



BEREITEN SIE IHR UNTERNEHMEN JETZT AUF IHREN URLAUB VOR

AWARENESS

Fördern Sie richtiges Verhalten
bei Datenpannen 1–2

KNOW-HOW

Mit dieser Checkliste
gibt es keine Patzer am
Messestand 3



Onlinebereich:
<https://kurzlink.ch/privacy>



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



PRIVACYXPERTS



Kooperation ist immer besser

Liebe Leserin, lieber Leser,

manchmal ist es zum Haareraufen: Sie geben die richtigen Hinweise, damit es mit dem Datenschutz klappt. Und trotzdem machen die Kollegen genau das Gegenteil von dem, was Sie empfohlen haben.

Nun könnten Sie sich ärgern, die zukünftige Zusammenarbeit verweigern oder die Kollegen rundmachen. Doch viel besser dürfte es sein, wenn Sie die Sache professionell angehen: Erstens sollten Sie sich nicht ärgern und zweitens sollten Sie das Gespräch suchen. Bringen Sie Ihre Enttäuschung zum Ausdruck. Setzen Sie dann aber auch auf Kooperation. Unterstützen Sie beratend und werden Sie nicht müde, die erforderlichen Tipps zu geben.

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

Fördern Sie richtiges Verhalten bei Datenpannen

Seiten 1–2

Know-how

Mit dieser Checkliste gibt es keine Patzer am Messestand

Seite 3

Datenschutzberater

Bereiten Sie Ihr Unternehmen jetzt auf Ihren Urlaub vor

Seiten 4–5

Arbeitsorganisation

Mit diesen 7 Tipps arbeiten Sie sofort zielorientierter

Seite 6

❓ Fragen an die Redaktion

Cyberresilienz: Wie können wir den Handlungsbedarf besser vermitteln?

Seite 7

Was kann ich tun, wenn meine Weiterbildung verweigert wird?

Seite 7

Urteil aus dem Ausland

BGH: Verein muss E-Mail Adressen herausgeben

Seite 8



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



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

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 Chefredaktor:
RA Andreas Würtz, Freiberg am Neckar
Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | goodluz; Seite 1: Adobe Stock | blende11.photo
Erscheinungsweise: 17-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

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

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

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

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



Bei einer Datenpanne kommt es darauf an, schnell richtig zu reagieren.

Fördern Sie richtiges Verhalten bei Datenpannen

Wo Menschen arbeiten, kann auch etwas schiefgehen. Doch im Datenschutz können solche Pannen schnell zum grossen Problem werden, etwa für Betroffene, aber auch für Ihr Unternehmen. Und wenn es dann doch passiert ist, muss richtig reagiert werden. Hier spielen die Führungskräfte eine wichtige Rolle.

Sensibilisieren Sie Vorgesetzte

Im Fall der Fälle, sprich bei einer Datenpanne, sollte nichts dem Zufall überlassen bleiben. Denn dann wird alles meist nur noch schlimmer, weil unvorbereitete Mitarbeiter eventuell kopflos re-

agieren. Um dem vorzubeugen, sollten Sie für Sensibilität sorgen. Schärfen Sie das Bewusstsein bei den Führungskräften. Denn diese treffen im Ernstfall Entscheidungen oder sind Anlaufstelle für die Mitarbeiter. Umso wichtiger ist, dass Vorgesetzte, wissen, worauf es ankommt. Geben Sie die richtigen Tipps.



Muster: Awarenessinfo für Führungskräfte zu Datenpannen

Liebe Kolleginnen und Kollegen mit Führungsverantwortung,

in unserem Unternehmen arbeiten wir alle täglich mit Personendaten – von Kunden, Interessenten, Geschäftspartnern oder Beschäftigten. Diese Daten sind von grossem Wert und wir müssen sie unbedingt schützen. Geraten sie in falsche Hände, kann das zum ersten Problem für die Betroffenen, aber auch für unser Unternehmen werden.

Die Bedrohungslage ist real

Nicht nur das deutsche Bundesamt für Sicherheit in der Informationstechnik hat in seinem letzten Lagebericht festgestellt: Die Bedrohungen durch Hackerangriffe, Phishing und Ransomware-Aktionen sind hoch und nehmen weiter zu. Immer raffinierter und perfider werden die Methoden der Kriminellen. Auch für unser Unternehmen kann niemand ausschliessen, dass es irgendwann Opfer einer solchen Attacke wird. Geraten dann Personendaten in falsche Hände, haben wir eine ernst zu nehmende Datenschutzverletzung. Allerdings kann die auch ohne kriminelles Zutun passieren. Schon falsch versendete E-Mail-Anhänge oder ein falsch konfigurierter Server können schnell zu einer gravierenden Datenpanne führen.

Datenpannen haben es in sich

Sind Personendaten auf Abwegen, etwa weil Hacker Erfolg hatten, liegt regelmässig eine Verletzung des Schutzes von Personendaten vor. Das bedeutet für unser Unternehmen: Wir müssen nicht nur schnell handeln, um den Schaden für Betroffene und unser Unternehmen zu begrenzen. Unter Umständen müssen wir die Sache dem EÖDB melden, und zwar so rasch als möglich. Hier ist Eile geboten. Zudem kann es bei besonders hohem Risiko für die Betroffenen erforderlich sein, dass wir auch die Betroffenen selbst informieren. Nehmen wir es mit dem Ganzen nicht so genau, kann es für unser Unternehmen richtig teuer werden. Der Gesetzgeber lässt hohe Bussgelder zu.

