DATENSCHUTZAKTUELL Professional
OKT 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
HERBST-SPEZIAL 2025

WERBUNG FÜR MEHR UMSATZ IM 4. QUARTAL: SCHAUEN SIE HIER GENAUER HIN

VORSORGE
Immer gut vorbereitet sein: Checken Sie die Notfallpläne Ihres Unternehmens 1–2

GESCHICKT VORGEHEN
Das sind Ihre Möglichkeiten, wenn Mitarbeiter aus der Reihe tanzen 4–5

Das Leben ist kein Ponyhof

Liebe Leserin, lieber Leser,

die Redewendung aus der Überschrift kennen Sie bestimmt. Und sie beschränkt sich nicht nur auf das Leben an sich, sondern gilt auch für Ihre Arbeit als Datenschutzbeauftragter. Gerade die Wahrnehmung Ihrer Aufgaben steckt voller Herausforderungen und Schwierigkeiten. Auch manche Enttäuschung kann es geben.

Doch auch wenn einiges eben nicht einfach oder angenehm ist, sollten Sie immer das Positive an Ihrer Arbeit sehen. Sie bewegen viel, auch im Interesse des Unternehmens. Machen Sie sich klar, was Sie leisten, und klopfen Sie sich mal selbst auf die Schulter. Dann kann Ihnen Negatives weniger anhaben.

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

Vorsorge
Immer gut vorbereitet sein: Checken Sie die Notfallpläne Ihres Unternehmens
Seiten 1–2

Prüfung
Werbung für mehr Umsatz im 4. Quartal: Schauen Sie hier genauer hin
Seite 3

Geschickt vorgehen
Das sind Ihre Möglichkeiten, wenn Mitarbeiter aus der Reihe tanzen
Seiten 4–5

Arbeitsorganisation
Sie wollen an Effizienz gewinnen? Diese 10 Tipps helfen
Seite 6

Fragen an die Redaktion
? *Reicht beim Löschen das Vernichten des Schlüssels aus?*
? *Wie soll ich mit einer nicht passenden Software umgehen?*
Seite 7

Rechtsprechung
BGH: Rein hypothetischer Kontrollverlust berechtigt nicht zum Schadensersatz
Seite 8

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
https://t1p.de/andreas-wuertz

Bildnachweise:
Titel: Adobe Stock | Jibber
Seite 1: Adobe Stock | Zerbor

Impressum

PRIVACYXPERTS

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

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda
(Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn

Satz: Deinzer Grafik, Gartow

Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 36-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

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

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

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

Besser rechtzeitig vorbereitet sein.

Immer gut vorbereitet sein: Checken Sie die Notfallpläne Ihres Unternehmens

Nicht nur Piloten wissen: Geht etwas schief und findet man sich in einer Notsituation wieder, ist es entscheidend, dass es funktionierende Notfallpläne und entsprechende Checklisten gibt. Auch wenn es um IT-Notfälle im Unternehmen geht, ist ein gutes Management der Situation entscheidend. Meist besteht hier auch eine Datenschutzrelevanz. Also sollten Sie einmal genauer hinschauen.

Die meisten Pläne haben mit Personenbezogenem zu tun

Viele Notfallpläne wird es im Zusammenhang mit der IT Ihres Unternehmens geben. Doch auch im Bereich Business Continuity, sprich in Sachen Fortsetzung des Geschäftsbetriebs, kann es Pläne für Notfälle geben. Dabei spielen bei den Plänen an sich, aber auch bei der Umsetzung der Pläne, personenbezogene Daten oft eine erhebliche Rolle. Etwa bei einem Sicherheitsvorfall können Sie selbst betroffen sein. Doch auch wenn Sofortmaßnahmen ergriffen werden, etwa wenn ein anderer IT-Dienstleister beauftragt wird, muss unter Datenschutzaspekten einiges bedacht werden.

Schauen Sie genauer hin

Generell liegt es im Interesse Ihres Unternehmens, dass Notfallpläne existieren und im Fall der Fälle funktionieren. Ansonsten könnte man sie sich auch gleich sparen. Also ist es gut, wenn Sie sich die Dokumente anschauen. Dabei brauchen Sie sich nicht auf die speziell für Datenschutzsachverhalte vorgesehenen Pläne zu beschränken. Und das können Sie auch gut begründen: Als Datenschutzbeauftragter haben Sie gemäß Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO) den gesetzlichen Auftrag, in allen Datenschutzfragen zu beraten und die Umsetzung der Anforderungen an den Datenschutz zu kontrollieren. Das umfasst auch, dass Sie Gefahren und Risiken ausmachen. Es liegt dann eben auch in der Natur der Sache, dass Sie festgestellte Defizite benennen und zum Ergreifen der nötigen Maßnahmen auffordern.

Machen Sie zudem klar: Das Reagieren auf Notfälle ist gerade im Hinblick auf den Datenschutz kein Freifahrtschein. Kommt es zu einer Verarbeitung personenbezogener Daten, müssen die Rahmenbedingungen stimmen. So müssen vor allem die Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) eingehalten werden. Passiert das nicht, drohen Ärger und hohe Bußgelder.

Sie wollen einen Notfallplan unter die Lupe nehmen? Kein Problem! Dazu können Sie die folgende Checkliste nutzen. Stellen Sie aus Ihrer Sicht Defizite fest, geben Sie den zuständigen Kollegen die entsprechenden Hinweise.

CHECKLISTE: Notfallpläne prüfen

Frage	Darauf kommt es besonders an	Geklärt?
Wie ist der Notfallplan bezeichnet?	Eine aussagekräftige Kurzbezeichnung ist wichtig, damit man im Fall der Fälle schnell zum richtigen Plan bzw. zur richtigen Checkliste greift. Gibt es viele Pläne, kann es sinnvoll sein, Kategorien zu bilden.	☐ Ja ☐ Nein
Wo ist der Notfallplan verfügbar?	Notfallpläne sollten an mehreren Stellen und idealerweise auf verschiedenen Trägermedien zur Verfügung stehen. Fällt die IT aus oder wurde der Ordner von Cyberkriminellen verschlüsselt, sind elektronische Versionen unbrauchbar. Gold wert sind dann ausgedruckte Pläne, etwa in einem roten Notfallordner. Auch eine Notfall-CD kann sinnvoll sein, die etwa an einem sicheren Ort aufbewahrt wird.	☐ Ja ☐ Nein

