DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
FEB 2026
Schweiz

ALLES FAKE: SENSIBILISIEREN SIE FÜR PHISHING & CO.

VERÄNDERUNGSPROZESSE
Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin 3

BERATUNG
Daten auf Vorrat sammeln? So erläutern Sie Ihr „Besser nicht“ 6

Onlinebereich:
https://kurzlink.ch/onlinebereich

PRIVACYXPERTS

Finden Sie Antworten gemeinsam

Liebe Leserin, lieber Leser,

Sie kennen das bestimmt: Man hat eine Frage zum Datenschutz und Sie sollen die perfekte Lösung liefern. Es mag zwar kein falsches Vorgehen sein, wenn Sie sich dementsprechend an die Erarbeitung der Lösung machen. Doch warum sollte das allein Ihr Ding sein? Ist es eben nicht!

Nehmen Sie andere für das Erarbeiten der Lösung mit ins Boot. Erklären Sie die relevanten Rahmenbedingungen im Datenschutz und lassen Sie die Kollegen zur Lösung beitragen. Das entlastet nicht nur Sie. Sie finden so Lösungen, über die sich später niemand beschweren kann. Schliesslich hat man daran mitgearbeitet.

Viele Grüsse

Andreas Würtz,
Rechtsanwalt und Chefredaktor

Inhalt

Datenschutz organisieren
Schutz Ihres Unternehmens: Machen Sie den Check
Seiten 1–2

Veränderungsprozesse
Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin
Seite 3

Sensibilisierung
Alles Fake: Sensibilisieren Sie für Phishing & Co.
Seiten 4–5

Beratung
Daten auf Vorrat sammeln? So erläutern Sie Ihr „Besser nicht"
Seite 6

Fragen an die Redaktion
? *Videoüberwachung prüfen: Wie soll ich hier vorgehen?*
? *KI-Übersetzungstool: Worauf sollte ich achten?*
Seite 7

Urteil aus dem Ausland
BGH: Rein hypothetischer Kontrollverlust berechtigt nicht zum Schadensersatz
Seite 8

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.

Expertensprechstunde:
https://kurzlink.ch/kontakt-wuertz

Bildnachweise:
Titel: Adobe Stock | Anwesha Dey
Seite 1: Adobe Stock | brokglas
Seite 6: Adobe Stock | blende11.photo

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80
ISSN: 1614 – 5674
Vorstand: Richard Rentrop, Bonn
V.i.S.d.P.: Michael Jodda
(Adresse s. oben)
Produktmanagement: Franziska Rohrbach, Bonn

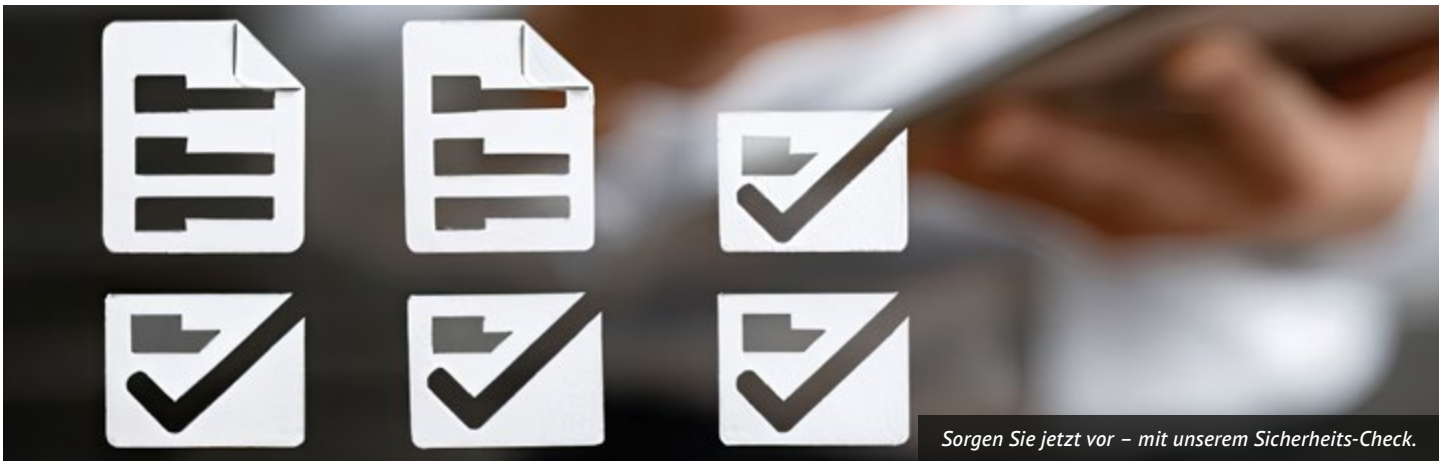
Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar
Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Deinzer Grafik, Gartow
Druck: Warlich Druck Meckenheim GmbH, Meckenheim
Erscheinungsweise: 16-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

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 Frauen und Männer 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



Sorgen Sie jetzt vor – mit unserem Sicherheits-Check.

Schutz Ihres Unternehmens: Machen Sie den Check

Obwohl die Wintersonnenwende am 25. Dezember 2025 schon wieder die helle Jahreshälfte angekündigt hat, sind wir derzeit gefühlt noch mittendrin in der „dunklen Jahreszeit". Und damit ist Hochsaison für Einbrecher, Saboteure und Spione. Schliesslich geht im Dunklen vieles einfach besser. Werden Technik, Computer oder Datenträger entwendet, sind regelmässig auch Personendaten betroffen. Gerade für Datenschutzberater bedeutet dies, dass technische und organisatorische Massnahmen verstärkt auf ihre Praxistauglichkeit und Wirksamkeit geprüft werden müssen. Also liegt für Sie die Frage auf der Hand: Wie steht es um die Sicherheit?

Blinde Flecken darf es nicht geben

Klar ist: Das Risiko, Opfer von Cyberkriminellen zu werden, steigt für jedes Unternehmen zusehends. Kein Wunder also, dass man in vielen Unternehmen hier mit Gegenmassnahmen besonders aktiv ist.

