



GUTE VORSÄTZE FÜR 2026: MOTIVIEREN SIE DIE MITARBEITER ZUM DATENSCHUTZ

AWARENESS ORGANISIEREN

Interne Schulungen einkaufen?
Schauen Sie genau hin

1-2

SCHLAU VORGEHEN

Kein Ding der Unmöglichkeit:
7 Tipps, damit Sie ab 2026
jeder kennt

3





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

Ihr Experte für Datenschutz

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

Inhalt

Awareness organisieren

Interne Schulungen einkaufen?
Schauen Sie genau hin

Seiten 1–2

Schlau vorgehen

Kein Ding der Unmöglichkeit:
7 Tipps, damit Sie ab 2026
jeder kennt

Seite 3

Sensibilisierung

Gute Vorsätze für 2026: Motivieren
Sie die Mitarbeiter zum Datenschutz

Seiten 4–5

Kontrolle

Organisatorisches Versagen:
Prüfen Sie diese 7 Hotspots

Seite 6

Fragen an die Redaktion

? Nicht im Urlaub erreichbar:
Droht mir Ärger?

? In welcher Sprache müssen die
Datenschutzhinweise sein?

Seite 7

Rechtsprechung

BAG: Daten für Systemtests dürfen
auch personenbezogen sein

Seite 8



Expertensprechstunde:

<https://kurzlink.ch/kontakt-wuertz>

Bildnachweise:

Titel: Adobe Stock | Jo Panuwat D

Seite 1: Adobe Stock | kasto

Impressum



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



Nutzen Sie unsere Checkliste mit den Auswahlkriterien für den richtigen Anbieter.

Interne Schulungen einkaufen? Schauen Sie genau hin

Als Datenschutzberater haben Sie viel um die Ohren. Da wären nicht nur die tagtäglichen Fragen rund um den Datenschutz. Sie sind wahrscheinlich auch Ansprechpartner Nummer eins, wenn es um das Vermitteln von Datenschutzwissen geht. Vielleicht will Ihnen die Unternehmensleitung etwas unter die Arme greifen und Sie bei Schulungen entlasten. Gute Idee, aber schauen Sie genau hin.

Sehen Sie ein solches Angebot positiv

Alles, was Sie bei Ihrer Arbeit als Datenschutzberater entlasten kann, sollten Sie nie sofort ablehnen. Schauen Sie lieber, wie Sie den grössten Nutzen ziehen können. Ein Beispiel: Sie können ein Training so ausrichten, dass die von einem externen Anbieter veranstaltete Schulung das Thema „Künstliche Intelligenz (KI) und Datenschutz“ abdeckt. Einerseits können Sie so wichtiges und aktuelles Wissen unter die Leute bringen, eben durch den externen Spezialisten. Andererseits können Sie selbst davon profitieren, falls Sie bei dem einen oder anderen Thema noch nicht sattelfest sind. Sie bekommen also Qualifikation ganz nebenbei.

Im Übrigen können eine gut abgestimmte Schulung und ein intensiver Austausch mit dem Referenten Ihre Situation als Datenschutzberater erheblich verbessern. Manchmal ist es sprichwörtlich so, dass der Prophet im eigenen Land nichts gilt. Sie können sich den Mund fusselig reden, doch erst wenn eine externe Kapazität die Dinge bestätigt, schenkt man dem Glauben.

Es gibt unzählige Anbieter, aber nicht jeder passt

Sollen Sie unterstützt werden, ist das zwar eine gute Nachricht. Doch zugleich beginnt für Sie und wahrscheinlich auch für die Personalabteilung die Suche nach einem passenden Angebot bzw. Anbieter oder Referenten. Suchen Sie mit der Suchmaschine Ihres Vertrauens nach Schulungen, finden Sie im Internet ganz schnell einige Anbieter. Und meist bieten diese an, eine Schulung speziell für Ihr Unternehmen zu konzipieren und auch im Unternehmen durchzuführen. Doch wie lässt sich bei all den Anbietern die Spreu vom Weizen trennen? Schliesslich sollte Ihr Unternehmen nicht dem erstbesten Anbieter den Zuschlag geben. Setzen Sie auf die folgende Checkliste:



Keine Auftragsbearbeitung bei Schulungen

Eine Auftragsbearbeitung liegt meist nicht vor. Der Anbieter bzw. der Referent entscheidet einerseits meist selbst über Zwecke und Mittel der Bearbeitung von Personendaten. Ausserdem steht die Bearbeitung von Personendaten nicht im Fokus der Leistung.



CHECKLISTE: Typische Auswahlkriterien bei Inhouse-Schulungen

Frage	Darauf kommt es besonders an	Geklärt?
Welche Inhalte müssen vermittelt werden und welche sind optional?	Überlegen Sie im Vorfeld, was thematisch vermittelt werden muss. Die Inhalte sollte auch Ihr Unternehmen vorgeben bzw. Schwerpunkte sollten angepasst werden können.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Wie setzt sich die Zielgruppe der Veranstaltung zusammen?	Prüfen Sie intensiv, wer an der Schulung teilnehmen soll. Das ist nicht nur für den Referenten wichtig. Ihr Unternehmen kann nur so beurteilen, ob das Vorgehen oder die Inhalte auch zielgruppengerecht gestaltet sind.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein




CHECKLISTE: Typische Auswahlkriterien bei Inhouse-Schulungen


Welches Budget steht zur Verfügung?	Ohne Moos nix los. Klären Sie frühzeitig, welches Budget für die Inhouse-Schulungen zur Verfügung steht. Dabei sollten Sie umfassend über Kostenpositionen nachdenken, die das für die Schulung an sich bestehende Budget schmälern. Das sind auch Kosten für Räume oder Technik.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Welche Anbieter kommen in Betracht?	Prüfen Sie zunächst die Onlineangebote von speziellen Anbietern. Sprechen Sie ggf. auch mit Branchenverbänden bezüglich Empfehlungen und auch mit anderen Datenschutzberatern. Vielleicht können Sie dort Erfahrungsberichte oder Empfehlungen erhalten.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Gibt es Referenzen für die Schulungen?	Klären Sie, inwieweit der Anbieter über Referenzen verfügt. Das können etwa andere Unternehmen sein, die zu den Kunden zählen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Verfügt der Referent über nachgewiesene Fachkompetenz in den betreffenden Themen?	Eine Schulung lebt auch von der Qualifikation des Referenten. Lassen Sie sich erläutern, welche Qualifikation generell beim Referenten vorhanden ist und wie es bei für Ihr Unternehmen besonders relevanten Aspekten aussieht.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Hat der Referent einschlägige Branchenkenntnisse?	Das kann nötig sein, wenn Ihr Unternehmen in einem sehr spezifischen Bereich tätig ist. Kennt sich der Referent nicht aus, kann er nicht auf typische Aspekte eingehen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Inwieweit besteht vorab die Möglichkeit, den Referenten persönlich kennenzulernen?	Bedenken Sie stets, dass die Chemie stimmen muss. Das ist nicht nur relevant für die Konzeption der Schulung. Auch muss der Referent eine gute Beziehung zu den Teilnehmern aufbauen können. Lassen Sie sich nicht damit abwickeln, dass der Referent erst nach Vertragsschluss gesucht werden kann.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Können Schulungsinhalte spezifisch an die Bedürfnisse des Unternehmens angepasst werden?	Die Schulung muss zu Ihrem Unternehmen und dessen Anforderungen passen. Ansonsten verpufft der Trainingseffekt. Das wäre nicht nachhaltig.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Welche Materialien werden den Teilnehmern zur Verfügung gestellt?	Schauen Sie sich an bzw. besprechen Sie, was die Teilnehmer erhalten. Fragen Sie sich, wie gut die Unterlagen später im Alltag brauchbar sind, beispielsweise um etwas nachzuschlagen. Knappe Folien können zwar im Vortrag ausreichen. Als Hilfe nach der Schulung sind sie ohne Erläuterungen meist jedoch unbrauchbar.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Welche Urheberrechte bzw. Nutzungsrechte bestehen, etwa an Schulungsunterlagen?	Klären Sie, was Ihr Unternehmen mit den Unterlagen machen darf. Ist Ihr Unternehmen hier eingeschränkt, sinkt eventuell der zukünftige Nutzwert. Ausserdem riskiert Ihr Unternehmen Ärger, wenn es sich nicht an die entsprechenden Vereinbarungen hält.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Wie soll das Wissen vermittelt werden?	Lassen Sie sich die in der Schulung eingesetzten Methoden erläutern. Ausschliesslich ein Vortrag kann zu wenig sein, damit etwas bei den Teilnehmern hängen bleibt. Achten Sie hier insbesondere darauf, dass die angedachten Methoden ausgewogen und praxisnah sind. Sie müssen auch zum Bedarf und zu den Fähigkeiten der Teilnehmer passen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Wie steht es um Teilnehmerzahl und Gruppengrösse?	Auch das sollte angesprochen werden. Ggf. berechnet sich die Vergütung nach der Anzahl der Teilnehmer. Eine Pauschale ist hier meist besser. Zudem sollten Sie darauf achten, dass Teilnehmerzahl und Gruppengrösse (z. B. zwecks Gruppenarbeit) zu Thema und Vorgehen passen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Wie wird Praxisnähe hergestellt?	Haben Sie ein Auge darauf, welche Elemente hierzu eingebaut werden. Praxisnahe Beispiele sind eine Sache. Gruppenübungen oder Teamarbeit auf Basis von realen Situationen aus Ihrem Unternehmen können einen erheblich grösseren Nutzen bringen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Welche Kosten entstehen für die Erstellung der Schulung, von Schulungsunterlagen und pro durchgeführte Veranstaltung?	Lassen Sie sich erläutern, was kostenmässig auf Ihr Unternehmen zukommt. Achten Sie hier insbesondere auch auf Kosten, die man zunächst nicht auf dem Radar hat. Das können Druckkosten für Unterlagen genauso sein wie Kosten für Anreise, Reisezeit, Unterkunft oder die Kosten für erforderliche Präsentationstechnik.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Inwieweit sind die zeitlichen Rahmenbedingungen und möglichen Termine rechtzeitig planbar?	Hier geht es darum, wie eine Schulung in den Jahresplan Ihres Unternehmens passt. Ausserdem ist ein zeitlicher Vorlauf unerlässlich, um die Veranstaltung zu planen, zu organisieren und anzukündigen.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Welche Kosten entstehen, wenn eine Schulung verschoben werden muss?	Auch das kann passieren: Viele Teilnehmer sind krank und die Schulung ergibt an einem bestimmten Termin wenig Sinn. Dann sollte eine Schulung abgesagt und ein anderer Termin vereinbart werden können, am besten ohne weitere Kosten.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Wie sehen die vertraglichen Regelungen aus?	Es kann vieles besprochen werden und gut klingen. Entscheidend ist, was später im Vertrag stehen wird. Schauen Sie unbedingt mit den Kollegen über die Vereinbarung, ob das Besprochene tatsächlich enthalten ist. Zudem sollten Sie auf Kündigungsmöglichkeiten achten. Sind die Teilnehmer oder Sie unzufrieden, sollte die Sache schnell beendet werden können.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein

Kein Ding der Unmöglichkeit: 7 Tipps, damit Sie ab 2026 jeder kennt

Damit Sie Ihren Aufgaben als Datenschutzberater gut nachkommen können, müssen die Kollegen Sie frühzeitig einbinden und mit Informationen versorgen. Dafür ist es unerlässlich, dass man Sie kennt und weiss, was Sie machen und wofür Sie zuständig sind. Doch im Unternehmen bekannt zu sein ist kein Selbstläufer. Setzen Sie auf diese sieben Tipps!