CHECKLISTE: Notfallpläne prüfen		
Welche Version liegt vor und wann war die letzte Aktualisierung?	Entscheidend für das Funktionieren von Plänen ist oftmals die Aktualität des Beschriebenen. Liegt die letzte Aktualisierung schon Jahre zurück, sollte schnellstens der Updatebedarf ermittelt werden.	☐ Ja ☐ Nein
Wer ist Ersteller bzw. Überarbeiter?	Schauen Sie, inwieweit Ersteller und Überarbeiter passen. Eventuell hat sich jemand darum gekümmert, der nicht im eigentlichen Thema steckt. Ein vom Qualitätsmanagement für die IT-Abteilung erstellter Notfallplan geht ggf. an den Erfordernissen vorbei.	☐ Ja ☐ Nein
Von wem wurde der Notfallplan freigegeben?	Notfallpläne machen viele Vorgaben zum Vorgehen bzw. zu Entscheidungen. Idealerweise werden Notfallpläne von denjenigen freigegeben, die die entsprechende Verantwortung tragen. Im Zweifel ist das die Unternehmensleitung.	☐ Ja ☐ Nein
Wie ist der Notfallplan kommuniziert worden?	Je nach Notfallplan muss dieser allgemein oder für eine spezifische Zielgruppe bekannt gemacht werden. Prüfen Sie auch, inwieweit die im Notfallplan vorgesehenen Stellen und Personen informiert sind.	☐ Ja ☐ Nein
Sind die relevanten Personen trainiert?	In jedem Notfallplan gibt es entscheidende Funktionen und Schlüsselpositionen. Die betreffenden Personen müssen mit ihrer Rolle zurechtkommen und auch im Notfall über nötiges Wissen verfügen. Fehlt es an der Handlungsfähigkeit, kann es zu verzögerten oder falschen Entscheidungen kommen.	☐ Ja ☐ Nein
Welche Rollen und Verantwortlichkeiten gibt es?	Prüfen Sie, inwieweit die zur Behandlung des entsprechenden Notfalls erforderlichen Funktionen und Rollen beschrieben sind. Dabei ist wichtig: Es kann entscheidend sein, dass Aufgaben oder Kompetenzen klar und eindeutig festgelegt wurden.	☐ Ja ☐ Nein
Ist der Notfallplan angemessen strukturiert?	Schauen Sie kritisch über den Notfallplan. Der sollte übersichtlich sein und alles Wesentliche sollte schnell erfasst werden können. Müssen erst „Bücher" gewälzt werden, kann das die Nutzer überfordern. Im Zweifel wird nur die Hälfte gelesen, schlimmstenfalls jedoch nicht das, worauf es ankommt. Vorsicht auch mit Querverweisen auf andere Regelungen.	☐ Ja ☐ Nein
Gibt es Sofortmaßnahmen und sind diese direkt erkennbar?	In Notfällen ist schnelles Handeln erforderlich. Prüfen Sie, inwieweit für die konkrete Situation Sofortmaßnahmen wichtig sind. Diese müssen gut erkennbar sein und sollten leicht umgesetzt werden können. Idealerweise handelt es sich um knappe und unmissverständliche Anweisungen.	☐ Ja ☐ Nein
Sind die enthaltenen Maßnahmen geeignet, das verfolgte Ziel zu erreichen?	Im Notfallplan sind Maßnahmen festgelegt. Die können passen, müssen es jedoch nicht. Auch hier kann sich seit der Erstellung des Plans einiges verändert haben.	☐ Ja ☐ Nein
Wurden Datenschutzaspekte berücksichtigt?	Nur weil es sich um einen Notfall handelt oder Schnellmaßnahmen ergriffen werden müssen, darf der Datenschutz nicht auf der Strecke bleiben. Haben Sie ein Auge darauf, wie die Zulässigkeit der Verarbeitung personenbezogener Daten gewährleistet wird.	☐ Ja ☐ Nein
Sind die Maßnahmen praktikabel und schnell umsetzbar?	Achten Sie auf die wahrscheinliche Wirksamkeit der vorgesehenen Aktivitäten. Dabei sollten die Maßnahmen so beschrieben sein, dass sie von einem Fachkundigen problemlos verstanden und umgesetzt werden können.	☐ Ja ☐ Nein
Ist beschrieben, wer welche Entscheidungen zu treffen hat?	Im Rahmen von Notfällen müssen Entscheidungen getroffen werden. Diese Befugnis kann einzelnen Personen oder einem Team zugewiesen werden. Bei einem Team sollte darauf geachtet werden, dass dieses entscheidungsfähig sein muss. Auch wichtig: Müssen erst andere Stellen gefragt werden, können sich zeitkritische Entscheidungen zu sehr verzögern.	☐ Ja ☐ Nein
Wurde festgelegt, welche Kommunikation es geben soll und wer diese übernimmt?	Gerade bei Notfällen mit Außenwirkung, etwa einer Datenpanne, sollte das Thema „Interne und externe Kommunikation" zumindest kurz im Notfallplan erwähnt werden. So z. B., dass jegliche Kommunikation über die entsprechenden Kollegen erfolgt.	☐ Ja ☐ Nein
Sind Stellen definiert, die zumindest themen- oder fallspezifisch einzubinden sind, beispielsweise der Datenschutzbeauftragte?	Was bzw. wer im Notfallplan nicht erwähnt wird, wird im Fall der Fälle unter Umständen vergessen, etwa auch der Datenschutzbeauftragte. Das kann bei datenschutzrelevanten Vorfällen auch schnell zum Problem werden, wenn etwa Meldefristen verpasst oder erforderliche Meldungen unterlassen werden. Sie unterstützen dabei, dass gerade das nicht passiert.	☐ Ja ☐ Nein
Wurde der Notfallplan geübt, erprobt bzw. in der Praxis bereits angewendet?	Papier ist geduldig. Ob ein Plan funktioniert, merkt man erst, wenn man ihn ausprobiert. Theoretische Trockenübungen sind hier zwar gut. Besser ist es jedoch, wenn der Ernstfall möglichst realistisch geprobt wird. Auch Planspiele helfen dabei, Fehler und Unzulänglichkeiten von Plänen zu erkennen.	☐ Ja ☐ Nein

Werbung für mehr Umsatz im 4. Quartal: Schauen Sie hier genauer hin

In vielen Wirtschaftszweigen laufen die Geschäfte 2025 allenfalls mittelprächtig. Kein Wunder also, dass man sich ins Zeug legen will, um in Sachen Umsatz im letzten Quartal noch etwas Boden gutzumachen. Und vielleicht denkt man in Ihrem Unternehmen auch über so manche umsatzsteigernde Maßnahme nach. Vieles ist hier datenschutzrelevant und damit ein Thema für Sie.