Aber wer sich nur auf dieses Risiko fokussiert, verliert schnell andere Risiken aus dem Blick. Und die gibt es natürlich zuhauf. Da wäre nicht nur der klassische Einbrecher, der es auf alles abgesehen hat, was sich leicht zu Geld machen lässt. Daneben gibt es auch diejenigen, die es auf Know-how oder Daten abgesehen haben oder als Saboteure einfach nur Schaden in Ihrem Unternehmen anrichten wollen. Auch hiergegen muss sich Ihr Unternehmen wappnen.

Machen Sie das Datenschutzrisiko klar

Wollen Sie sich einmal anschauen, wie es um grundlegende Schutzmassnahmen rund um Grundstück, Gelände oder Gebäude steht, hören Sie vielleicht, dass Sie das gern anderen überlassen können. Hier sollten Sie nicht gleich aufgeben. Zeigen Sie auf, dass grundlegende Schutzmassnahmen wie eine Zutrittskontrolleinrichtung oder ein Einbruchmeldesystem auch Schutzmassnahmen sind, um die Sicherheit der Bearbeitung von Personendaten zu gewährleisten.

Doch es geht nicht nur um risikoangemessenen Schutz im Sinne von Art. 8 Bundesgesetz über den Datenschutz (DSG). Passen die Schutzmassnahmen nicht und kommt es zu einem Diebstahl von Computern oder Unterlagen, gibt es schnell ein grösseres Problem: Es liegt eine Datenpanne vor, sprich eine Verletzung des Schutzes von Personendaten. Und die muss unter Umständen dem EDÖB gemeldet werden (Art. 24 Abs. 1 DSG). Wenn es zum Schutz der Betroffenen erforderlich ist, müssen auch diese informiert werden (Art. 24 Abs. 4 DSG).

Prüfen Sie, was Sache ist

Als Profi wissen Sie: Es ist keine Option, einfach zu vermuten, dass ggf. andere sich um ein Thema kümmern werden oder irgendwie schon alles passen wird. Daher: Machen Sie als Datenschutzberater den Check. Dabei sollten Sie systematisch vorgehen:

- **Starten Sie mit einer Risikoanalyse:** Bewerten Sie mögliche Gefahren und leiten Sie daraus unter Betrachtung von möglichem Schaden und Eintrittswahrscheinlichkeit die Risiken ab.
- **Identifizieren Sie die notwendigen Massnahmen:** Damit ist das Soll erfasst.
- **Bewerten Sie den Istzustand:** Erfassen Sie, was an Massnahmen umgesetzt ist.
- **Stellen Sie Schwachstellen und Defizite fest:** Gleichen Sie das Ist mit dem Soll ab. Dokumentieren Sie die Abweichungen.
- **Leiten Sie nötige Massnahmen ab:** Zeigen Sie auf, was zur Behebung der Defizite nötig ist.
- **Begleiten Sie die Umsetzung:** Beraten Sie im Rahmen Ihrer Aufgaben

Sie wollen sich ein Bild von der Situation machen? Für eine Kontrolle grundlegender Aspekte können Sie die folgende Checkliste einsetzen.