Sie sind als Führungskraft gefragt

Als Führungskraft tragen Sie nicht nur Verantwortung für den geschäftlichen Erfolg Ihres Bereichs oder Ihrer Abteilung. Sie führen Ihre Mitarbeiter und tragen zudem Verantwortung für die Bearbeitungen von Personendaten in Ihrem Zuständigkeitsbereich. Zudem agieren Sie als Führungspersönlichkeit mit Ihrem Handeln und Ihren Entscheidungen als Vorbild. Umso wichtiger ist, dass Sie selbst Datenschutz leben und Ihren Mitarbeitern Orientierung geben. Das kann im Ernstfall der entscheidende Faktor sein, damit schnell, professionell und richtig gehandelt wird.



So bekommen wir Datenpannen in den Griff

Datenschutz funktioniert nur, wenn alle an einem Strang ziehen. Das ist umso wichtiger, wenn es zu brenzligen Situationen kommt. Gerade im Fall von Datenpannen ist es wichtig, dass Sie und Ihre Mitarbeiter richtig reagieren. Damit Ihnen das leichter fällt, habe ich Ihnen einige Tipps zusammengestellt:

Ruhe bewahren

Ist eine Datenpanne passiert, ist der Schock erst einmal gross. Und dennoch ist wichtig: Vermeiden Sie Hektik und unüberlegtes Handeln. Vermeiden Sie Panik bei sich und Ihren Mitarbeitern. Schliesslich ist Panik nie ein guter Berater. Schlimmstenfalls werden die falschen Entscheidungen getroffen. Und die können die Situation noch verschlimmern. Daher: Bewahren Sie einen kühlen Kopf. Beruhigen Sie auch Ihr Team. Handeln Sie lieber nach der Devise: Eile mit Weile. Gehen Sie ruhig und strukturiert vor. Treffen Sie alle Entscheidungen überlegt und mit Bedacht.

Stoppen Sie die Panne

Wurde eine Datenpanne erkannt oder liegen starke Indizien für eine solche vor, ist wichtig: Beenden Sie schnellstmöglich das Schadensereignis. Gibt es etwa ein Datenleck, fliessen eventuell Daten so lange ab, wie es nicht gestopft ist. Handeln ist hier oberstes Gebot und abwarten ist keine Option. Sind Sie sich nicht sicher, was zu tun ist, holen Sie sich Rat von den Profis. Im Datenschutz steht Ihnen der Datenschutzberater zur Verfügung. Für alles rund um die IT sprechen Sie mit den Profis der IT-Abteilung.

Erfassen Sie schnell die Situation

Damit die zuständigen Stellen sich schnell einen Überblick verschaffen können, ist wichtig, dass Sie die erforderlichen Informationen liefern können. Am besten nutzen Sie strukturierte W-Fragen:

- › Was ist konkret passiert?
- › Wann ist es passiert?
- › Wer hat was wann bemerkt?
- › Wessen Daten sind betroffen?
- › Welche Daten sind betroffen?
- › Welches Ausmass hat der Vorfall?
- › Was wurde bereits unternommen?

Sofortige Meldung an den Datenschutzberater

Stellen Sie eine Panne fest oder vermuten Sie deren Vorliegen, müssen Sie schnellstens den Datenschutzberater informieren. Machen Sie das immer, wenn Daten im Spiel sind. Prüfen Sie nicht selbst, ob keine Datenschutzrelevanz besteht, weil Sie denken, dass es sich nicht um Personendaten handelt. Hier steckt der Teufel oft im Detail. Gemeinsam mit dem Datenschutzberater wird auch geprüft, ob es sich um einen meldepflichtigen Vorfall handelt oder ob Betroffene zu informieren sind. Dabei ist jedoch wichtig: Warten ist keine Option. Der EDÖB als Aufsichtsbehörde muss so rasch als möglich informiert werden. Nehmen Sie sich vor, das in maximal 72 Stunden zu erledigen.

Schalten Sie die IT Abteilung unverzüglich ein

Datenpannen können rein technisch bedingt sein. Denken Sie beispielsweise an eine Fehlkonfiguration. Doch auch bei einem Hackerangriff oder einer Ransomware-Attacke steht häufig das Technische im Mittelpunkt. Hier ist dann die IT-Abteilung mit ihren geschulten Spezialisten der wichtigste Akteur. Die Kollegen helfen nicht nur dabei die Schadensursache zu finden bzw. das Schadensereignis zu stoppen. Sie leiten auch alle nötigen Massnahmen ein, um das Funktionieren der IT zu sichern oder wiederherzustellen.

Kehren Sie nichts unter den Teppich

Für manchen mag es verlockend sein. Doch es ist keine gute Idee, einen Vorfall kleinzureden oder zu vertuschen. Auch mögliche Gefahren für Betroffene oder unser Unternehmen zu banalisieren ist schlecht. Darauf zu vertrauen, dass niemand etwas mitbekommen wird, kann ebenfalls richtig schiefgehen. Deshalb ist wichtig: Gehen Sie offen damit um, dass etwas passiert ist. Sie müssen sich hier weder schämen noch ernste Konsequenzen fürchten. Ganz im Gegenteil: Die Konsequenzen drohen gerade dann, wenn Sie schnelle Hilfe vereiteln oder dieser im Weg stehen.