Tipp 1: Gehen Sie den Ursachen auf den Grund

Sie meinen, jeder kennt Sie? Seien Sie sich mit dieser Einschätzung nicht zu sicher. Wechseln Sie beispielsweise in die Perspektive eines neuen Mitarbeiters oder Lehrlings. Fragen Sie sich, wie dieser wohl den Datenschutzberater wahrnimmt, wo es Berührungspunkte gibt und wie man in Kontakt kommen kann. Unter Umständen merken Sie schnell, dass Sie vielleicht altgediente Mitarbeiter kennen, doch gerade die Neuen keinen blassen Schimmer haben, wer Sie sind und was Sie machen.

Weiterer wichtiger Punkt, mit dem Sie sich auseinandersetzen sollten: Wie nehmen Sie sich selbst wahr und wie werden Sie von anderen wahrgenommen? Sprechen Sie hier beispielsweise mit Personen Ihres Vertrauens, wie diese Sie als Mensch und als Datenschutzberater wahrnehmen. Vielleicht erkennen Sie auf diese Weise, wo Sie an sich, Ihrem Auftreten und Ihrer Aussendarstellung arbeiten müssen. Das sollten Sie mit höchster Priorität angehen.

Tipp 2: Das A und O – Ihr Gesicht und Ihr Name

Damit alle im Unternehmen Sie kennen und vor allem wiedererkennen, müssen Sie genau das den Menschen leicht machen. Dazu nutzen Sie alle Gelegenheiten, um Ihr Gesicht und Ihren Namen bekannt zu machen. Hierzu einige Beispiele: Veröffentlichen Sie etwas im Intranet, etwa einen Awarenessartikel, sollten Sie nach Möglichkeit auch ein Foto von sich unterbringen. Nicht anders ist es bei einer Präsentation. Auch Ihren Namen sollten Sie wo immer möglich „anbringen“. Und hier ist die Präsentation ein Paradebeispiel. Achten Sie darauf, dass nicht nur ein Abteilkürzel oder die Funktion „Datenschutzberater“ als Ersteller genannt wird. Ihr Name muss auftauchen. Sind Sie bei einer internen Veranstaltung, tragen Sie nach Möglichkeit ein Namensschild. Auch wenn Sie an einer Besprechung mit Personen teilnehmen, die Sie vielleicht nicht kennen, sollten Sie ein Namensschild aufstellen. Achten Sie hier darauf, dass Ihr Name und ggf. Ihre Funktion aus der Ferne noch gut lesbar sind. Am besten, Sie bereiten einen gedruckten Aufsteller vor.

Tipp 3: Seien Sie auf allen Bühnen präsent

Lassen Sie keine Gelegenheit aus, um sich als Person, Ihr Gesicht und Ihren Namen präsent zu machen. Egal, wozu man Sie einlädt, machen Sie Ihre Teilnahme möglich. Das betrifft interne Veranstaltungen wie z. B. Feiern oder Feste genauso wie wichtige Informationsveranstaltungen wie etwa Vorstellungen der Geschäftsentwicklung oder Betriebsversammlungen. Hat man Sie bei etwas aus Ihrer Sicht für Sie Wichtigem „vergessen“ einzuladen, lassen Sie die Sache nicht einfach auf

sich beruhen. Haken Sie schnellstens nach und klären Sie, inwieweit man Sie tatsächlich einfach vergessen hat. Ist das nicht der Fall, können Sie den Veranstalter ggf. davon überzeugen, dass Ihre Teilnahme sinnvoll ist. Gute Argumente sind etwa, dass Sie so wichtige Informationen erhalten oder das Thema Datenschutz vertreten können. Beissen Sie etwa wegen hierarchischer Aspekte auf Granit, können Sie ggf. mit der Unternehmensleitung sprechen.

Tipp 4: Gespräche, Gespräche, Gespräche

Bekannt machen Sie sich auch dadurch, dass Sie ins Gespräch kommen. Laden Sie beispielsweise Führungskräfte oder Abteilungsleiter ab und an zum Statusgespräch ein. Denken Sie insbesondere an den IT-Leiter oder den Leiter des Vertriebs. Doch auch ein Gespräch mit der Arbeitnehmervertretung kann sich für Sie lohnen. Gerade wenn man merkt, dass man mit Ihnen „reden“ kann und Ihnen an einem praxisnahen Datenschutz gelegen ist, fasst man Vertrauen und prägt Sie sich ein.

Tipp 5: Räumen Sie Hindernisse aus dem Weg

Mit Ihnen zu sprechen muss jedem im Unternehmen leichtfallen. Um das zu erreichen, können Sie eine offene Sprechstunde anbieten. Auch der Hinweis, dass Ihre Tür im wahrsten Sinn des Wortes offen steht, kann manchem die Kontaktaufnahme erleichtern. Weiss man, dass man mit einem Anliegen auch spontan bei Ihnen vorbeischauen kann, kann auch das der Schubs in die richtige Richtung für die betreffende Person sein.

Tipp 6: Datenschutz muss Gesprächsthema werden

Je mehr der Datenschutz bei den Mitarbeitern im Gespräch ist, desto besser. Dazu bieten sich nicht nur Awarenessmassnahmen an. Besonders geeignet sind auch alle internen Medien in Ihrem Unternehmen. Schauen Sie zunächst, was andere machen, und überlegen Sie sich, was auch Sie anbieten können, idealerweise noch etwas besser oder innovativer als die Kollegen. Auch wenn bei einer guten „Show“ Datenschutz anscheinend zur Nebensache wird, leisten Sie ihm und sich einen grossen Dienst.

Tipp 7: Nehmen Sie es positiv und vor allem mit Humor

Datenschutz mag ab und an eine bierernste Sache sein. Allerdings muss das nicht auch für Sie gelten und wie Sie mit dem Thema umgehen. Versuchen Sie bei allem, was Sie tun, locker zu bleiben, und beweisen Sie Humor. Ganz nebenbei zeigen Sie so: Sie sind nicht die „Datenschutzpolizei“. Sie sind Mensch und Kollege, der niemandem den Kopf abreisst, wenn mal etwas schiefgeht.



Gute Vorsätze für 2026: Motivieren Sie die Mitarbeiter zum Datenschutz

Als jemand mit Know-how in der praktischen Datenschutzarbeit wissen Sie: Das Thema Datenschutz ist kein Selbstläufer. Sie sind als Datenschutzberater immer als Botschafter und Impulsgeber gefragt. Nur so besteht die Chance, dass sich Unternehmensleitung, Führungskräfte und Beschäftigte datenschutzfreundlich verhalten.