CHECKLISTE: Prüfung grundlegender Sicherheitsmassnahmen

Prüfschwerpunkte	Das ist wichtig	Okay?
Regelwerke	› Prüfen Sie, welche relevanten Festlegungen es zu sicherheitsrelevanten Aspekten gibt. Gemeint sind insbesondere Sicherheitskonzepte. Werfen Sie hier auch einen Blick auf die letzte Überarbeitung. Liegt diese lange zurück, kann das schon darauf hindeuten, dass manches veraltet ist, etwa Zuständigkeiten. › Haben Sie auch ein Auge auf relevante betriebliche Reglements, beispielsweise zur Zutrittskontrolle oder zur Videoüberwachung. Diese können umfassende Vorgaben zur Umsetzung und zum erlaubten Einsatz von Systemen machen. Prüfen Sie, inwieweit die Vorgaben aus betrieblichen Reglements zu den Regelwerken passen.	☐ Ja ☐ Nein
Dokumentation	› Für Sicherheitsmassnahmen sind in der Regel Konzepte oder Betriebshandbücher unerlässlich. Diese enthalten oft auch Vorgaben zu Prozessen und einzubindenden Stellen. › Prüfen Sie auch hier auf Aktualität und Vollständigkeit. › Schauen Sie zudem ins Verzeichnis von Bearbeitungstätigkeiten. Sind Personendaten im Spiel, müssen auch bei Sicherheitsmassnahmen entsprechende Bearbeitungstätigkeiten im Verzeichnis nach Art. 12 Abs. 2 Buchst. f DSG enthalten sein.	☐ Ja ☐ Nein
Vertragliche Regelungen	› Hier können Sie den Fokus auf (Sicherheits-)Dienstleister oder Auftragsbearbeiter legen. Schauen Sie, was zum Datenschutz vereinbart wurde. › Bewerten Sie die Rollen der Beteiligten. Es kann passieren, dass man sich dazu keine Gedanken macht, weil man nur die Dienstleistung im Bereich Sicherheit sieht und das Bearbeitung von Personendaten übersieht.	☐ Ja ☐ Nein
Qualifikation zuständiger Mitarbeiter	› Systeme müssen bedient werden. So z. B. die Videoüberwachung, ein Besuchermanagementsystem oder die Zutrittskontrolleinrichtung. Die zuständigen Mitarbeiter sollten über die nötige Qualifikation verfügen. › Hinterfragen Sie die Qualifikation im Datenschutz. Die von den betreffenden Mitarbeitern bearbeiteten Daten unterliegen regelmässig einer strengen Zweckbindung. Also sollten die Mitarbeiter über spezifische Grundlagenkenntnisse im Datenschutz verfügen.	☐ Ja ☐ Nein
Allgemeine Sensibilisierung	› Auch dem Otto-Normal-Mitarbeiter müssen Basics zur Sicherheit vermittelt werden. Die beste Zutrittskontrolle bringt nichts, wenn ein unvorsichtiger Mitarbeiter dem Unbefugten die Tür aufhält. › Schauen Sie sich Materialien und Konzepte an. Klären Sie, wie man sicherstellt, dass kein Mitarbeiter durchrutscht.	☐ Ja ☐ Nein
Physische Absicherung von Grundstück, Gelände und Gebäuden	› Kontrollieren Sie Zäune, Tore, Aussentüren und Fenster. Diese sollten zu einem angemessenen Sicherheitsniveau beitragen und nicht nur „Fassade“ sein. › Idealerweise machen Sie eine Begehung. Zudem bietet sich ein Check zu Zeiten an, bei denen eigentlich niemand mehr da ist. Testen Sie hier auch, inwieweit Türen und Fenster tatsächlich verschlossen sind oder Zutrittskarten ausserhalb der Regelarbeitszeiten nicht mehr funktionieren.	☐ Ja ☐ Nein
Umgebungssicherheit	› Haben Sie auch ein Auge auf die Umgebung Ihres Unternehmens. Auch dort können Risiken lauern, die etwa unter dem Aspekt „Verfügbarkeit“ ein Problem für den Datenschutz sein können. › Schauen Sie insbesondere nach grundlegenden Risiken, etwa eine erhöhte Gefahr für Feuer oder Hochwasser. Ist der Server Ihres Unternehmens im Keller, kann der bei Hochwasser schlimmstenfalls auch unter Wasser stehen.	☐ Ja ☐ Nein
Zutrittskontrolleinrichtungen	› Bewerten Sie die Zugangsregelungen zu Grundstück, Gebäuden und kritischen Bereichen. › Klären Sie insbesondere, inwieweit verlorene Zutrittsmittel (z. B. Chipkarten) gesperrt werden oder der Zutritt bei Beschäftigungsende schnell entzogen wird.	☐ Ja ☐ Nein
Einbruchmeldetechnik	› Prüfen Sie die Dokumentation. Besprechen Sie zudem, wann die Anlage zuletzt gewartet bzw. getestet wurde. › Klären Sie auch die Prozesse. Eine Meldung darf nicht ins Leere laufen.	☐ Ja ☐ Nein
Videoüberwachung	› Diese muss funktionieren. Machen Sie die Sichtprüfung. Nicht selten ist die Funktion durch verschmutzte Linsen oder verstellte Kameras erheblich beeinträchtigt. › Prüfen Sie das System auch unter Datenschutzaspekten. Klären Sie vor allem die Speicherdauer der aufgezeichneten Videos. Eine lange Speicherdauer sollte man gut begründen können. Lassen Sie sich auch schildern, in welchen Fällen auf Bildmaterial zugegriffen wird und wie hier die Zulässigkeit eines Zugriffs bzw. der Weitergabe geprüft wird.	☐ Ja ☐ Nein
Besondere Sicherung besonderer Bereiche	› Es gibt in jedem Unternehmen Bereiche, die nicht für jedermann gedacht sind. Typischerweise sind hier der Serverraum, ein Aktenarchiv oder die Aufbewahrung von Datensicherungen zu nennen. Lassen Sie sich erläutern, wie man dem besonderen Schutzbedarf nachkommt. › Machen Sie die Probe aufs Exempel. Prüfen Sie, ob die Sicherheitsmassnahmen das halten, was man Ihnen versprochen hat.	☐ Ja ☐ Nein
Aufbewahrung, Löschung und Entsorgung von Schutzwürdigem	› Das betrifft beispielsweise die Aufbewahrung von Zutrittsmitteln (insbesondere Schlüssel, Chipkarten) am Empfang. Schauen Sie sich an, wo man Entsprechendes sicher verwahrt. › Auch im Unternehmen gibt es besonders Schutzwürdiges, etwa Akten oder Datenträger. Prüfen Sie hier die spezifischen Schutzmassnahmen.	☐ Ja ☐ Nein

Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin

Manch ein Unternehmen wird derzeit umstrukturiert, beispielsweise um die aktuellen wirtschaftlichen Herausforderungen besser meistern zu können. Vielleicht ist das auch bei Ihrem Unternehmen der Fall. Und bei den meisten Veränderungen und Umstrukturierungen gibt es auch einen Bezug zu Personendaten. Kein Wunder, dass es dabei so manchen Fallstrick gibt. Gut, wenn Sie frühzeitig darauf hinweisen.

Öffnen Sie die Augen

Bei Umstrukturierungen oder Veränderungen im Unternehmen haben die verantwortlichen Kollegen alles Mögliche im Kopf. Das ist auch verständlich. Da kann es passieren, dass man das Thema Datenschutz vergisst oder dem nicht die nötige Relevanz beimisst.

Dabei ist klar: Das Bundesgesetz über den Datenschutz (DSG) verzeiht keine Patzer. Schlimmstenfalls drohen viel Ärger und hohe Kosten, etwa für Bussgelder. Steuern Sie dem entgegen. Erläutern Sie beispielsweise in einem Gespräch die folgenden Fallstricke:

Fallstrick Nr. 1: Unklare Verantwortlichkeiten

Veränderungen, etwa der Neuzuschnitt von Abteilungen oder die Verlagerung von (Datenbearbeitungs-)Prozessen, können zu einer Art Verantwortungsvakuum führen. So fühlt sich der abgebende Bereich nicht mehr verantwortlich und der neue Bereich noch nicht verantwortlich. Hier sollten die Übergänge der Verantwortung vom einen zum anderen Bereich klar definiert und dokumentiert sein.

Fallstrick Nr. 2: Fehlende Rechtsgrundlage

Für jede Bearbeitung von Personendaten bedarf es einer Rechtsgrundlage. Daneben muss schon bei der Erhebung der Zweck definiert sein. Sollen Daten ausgelagert werden, etwa an eine neue Tochtergesellschaft, wird das unter Umständen nicht von der bisherigen Rechtsgrundlage gedeckt sein. Insofern muss genau geprüft werden, unter welchen Umständen eine Übertragung von Prozessen und Personendaten möglich ist, etwa auf Basis der Vorgaben von Art. 31 DSG.