Etablieren Sie eine positive Fehlerkultur

Es liegt nicht nur an Ihnen, ob im Fall der Fälle richtig gehandelt wird. Genauso entscheidend sind Ihre Mitarbeiter. Doch die dürfen keine Angst vor Konsequenzen haben, wenn sie Ihnen Auffälligkeiten oder gemachte Fehler melden. Vermitteln Sie Ihren Mitarbeitern zudem: Wer Vorfälle meldet, handelt genau richtig. Und das verdient die Anerkennung aller. Wer hingegen die Augen verschliesst und schweigt, der gefährdet das ganze Unternehmen.

Dokumentieren Sie lückenlos

Auch wenn Sie etwa technische Probleme selbst lösen oder die durch einen Hackerangriff verursachte Datenpanne beheben können, gilt: Sichern Sie aussagekräftige Beweise, bevor Sie sich ans Arbeiten und Reparieren machen. Fragen Sie im Zweifel vorab bei IT-Abteilung und Datenschutzberater nach. Schliesslich können Beweise unerlässlich sein, wenn die Sache strafrechtlich verfolgt werden soll oder wenn es um eine Schadensregulierung durch eine Versicherung geht.

Sorgen Sie für Awareness

Viele Datenpannen beginnen mit einem einfachen Klick, und zwar auf einen Link oder einen Anhang einer Phishing-E-Mail. Sind die sensiblen Zugangsdaten erst einmal eingegeben, ist es häufig schnell zu spät. Die Kriminellen haben Zugriff und nehmen sich alles an Daten, was nicht niet- und nagelfest ist. Als Führungskraft können auch Sie viel dazu beitragen, dass es nicht zu solchen Vorfällen kommt. Sensibilisieren Sie Ihre Mitarbeiter immer wieder für Phishing-Angriffe. Besprechen Sie gemeinsam in einem Meeting, worauf zu achten ist, wie man sich richtig verhält und was zu tun ist, wenn etwas schiefgegangen ist.

Ich danke Ihnen für Ihre Unterstützung!

Ihr Ben Jamin

Betrieblicher Datenschutzberater

Mit dieser Checkliste gibt es keine Patzer am Messestand

Als Datenschutzberater können Sie nicht überall sein und dafür sorgen, dass in Sachen Datenschutz nichts schief läuft. Dabei gibt es Hotspots, bei denen das Risiko für Patzer einfach grösser ist. So z. B. bei Messeständen. Es liegt auf der Hand, dass hier Marketing oder Vertrieb im Vordergrund stehen. Doch der Datenschutz darf dabei nicht auf der Strecke bleiben.

Bauen Sie mit dieser Checkliste vor

Natürlich wäre es eine tolle Sache, wenn Sie vorab die Kollegen für den Messestand umfassend betreuen oder auch vor Ort einmal nach dem Rechten schauen könnten. Häufig wird das jedoch schon allein aus Kapazitätsgründen kaum möglich sein. Um dennoch

Ihrem Beratungsauftrag aus Art. 10 Abs. 2 Bundesgesetz über den Datenschutz (DSG) gut und risikoorientiert nachkommen zu können, haben Sie verschiedene Möglichkeiten: Sie können einerseits die zuständigen Kollegen zu einem Austauschtermin einladen. Andererseits können Sie Hilfe zur Selbsthilfe leisten. In beiden Fällen können Sie Ihre Aktivitäten auf die folgende Checkliste stützen.