Setzen Sie auf die Verarbeitungsgrundsätze

Wann auch immer personenbezogene Daten eine Rolle spielen, ist die Sache an und für sich klar: Es müssen bei der betreffenden Verarbeitung die Grundsätze aus Art. 5 Abs. 1 Datenschutz-Grundverordnung (DSGVO) eingehalten werden. Das bedeutet, Ihr Unternehmen muss die folgenden Basics beachten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung und Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Das UWG ist häufig die entscheidende Hürde

Werbung ist oft das Mittel der Wahl, um Umsätze zu steigern. Doch wenn Werbung im Spiel ist, muss Ihr Unternehmen nicht nur ein Auge auf die DSGVO haben. Auch das Gesetz gegen den unlauteren Wettbewerb (UWG) setzt in Sachen Werbung wichtige Rahmenbedingungen. So kann manche Werbung nicht machbar sein, weil etwa § 7 UWG eine vorherige ausdrückliche Einwilligung vorschreibt.

Hier können Sie fündig werden

Sie wollen bei typischen Werbeaktivitäten einmal stichprobenartig prüfen? Kein Problem. Hier können Sie ansetzen.

CHECKLISTE: Prüfpunkte bei Werbeaktivitäten

Aktivität	Das sollten Sie berücksichtigen	Alles in Ordnung?
Adressgewinnung für Werbezwecke	› Um an Adressdaten von Verbrauchern zu kommen, denkt man vielleicht daran, das Internet, Webseiten oder soziale Netzwerke nach Adressen zu durchforsten und diese zu nutzen. Das kann nach hinten losgehen. Einerseits liegt ggf. ein Verstoß gegen die Nutzungsbedingungen vor. Andererseits sind manche Daten nur zur Erfüllung gesetzlicher Anforderungen veröffentlicht, z. B. in einem Impressum. Will man diese Daten verwenden, wird es mit der Rechtsgrundlage schwierig. › Der Zukauf von Adressen kann ebenso problematisch sein. Auch für deren Verarbeitung bedarf es einer Rechtsgrundlage. Besser ist es, etwa Daten im „Lettershop"-Verfahren zu nutzen. Ihr Unternehmen kommt mit den Daten nicht in Kontakt. Der Lettershop-Betreiber versendet dann eigenständig die Werbung Ihres Unternehmens an die von ihm verwalteten Adressen.	☐ Ja ☐ Nein
E-Mail-Newsletter mit integrierten Angeboten	› Hier ist entscheidend, dass der Inhaber der betreffenden E-Mail-Adresse in den Empfang des Newsletters wirksam eingewilligt hat. Das gilt für jede E-Mail-Adresse, und zwar unabhängig, ob diese einem Verbraucher gehört oder es sich um eine geschäftliche E-Mail-Adresse handelt. › Prüfen Sie, ob das Double-opt-in-Verfahren richtig funktioniert. Das ist wichtig. Schließlich muss Ihr Unternehmen das Vorliegen einer Einwilligung beweisen können (Art. 7 Abs. 1 DSGVO).	☐ Ja ☐ Nein
Werbe- und Rabattaktionen gegenüber Bestandskunden	› Vielleicht wird überlegt, Bestandskunden per E-Mail anzuschreiben und ihnen einen Gutschein zukommen zu lassen. Das ist jedoch nicht zulässig. Bei solchen E-Mail-Werbeaktionen bedarf es der vorherigen ausdrücklichen Einwilligung des Empfängers (§ 7 Abs. 2 Nr. 2 UWG). › Zwar kann die Sache auch ohne Einwilligung zulässig sein. § 7 Abs. 3 UWG formuliert jedoch strenge Anforderungen, die alle erfüllt sein müssen.	☐ Ja ☐ Nein
Cashback-Aktionen	› Hier wird versucht, den Absatz durch Rückerstattungen zu steigern. Wird z. B. Produkt A gekauft, werden 50 € erstattet. Die Rechtsgrundlage ist an sich meist nicht das Problem. Hier kann sich Ihr Unternehmen oft auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO stützen. › Schwierig kann es werden, wenn Rechnungen eingereicht werden müssen oder Bankverbindungsdaten erfasst werden. Achten Sie hier auf passende Schutzmaßnahmen.	☐ Ja ☐ Nein
Empfehlungswerbung durch Kunden	› Auch hier ist die Umsetzung entscheidend. Zum Problem kann es werden, wenn Ihr Unternehmen bei Kunden etwa E-Mail-Adressen anderer potenzieller Kunden sammelt und für Werbezwecke verwendet. Hier fehlt Ihrem Unternehmen die Einwilligung des Adressaten. › Eine unproblematische Ausgestaltung kann hingegen folgende sein: Ein Kunde kann sich Rabattcodes generieren. Diese kann er dann in Eigenregie an Freunde und Bekannte weiterleiten.	☐ Ja ☐ Nein
Gewinnspiele	› Prüfen Sie, inwieweit die in diesem Zusammenhang verarbeiteten personenbezogenen Daten erforderlich sind. › Sollen Daten (auch) für Werbezwecke verarbeitet werden, muss die Rechtsgrundlage passen. Oft geht es nicht ohne Einwilligung.	☐ Ja ☐ Nein

Das sind Ihre Möglichkeiten, wenn Mitarbeiter aus der Reihe tanzen

Datenschutz ist nicht unbedingt ein Thema, das alle im Unternehmen gut finden. Manche Führungskraft sieht darin nur Bürokratie und einen Bremsklotz, der die wirtschaftliche Entwicklung des Unternehmens hemmt. Doch auch bei Mitarbeitern kann es Verweigerer geben. Etwa, wenn es um die Teilnahme an Schulungen geht. Verweigerer sind ein Risiko, das Sie nicht einfach hinnehmen sollten.

Auch Schulungen sind wichtige Schutzmaßnahmen

Ihr Unternehmen ist in Sachen Datenschutz in der Pflicht. So sieht Art. 24 Abs. 1 Datenschutz-Grundverordnung (DSGVO) vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen muss, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Typische organisatorische Maßnahmen sind Regelungen, Anweisungen und eben das Vermitteln des nötigen Wissens. Letzteres klappt meist am besten, indem es Schulungen gibt.