Fallstrick Nr. 3: Verletzung von betrieblichen Reglements

Betriebliche Reglements legen oft fest, wie technische Einrichtungen, beispielsweise ein System, im Unternehmen eingesetzt werden dürfen. Es können wichtige Rahmenbedingungen für die Bearbeitung von Personendaten enthalten sein. So z. B., welche Daten für welchen Zweck berarbeitet werden dürfen, welche Auswertungen erlaubt sind oder an wen die Weitergabe von Daten möglich ist.

Solche Einschränkungen spielen immer eine Rolle. Werden Rahmenbedingungen im Unternehmen verändert oder Prozesse ausgelagert, kann es schnell zum Verstoss gegen ein betriebliches Regelement kommen. Das würde zumindest Unruhe in der Belegschaft verursachen. Dem können und sollten Sie vorbeugen.

Fallstrick Nr. 4: Reduzierte Schutzmassnahmen

Werden Bearbeitungen oder Prozesse verändert oder andere Stellen im oder ausserhalb des Unternehmens verlagert, muss das so passieren, dass auch während dieses Veränderungsprozesses die Sicherheit der Bearbeitung und der betreffenden Daten gewährleistet bleibt (Art. 8 DSG). Abstriche bei den Schutzmassnahmen können grundsätzlich nicht gemacht werden. Denkt man hierüber nach, ist eine Risikobewertung unerlässlich. Denn nur auf deren Basis kann bewertet werden, inwieweit andere oder geringere Schutzmassnahmen risikoangemessen sind.

Fallstrick Nr. 5: Cyberkriminelle haben leichteres Spiel

Veränderungen bringen Unsicherheiten mit sich. So erhalten Beschäftigte neue Aufgaben oder neue Vorgesetzte. Auch Berichtslinien können sich ändern. Gerade in der Übergangsphase steigt das Risiko, dass Cyberkriminelle die Situation ausnutzen und etwa mit Phishing-E-Mails leichteres Spiel haben. Umso wichtiger ist, dass Beschäftigte in Sachen Veränderungen auf dem Laufenden gehalten werden. Auch das Sensibilisieren für mögliche Gefahren ist in der Übergangszeit unerlässlich.

Fallstrick Nr. 6: Vergessene Datenschutzvereinbarungen

Werden Bearbeitungen verlagert oder Dienstleister mit der Bearbeitung beauftragt, muss geklärt werden, wie sich die Situation der Beteiligten unter Datenschutzaspekten darstellt. Bestimmt Ihr Unternehmen weiterhin allein über Mittel und Zwecke, kann eine Auftragsbearbeitung im Sinne von Art. 9 DSG vorliegen. Eventuell besteht auch eine gemeinsame Verantwortung. Doch auch bei einer Übermittlung von Daten zwischen Verantwortlichen kann Regelungsbedarf bezüglich der betreffenden Personendaten bestehen. Und das muss erledigt sein, bevor es in die praktische Umsetzung geht.

Fallstrick Nr. 7: Unzureichende Datenschutzorganisation

Kommt es zu Veränderungen, kann das erhebliche Folgen für die Datenschutzorganisation haben. Da wären etwa Know-how-Träger, die das Unternehmen verlassen. Eventuell passen auch Strukturen oder Regelungen nicht mehr zum zukünftigen Zuschnitt. Was ausserdem gern vergessen wird: Wird eine Tochtergesellschaft gegründet, kann für diese ein Datenschutzberater erforderlich sein. Ob Sie das übernehmen können, ist meist auch eine Frage der Kapazität. Schliesslich gibt es gerade bei neuen Unternehmen vieles zu erledigen. Zugleich ist der Beratungsbedarf oft ziemlich gross und die Fälle sind eher kein Standard.

Alles Fake: Sensibilisieren Sie für Phishing & Co.

Künstliche Intelligenz (KI) ist als Trendthema Nummer eins in aller Munde. Kaum ein Unternehmen, das sich nicht damit beschäftigt. Doch wo viel Licht ist, ist auch viel Schatten. Cyberkriminelle setzen immer mehr auf die Möglichkeiten, die KI bietet. Phishing wird zunehmend perfekter. Damit Mitarbeiter gut gerüstet sind, sollten Sie sensibilisieren.

Know-how ist unerlässlich

Die Mitarbeiter werden schon Bescheid wissen – denkt Ihre Unternehmensleitung so, dann ist es nur eine Frage der Zeit, bis es zum grossen Schaden kommt. Vielmehr ist eine solche Denke grob fahrlässig. Ihr Unternehmen muss alles daransetzen, die Beschäftigten mit dem relevanten Wissen auszustatten, das sie im Fall der Fälle brauchen.

Neue Herausforderungen durch KI

Natürlich versuchen Cyberkriminelle, ganz klassisch an sensible Informationen zu kommen oder Zahlungen zu veranlassen. Dementsprechend sind auch die klassischen Erkennungsmerkmale weiterhin relevant. So z. B.:

- unpersönliche, unpassende oder falsche Anrede
- gefälschte Absender- oder Linkadressen unter Verwendung von Buchstaben oder Zahlendrehern
- Aufbau von Handlungsdruck, nach dem Schema „Ihr Konto wird sofort gesperrt“

Allerdings bietet KI Cyberkriminellen ganz neue Möglichkeiten, Menschen und damit auch die Beschäftigten Ihres Unternehmens in die Falle zu locken.

So wird KI eingesetzt, um

- täuschend echte Fälschungen von E-Mails, Schreiben oder Webseiten zu erstellen,
- das Opfer zu analysieren und typische Schwachpunkte zu finden,
- Stimmen und Nachrichten zu fälschen, um z. B. Forderungen des falschen Chefs echt wirken zu lassen,
- SMS und Messenger-Nachrichten so zu gestalten, dass diese tatsächlich vom echten Absender zu stammen scheinen.