Kurzcheckliste: Datenschutz am Messestand



To-do	Das ist wichtig	Okay?
Sind die Datenschutzaspekte für alle relevanten Bearbeitungen geklärt?	- Denken Sie hier insbesondere an die Grundsätze der Bearbeitung nach Art. 6 DSG. Die müssen bei allen Bearbeitungen von Personendaten umgesetzt sein. - Berücksichtigen Sie vor allem die an Messeständen typischerweise vorkommenden Bearbeitungen. So z. B. „Erfassung von Interessenten (Lead-Generierung)“, „Erhalt von Visitenkarten zur Kontaktaufnahme“, „Gesprächsnotizen“, „Bestellungen“. - Sind einzelne Aspekte unklar, sprechen Sie den Datenschutzberater unverzüglich und vorab darauf an.	☐ Ja ☐ Nein
Werden die Transparenz- und Informationspflichten vor Ort erfüllt?	- Werden Personendaten beschafft, muss über die Rahmenbedingungen informiert werden. Die erforderlichen Transparenzinformationen ergeben sich aus Art. 19 DSG. - Grundsätzlich ist ein abgestuftes Vorgehen möglich: Kernangaben werden mündlich oder kurz schriftlich gegeben. Details stehen auf einem Infoblatt bzw. auf der Webseite.	☐ Ja ☐ Nein
Werden Einwilligungen richtig eingeholt und dokumentiert?	- Sollen Daten werblich genutzt werden, ist oft die Einwilligung des Empfängers erforderlich. Idealerweise werden Newsletterregistrierungen online durchgeführt, damit die Dokumentation über das Double-Opt-in-Verfahren zweifelsfrei gegeben ist. - Eine wirksame Einwilligung bedarf einer aktiven Zustimmungshandlung. Diese darf regelmässig nicht vermutet werden. Auch vorgelegte Ankreuzfelder sind ein No-Go.	☐ Ja ☐ Nein
Gibt es Möglichkeiten, um Gespräche vor Ort vertraulich zu führen?	- Gerade auf Messen kann es turbulent zugehen. Zudem gibt es viele neugierige Augen und Ohren. Sorgen Sie für Rückzugsmöglichkeiten, um Vertrauliches geschützt besprechen zu können. - Sind vertrauliche Gespräche vor Ort nicht möglich, bieten Sie einen späteren Termin ausserhalb der Messe an.	☐ Ja ☐ Nein
Sind Listen und Eintragungen vor unbefugten Blicken geschützt?	- Egal ob Terminlisten oder Listen, in die sich jemand eintragen kann. Es ist problematisch, wenn hier nicht Erforderliches sichtbar ist. Decken Sie Voreinträge unbedingt ab. - Um allen Eventualitäten vorzubeugen, setzen Sie auf Einzelerfassungsbögen oder ausgedruckte und zeitlich sortierte Termine.	☐ Ja ☐ Nein
Wird Clean Desk auch am Messestand umgesetzt?	- Alles, was Personendaten oder sonst Schützenswertes enthält, darf nicht offen herumliegen. Abdecken oder Wegschliessen bei Nichtgebrauch ist oberstes Gebot. - Sorgen Sie für Möglichkeiten, Unterlagen sicher wegzuschliessen. Sensibles oder für Langfinger Interessantes sollte am Abend nicht vor Ort bleiben. Nehmen Sie entsprechende Unterlagen, Geräte und Datenträger mit.	☐ Ja ☐ Nein
Sind bei Geräten grundlegende Schutzmassnahmen umgesetzt?	- Verschlüsselung ist ein Muss, und zwar bei Notebooks, Tablets und Datenträgern. - Mobile Geräte sind am Messestand vor spontanen Diebstählen zu schützen, etwa durch Kabelschlösser. - Daten werden auf Zentralsystemen gespeichert. Die Einwahl erfolgt über Mobilfunk (kein WLAN!) unter Nutzung von VPN-Verschlüsselung.	☐ Ja ☐ Nein
Ist die sichere Entsorgung von Unterlagen gewährleistet?	- Personendaten dürfen nicht über den Papiermüll vor Ort entsorgt werden. - Vernichten Sie Papiere vor Ort? Nutzen Sie einen Schredder mit Partikelschnitt, sodass ein erneutes Zusammensetzen der Unterlagen praktisch nicht möglich ist.	☐ Ja ☐ Nein
Erfolgt eine eventuelle Berichterstattung unter Wahrung des Datenschutzes?	- Sollen etwa Fotos oder Videos gemacht und veröffentlicht werden, müssen die geltenden Rahmenbedingungen beachtet werden. - Generell gilt: Einerseits ist eine Rechtsgrundlage aus der DSG erforderlich (→ häufig Einwilligung). Zudem muss das Persönlichkeitsrecht beachtet werden. Nur selten ist keine Einwilligung erforderlich.	☐ Ja ☐ Nein
Werden Pannen und Vorfälle mit Datenschutzrelevanz sofort gemeldet?	- Mitarbeiter sind entsprechend zu instruieren, dass Vorfälle wie z. B. der Verlust eines Datenträgers sofort dem Datenschutzberater und der IT-Abteilung zu melden sind. - Mit dem Datenschutzberater wird die Datenschutzrelevanz geklärt. Das gilt auch für eventuell bestehende Meldepflichten oder zu ergreifende Sofortmassnahmen.	☐ Ja ☐ Nein



Bereiten Sie Ihr Unternehmen jetzt auf Ihren Urlaub vor

Die Herausforderungen, denen Sie sich als Datenschutzberater tagtäglich stellen müssen, haben es in sich. Sie sind nicht nur fachlich anspruchsvoll. Auch Stress und Hektik können Ihnen ganz gewaltig zusetzen. Umso wichtiger ist, dass Sie bei Ihrem wahrscheinlich und hoffentlich bald anstehenden Urlaub Ihre Akkus aufladen können. Das klappt besser, wenn Sie von Ihrem Unternehmen nichts hören.

Bessere Vorbereitung = mehr Erholung im Urlaub

Stellen Sie sich in den Mittelpunkt. Geben Sie für sich das Ziel aus, die Auszeit bestmöglich zu organisieren. Idealerweise schaffen Sie es, dass man Sie während Ihres Urlaubs in Ruhe lässt und Sie unbesorgt abschalten können. Dazu ist eines wichtig: Bereiten Sie Ihr Unternehmen so auf Ihre Abwesenheit vor, dass es nicht nur ohne Sie zurechtkommt. Idealerweise bleibt auch alles aus, was Ihnen nach Ihrem Urlaub die Erholung schnell wieder zunichtemacht.

Gehen Sie Schritt für Schritt vor

Hat Ihr Handeln Hand und Fuss, stellen Sie nicht nur sicher, dass Sie alles Wichtige bedenken. Sie tragen dazu bei, dass Stress erst gar nicht aufkommt. Orientieren Sie sich an folgenden fünf Schritten:

Schritt 1: Aufgaben und Infos sammeln

Starten Sie möglichst früh in ein Brainstorming. Nehmen Sie sich Zeit und notieren Sie alle Einfälle zu folgenden Impulsfragen:

- Welche Aufgaben erlauben auch während meines Urlaubs keinen Aufschub?
- Was kann eine Urlaubsvertretung übernehmen?
- Wer muss über meinen Urlaub informiert werden?
- Wie kann ich sicherstellen, dass im Notfall nichts schief läuft?

Schritt 2: E-Mails und Kalender durchforsten

Gehen Sie systematisch Ihr Postfach und Ihren Kalender durch. Suchen Sie nach offenen Anfragen, Fristsachen, anstehenden Be-

ratungen oder Projekten, die in Ihrem Urlaub relevant werden könnten. Sortieren Sie das Gefundene danach, was Sie erledigen müssen, was verschoben oder delegiert werden kann.