Und dabei ist klar: Es gibt keinen Vorrang von technischen gegenüber organisatorischen Maßnahmen. Organisatorische Maßnahmen können im Einzelfall sogar entscheidend sein, damit bei der Verarbeitung personenbezogener Daten nichts schiefgeht.

Risiken nicht auf die leichte Schulter nehmen

Vielleicht tut mancher Schulungen im Datenschutz als „nicht so wirklich wichtig“ ab. Begegnen Sie jemandem mit dieser Ansicht, sollten Sie klarmachen: Jeder unsachgemäße Umgang mit personenbezogenen Daten bzw. jeder Verstoß gegen die DSGVO kann teuer werden. Da wäre nicht nur das Bußgeld, das in die Millionen gehen kann. Auch Imageschäden, Vertrauensverlust bei Kunden oder Umsatzrückgänge können die Folge sein. Dem allen kann auch mit Schulungen und dem Vermitteln des nötigen Know-hows entgegengesteuert werden.

„Durchrutscher“ sind nicht akzeptabel

Haben Sie immer ein Auge darauf, ob wirklich allen Mitarbeitern das nötige Know-how im Datenschutz vermittelt wurde. Dazu ist meist erforderlich, dass Sie etwa eine Übersicht führen, wer wann zu welchen Themen sensibilisiert wurde bzw. wer an welcher Schulung teilgenommen hat. Stellen Sie fest, dass manche Personen irgendwie immer durchs Raster fallen, sollten Sie hier schnellstens aktiv werden. Schließlich gilt auch im Datenschutz: Eine Kette ist nur so stark wie ihr schwächstes Glied. Viele Schutzmaßnahmen bringen nichts, wenn auch nur eine Person falsch handelt.

Wenn Mitarbeiter nicht mitziehen: Das sind Ihre Optionen

Was Sie typischerweise in Erwägung ziehen können, finden Sie in der folgenden Checkliste. Überlegen Sie jedoch stets, welche Maßnahme im konkreten Fall passend und angemessen ist. Versuchen Sie zunächst, den Mitarbeiter zu überzeugen. Klappt das nicht, können Sie schwerere Geschütze auffahren und beispielsweise den Vorgesetzten oder die Unternehmensleitung einbinden.

Schauen Sie nicht einfach weg
Teil Ihres Jobs als Datenschutzbeauftragter ist es, auch auf Risiken im Datenschutz hinzuweisen. Und jeder Mitarbeiter, der sich wichtigem Wissen verweigert, kann im Datenschutz eine tickende Zeitbombe sein.

CHECKLISTE: Reaktionsmöglichkeiten auf Datenschutzverweigerer

Ihre Möglichkeit	Das ist wichtig	Umgesetzt?
Suchen Sie das Gespräch.	› Verweigert ein Mitarbeiter die Teilnahme an einer Schulung, sollten Sie am besten den persönlichen Austausch suchen. › Im Gespräch können Sie schnell Licht ins Dunkel bringen. Sie können klären, warum jemand seine Teilnahme für nicht erforderlich hält. Vielleicht trifft das zu. Außerdem haben Sie die Gelegenheit zu begründen, warum die Teilnahme an einer Schulung immer eine gute Sache ist. › Stellen Sie im Gespräch fest, dass Inhalte oder die Aufbereitung nicht passen oder nicht mehr zeitgemäß sind, sollten Sie über eine Überarbeitung nachdenken. Bevor Sie jedoch alles infrage stellen, sollten Sie die Meinung anderer einholen, etwa von Kollegen mit entsprechendem Fachwissen oder anderen Teilnehmern Ihrer Schulung.	☐ Ja ☐ Nein
Überzeugen Sie mit guten Argumenten.	› Machen Sie sich im Vorfeld Gedanken dazu, was man Ihnen an Gründen für eine Nichtteilnahme liefern kann. So hält man die Schulung vielleicht für veraltet, langweilig oder praxisfern. Sammeln Sie dazu die passenden Gegenargumente. › Denken Sie bei den Argumenten auch an folgende: ○ Vermitteln von neuen Anforderungen, ○ Aufklärung über aktuelle Risiken, ○ Wissensaufbau und -aktualisierung, ○ Risikominimierung für das Unternehmen durch Mitarbeiter mit aktuellem Know-how und ○ Klärung individueller Fragen.	☐ Ja ☐ Nein