Nutzen Sie das junge 2026

Soll Werbung für ein Produkt funktionieren, brauchen Sie ein tolles Produkt und den passenden Zeitpunkt. Nur dann fällt Ihre Botschaft auch auf fruchtbaren Boden und Ihr Anliegen wird wahrgenommen. Eine gute Gelegenheit bieten die ersten Arbeitswochen im neuen Jahr. Nach der Rückkehr an den Arbeitsplatz haben viele Mitarbeiter noch Zeit, sich über Neues im Unternehmen zu informieren. Ausserdem: Viele Menschen stehen guten Vorsätzen für das neue Jahr offen gegenüber. Warum sollten Sie also nicht die Gunst der Stunde nutzen und beispielsweise einige wichtige Tipps zum richtigen Umgang mit Personendaten geben?

Gehen Sie es geschickt an

Hals über Kopf eine Sensibilisierungsaktion durchzuführen ist meist nicht ganz so schlau. Unter Umständen machen Sie sich viel Arbeit, doch das Ergebnis ist nicht zufriedenstellend oder zeigt bei der Zielgruppe überhaupt keine Wirkung. Damit Sie das Beste rausholen, sollten Sie planvoll und Schritt für Schritt vorgehen.

Schritt 1: Schauen Sie, was Sie vermitteln wollen

Stellen Sie sich eine Ideenliste zusammen, was (Ihnen) rund um den Datenschutz besonders wichtig ist. Überlegen Sie, welches Verhalten Sie sich von den Beschäftigten Ihres Unternehmens wünschen. Notieren Sie sich alles, was Ihnen einfällt. Prüfen Sie später, ob es sinnvoll ist, daraus einen guten Vorsatz für 2026 zu machen. Beispiel gefällt? Kommt Ihnen sofort in den Sinn, dass Sie andauernd feststellen, dass Unterlagen nicht datenschutzkonform entsorgt werden, sollten Sie das unbedingt adressieren. Also rauf damit auf Ihre Ideenliste.

Aus den so zusammengestellten Ideen wählen Sie z. B. die zehn wichtigsten aus. Aber Vorsicht: Haben Sie hier auch die Zielgruppe bzw. den Adressatenkreis Ihrer Vorsätze im Blick. Sind Themen zu speziell, sollten Sie diese nicht bei den guten Vorsätzen für alle Mitarbeiter bringen. Eventuell kann es dann sinnvoll sein, gute Vorsätze für spezielle Zielgruppen zu formulieren, beispielsweise für Führungskräfte oder Mitarbeiter im Aussendienst.

Schritt 2: Überlegen Sie, wie Sie am besten die Mitarbeiter erreichen

Wie Sie Ihre Botschaft am besten an die Frau oder an den Mann bringen, hängt in erster Linie davon ab, wie Ihr Unternehmen funktioniert. Haben alle Mitarbeiter ein E-Mail-Postfach, können Sie eine E-Mail in Betracht ziehen, die Sie zum nächsten passenden Zeitpunkt verschicken. Verfügt jedoch ein

Teil der Mitarbeiter nicht über ein eigenes Postfach, kann eine Information per E-Mail nicht alle Mitarbeiter erreichen. Zudem kann sie schnell übersehen werden, wenn sie nach dem ersten Öffnen als „gelesen“ markiert ist. Hier kann es geschickt sein, wenn Sie Aushänge machen, die Sie an einem Schwarzen Brett oder im Kopierraum aufhängen. Daneben können Sie auch auf ein ausgedrucktes Schreiben setzen, das Sie am Arbeitsplatz deponieren.

Natürlich können Sie auch in eine ganz andere Richtung denken. Digital bietet sich das Intranet an, wo Sie einen Artikel mit guten Vorsätzen für 2026 platzieren können. Auch eine virtuelle Sprechstunde ist schnell organisiert. Diese hat den Vorteil, dass Sie die Informationen viel persönlicher vermitteln können und auch für Rückfragen zur Verfügung stehen.

Schritt 3: Erstellen Sie sich einen Zeitplan

Egal, für welche Variante Sie sich entscheiden, Sie brauchen unbedingt einen Zeitplan. Wählen Sie ein passendes Datum, damit Ihre Aktion auch tatsächlich wahrgenommen wird. Ggf. ist der Tag einer Betriebsversammlung genauso ungeeignet wie der Tag, an dem eine neue Unternehmensstruktur bekannt gegeben wird. Hier geht Ihr Thema unter und der Effekt ist gleich null.

Haben Sie einen Tag gefunden, überlegen Sie, welche Aufgaben Sie vorab erledigen müssen. Planen Sie für Ihre To-dos alles Relevante ein, das Sie oder andere beisteuern sollen. Denken Sie auch an etwas zeitlichen Puffer. Geraten Sie in Zeitnot, passieren Fehler. Patzer und Fehler können die Wirkung Ihrer Aktion schnell zerstören.

Schritt 4: Gehen Sie in die Umsetzung

Nicht nur ein Zeitplan ist wichtig. Machen Sie sich für die Umsetzung eine Checkliste bzw. einen Ablaufplan. So stellen Sie etwa sicher, dass Sie den richtigen Verteiler wählen oder niemand Relevanten in Kopie vergessen. So wäre es fatal, wenn Sie gerade die Unternehmensleitung bei Ihrer Awareness-Information übergehen. Machen Sie eventuell auch einen Testlauf. Wollen Sie eine E-Mail verschicken, sollten Sie diese vorab an sich und vielleicht noch einige ausgewählte Kollegen schicken. Fehler fallen dann noch rechtzeitig auf, etwa eine unvorteilhafte Darstellung oder nicht funktionierende Links.