Cyberkriminelle entdecken den Brief für sich

Die Leichtgläubigkeit und Täuschbarkeit von Menschen ausnutzen – darauf setzen Cyberkriminelle besonders. Und das klappt besonders gut mit Schreiben, die anscheinend von Behörden stammen oder die klassisch per Post verschickt werden. Wirkt das Schreiben oder etwa eine Rechnung echt, denkt mancher Mitarbeiter nicht lange nach. Das, was gefordert wird, wird ohne Umwege umgesetzt.

Mancher vertrauensselige Mensch macht das nicht anders, wenn es um QR-Codes geht. Die werden inzwischen ebenfalls gern gefälscht und über die echten QR-Codes an Ladesäulen geklebt. Das Ziel: Die Opfer werden zur Eingabe von Kreditkartendaten auf gefälschten Seiten von Stromanbietern verleitet.

Sensibilisieren Sie auf die Schnelle

Sprechen Sie etwa mit der IT-Abteilung, dem Finanzbereich oder den zuständigen Kollegen im Bereich Cybersecurity, inwieweit sie aktuelle Beispiele für neue Vorgehensweisen von Cyberkriminellen haben. Passen Sie dann das nachfolgende Muster so an, dass dieses auf Ihr Unternehmen zugeschnitten ist und die spezifischen Vorfälle berücksichtigt.

Sorgen Sie für Abwechslung
Damit die Mitarbeiter mit dem nötigen Wissen versorgt werden, muss es nicht immer eine E-Mail sein. Denken Sie auch an einen Artikel im Intranet. Hier haben Sie meist viel mehr Platz, um etwa auch echte Beispiele aus dem Unternehmen unterzubringen. Alternativ können Sie auch eine kurze virtuelle Schulung oder Sprechstunde anbieten. Das kann im Ergebnis nachhaltiger wirken, gerade wenn individuelle Fragen beantwortet werden können. Möglicherweise ist Ihre Unternehmensleitung auch bereit, aufmerksamkeitsstarke Plakate drucken zu lassen. Dort können Sie im Wortsinn plakativ auf die wichtigsten Fallen hinweisen.

Schauen Sie auch auf das Drumherum

Dass Cyberkriminelle sich immer wieder etwas Neues einfallen lassen und dass die Mitarbeiter sensibilisiert werden müssen, damit sie darauf nicht hereinfallen, ist eine Sache. Eine andere Sache ist, dass Ihr Unternehmen passende Anlaufstellen und Prozesse hat, um im Fall der Fälle schnell und professionell mit einem entsprechenden Vorfall umgehen zu können. Denn die beste Hotline bringt nichts, wenn dort ständig besetzt ist oder eine Bandansage läuft. Entscheidend ist, dass Zuständigkeiten, Abläufe und Kommunikationswege klar definiert, bekannt und im Ernstfall auch tatsächlich funktionsfähig sind. Prüfen Sie daher im Rahmen Ihrer Aufgaben auch die folgenden Aspekte:

- **Regelungen:** Bestehen klar kommunizierte Anweisungen für die Mitarbeiter, wie diese bei einem Vorfall reagieren müssen? Nur wenn bekannt ist, was zu tun ist, besteht eine erhöhte Wahrscheinlichkeit, dass entsprechend gehandelt wird.
- **Meldewege:** Bestehen niederschwellige Möglichkeiten, Vorfälle zu melden oder speziellen Rat einzuholen, etwa bei der Hotline eines Cybersecurity-Teams? Es den Mitarbeitern leicht zu machen kann entscheidend sein. Komplizierte Formulare wirken eher abschreckend. Besser sind E-Mail, Telefon oder ein Chat mit direktem Kontakt zu den Spezialisten.
- **Erreichbarkeit:** Wenn etwas schiefgeht, muss schnell gehandelt werden. Sind die Kontaktmöglichkeiten oder Spezialisten auch zu Randzeiten oder am Wochenende verfügbar?

MUSTER: Phishing-Sensibilisierung für Mitarbeiter

Gehen Sie Cyberkriminellen nicht auf den Leim

Liebe Kolleginnen und Kollegen,

Cyberkriminelle haben es auf unser Unternehmen und auf Sie als Mitarbeiter abgesehen. Wichtig ist es also, dass Sie den Cyberkriminellen nicht auf den Leim gehen und nicht in die Phishing-Falle tappen. Das gelingt Ihnen, indem Sie vor allem die Hinweise in diesem Schreiben beachten.

Was mit Phishing gemeint ist, wissen Sie bestimmt. Das sind Versuche von Cyberkriminellen, mit gefälschten E-Mails, Nachrichten, SMS, Briefen oder Anrufen an sensible Daten zu gelangen. Oder: Man will Sie zu einem Verhalten oder Handeln veranlassen, das den Kriminellen ihre weiteren Machenschaften ermöglicht, etwa den Diebstahl oder das Verschlüsseln von Daten.

Auch Cyberkriminelle finden KI super
Künstliche Intelligenz (KI) macht nicht nur Ihr Leben leichter – das Potenzial von KI sehen und nutzen auch Cyberkriminelle. So setzen sie darauf, um täuschend echte E-Mails zu erstellen, die nicht nur personalisiert sind und ohne Rechtschreib- und Grammatikfehler daherkommen. Mit den entsprechenden Bild- und Audiogeneratoren werden Deepfakes erstellt, also Stimmen, Bilder oder Videos von Entscheidungsträgern oder Vertrauenspersonen nachgeahmt. Wer nicht genau hinschaut, merkt ggf. nicht, dass die Nachricht oder das Video gerade nicht vom Geschäftsführer oder Verhandlungspartner stammt.

KI hilft zudem dabei, Prozesse zu automatisieren, auch bei Cyberkriminellen. So werden echte Webseiten kopiert, um die Kopie so zu manipulieren, dass Opfer darauf hereinfallen und etwa sensible Anmeldedaten oder Kreditkarteninformationen eingeben.