CHECKLISTE: Reaktionsmöglichkeiten auf Datenschutzverweigerer

Ihre Möglichkeit	Das ist wichtig	Umgesetzt?
Testen Sie das Wissen des Mitarbeiters.	› Im Gespräch können Sie einen Mitarbeiter auch dadurch überzeugen, dass Sie Fragen zu Themen stellen, die in der Schulung vermittelt werden. Das ist insbesondere dann angezeigt, wenn der Mitarbeiter äußert, die Inhalte alle schon zu kennen und zu wissen, worauf es ankommt. › Hinterfragen Sie vor allem die Aspekte, die in der täglichen Arbeit von Bedeutung sind. Gibt es in Ihrem Unternehmen einen neuen Prozess zum Vorgehen bei Datenpannen, fragen Sie konkret danach, wie der Mitarbeiter in einem solchen Fall vorgehen wird. Passt die Antwort nicht zu den Vorgaben, ist der Schulungsbedarf offensichtlich. So wird auch dem Mitarbeiter schnell klar, dass er doch besser an der Schulung teilnehmen sollte.	☐ Ja ☐ Nein
Machen Sie klar, dass Sie den Vorgesetzten einbinden müssen.	› Sie müssen hier nicht mit dem Vorgesetzten drohen. Erwähnen Sie nur, dass es Ihre Pflicht ist, auf Datenschutzrisiken angemessen zu reagieren. Dazu zählt es auch, mögliche Defizite oder Handlungsbedarf aufzuzeigen. › Verdeutlichen Sie, dass es hier nicht um „Petzen" geht. Der Vorgesetzte trägt die Verantwortung in seinem Zuständigkeitsbereich, etwa in seiner Abteilung. Das gilt auch für den Datenschutz und das richtige Verhalten der Mitarbeiter.	☐ Ja ☐ Nein
Sprechen Sie mit dem Vorgesetzten.	› Können Sie einen Mitarbeiter nicht mit Argumenten überzeugen, kann ein Gespräch mit dessen Vorgesetztem Wunder wirken. Machen Sie diesem klar, warum die Teilnahme an einer Schulung wichtig ist, etwa um aktuelles Wissen zu erhalten. › Zeigen Sie dem Vorgesetzten auf, dass er auch in der Datenschutzverantwortung steht. Handelt ein Mitarbeiter falsch, etwa weil ihm das nötige Wissen fehlt, ist das nicht allein das Problem des Mitarbeiters. Auch der Vorgesetzte hat Erforderliches zu unterlassen. Er hat nicht dafür Sorge getragen, dass die Mitarbeiter über das nötige Datenschutzwissen verfügen. › Verdeutlichen Sie, dass der Vorgesetzte sich bestimmt keinem Haftungsrisiko aussetzen will. Schaut er weg oder unterlässt er das Gebotene, kann unter Umständen auch er haftbar gemacht werden.	☐ Ja ☐ Nein
Zwingen Sie den Vorgesetzten zum Handeln.	› Geht es beispielsweise um einen Mitarbeiter, der sich schon mehrfach vor der Teilnahme an einer Schulung gedrückt hat, sollten Sie in Erwägung ziehen, dem Vorgesetzten einen Handlungsauftrag zu geben. Leiten Sie diesem die Schulungsfolien zu. Machen Sie deutlich, dass der Mitarbeiter leider wiederholt keine Teilnahme ermöglichen konnte, obwohl das Wissen wichtig ist. Nun ist es an ihm, dafür zu sorgen, dass der Mitarbeiter das nötige Wissen erhält. › Vergessen Sie nicht, die mögliche und für ihn einfachere Alternative zu erwähnen: Der Vorgesetzte sorgt dafür, dass der Mitarbeiter seine Teilnahme an der nächsten Schulung möglich macht.	☐ Ja ☐ Nein
Informieren Sie die Unternehmensleitung.	› Beißen Sie bei Mitarbeiter und Vorgesetztem auf Granit, sollten Sie mit der Unternehmensleitung sprechen. Diese kann problemlos ein Machtwort sprechen und beispielsweise auch direkt einem Mitarbeiter die Teilnahme an einer Schulung anweisen. › Machen Sie gegenüber der Unternehmensleitung klar: Auch Schulungen sind organisatorische Maßnahmen, um die DSGVO umzusetzen (Art. 24 Abs. 1 DSGVO). Geht etwas in Sachen Datenschutz schief und ist das auf unzureichendes Wissen zurückzuführen, kann das zum Problem für das Unternehmen und den Geschäftsführer werden. Dieser haftet nämlich auch gegenüber dem Unternehmen. › Erklären Sie zudem, dass geschulte Mitarbeiter Teil der Risikovorsorge sind. Werden Fehler und Pannen vermieden, kann ein entsprechender Schaden nicht eintreten.	☐ Ja ☐ Nein
Empfehlen Sie, dass das Nötige angewiesen wird.	› Das können Sie gegenüber dem Vorgesetzten bzw. der Unternehmensleitung anbringen. › Wird eine zumutbare Weisung erteilt, muss diese vom betreffenden Mitarbeiter auch befolgt werden. In der Regel wird es zumutbar sein, eine Schulung zu besuchen. › Alternativ können Sie dem Vorgesetzten die Schulungsunterlagen zur Verfügung stellen. Dieser kann die Unterlagen mit der Weisung an den Mitarbeiter weitergeben, dass die Inhalte zu beachten sind.	☐ Ja ☐ Nein
Bringen Sie mögliche arbeitsrechtliche Konsequenzen ins Spiel.	› Wird beharrlich eine Teilnahme verweigert, können Sie auch ins Spiel bringen, dass arbeitsrechtliche Konsequenzen in Betracht zu ziehen sind. Das kann zunächst eine Ermahnung bzw. eine Abmahnung sein. Letztere ist drin, wenn etwa Weisungen nicht befolgt werden. › Beherzigen Sie, dass Sie selbst nicht befugt sind, entsprechende Maßnahmen umzusetzen. Das ist Sache des Vorgesetzten, der Personalabteilung bzw. der Unternehmensleitung.	☐ Ja ☐ Nein
Dokumentieren Sie Ihr Vorgehen.	› Egal, wie die Sache verläuft: Achten Sie darauf, dass Sie Ihr Handeln und Ihre Vorschläge dokumentieren. Das gilt gerade dann, wenn man Sie bzw. Ihre Argumentation nicht unterstützt. › Lassen Sie dem betreffenden Mitarbeiter beispielsweise Schulungsunterlagen zukommen, sollten Sie auch das dokumentieren. › Führen Sie Buch über Mitarbeiter, die in Sachen Schulungen Nachholbedarf haben. Abhängig von Tätigkeit und Tätigkeitsbereich können solche Mitarbeiter auch zum Datenschutzrisiko werden. Fehlt etwa grundlegendes Know-how, kann hier leichter etwas schiefgehen oder Cyberkriminelle können leichter Erfolg haben.	☐ Ja ☐ Nein

Sie wollen an Effizienz gewinnen? Diese 10 Tipps helfen

Wer wenig Zeit für die Erledigung seiner Aufgaben hat, der ist schnell frustriert, gerade wenn es danach aussieht, dass einem alles über den Kopf wächst. Doch manches an solch einer Situation ist unter Umständen hausgemacht. Sie können jedoch schnell wieder Oberhand gewinnen und auch mit wenig Zeit gut zurechtkommen. Setzen Sie auf diese zehn Tipps:

Tipp 1: Arbeitstagebuch für 2 Wochen führen

Ärzte empfehlen Abnehmwilligen oft zunächst, ihr Essverhalten kennenzulernen und dieses entsprechend für einen längeren Zeitraum zu dokumentieren. Das ist auch ein guter Ansatz fürs Arbeitsleben. Halten Sie beispielsweise für zwei Wochen in einem Kalender oder in einer Tabelle fest, was Sie erledigt bzw. woran Sie gearbeitet haben. Befüllen Sie Ihr Arbeitstagebuch möglichst detailliert. So können Sie nämlich leichter ausmachen, was Sie machen und wofür Ihre Zeit hauptsächlich draufgeht. Vielleicht erkennen Sie so, dass Sie zu viel Zeit mit dem Beantworten von E-Mails verbringen.