Schritt 5: Bringen Sie die Punkte immer wieder auf den Tisch

Haben Sie Ihre Aktion durchgezogen, sollten Sie nicht einfach einen Haken an die Sache machen. Wie jeder weiss, werden

gute Vorsätze unterjährig gern über Bord geworfen. Überlegen Sie also, wie Sie die guten Vorsätze immer wieder thematisieren und ansprechen können. Erinnern Sie beispielsweise dar-

an, wenn Sie die Kollegen in Datenschutzfragen beraten oder wenn Sie etwas sehen, was nicht zu den ausgegebenen guten Vorsätzen passt.



MUSTER: Information „Gute Vorsätze im Datenschutz für 2026“

Liebe Kollegin,
lieber Kollege,

das Jahr 2026 ist noch ziemlich jung. Und klar ist schon jetzt: Es wird so manche Herausforderung für unser Unternehmen und uns alle geben. Doch gemeinsam können wir die anstehenden Herausforderungen meistern, und zwar die grossen und die kleinen. Mal eher grosse und mal eher kleine Herausforderungen gibt es auch im Datenschutz. Denken Sie nur an künstliche Intelligenz und Cyberkriminelle, die ebenfalls mit der Zeit gehen. Hier sind wir alle gefordert.

Im Übrigen können gerade Sie einen wertvollen Beitrag dazu leisten, dass es im Umgang mit Personendaten zu keinen Pannen oder Verstössen kommt. Nehmen Sie sich die folgenden guten Vorsätze zu Herzen und setzen Sie diese 2026 um.

Halten Sie sich an Gesetze und Regeln

Klar ist: Datenschutz funktioniert dann am besten, wenn jeder die Sache ernst nimmt, auch Sie. Insofern ist es wichtig, dass gesetzliche wie betriebliche Regelungen mit Datenschutzbezug eingehalten werden. Sind Regelungen unklar, unpraktisch oder anscheinend realitätsfremd, sollten Sie das Gespräch suchen, beispielsweise mit dem Datenschutzberater. Gemeinsam lässt sich eine praktikable Lösung finden. Garantiert!

Sehen Sie Datenschutz als etwas Positives

Auch wenn manche Politiker gern über Datenschutz schimpfen. Der Datenschutz ist keine unnötige Gängelei der Unternehmen. Die Regeln sind gesetzlich verankert und gehen auf Grundrechte zurück. Auch die Sensibilität für das Thema steigt bei Betroffenen, etwa Kunden oder Beschäftigten. Daher ist es besser, sich der Herausforderung „Datenschutz“ zu stellen und diese pragmatisch anzugehen. Und können wir im Datenschutz glänzen, freut das alle.

Helfen Sie Ihren Kollegen

Datenschutz ist ein Gemeinschaftswerk und alle müssen an einem Strang ziehen. Stellen Sie fest, dass es ein Kollege mit dem Datenschutz nicht so genau nimmt oder etwas falsch macht, sollten Sie ihn darauf ansprechen. Erklären Sie, wie es aus Ihrer Sicht richtiggeht. Lässt sich so vermeiden, dass etwas schiefgeht, haben wir alle etwas davon.

Achten Sie auf Datenschutz, egal, wo Sie arbeiten

Bestimmt arbeiten auch Sie ab und an im Homeoffice oder unterwegs auf einer Dienstreise im Hotel. Doch auch dort sollten Sie alle Regeln zum Datenschutz beachten, die auch im Büro gelten. Das bedeutet beispielsweise, dass Sie darauf achten, dass Informationen nicht in die Hände Unbefugter geraten können. Ferner sollten Sie vertrauliche Gespräche so führen, dass sie vertraulich bleiben. Auch wenn es um das Entsorgen von Unterlagen oder anderen Datenträgern geht, sind die geltenden Regeln umzusetzen. Idealerweise entsorgen Sie dort, wo es sicher ist – im Unternehmen!

Gehen Sie Cyberkriminellen nicht auf den Leim

Bekommen Sie eine E-Mail, in der etwas Ungewohntes gefordert wird, etwa eine Zahlung zu veranlassen oder Daten und Anmeldeinformationen weiterzugeben, sollten Sie Vorsicht walten lassen. Halten Sie es hier mit dem Prinzip „Always think twice“. Denken Sie zweimal über eine Sache nach, bevor Sie handeln. Fragen Sie lieber auch Kollegen bzw. Vorgesetzte, ob das denn wirklich sein kann.

Übrigens: Nehmen Sie sich aktuell gerade vor gefälschten QR-Codes in Acht. Über falsche Codes, etwa bei E-Ladesäulen oder Parkscheinautomaten, locken die Kriminellen ihre Opfer auf gefälschte Webseiten. Fallen Sie darauf rein und geben Sie etwa Kreditkartendaten an, ist es meist zu spät. Die Kriminellen bedienen sich an Ihrem Geld und das sehen Sie meist nie wieder. Daher: Nutzen Sie QR-Codes, schauen Sie genau hin, wohin Sie der betreffende Link führt. Haben Sie Zweifel, hören Sie auf Ihre innere Stimme und machen Sie nicht weiter.

Bei Pannen & Co.: Warten Sie nicht mit dem Melden

Kommt es zu einer Panne mit Datenschutzrelevanz, ist eines ganz wichtig: schnelles Handeln, und zwar indem Sie die zuständigen Kollegen bzw. den Datenschutzberater informieren. Die Eile hat ihren Grund: Unter Umständen beginnen gesetzliche Meldepflichten, die das Unternehmen einhalten muss. Auch können Sie mit der schnellen Meldung dafür sorgen, dass eine technische Panne schnell behoben wird. So lässt sich möglicher Schaden beschränken oder sogar ganz abwenden. Das liegt in aller Interesse.

Sprechen Sie frühzeitig mit dem Datenschutzberater

Datenschutz ist kein triviales Thema und der Teufel steckt im Detail. Manchmal steht das Relevante zwischen den Zeilen oder muss auf Basis der einschlägigen Rechtsprechung interpretiert werden. Geht es bei einem Vorhaben auch um Personendaten, sollten Sie das Gespräch mit dem Datenschutzberater suchen, idealerweise möglichst frühzeitig. Hier bekommen Sie Beratung und Unterstützung aus einer Hand, damit Sie an das Thema Datenschutz schnell einen Haken machen können.