Schritt 3: Sprechen Sie mit wichtigen Personen

Eventuell haben Sie manch Wichtiges überhaupt noch nicht auf dem Radar. Und dennoch könnte genau das während Ihres Urlaubs hohe Priorität erhalten. Sprechen Sie also frühzeitig mit der Unternehmensleitung oder den Leitern von IT bzw. Kundenservice. Einerseits können Sie schon früh über Ihre Abwesenheit informieren. Andererseits können Sie ausmachen, ob Wichtiges ansteht.

Schritt 4: Planen Sie mit Vorlauf

Stellen Sie zusammen, was Sie im Vorfeld Ihres Urlaubs in Angriff nehmen müssen. Dazu können Sie auch auf die folgende Checkliste setzen. Viele Erledigungen, sprich To-dos, brauchen jedoch einiges an Vorlauf für Gespräche, Abstimmungen oder Entscheidungen. Warten Sie also nicht zu lange.

Schritt 5: Prüfen Sie die Umsetzung

Die Vorbereitung des Unternehmens auf Ihre Abwesenheit kann eine längere Sache sein. Prüfen Sie also regelmässig, wie weit Sie mit den einzelnen, zur organisierenden Punkten sind. Und machen Sie den finalen Check am besten nicht erst am letzten Arbeitstag. Besser ist das einige Tage davor. Denn dann haben Sie zumindest noch eine Chance, eventuell nötige Alternativen zu organisieren und können sicher sein, dass für alle Aufgaben vorgesorgt ist.

Checkliste: So bereiten Sie das Unternehmen auf Ihren Urlaub vor



To-do	Erläuterung	Erledigt
Urlaubsvertretung		
Vertretung oder Stellvertreter mit Unternehmensleitung abstimmen	➤ Klären Sie mit der Leitung, inwieweit eine Abwesenheitsvertretung ausreicht oder ob es einen Stellvertreter geben soll. Für einen Urlaub reicht oft eine Urlaubsvertretung aus. ➤ Suchen Sie frühzeitig das Gespräch, um grünes Licht für die Auswahl einer Vertretung bzw. eines Stellvertreters zu haben. Suche und Auswahl können Zeit in Anspruch nehmen.	☐ Ja ☐ Nein
Vertreter auswählen und Zustimmungen einholen	➤ Machen Sie Wunschkandidaten aus. Achten Sie hier insbesondere auf die persönliche und charakterliche Eignung sowie ein positives und professionelles Auftreten. Schliesslich geht es bei Ihnen um eine Vertretung mit besonderer Verantwortung. ➤ Klären Sie mit der betreffenden Person und im Anschluss auch mit deren Vorgesetzten, inwieweit man mit der Übernahme der Aufgabe einverstanden ist. Besprechen Sie zudem die Verfügbarkeit während Ihrer Abwesenheit. ➤ Vermeiden Sie faule Kompromisse. Was Ihre Vertretung macht, kann im Zweifel auch auf Sie zurückfallen.	☐ Ja ☐ Nein