Tipp 2: Zeitfresser identifizieren

Jeder kennt das: Manche Aufgabe oder Tätigkeit frisst viel Zeit, ohne dass am Ende ein gutes oder zumindest akzeptables Ergebnis steht. Stellen Sie zusammen, wofür Sie große Teile Ihrer Arbeitszeit aufwenden. Denken Sie aber hier nicht nur an das Arbeiten selbst, sondern auch das Drumherum. Kämpfen Sie tagtäglich längere Zeit mit Computer und Technik, geht auch das von Ihrer Arbeitszeit ab. Auch hier sollten Sie sich an die Problemlösung machen, um wieder mehr Zeit für die wirklich wichtigen Dinge zu haben.

Tipp 3: Bändigen Sie die E-Mail-Flut

Probieren Sie mal Folgendes aus: Lesen Sie E-Mails nur zu festen Zeiten am Tag, beispielsweise jeweils eine Stunde morgens, mittags und am Nachmittag. Die Zeiten dazwischen verwenden Sie auf konzentriertes Arbeiten. Sichten Sie den Posteingang und nehmen Sie gleich eine Bewertung vor. Was Sie bearbeiten oder beantworten müssen, terminieren Sie direkt mit einem Datum. Was eine lesenswerte Information ist, packen Sie in einen entsprechenden Ordner. Was ohne Relevanz ist, verschieben Sie direkt in den Papierkorb.

Tipp 4: „Schnell Erledigbares“ sofort abarbeiten

Vieles im Arbeitsalltag ist Kleinkram und lässt sich in fünf bis zehn Minuten erledigen. Diese Sachen sollten Sie nie erst auf eine To-do-Liste setzen und später bearbeiten. Das kostet garantiert zusätzliche Zeit, wenn Sie sich erst erneut mit der Sache beschäftigen müssen. Erledigen Sie die Sache lieber sofort. Nicht anders ist es, wenn Sie eine E-Mail schnell beantworten können. Dabei muss das nicht zwangsläufig per E-Mail passieren. Telefonieren geht ab und an noch schneller.

Tipp 5: „Salami-Taktik“ bei Komplexem anwenden

Manchmal müssen Sie auch als Datenschutzbeauftragter ganz schön dicke Bretter bohren. Das kann etwa eine komplexe Beratung sein oder das Entwickeln einer Managementpräsentation. Damit Ihnen das leichter von der Hand geht, sollten Sie den großen Brocken in kleine Häppchen zerlegen. Die lassen sich nicht nur schneller und leichter bearbeiten. Sie erzielen auch immer wieder Teilerfolge. Das hebt die Stimmung und hilft Ihnen, am Ball zu bleiben.

Tipp 6: Zuständigkeitscheck zum Standard machen

Machen Sie es wie der Sachbearbeiter in einer Behörde oder ein Richter bei Gericht: Bevor man dort in die Details einsteigt und sich intensiv mit einer Sache auseinandersetzt, fragt man sich: Ist das mein Thema? Bin ich überhaupt zuständig? Das sollten auch Sie sich fragen, und zwar bei allem, was Sie erledigen wollen. Eventuell merken Sie so nämlich, dass die Sache überhaupt nicht Ihr Ding und vielmehr die Bearbeitung anderswo besser aufgehoben ist. Will man z. B. einen Entwurf einer Betriebsvereinbarung von Ihnen, sollten Sie auf die Zuständigen verweisen, sprich Arbeitgeber und Betriebsrat.

Tipp 7: Konzentriertes Arbeiten ermöglichen

Blockieren Sie sich im Kalender Zeiten, in denen Sie ungestört und konzentriert arbeiten können. Idealerweise richten Sie sich Regeltermine ein, damit Ihnen hier niemand in die Quere kommt. Außerdem wichtig: Schalten Sie alles aus, was Sie ablenken kann, etwa Telefon und E-Mail-Benachrichtigungen.

Tipp 8: Fremdaufgaben abgeben

Halten Sie Ausschau nach Erledigungen, die Sie zwar machen, die aber nicht zu Ihren Kernaufgaben gehören. Versuchen Sie, diese wieder loszuwerden. Machen Sie dazu die Zuständigen aus und bitten Sie diese, dass sie ihre Aufgaben wieder selbst erledigen.

Tipp 9: Ziele kurz-, mittel- und langfristig planen

Damit Sie besser mit der Zeit zurechtkommen, sollten Sie Ziele haben und diese kurz-, mittel- und langfristig planen. Machen Sie auch immer wieder einen Check, ob Ziele oder Prioritäten noch passen. Ist etwas nicht mehr so wichtig bzw. dringend, können Sie es nach hinten verschieben. Dann haben Sie Zeit für Wichtigeres.

Tipp 10: Mehrbedarf adressieren

Auch das kann passieren: Trotz aller Bemühungen reicht Ihre Zeit nicht aus, um Ihre Aufgaben sachgerecht und professionell zu erledigen. Dann gibt es nur eines: Reden Sie mit der Unternehmensleitung und besprechen Sie den bestehenden Mehrbedarf.

Reicht beim Löschen das Vernichten des Schlüssels aus?

FRAGE: Bei einer kürzlich durchgeführten Schulung zum Datenschutz kam eine Diskussion zum Thema Löschen auf. So ging es um Datenträger und Smartphones, auf denen Daten verschlüsselt abgelegt sind. Ein Teilnehmer meinte, dass ein Löschen überflüssig sei, weil man beispielsweise an verschlüsselte Daten auf einem Datenträger nur mit dem betreffenden Schlüssel herankommen könne. Auch reiche es in der Regel aus, wenn ein Smartphone in den Werkszustand zurückgesetzt werde. Ich war bislang der Auffassung, dass man immer auf Nummer sicher gehen muss und Datenträger etwa mit spezieller Löschsoftware zu löschen sind. Was meinen Sie: Reicht das Vernichten eines Schlüssels oder das Zurücksetzen in den Werkszustand aus Datenschutzsicht aus?

ANTWORT: Ihr Unternehmen muss als Verantwortlicher immer sicherstellen, dass den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprochen wird. Das gilt für jede Form der Verarbeitung personenbezogener Daten und somit auch für das Speichern von Daten auf Datenträgern. Damit beispielsweise unbefugter Zugriff ausgeschlossen wird, müssen risikoangemessene Schutzmaßnahmen ergriffen werden (Art. 32 DSGVO). Insofern kann es eine gute technische Maßnahme sein, personenbezogene Daten auf Datenträgern zu verschlüsseln. Entscheidend ist hier, dass die Verschlüsselung dem Stand der Technik entspricht, sprich auf der Höhe der Zeit ist.