Ihr Datenschutzberater
Heinz Elmann



Organisatorisches Versagen: Prüfen Sie diese 7 Hotspots

Als Datenschutzexperte wissen Sie: Datenschutz ist eine ziemlich grosse Herausforderung, und zwar für Ihr Unternehmen und Sie als Datenschutzberater. Und damit Datenschutz bei der Bearbeitung von Personendaten funktioniert, kommt es nicht nur auf die technische Umsetzung an. Entscheidend ist auch das Organisatorische.

Organisatorisches kann zum Problem werden

Art. 7 und Art. 8 Bundesgesetz über den Datenschutz (DSG) machen unmissverständlich klar: Ihr Unternehmen muss risikoorientiert geeignete technische und organisatorische Massnahmen umsetzen. Es muss so sicherstellen und nachweisen können, dass die Bearbeitung gemäss der DSG erfolgt bzw. sicher ist. Auch muss es fortlaufend prüfen, ob die Massnahmen noch angemessen sind bzw. inwieweit diese angepasst werden müssen.

Dabei ist klar: Nicht nur technisch kann beim Bearbeiten von Personendaten so einiges schiefgehen. Das ist auch möglich, wenn Sie den Blick auf das Organisatorische richten. Beispielsweise können

- › fehlende Regeln und Vorschriften dazu führen, dass Beschäftigte Daten falsch bearbeiten und es zum Datenschutzverstoß kommt;
- › unzureichendes Wissen und fehlende Sensibilität zu Fehlverhalten im Umgang mit Personendaten führen;
- › überhaupt nicht, falsch oder unzureichend erfüllte Betroffenenrechte für grossen Ärger sorgen, etwa mit Betroffenen;
- › wiederholte oder fortgesetzte Verstöße auf systemische Organisationsmängel hinweisen, die ein Bussgeld unumgänglich machen und dieses ggf. höher ausfallen lassen;
- › fehlende oder unzureichende Kontrollen die Risiken und Schäden grösser machen.

Übrigens: Ihr Unternehmen und dessen Leitung sollten nie nur das Bussgeldrisiko im Blick haben. Werden die gebotenen Massnahmen nicht ergriffen, wird nicht angemessen mit Risiken umgegangen. Das kann auch das persönliche Haftungsrisiko erhöhen.

Halten Sie Ausschau nach diesen 7 Hotspots

Prüfen Sie, ob Sie diese Hotspots, sprich diese Schwachpunkte, in Ihrem Unternehmen wiederfinden. Ist dem so, sollten Sie zügig das Gespräch mit der Unternehmensleitung suchen. Diskutieren Sie Ihre Feststellung und suchen Sie gemeinsam nach Wegen, um die Situation zu verbessern.

Hotspot 1: Fehlende Vorgaben, Regelungen und Verträge

Schauen Sie zunächst ins Verzeichnis der Bearbeitungstätigkeiten gemäss Art. 12 Abs. 2 DSG. Darin sollten alle Bearbeitungsverfahren bzw. Bearbeitungsprozesse abgebildet und umfassend dokumentiert sein. Prüfen Sie zumindest stichprobenhaft für die risikobehafteten Bearbeitungstätigkeiten, inwieweit Regelungen, Arbeitsanweisungen und Festlegungen bestehen. Denken Sie in dem Zusammenhang auch an Ver-

träge und Vereinbarungen mit Datenschutzrelevanz. Das sind nicht nur Datenschutzverträge, etwa zur Auftragsbearbeitung. Auch betriebliche Reglements können Defizite aufweisen und nicht alles Relevante regeln bzw. schlichtweg veraltet sein.

Hotspot 2: Unzureichende Umsetzung von Festlegungen

Nur weil es Vorgaben oder Festlegungen gibt, werden diese nicht automatisch umgesetzt. Manchmal entwickeln oder etablieren sich auch Handhabungen, die dem Geregelter widersprechen. Kontrollieren Sie also die tatsächliche Umsetzung und machen Sie insofern einen Abgleich von Ist und Soll.

Hotspot 3: Fehlende oder nicht funktionierende Prozesse

Prozesse sind entscheidend. Denn sie geben Abläufe vor und stellen sicher, dass erforderliche Entscheidungen von den zuständigen und befugten Personen getroffen werden. Haben Sie hier zunächst ein Auge auf Prozesse, die direkten Datenschutzbezug haben bzw. der Umsetzung der Vorgaben des DSG dienen, etwa Prozesse zum strukturierten Vorgehen bei Datenpannen.

Hotspot 4: Mangelndes Risikobewusstsein

In manchem Unternehmen wird nach dem Prinzip gehandelt, dass alles schon irgendwie gutgehen wird. So zu denken und zu arbeiten ist geradezu grob fahrlässig. Dass irgendwann etwas schiefgehen wird, ist quasi vorprogrammiert.

Hotspot 5: Unzureichende Awareness und Sensibilität

Hier liegt der Fokus auf Führungskräften und Mitarbeitern. Schätzen Sie ein, wie es um Sensibilität für die Anforderungen des Datenschutzes steht. Ausserdem ist die positive Grundeinstellung zum Thema entscheidend. Kämpft man eher gegen den Datenschutz, wird es mit der Umsetzung schwierig.

Hotspot 6: Defizite bei der Datenschutzorganisation

Bewerten Sie kritisch, inwieweit die Organisation zu den bestehenden Herausforderungen passt. Verfügen Sie nicht über die nötigen Ressourcen oder verweigert man Ihnen die nötige Unterstützung, wird dem Datenschutz ein Bärendienst erwiesen.

Hotspot 7: Fehlende Kontrollen

Ob etwas funktioniert, sieht man erst, wenn man nachprüft, ob dem so ist. Dabei müssen es nicht immer Ihre Kontrollen sein, um ein Funktionieren oder Nichtfunktionieren auszumachen. Prozesse oder Regelungen können auch andere Stellen prüfen.

Nicht im Urlaub erreichbar: Droht mir Ärger?