Aufgaben für Vertretung festlegen	- Legen Sie konkret fest, was die Vertretung während Ihrer Abwesenheit übernehmen soll bzw. darf. - Halten Sie die Aufgaben am besten schriftlich fest, damit es später keine Unklarheiten gibt. Informieren Sie den Vertreter über die Aufgaben und das, was nicht dazuzählt.	☐ Ja ☐ Nein
Erforderliches Know-how vermitteln	- Vermitteln Sie einige grundlegende Basics zum Datenschutz. - Informieren Sie über kritische Themen und das richtige Verhalten in entsprechenden Fällen. - Legen Sie grossen Wert auf den Aspekt „Vertraulichkeit“. Vermitteln Sie, dass jegliche Informationen im Rahmen der Vertretung nichts für unbefugte Augen und Ohren sind. - Sprechen Sie das richtige Verhalten in bestimmten (Not-)Situationen durch, etwa zum richtigen Verhalten bei Anrufen oder Anfragen sowie bei Datenpannen oder Betroffenenanfragen.	☐ Ja ☐ Nein
Vertretung arbeitsfähig machen	- Leiten Sie alles in die Wege, was für die Arbeitsfähigkeit der Vertretung nötig ist. Denken Sie insbesondere an den lesenden Zugriff auf Daten oder Postfächer. Auch sind passende Berechtigungen unerlässlich. - Probieren Sie gemeinsam aus, ob relevante Zugriffe auch tatsächlich funktionieren. Dann klappt alles auch dann, wenn es gebraucht wird. - Denken Sie bereits bei der Vergabe von Berechtigungen an deren Entzug nach dem Urlaub.	☐ Ja ☐ Nein
Plan B für den Ausfall der Vertretung erstellen	- Auch Ihre Vertretung kann plötzlich für längere Zeit ausfallen. Gut ist es dann, wenn Sie eine alternative Lösung haben. - Stellen Sie sicher, dass Sie über einen Ausfall informiert werden. Nur so können Sie rechtzeitig reagieren.	☐ Ja ☐ Nein
Briefing am letzten Arbeitstag planen und durchführen	- Dieser Termin ist wichtig: Einerseits kann Ihre Vertretung noch offene Fragen klären. Andererseits können Sie auf Ihnen besonders Wichtiges hinweisen. - Machen Sie den Termin vormittags, damit Sie im Bedarfsfall noch bis zum Feierabend Antworten auf offene Fragen geben können.	☐ Ja ☐ Nein
Termin für Briefing nach dem Urlaub festlegen	- Legen Sie unbedingt einen ersten Rücksprachetermin fest, damit Sie schnell erfahren können, was während Ihrer Abwesenheit passiert ist. - Ist kein persönlicher Termin möglich, bitten Sie darum, dass alles Wichtige in einer E-Mail zusammengestellt wird.	☐ Ja ☐ Nein
Ihre Arbeit		
Wichtige laufende Themen, Projekte und Beratungen abschliessen	- Gehen Sie Ihre offenen Anfragen durch und versuchen Sie, diese vor Urlaubsbeginn zu erledigen. - Ist das nicht oder nur teilweise möglich, informieren Sie die betreffenden Kollegen. - Müssen andere noch etwas erledigen oder zuliefern, fordern Sie das bis nach Ihrem Urlaub ein.	☐ Ja ☐ Nein
Stand und Handlungsbedarf zu laufenden Anfragen von Betroffenen und der Aufsichtsbehörde klären	- Idealerweise werden solche Vorgänge vor Ihrem Urlaub abgeschlossen. Ist das nicht machbar, bieten Sie vorab noch Ihre Unterstützung an, damit während Ihrer Abwesenheit nichts liegen bleibt. - Vermitteln Sie, dass solche Vorgänge nicht auf Ihre Rückkehr warten können. Meist sind Fristen einzuhalten. Ist das nicht machbar, sollte um Fristverlängerung gebeten werden. Bei Betroffenenanfragen sollte der Betroffene entsprechend informiert werden.	☐ Ja ☐ Nein
Wichtige Termine verschieben	- Finden während Ihrer Abwesenheit wichtige Termine statt, an denen Sie teilnehmen sollten, versuchen Sie, diese zu verschieben. - Können Termine nicht verschoben werden, sollten Sie dafür sorgen, dass Sie über die Ergebnisse informiert werden. Eventuell kann auch ein Vertreter teilnehmen. Dann ist wichtig, dass Sie ihn instruieren.	☐ Ja ☐ Nein
Wichtige Ansprechpartner über Abwesenheit und Urlaubsvertretung informieren	- Informieren Sie wichtige Stellen rechtzeitig über Ihre Abwesenheit. - Wer für Ihre Arbeit wichtig ist, sollte rechtzeitig telefonisch informiert werden. Hier besteht die Möglichkeit, noch kurz Wichtiges zu besprechen. - Senden Sie rechtzeitig eine E-Mail an die Kollegen, in der alles Relevante enthalten ist. Dazu zählt auch die Info, wer Sie während Ihres Urlaubs vertritt.	☐ Ja ☐ Nein
Awarenessaktivitäten zum Urlaub der Mitarbeiter durchführen	- Auch die Mitarbeiter gehen bald in Urlaub. Eventuell wollen Sie im Vorfeld noch einige wichtige Tipps geben, etwa zu Clean Desk vor dem Urlaub. - Bieten Sie eventuell eine offene Sprechstunde an. Oft gibt es Fragen auch rund um Abwesenheit und Urlaub, auf die Sie so nicht gekommen wären.	☐ Ja ☐ Nein
Notfallpläne erstellen und prüfen	- Überlegen Sie, inwieweit einige Checklisten sinnvoll sind, damit Sie etwa bei Betroffenenanfragen oder Datenpannen nichts dem Zufall überlassen. Falsche Entscheidungen können später auch Ihnen viel Arbeit bescheren. - Vielleicht gibt es Pläne für Notsituationen mit Datenschutzrelevanz. Checken Sie vorab, inwieweit diese noch passen.	☐ Ja ☐ Nein
Notfallerreichbarkeit festlegen und kommunizieren	- Machen Sie aus, in welchen Fällen man Sie trotz Ihres Urlaubs kontaktieren kann oder muss. Legen Sie zudem fest, wie man Sie erreichen kann. - Bei wichtigen Ansprechpartnern oder Ihrer Urlaubsvertretung können Sie Kontaktdaten hinterlegen. Achten Sie darauf, dass Sie hierüber auch tatsächlich erreichbar sind.	☐ Ja ☐ Nein
Abwesenheitsnotiz erstellen und terminieren	- Setzen Sie am besten auf eine interne und eine externe Version. Geben Sie vor allem extern nur die unbedingt erforderlichen Informationen. - Stellen Sie ggf. schon vorab den Aktivierungszeitraum ein.	☐ Ja ☐ Nein
Technikcheck durchführen	- Wollen Sie von unterwegs Zugriff auf Daten oder E-Mails haben, muss die nötige Technik funktionieren, etwa eine externe Anmeldung und eine VPN-Software. - Führen Sie den Check frühzeitig durch. Klappt etwas nicht, haben Sie noch ausreichend Zeit, das Problem zu lösen.	☐ Ja ☐ Nein
Arbeitsplatz aufräumen und organisieren	- Auch für Ihren Arbeitsplatz gilt Clean Desk. Räumen Sie und schliessen Sie alles Schützenswerte weg. - Entsorgen Sie nicht mehr benötigte Unterlagen datenschutzkonform. - Haben Sie wichtige Daten, führen Sie eine Datensicherung durch. Dann können Sie auch im Fall der Fälle weiterarbeiten, etwa wenn Ihre Notebookfestplatte bei einem Sturz beschädigt wird.	☐ Ja ☐ Nein

Mit diesen 7 Tipps arbeiten Sie sofort zielorientierter

Wer wenig Zeit für seine Aufgaben als Datenschutzberater zur Verfügung hat, der kann ein Lied davon singen: Oft kommt vieles zu kurz, manchmal verzetteln man sich bei der Erledigung selbst einfacher Aufgaben und hier und da wächst einem manches über den Kopf. Das Ruder können Sie herumreissen. Arbeiten Sie strikt ziel- und ergebnisorientiert.