Auch das Löschen von personenbezogenen Daten ist eine Form der Verarbeitung personenbezogener Daten, was sich aus Art. 4 Nr. 2 DSGVO ergibt. Insofern müssen auch hier risikoangemessene Schutzmaßnahmen ergriffen werden, damit den Anforderungen der DSGVO entsprochen wird und solche Daten nicht in falsche Hände geraten.

Es kommt ganz darauf an

In der Tat kann es ggf. ausreichen, wenn Daten verschlüsselt bleiben und der Schlüssel zum Entschlüsseln der Daten „weggeworfen", sprich vernichtet wird. Allerdings ist hier zu bedenken: Die Daten sind noch vorhanden. Es ist lediglich der Zugriff auf die Daten erschwert. Im Einzelfall kann jedoch mit entsprechendem Aufwand die Verschlüsselung überwunden oder ein Schlüssel neu generiert werden. Auch ist zu beachten: Eine Verschlüsselung bzw. ein verwendetes Format oder eine genutzte Software mag heute sicher sein. Ob sie das morgen noch ist, kann niemand vorhersagen.

So kann die Methode oder die Verschlüsselungstechnologie einfach veralten und nicht mehr zeitgemäß sein. Auch können Bugs oder Sicherheitslücken dazu führen, dass eine Methode nicht mehr sicher ist. Um dieses Risiko auszuschließen, kann es geboten sein, auch verschlüsselte Daten zu löschen. Das passiert meist durch Überschreiben der entsprechenden Speicherbereiche. Ist das passiert, kann nach menschlichem Ermessen nichts wiederhergestellt werden. Ob ein Löschen verschlüsselter Daten geboten ist, sollten Sie auch von der Schutzwürdigkeit der betreffenden Daten abhängig machen.

Beim Smartphone sollte auch genau hingeschaut werden. Entscheidend ist auch hier die Frage, inwieweit mit dem „Zurücksetzen in den Werkszustand" tatsächlich eine Wiederherstellung von Informationen ausgeschlossen ist. Waren das Gerät bzw. die darauf gespeicherten Daten verschlüsselt und wird der Werkszustand wiederhergestellt, muss das Gerät neu eingerichtet werden. Das führt dazu, dass für die Verschlüsselung der Daten ein neuer Schlüssel erzeugt wird und beispielsweise an eine PIN oder andere ID geknüpft wird. Aber auch hier sollten Sie immer genau hinschauen. Beim Zurücksetzen sollte alles gelöscht werden und nicht nur die Einstellungen.

Wie soll ich mit einer nicht passenden Software umgehen?

FRAGE: Bei uns wurde eine Software zum Kundenmanagement beschafft. Die Datensätze enthalten zahlreiche Felder, die ggf. problematisch sein könnten, etwa Freitextfelder zu Kundenvorlieben. Ich habe als Datenschutzbeauftragter darauf hingewiesen, dass bestimmte Felder nicht genutzt oder am besten deaktiviert werden sollen. Das lässt sich technisch nicht bzw. nur für viel Geld durch den Anbieter umsetzen. Also will man die Software unverändert einsetzen. Wie soll ich mit der nicht passenden Software umgehen?

ANTWORT: Sie sollten mit den Kollegen daran arbeiten, die Sache datenschutzkonform auszugestalten. Zwar wäre es besser, wenn sich bestimmte Felder deaktivieren ließen. Dann kann dort auch nichts Unzulässiges eingetragen werden. Ist das nicht machbar, ist das nur die technische Seite. Auch organisatorisch kann dafür gesorgt werden, dass es zu keinen entsprechenden Eintragungen kommt. So kann in einer Regelung festgelegt werden, dass keine entsprechenden Angaben gemacht werden dürfen oder die Felder leer bleiben müssen. Dass dies umgesetzt wird, lässt sich ggf. mit einer Auswertung kontrollieren. Das kann eine zuständige Person übernehmen und regelmäßig prüfen, ob es Eintragungen gibt. Ist das der Fall, werden diese gelöscht und die Beschäftigten werden entsprechend sensibilisiert.

BGH: Rein hypothetischer Kontrollverlust berechtigt nicht zum Schadensersatz

Auf den ersten Blick hat die Datenschutz-Grundverordnung (DSGVO) die Rechte der Betroffenen gestärkt. Zwar kann nunmehr leichter der Ersatz eines durch einen Datenschutzverstoß erlittenen immateriellen Schadens gefordert werden. Der Teufel steckt jedoch im Detail. Das zeigt auch ein Urteil des Bundesgerichtshofs (BGH) vom 13.5.2025 (Az. VI ZR 186/22).

Das war Auslöser des Rechtsstreits

Ein Mann hatte eine Firma, die Explosiv- und Sprengmittel verkaufte, beispielsweise an nationale Sicherheitsbehörden. Die entsprechenden Produkte wurden in besonders gesicherten Liegenschaften in verschiedenen Bundesländern gelagert. Aufgrund dieser Geschäftstätigkeit sah sich der Mann besonderen Risiken ausgesetzt, etwa durch Kriminelle. Insofern setzte er alles daran, seine Privatanschrift geheim zu halten.

Mann wehrt sich gegen unverschlüsselte Faxe

Bereits 2015 widersprach der Mann, der spätere Kläger, jeder unverschlüsselten Übermittlung ihn betreffender Daten durch die Stadt, in der er wohnte, die spätere Beklagte. Hier berief er sich auf besondere persönliche Gründe. Die Stadt bestätigte im Februar 2016, dass sie keine personenbezogenen Daten unverschlüsselt auf elektronischem Weg übermitteln würde.

Knapp ein Jahr später schickte die Stadt per Fax an ihren Anwalt eine Übermittlungssperre unter Nennung des vollen Namens und der Anschrift des Mannes. Das bekam auch der Mann mit. Er klagte vor dem Verwaltungsgericht. Das stellte fest, dass die Übermittlung per Fax rechtswidrig war. Die Berufung der Stadt gegen diese Entscheidung wies das Oberverwaltungsgericht zurück.

