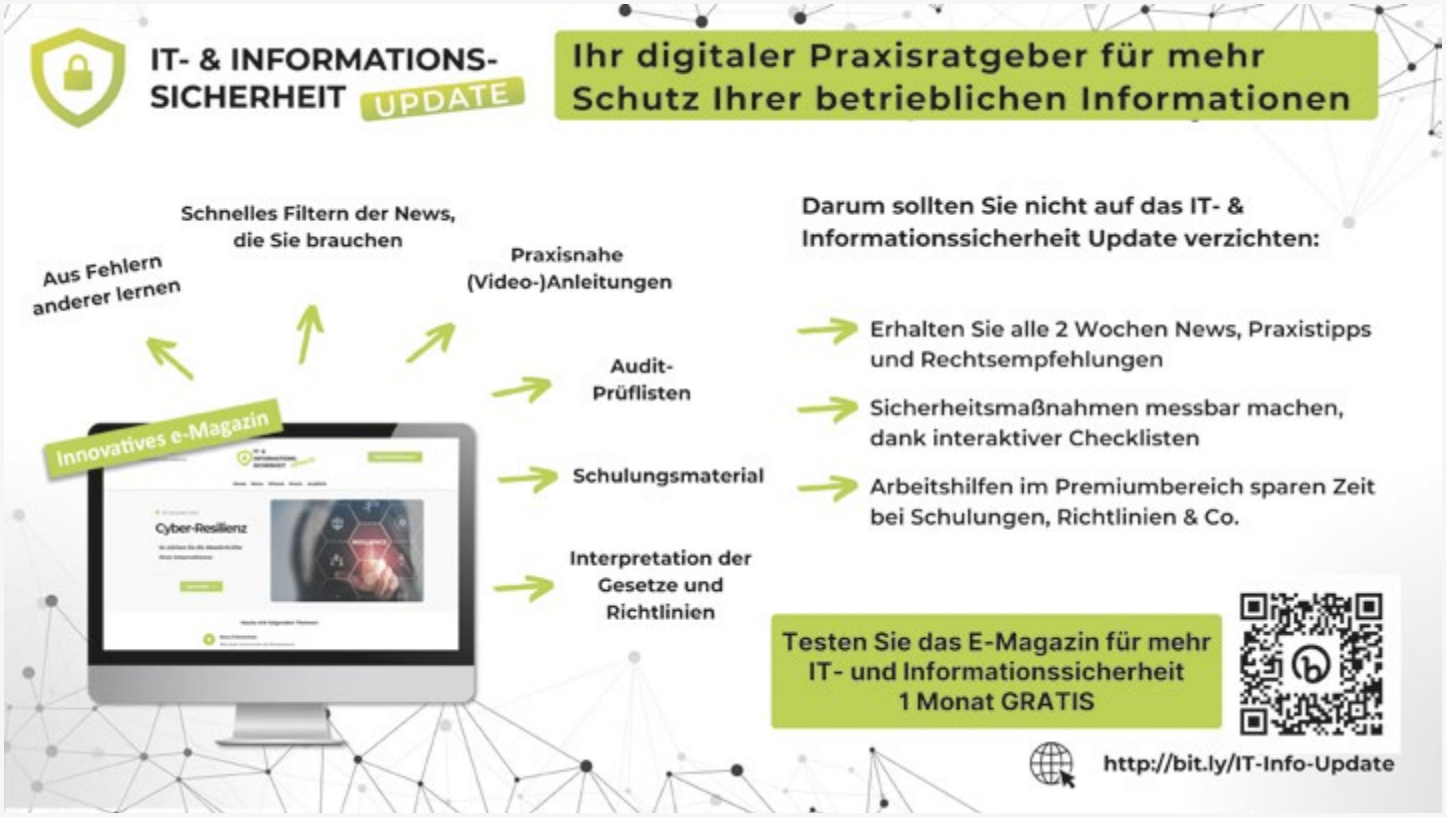
Der entschiedene Fall eignet sich bestens als Praxisfall für Schulungen. Er verdeutlicht, dass der unbedachte Umgang mit personenbezogenen Daten schnell zum Problem werden kann. Außerdem wird klar: Wer einen anderen schädigt, kann selbst haften müssen.

„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:

Zukunftstag 2025: Das sollten Sie ansprechen
Verstorbener Mitarbeiter: Was passiert mit dem Auskunftsanspruch?

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