FRAGE: Ich bin Datenschutzberater und nehme die Funktion nebenbei wahr. Während meiner dreiwöchigen Ferien kam es zu einem Hackerangriff. Bei dem wurden Daten gestohlen. Gegenmassnahmen wurden ergriffen. Was aber wohl nicht passiert ist, ist die Meldung dieser Datenpanne an den EDÖB. Nach meinen Ferien hatte ich ein Gespräch mit einem verärgerten Geschäftsführer. Der meinte, dass die vergessene Meldung meine Schuld wäre. Es könne nicht sein, dass ich während der Ferien nicht erreichbar wäre. Er meinte, dass er mir nun die Weisung erteile, vor den nächsten Ferien Kontaktdaten zu hinterlegen, damit ich für den Fall der Fälle erreichbar bin. Meine Frage daher: Muss ich das mit mir machen lassen? Kann mir arbeitsrechtlicher Ärger drohen, weil ich in den letzten Ferien nicht erreichbar war?

ANTWORT: Zunächst einmal zu den letzten Ferien: Arbeitsrechtlicher Ärger, etwa eine arbeitgeberseitige Abmahnung, dürfte nicht drohen. Hier fehlt jeder Grund, weil Ihnen kein Verstoß gegen den Arbeitsvertrag oder Ihre Pflichten als Arbeitnehmer vorzuwerfen ist. Sie waren in den Ferien und das war und ist Ihr gutes Recht.

Dabei ist wichtig: Der Zweck der Ferien ist Erholung. Der Erholungszweck der Ferien sollte nicht beeinträchtigt werden. Sollte es dennoch zu einer Abmahnung kommen, heisst es handeln. Diese sollten Sie nicht hinnehmen. Vielmehr sollten Sie mit Hilfe eines Rechtsbeistands dagegen vorgehen. Schliesslich wäre sie haltlos.

Sie dürfen nicht erreichbar sein

Generell sollten Sie hinsichtlich einer „Mitteilungspflicht von Kontaktdaten“ eines wissen: Eine solche Pflicht besteht nicht. Denn es gilt Folgendes:

- › Das Bundesgesetz über den Datenschutz (DSG) sieht nicht vor, dass Sie als Datenschutzberater immer erreichbar sein müssen, etwa um bei Fragen zum Datenschutz zur Verfügung zu stehen. Das gilt auch für Fragen oder eine Beratung im Zusammenhang mit einem Hackerangriff oder sonstigen Datenpannen.
- › Die Anforderungen des DSG richten sich an den Verantwortlichen. Er muss die nötigen Massnahmen ergreifen, um das DSG umzusetzen. Braucht er hierfür Beratung, muss

er sicherstellen, dass diese jederzeit verfügbar ist. Und hier gibt es einige Möglichkeiten: So kann er einen Stellvertreter für Sie benennen. Daneben kann jedoch auch auf externe Beratungslösungen zurückgegriffen werden. So kann im Fall der Fälle ein externer Datenschutzberater unterstützen oder eben auch ein Anwalt.

- › Für Sie besteht keine Verpflichtung mitzuteilen, wo Sie Ihre Ferien verbringen oder wie man Sie während Ihrer Ferien erreichen kann. Das lässt sich einerseits arbeitsrechtlich nicht begründen. Andererseits ist es auch datenschutzrechtlich nicht drin. So lässt sich die Bearbeitung der betreffenden Kontaktinformationen nicht auf § 31 Abs. 1 und 2 DSG stützen. Besondere Fälle nach Art. 31 Abs. 2 DSG treffen nicht zu. Die Informationen sind für die Durchführung des Beschäftigungsverhältnisses bzw. eines Vertrags mit dem Betroffenen nicht erforderlich. Ein überwiegendes berechtigtes Interesse scheidet aus, weil schon wegen der gesetzgeberischen Wertungen zum Ferienzweck Ihre Interessen überwiegen dürften. Möglich wäre nach Art. 31 Abs. 1 DSG, dass Sie Ihre Einwilligung geben und Ihre Kontaktdaten in den Ferien freiwillig mitteilen. Dazu sind Sie aber nicht verpflichtet.

Suchen Sie das klärende Gespräch

Meist ist es besser, in einem Gespräch nach einer Lösung zu suchen, die allen Interessen gerecht wird. Das dürfte im Fall der Fälle ein externer Datenschutzberater sein, der eingebunden werden kann, wenn es wirklich brennt.

In welcher Sprache müssen die Datenschutzhinweise sein?

FRAGE: Als in der Schweiz ansässiges Unternehmen überarbeiten wir gerade die Datenschutzhinweise für unsere Webseite und unseren Onlineshop. In diesem Zusammenhang haben wir nun diskutiert: In welchen Sprachen müssen diese Hinweise veröffentlicht werden?

ANTWORT: Zunächst einmal brauchen Sie die Hinweise und ggf. andere relevante Erklärungen (z. B. Allgemeine Geschäftsbedingungen, Nutzungsbedingungen, Einwilligungen) in den Amtssprachen der Schweiz. Das sollte dann noch Französisch, Italienisch und unter Umständen Rätomanisch sein. Einerseits haben Sie wahrscheinlich Kunden, die diese Sprachen sprechen. Aber auch der EDÖB dürfte es schnell beanstanden, wenn es keine entsprechende Version gibt. Zudem brauchen Sie Versionen für alle Sprachen, die von denjenigen gesprochen

werden, an die sich die Webseite oder der Onlineshop richtet. Für Letzteren können Sie die betreffenden Länder meist schnell ausmachen. Schauen Sie, in welche Länder Ihr Unternehmen liefert, sprich aus welchen Ländern man in Ihrem Shop einkaufen kann. Bei der Webseite können Sie ein Auge auf die auswählbaren Sprachversionen werfen. Ggf. werden Sie die zuständige Abteilung fragen müssen. Zumindest für die Fokusländer wird man die relevanten Dokumente und Informationen in der jeweiligen Landessprache bereithalten müssen.