Weitere Rechtsstreite folgen

In der Folgezeit gab es weitere juristische Auseinandersetzungen zwischen dem Mann und der Stadt. Im Zeitraum April 2019 bis Dezember 2020 verschickte die Stadt siebenmal Empfangsbekenntnisse per unverschlüsseltem Fax an das Verwaltungsgericht. Diese Bekenntnisse enthielten Informationen zu den Beteiligten der Verwaltungsrechtssache, eben die Namen des Mannes und der Stadt sowie die Aktenzeichen.

Der Mann hielt den Versand der Empfangsbekenntnisse per Fax für datenschutzrechtlich unzulässig. Diese hätten auf dem Postweg versendet werden müssen, was der Stadt auch zumutbar gewesen wäre. Die Faxe hätten abgefangen werden können. So wäre es potenziellen Tätern möglich, weitere Daten auszuspähen, um ihn zu überfallen und so an die Schlüssel zu den Lagern oder an die Sprengstoffe selbst zu kommen. Also verklagte er die Stadt auf Schadensersatz von 2.500 € je versendetem Fax, ingesamt 17.500 €. Das Landgericht bejahte zwar einen Schadensersatzanspruch wegen einer schwerwiegenden Persönlichkeitsrechtsverletzung, sprach ihm jedoch nur 7.000 € zu. Sowohl der Mann als auch die Stadt waren mit dem Urteil nicht einverstanden und zogen vor den BGH. Dieser fällte ein Urteil, und zwar zugunsten der Stadt. Der BGH sprach dem Mann keinen Schadensersatz zu.

So entschieden die Richter des BGH

Entgegen der Ansicht der Vorinstanz besteht gegen die Stadt kein Anspruch auf Schadensersatz aus Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO).

Generell bedarf es aus Sicht des Gerichts keiner Entscheidung, ob das unverschlüsselte Versenden gerichtlicher Empfangsbekenntnisse per Fax als Verstoß gegen die DSGVO zu werten ist. Streitentscheidend ist: Der Kläger hat nicht dargelegt, dass er einen immateriellen Schaden erlitten hat.

Mehr als DSGVO-Verstoß erforderlich

Es reicht für einen Ersatzanspruch nicht aus, dass gegen die DSGVO verstoßen wurde. So ist zusätzlich erforderlich, dass ein materieller bzw. immaterieller Schaden vorliegt. Zudem muss es einen Ursachenzusammenhang zwischen Verstoß gegen die DSGVO und Schaden geben. Diese drei Voraussetzungen müssen erfüllt sein, um einen Ersatzanspruch zu begründen. Der Betroffene muss das Vorliegen dieser Voraussetzungen nachweisen. Eine Vermutung, dass aus einem Verstoß auch ein Schaden folgt, ist nicht ausreichend.

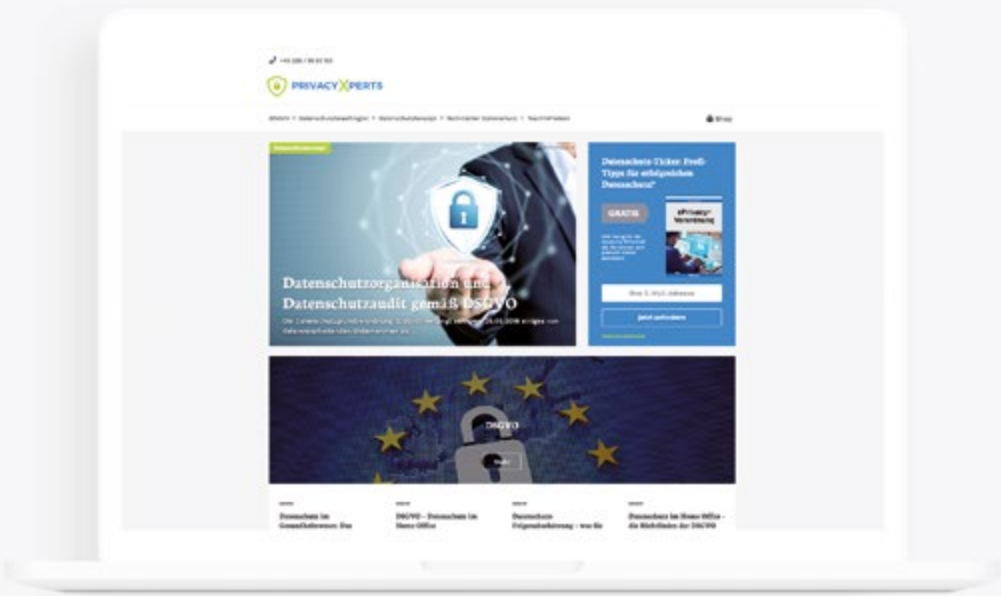
Es reicht zudem nicht aus, sich auf die Befürchtung zu berufen, dass resultierend aus einem Verstoß personenbezogene Daten missbräuchlich verwendet werden. Das rein hypothetische Risiko des Missbrauchs durch unbefugte Dritte führt nicht zu einer Entschädigung. Im konkreten Fall wurde seitens des Klägers auch kein Kontrollverlust über die in den Empfangsbekenntnissen enthaltenen Daten dargelegt. Dieser ist nicht schon anzunehmen, weil mit dem unverschlüsselten Versand per Fax die theoretische Möglichkeit bestand, dass diese abgefangen werden. Die Befürchtungen des Klägers ergeben sich nur aus einem rein hypothetischen Risiko.

Art. 82 DSGVO hat nur eine Ausgleichsfunktion. Eine Strafe zum Schutz vor zukünftigen Verstößen kommt über einen Schadensersatzanspruch nicht in Betracht.

Das können Sie aus dem Urteil folgern

Der BGH orientiert sich mit dieser Entscheidung an den Vorgaben des Europäischen Gerichtshofs. Ein Schaden muss tatsächlich entstanden sein. Den Nachweis muss der Betroffene erbringen. Das gilt auch im Fall von immateriellen Schäden, etwa im Zusammenhang mit der Befürchtung eines Kontrollverlusts. Pauschale Behauptungen eines Schadens reichen nicht aus. Ein Betroffener muss schon konkret werden. Er muss nachvollziehbar darauf eingehen, wie er durch die Befürchtung beeinträchtigt wurde.

„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

Automatisieren Sie Ihre Mitarbeiterschulung!

Jetzt Test-Account gratis aktivieren:

https://t1p.de/cyberxperts-gratis-test

Vorschau:

Richtig gelöscht? So können Sie prüfen
Sie wollen mit der Aufsicht sprechen? Beachten Sie diese Tipps

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