Vorsicht vor derzeit aktuellen Maschen
Cyberkriminelle schlafen nicht und sie kommen immer wieder auf neue Ideen. So z. B.:

- **Behördenschreiben:** Zwar ist die Masche nicht neu. Allerdings ist die Täuschung zunehmend perfekt. So passen nicht nur Aussehen und Inhalt auf den ersten Blick. Solche Fake-Behördenbriefe werden nicht nur per E-Mail, sondern auch per Briefpost verschickt. Seien Sie also auf der Hut, wenn Behörden (z. B. Statistikämter, Finanzämter, Bundeskriminalamt) etwas von unserem Unternehmen oder Ihnen wollen. Lassen Sie sich nicht irritieren, nur weil etwas amtlich daherkommt oder per Post verschickt wird. Auch wenn direkt mit einem Bussgeld gedroht wird, sollten Sie nichts überstürzen. Hinterfragen Sie das Anliegen und stimmen Sie sich mit Kollegen und Vorgesetzten ab.

- **Geheimhaltung:** Heisst es, dass man nur Sie ins Vertrauen zieht und Sie niemandem etwas erzählen dürfen, heisst es Stopp. Ignorieren Sie das. Sie können sich immer mit dem Vorgesetzten abstimmen.

- **Anhänge von Fremden:** Kennen Sie den Absender nicht und sind Anhänge enthalten, ist besondere Vorsicht geboten. Sprechen Sie im Zweifel vorab mit dem Vorgesetzten oder den Spezialisten der IT-Hotline. Öffnen Sie die Anhänge nicht, laden Sie nichts herunter und installieren Sie nichts. Auch bei bekannten Absendern ist Vorsicht angebracht, wenn Anhänge unüblich sind.

- **Widersprüchliches Verhalten:** Seien Sie besonders vorsichtig, wenn etwas nicht wie üblich abläuft oder nicht zum Bisherigen passt. Ändert sich plötzlich die Bankverbindung oder gab es noch nie eine Audionachricht vom Chef? Waren bislang andere Ansprechpartner zuständig oder war noch nie ein Behördenschreiben bei Ihnen gelandet? Dann heisst es Stopp. Machen Sie nicht das, was gefordert wird.

Und ganz wichtig: Hören Sie auf Ihr Bauchgefühl. Kommt Ihnen etwas seltsam oder komisch vor, heisst es immer: Vorsichtig sein. Machen Sie nicht gleich das, was von Ihnen gefordert wird.

Reagieren Sie am besten so: Behalten Sie die Nerven, bewahren Sie einen kühlen Kopf und reden Sie mit anderen darüber. Bekommen Sie etwa eine E-Mail von einem Dienstleister, den Sie kennen, aber die E-Mail ist merkwürdig? Dann fragen Sie dort nach. So wird häufig klar, dass Sie mit Ihrem Bauchgefühl nicht falschlagen.

Das machen Sie bei Verdächtigem
Dann heisst es zunächst Ruhe bewahren und nicht unüberlegt handeln. Sie haben immer Zeit, die nächsten Schritte zu durchdenken. Fragen Sie bei Zweifeln nach, und zwar bei Kollegen, Vorgesetzten, der IT-Hotline oder beim Datenschutzberater. Melden Sie Verdächtiges. Und: Sind Sie jemandem auf den Leim gegangen, können Sie grösseren Schaden vermeiden helfen. Melden Sie die Sache sofort Ihrem Vorgesetzten und der IT-Hotline.

Noch Fragen? Die Antworten bekommen Sie bei der IT-Hotline unter der Durchwahl -1234 oder beim Datenschutzberater. Wir beissen nicht und stehen Ihnen mit Rat und Tat zur Seite – immer und jederzeit!

Viele Grüsse

Ingo Nesien
Datenschutzberater

Daten auf Vorrat sammeln? So erläutern Sie Ihr „Besser nicht“

Gerade in Zeiten von künstlicher Intelligenz (KI) kommen vielleicht auch in der einen oder anderen Abteilung Ihres Unternehmens Begehrlichkeiten auf. Man könnte doch bestimmt mehr Personendaten sammeln als erforderlich oder vorhandene Daten nicht löschen bzw. für andere Zwecke nutzen. KI macht zudem vieles möglich. Schieben Sie solchen Ideen einen Riegel vor.

Machbar ist vieles, zulässig aber nicht

Einfach Personendaten ohne Rechtsgrundlage oder konkreten Zweck zu bearbeiten ist nicht machbar. Das wissen Sie als Datenschutzprofi nur zu gut. Doch mancher will das vielleicht nicht so recht glauben. Schliesslich ist das Thema KI in aller Munde und es muss doch einfach möglich sein, diese neue Technologie wertbringend einzusetzen. Also müssen Sie klarmachen, warum das alles nicht so einfach geht.

Erläutern Sie, was Sache ist

Wollen Sie darstellen, dass das Speichern von Daten auf Vorrat oder für einen nicht klar umrissenen Zweck nicht zulässig ist, sollten Sie mit Feingefühl vorgehen. Schliesslich müssen Sie vielleicht bei einer persönlich als gut empfundenen Idee den Stecker ziehen. Zeigen Sie also nachvollziehbar auf, wo die Knack- oder Problempunkte liegen. Für Ihr Gespräch können Sie auf die folgende Checkliste setzen:

CHECKLISTE: Knackpunkte bei „Daten auf Vorrat“

Knackpunkt	Das ist wichtig	Besprochen?
Fehlende Rechtsgrundlage	› Sollen Personendaten bearbeitet werden, bedarf es für die gesamte Dauer, sprich von Anfang bis Ende der Bearbeitung, einer Rechtsgrundlage. › Werden Daten ohne eindeutigen und konkret umrissenen Zweck auf Vorrat gespeichert, wird es mit der Rechtsgrundlage schwierig. Es lässt sich nämlich nicht die Frage nach der Erforderlichkeit der Daten und der Bearbeitung im Hinblick auf den Zweck beurteilen.	☐ Ja ☐ Nein
Verstoss gegen den Grundsatz der Zweckbindung	› Aus Art. 6 Abs. 3 Bundesgesetz über den Datenschutz (DSG) ergibt sich die Zweckbindung. Damit ist gemeint, dass Daten eben bloss für den bei der Erhebung festgelegten Zweck bearbeitet werden dürfen. › Eine Zweckänderung ist nur auf Basis einer entsprechenden neu erteilten Einwilligung möglich. Das scheitert dann jedoch oft an der Praktikabilität oder der geringen Einwilligungsfreudigkeit der Betroffenen.	☐ Ja ☐ Nein
Verstoss gegen das Verhältnismässigkeitsprizip	› Auch hierbei handelt es sich um ein wichtiges Grundprinzip des DSG, das in Art. 6 Abs. 2 DSG verankert ist. Personendaten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Bearbeitung notwendige Mass beschränkt sein. › Werden Daten für noch nicht festgelegte oder allgemeine Zwecke bearbeitet, lässt sich dieses Prinzip praktisch nicht einhalten. › Wie bei allen Prinzipien kann ein Verstoss erheblichen Ärger verursachen bis hin zu schmerzhaftem Bussgeld.	☐ Ja ☐ Nein
Unzureichende Transparenz	› Betroffene müssen wissen und nachvollziehen können, was mit ihren Personendaten passiert. Entsprechend machen Art. 19, 20 DSG umfassende Vorgaben zu den Informationspflichten. Sind allerdings Informationen zum Zweck zu allgemein oder wird überhaupt kein Zweck genannt, ist das ein Verstoss gegen die Transparenzpflicht. › Prüfen Sie Datenschutzhinweise stets dahin gehend, ob klar wird, welche Daten für welchen Zweck für welchen Zeitraum bearbeitet werden.	☐ Ja ☐ Nein
Mangelhafte Umsetzung der Betroffenenrechte	› Denken Sie hier vor allem an das Recht auf Löschung von Personendaten (Art. 32 Abs. 2 Buchst. c DSG). Selbst wenn Daten berechtigterweise bearbeitet werden, müssen sie nach einer festgelegten Zeit (z. B. gemäss gesetzlicher Aufbewahrungspflicht) gelöscht werden. Sie dann weiterhin zu bearbeiten, weil man sie „vielleicht noch brauchen könnte“, ist ein Datenschutzverstoss. › Auch das Recht auf Auskunft (Art. 25 DSG) kann nur unvollständig umgesetzt werden, wenn Daten auf Vorrat gespeichert werden. So kann man ggf. den Zweck, die Empfänger oder die Speicherdauer nicht benennen. Auch eine falsche Auskunft kann Ihr Unternehmen teuer zu stehen kommen.	☐ Ja ☐ Nein
Das Prinzip von Treu und Glauben	› Jede Bearbeitung von Personendaten muss diesem Prinzip entsprechen. › Das Bearbeiten von Personendaten muss fair und. transparent sein. Fair bedeutet auch, dass die Interessen von Betroffenen berücksichtigt werden.	☐ Ja ☐ Nein

Videoüberwachung prüfen: Wie soll ich hier vorgehen?

FRAGE: Ich soll als Datenschutzberater die neue Videoüberwachungsanlage datenschutzrechtlich prüfen. Darum hat mich die zuständige Abteilung gebeten. Dazu hatte ich mir überlegt, dass ich mir alle von den Videokameras erfassten Bereiche vor Ort und die von den Kameras erzeugten Bildausschnitte am Computer des Werkschutzes anschaue. Nun meinte man, dass das ja wohl nicht nötig wäre und ich doch eine generelle Einschätzung abgeben könnte. Dazu will man mir Screenshots der jeweiligen Bildeinstellungen und des Aufnahmebereichs zur Verfügung stellen. Zudem hätte die Installationsfirma versichert, alles im Einklang mit dem Datenschutz umgesetzt zu haben. Ich habe mit einer Einschätzung vom Schreibtisch aus so meine Bauchschmerzen. Was meinen Sie: Wie soll ich hier als Datenschutzberater am besten vorgehen?

ANTWORT: Als Datenschutzberater haben Sie es selbst in der Hand, wie Sie vorgehen. Art. 10 Abs. 2 Bundesgesetz über den Datenschutz (DSG) beschreibt Ihre Aufgaben als Datenschutzberater. Dazu zählen das Beraten und Schulen in allen Datenschutzfragen sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Damit Sie diese Aufgaben gut wahrnehmen können, hat der Gesetzgeber mehrere wichtige Aspekte in das DSG aufgenommen. Entscheidend ist, dass Sie bei der Wahrnehmung Ihrer Aufgaben unabhängig sind und keinen Weisungen unterliegen (Art. 10 Abs. 3 Buchst. a DSG). Ihnen kann also niemand vorschreiben, wie Sie zu arbeiten haben, wie Sie die Dinge sehen sollen oder wie Sie bei einer Prüfung vorzugehen haben.

Machen Sie sich selbst ein Bild

Grundsätzlich können Sie natürlich eine Prüfung „vom Schreibtisch aus" machen und Ihre Prüfung auf vorgelegte Dokumente stützen. Allerdings wissen viele Datenschutzberater aus eigener Erfahrung: In der Theorie bzw. auf dem Papier mag alles passen. In der Praxis bzw. vor Ort sieht die Sache ganz anders aus. Gerade bei der Videoüberwachung kann es für Ihre Bewertung entscheidend sein, dass Sie sich selbst ein Bild von den Gegebenheiten und der Umsetzung vor Ort machen. Nehmen Sie also nicht nur die bereitgestellten Unterlagen als Basis für Ihre Prüfung. Entscheidender kann Ihr Eindruck von der tatsächlichen Umsetzung sein. Hier können Sie auch konkret dort in die Tiefe gehen, wo Sie den Eindruck haben, dass das genau hier nötig ist. Denken Sie beispielsweise an Bildeinstellungen, Zoommöglichkeiten bei Kameras, die Speicherdauer des Bildmaterials oder die Zugriffsberechtigungen.