AG Wesel: Falsch adressierter Brief führt zu 500 € Schmerzensgeld

Mit Personendaten muss sorgsam umgegangen werden. Das predigen vielleicht auch Sie den Beschäftigten Ihres Unternehmens. Ein „Wo gehobelt wird, da fallen Späne“ ist keine Rechtfertigung für Unvorsichtigkeiten. Dass auch ein falsch adressierter Brief teuer werden kann, zeigt eine Entscheidung des Amtsgerichts (AG) Wesel aus Deutschland (Urteil vom 23.7.2025, Az. 30 C 138/21).

Der Sachverhalt

Zwei Personen, die späteren Kläger, liessen sich von einer Steuerberaterkanzlei in Steuerfragen beraten. Diese Kanzlei wurde durch fünf Gesellschafter vertreten. Sowohl Kanzlei als auch Gesellschafter waren die späteren Beklagten. Die Kläger zogen um. Im Sommer 2019 teilten sie der Steuerberaterkanzlei mit, dass sich ihre Anschrift geändert habe. Die bisherige Anschrift wäre nicht mehr aktuell. Sie wären fortan unter einer neuen Adresse zu erreichen. Zur Sicherheit wiesen die Kläger die Kanzlei wiederholt auf die neue Anschrift hin.

Steuererklärung geht an veraltete Adresse

Im Sommer 2020 beauftragten die Kläger die Kanzlei mit dem Anfertigen von Steuererklärungen für 2019. Die Kanzlei nutzte ein Programm für die Erstellung der Steuererklärungen. Bei der Aktivierung des Programms wurden automatisch die Kontaktdaten der Mandanten aus vorherigen Steuererklärungen eingelesen. Das führte dazu, dass auch die ehemalige Postadresse der Kläger eingelesen wurde. Die war nämlich noch auf der vorherigen Steuererklärung angegeben.

Die Folge: Die neue Steuererklärung wurde an die frühere Adresse der Kläger geschickt. An der alten Adresse lebten inzwischen andere Personen, die späteren für das Gerichtsverfahren relevanten Zeugen. Der falsch adressierte Brief ging den neuen Bewohnern zu. Weil deren Namen dem Namen der Kläger ähnelte, öffneten sie versehentlich den Brief.

Kläger wollen Schadensersatz

Nach Ansicht der Kläger müssten in diesem Zusammenhang die falschen Empfänger auch vom Inhalt Kenntnis genommen haben. Insofern hätten die falschen Empfänger von sensiblen persönlichen Informationen der Kläger erfahren. Diese wiederum hätten sich dadurch exponiert, stigmatisiert und blossgestellt gefühlt. Aufgrund des Datenschutzverstosses und des daraus resultierenden Schadens zogen die Kläger vor das AG Wesel. Ihre Forderung: insgesamt mindestens 15.000 € Schmerzensgeld. Dieser Forderung erteilte das AG eine Absage. Es billigte den Klägern jeweils einen Schadensersatzanspruch in Höhe von 500 € zu.

So entschied das AG

Es besteht für die Kläger ein Anspruch auf Ersatz des immateriellen Schadens nach Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Die Steuerberatungkanzlei ist eine juristische Person. Sie entscheidet über die Zwecke und Mittel der Bearbeitung von Personendaten und ist somit Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

Kanzlei verletzt Datenschutzgrundsatz

Die Kanzlei hat gegen Art. 5 Abs. 1 Buchst. d DSGVO verstossen. Gemäss dieser Vorgabe müssen Personendaten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. In der Folge müssen alle angemessenen Massnahmen getroffen werden, damit unrichtige Personendaten unverzüglich gelöscht oder berichtigt werden.

Die Kanzlei hat gegen den Grundsatz der Richtigkeit verstossen, weil sie die frühere Adresse der Kläger nicht vollständig aus ihrem Datenbestand gelöscht hat. Dass die falsche Adresse durch ein Programm automatisch eingefügt wurde, ist ohne Relevanz. Vielmehr hätte die Kanzlei dafür sorgen müssen, dass die Adresse im System überhaupt nicht mehr vorhanden ist. Aus dem Verstoß gegen den Grundsatz der Richtigkeit ergibt sich eine unrechtmässige Datenbearbeitung. Diese wiederum kann die Schadensersatzpflicht nach Art. 82 DSGVO auslösen.

Der Verstoß hat bei den Klägern zu einem Schaden geführt. Dabei ist der Begriff des immateriellen Schadens weit zu verstehen. Insofern kann auch der kurzfristige Kontrollverlust einen solchen Schaden darstellen, wobei keine zusätzlichen negativen Folgen nachgewiesen werden müssen.

Schon Fehlversand führt zu Schaden

Vorliegend haben die Kläger einen Kontrollverlust erlitten. Dieser besteht bereits in der Versendung der Unterlagen an die falsche Adresse und dem Zugang an die nunmehr dort lebenden Zeugen. Bereits mit dem Versenden ist der Schaden eingetreten, weil die Daten dem Verfügungsbereich der Kläger entzogen wurden. Sie konnten nicht mehr steuern, wer Kenntnis von ihren Daten nehmen kann.

Der eingetretene Schaden liegt erheblich unter dem, der von den Klägern geltend gemacht wurde. Bei der Schätzung des Schadens sind die Sensibilität der Daten, der Umfang und die Dauer des Kontrollverlusts zu berücksichtigen. Unter anderem, weil unklar blieb, ob weitere Dritte die Daten überhaupt zur Kenntnis nehmen konnten, sind 500 € als Schmerzensgeld angemessen.



Das können Sie aus der Entscheidung folgern

Nachlässigkeiten und Unachtsamkeiten im Umgang mit Personendaten führen zwar vielleicht nicht zu einem Bussgeld. Betroffene können jedoch Schmerzensgeld fordern. Und hier können 500 € je Fall auch schnell die „Portokasse“ sprengen. Nutzen Sie die Entscheidung, um Mitarbeiter zu sensibilisieren.

„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>



DEUTSCHE
FACHPRESSE
**FACHMEDIUM
DES JAHRES 2024
GEWINNER**

Beste Workflow-Lösung

Vorschau:

Prüfen Sie: Sind zu löschende Daten auch wirklich weg?
Schutz Ihres Unternehmens: Machen Sie den Check



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