Diese 7 Tipps helfen garantiert

Sie fragen sich, wie Sie denn bloss zielorientierter arbeiten können? Die folgenden sieben Tipps tragen ganz automatisch dazu bei, dass Ziel- und Ergebnisorientierung steigen:

1. Fragen Sie Löcher in den Bauch

Um zielorientiert arbeiten und vor allem beraten zu können, brauchen Sie viele Informationen. Trauen Sie sich also, schon im Vorfeld von Besprechungen Fragen zu stellen und Informationen einzufordern. Damit steigern Sie nicht nur Ihre eigene Effizienz, weil Sie sich besser vorbereiten können. Sie zwingen auch andere dazu, sich mit vielen Aspekten aktiv auseinanderzusetzen. Und manchmal passiert Folgendes: Der Termin wird verschoben, weil man erst einmal die eigenen Hausaufgaben erledigen muss. Also sparen Sie sich die Zeit für einen nicht zielführenden Termin.

2. Arbeiten Sie nach Plan

Idealerweise haben Sie für Ihre Arbeit als Datenschutzberater einen Fahrplan fürs komplette Jahr. Ist Ihnen klar, was Sie umsetzen wollen oder angehen müssen, fällt es leichter, das rechtzeitig in Angriff zu nehmen. Ausserdem können Sie besser Prioritäten setzen, wenn etwas Unvorhergesehenes eintritt. Dabei ist klar: Sie müssen keinen komplexen Plan erstellen. Schon eine einfache Tabelle mit Themen kann ausreichen. Bewerten Sie diese unter Prioritäts Gesichtspunkten und vergeben Sie einen realistischen Erledigungstermin. Überprüfen Sie regelmässig den Stand der Dinge und passen Sie Ihre Liste bei Bedarf an.

3. Setzen Sie risikobasiert Schwerpunkte

Ihre Aufgaben als Datenschutzberater ergeben sich grundsätzlich aus Art. 10 Abs. 2 Bundesgesetz über den Datenschutz (DSG). Im Wesentlichen beraten Sie in allen Fragen des Datenschutzes und kontrollieren dessen Umsetzung. Zwar fordert der Gesetzgeber in Art. 10 Abs. 2 DSG von Ihnen nicht ausdrücklich, dass Sie risikoorientiert vorgehen sollen. Aber das ergibt sich etwa aus Art. 7 und 8 DSG, weil der Verantwortliche, den sie schulen sollen, risikoorientiert vorgehen muss.

Eine wichtige Massnahme zur entsprechenden Schwerpunktsetzung ist folgende: Bei jeder neuen Beratung oder Kontrollidee Ihrerseits machen Sie eine kurze Risikobewertung. Betrachten Sie die Schutzwürdigkeit der Daten, das Schadenspotenzial und die Eintrittswahrscheinlichkeit. Setzen Sie mit Ihrer Tätigkeit dann dort an, wo das Risikopotenzial am grössten ist.

4. Nutzen Sie To-do-Listen zur Steuerung

Egal, ob Sie diese auf Tages-, Wochen- oder Monatsebene führen: Aufgabenlisten, neudeutsch To-do-Listen, sollten Sie zu einem Ihrer wichtigsten Hilfsmittel machen. Notieren Sie alle offenen Aufgaben an einem zentralen Ort. Dazu können Sie beispielsweise Bordmittel Ihres Computers, des E-Mail-Programms oder Smartphones nutzen und entsprechende Listen verwalten.

Aber es gibt auch Alternativen, damit Sie alles Relevante am Arbeitsplatz immer direkt vor Augen haben: Arbeiten Sie mit Klebezetteln. Erstellen Sie sich an der Wand vor dem Schreibtisch verschiedene „Klebezonen“, etwa mit „Wichtig und dringend“ oder „Diese Woche erledigen“. Kleben Sie dann Ihr To-do in die passende Zone.

5. Vergessen Sie Multitasking

Das menschliche Gehirn ist einfach nicht für Multitasking gemacht, sprich eben nicht für das gleichzeitige Abarbeiten mehrerer Aufgaben. Und wer ehrlich zu sich ist, kann die Erkenntnis nur bestätigen. Wird parallel an mehreren Dingen gearbeitet, kommt meist nichts Gutes dabei heraus. Es passieren Fehler oder die Qualität leidet erheblich. Und das wäre gerade in Ihrem Job als Datenschutzberater ein grosses Problem.

Daher: Arbeiten Sie nach Möglichkeit konzentriert eine Sache nach der anderen ab. Ist das nicht möglich, sollten Sie zumindest versuchen, saubere Schnitte zu machen und Teilergebnisse zu sichern. Dann können Sie später auf einer soliden Basis neu einsteigen. So machen Sie es sich leichter.

6. Lernen Sie, Nein zu sagen

Auch das ist wichtig: Sie müssen Ihre Aufgabenwahrnehmung und die diesbezügliche Qualität sichern und manches ablehnen. Akzeptieren Sie vor allem kein „Das macht der schon“, wenn man Ihnen Arbeit über den Zaun wirft. Sagen Sie in solchen Fällen professionell Nein. Erklären Sie, warum Sie sich nicht um eine Sache kümmern können. Und sind Sie nicht zuständig, spielen Sie den Ball sofort zurück.