Was ein Dritter zusichert, muss nichts heissen

Lassen Sie sich auch nicht davon beeindrucken, dass ein Dritter, in Ihrem Fall die Installationsfirma, meint, dass alles datenschutzkonform umgesetzt wurde. Nicht selten handelt es sich dabei eher um eine Art „Beruhigungspille". Meist wird nämlich gerade nicht darauf geachtet, ob die datenschutzrechtlichen Rahmenbedingungen eingehalten sind. Schliesslich wird ein Techniker in aller Regel nicht prüfen, inwieweit beim Videoüberwachungssystem an sich bzw. bei jeder Kamera die Grundsätze der Bearbeitung von Personendaten (Art. 6 DSG) berücksichtigt wurden.

Zudem lässt sich die „Datenschutzkonformität" meist schnell als etwas nicht so Ernstgemeintes entlarven. Bitten Sie um die Vorlage einer schriftlichen Bestätigung. Die wird Ihr Unternehmen meist nicht haben. Schliesslich wird auch die Installationsfirma so etwas eher nicht zusichern.

Das machen Sie, wenn man Sie nicht prüfen lässt
Will man nicht zulassen, dass Sie so prüfen, wie Sie es für richtig halten, sollten Sie nicht generell die Arbeit verweigern. Dokumentieren Sie, was die Basis Ihrer Prüfung ist und warum eine wie von Ihnen beabsichtigte Prüfung nicht möglich war.

KI-Übersetzungstool: Worauf sollte ich achten?

FRAGE: Ich muss immer wieder E-Mails auf Englisch verfassen. Ich möchte dazu ein auf künstlicher (KI) Intelligenz basierendes Übersetzungstool im Internet nutzen. Haben Sie Tipps, worauf ich hier achten sollte?

ANTWORT: Wichtig ist zunächst, dass Sie sich aufschlauen, was das betreffende Tool macht, wo Eingaben landen bzw. für welche Zwecke diese verwendet werden. So gibt es Tools, die Eingaben nicht speichern oder für Trainingszwecke verwenden. Das kann jedoch mit Kosten verbunden sein. Daneben ist entscheidend, dass Sie auf alles verzichten, was auch nur nach Personenbezug riecht. Verwenden Sie allenfalls erfundene Namen und tauschen Sie Geschlechter bzw. Anreden aus. Verfremden Sie auch alles, was Rückschlüsse auf einen konkreten Sachverhalt oder auf Ihr Unternehmen zulassen kann. Das können Sie mit Dummy-Informationen ersetzen. Diese können Sie in der Übersetzung leicht wieder mit den richtigen Informationen austauschen Im Übrigen gibt es auch datenschutzkonforme Lösungen. Dann entfällt das Austauschen.

BGH: Rein hypothetischer Kontrollverlust berechtigt nicht zum Schadensersatz

Die Datenschutz-Grundverordnung (DSGVO) hat die Rechte der betroffenen EU-Bürger gestärkt. Zwar kann der Ersatz eines durch einen Datenschutzverstoss erlittenen immateriellen Schadens nun leichter gefordert werden. Der Teufel steckt jedoch im Detail. Das zeigt auch ein Urteil des höchsten deutschen Zivilgerichts, 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 entschied der BGH

Entgegen der Ansicht der Vorinstanz besteht für den Mann kein Anspruch auf Schadensersatz aus Art. 82 Abs. 1 DSGVO gegen die Stadt.

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 Personendaten 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.

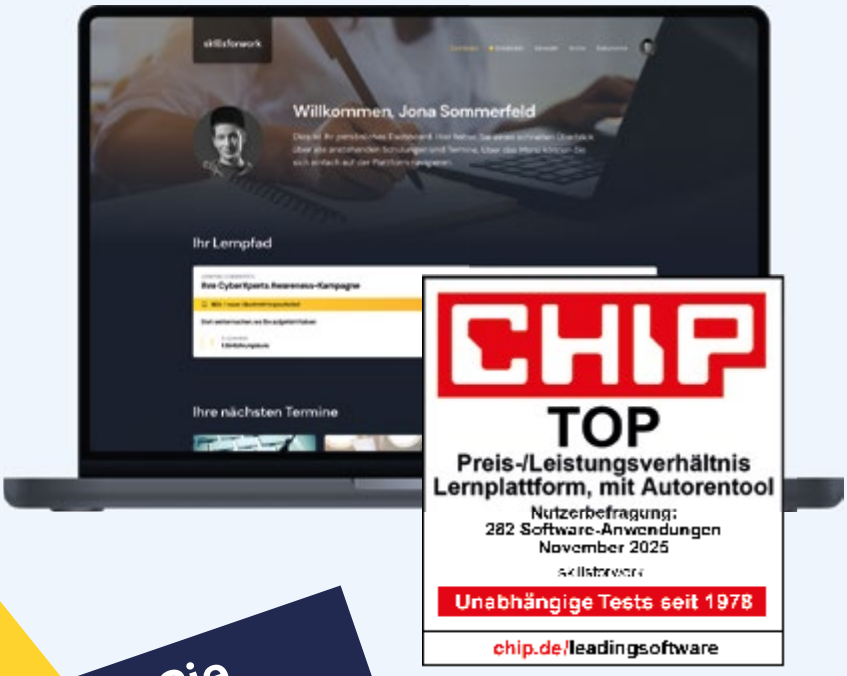
Das können Sie aus dem Urteil mitnehmen

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. Das ist bei uns genauso.

Die digitale Lösung für Ihre Pflichtschulungen

Arbeitssicherheit & Datenschutz

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



Testen Sie skillsforwork kostenlos

Compliance & ESG

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

Cyber Security

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

skillsforwork

PRIVACYXPERTS

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

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

Vorschau:

Wie Sie Zweifler vom Datenschutz überzeugen
Kein Hexenwerk: So vermeiden Sie Fehleinschätzungen mit links