7. Schärfen Sie Ihr Rollenbewusstsein

Machen Sie sich immer klar: Sie beraten und kontrollieren. Zum Entscheiden und Umsetzen sind andere berufen. Führen Sie sich immer wieder vor Augen, was zu Ihrer Rolle und Ihren Aufgaben zählt. Damit vermeiden Sie unnötige Aufwände und können sich mehr auf Ihre Ziele konzentrieren.

Cyberresilienz: Wie können wir den Handlungsbedarf besser vermitteln?

FRAGE: Der Leiter der IT und ich als Datenschutzberater wollen mit der Unternehmensleitung sprechen. Aus unserer Sicht muss im Unternehmen mehr zum Schutz vor Cyberrisiken unternommen werden. Haben Sie Argumente, die die Notwendigkeit zum Handeln unterstreichen?

ANTWORT: Es lassen sich viele Argumente finden, warum Ihr Unternehmen aktiv werden sollte. Darauf basierend sollte eine durchdachte Gesamtstrategie entwickelt werden. Dabei brauchen Sie nicht zu sehr zwischen IT-Sicherheit und Datenschutz unterscheiden. Denn meist ist gute IT-Sicherheit auch eine geeignete Grundlage für guten Datenschutz.

Denken Sie an diese Argumente

- **Schutz geschäftskritischer Informationen:** Jedes Unternehmen hat solche Informationen. Dabei können auch Personendaten von Kunden, Vertragspartnern oder Mitarbeitern zu dieser Datenkategorie zählen. Stellen Sie einfach die Frage: Was wäre, wenn solche Daten nicht mehr zur Verfügung stünden oder wenn sie von Kriminellen zwecks Erpressung verschlüsselt würden?
- **Einhaltung von relevanten Anforderungen:** Typischerweise sind das gesetzliche Anforderungen. Daneben kann es auch vertragliche Festlegungen geben, die Ihr Unternehmen erfüllen muss. Zugleich müssen Ihr Unternehmen und dessen Management Vorsorge treffen, um Risiken zu minimieren.
- **Schutz der Reputation:** Ein gutes Image kann entscheidend für den Geschäftserfolg sein. Leidet die Reputation, kann das die Vertrauensbasis von Geschäftspartnern zunichtemachen. Doch auch die Gewinnung von Neukunden wird schwieriger bzw. teurer.
- **Sicherung des Fortbestands des Unternehmens:** Das

Schlagwort ist hier „Business Continuity Management“. Mit geeigneten Massnahmen muss Ihr Unternehmen am Laufen gehalten werden, auch wenn es zu erfolgreichen Angriffen kommt. Denn: Haben Kriminelle etwa mit einem Phishing-Angriff Erfolg, können Systeme und Daten für längere Zeit nicht oder nur eingeschränkt zur Verfügung stehen. Nur mit einer guten Gegenstrategie sowie Plänen für die Wiederherstellung der Arbeitsfähigkeit kann hier schnell und effektiv reagiert werden.

- **Vermeidung finanzieller Schäden:** Die können vielfältige Ursachen haben. So kann etwa bei einer Datenpanne nicht nur ein Bussgeld durch den EDÖB als Datenaufsichtsbehörde drohen. Vertragspartner oder Betroffene können Schadensersatz fordern. Hinzu kommt, dass etwa schlechte Presse bzw. ein ramponiertes Image auch die Umsätze schrumpfen lassen kann.

Dokumentieren Sie Ihre Empfehlungen

Zwar ist das Vorbringen guter Argumente meist nur ein erster Schritt. Der ist jedoch wichtig. Schliesslich schärfen Sie das Risikobewusstsein beim Management. Gemeinsam mit Ihrem Kollegen sollten Sie jedoch auch Handlungsempfehlungen geben. Idealerweise führen Sie konkrete Entscheidungen herbei. Auf jeden Fall ist wichtig, dass Sie Ihre Empfehlungen konkret dokumentieren.

Was kann ich tun, wenn meine Weiterbildung verweigert wird?

FRAGE: Meine Weiterbildung soll aus finanziellen Gründen gestrichen werden. Was kann ich nun bezüglich der verweigten Weiterbildung unternehmen? Kann ich die irgendwie erzwingen?

ANTWORT: Erzwingen können Sie Ihre Weiterbildung nicht. Allerdings sollten Sie eventuell erneut das Gespräch suchen. Machen Sie sich für das Gespräch zum Ziel, Folgendes zu klären:

- **Welche Gründe haben zur Ablehnung geführt?** Sparzwänge sind als Grund sehr allgemein. Klären Sie, an welchen Kosten genau es lag. Hängt es an den Teilnahmegebühren, den Reise- und Übernachtungskosten oder an beidem? Das eröffnet Ihnen die Möglichkeit, hier neue Varianten ins Spiel zu bringen. Sind etwa Hotelkosten das Problem, können Sie ggf.

eine kostenfreie Übernachtung bei Freunden vorschlagen.

- **Welche genehmigungsfähigen Möglichkeiten gibt es?** Sind Reisen nicht drin, können Sie an der Veranstaltung vielleicht auch virtuell teilnehmen. Das spart Kosten. Sind die Teilnahmekosten zu hoch, können Sie mit dem Veranstalter sprechen. Ggf. sind Rabatte drin, auch wenn die nirgendwo stehen.
- **Welche Alternativen kommen in Betracht?** So können Sie sich selbst weiterbilden. Studieren Sie beispielsweise Leitfäden von Aufsichtsbehörden. Manchmal gibt es kostenfreie Veranstaltungen von Behörden.

BGH: Verein muss E-Mail-Adressen herausgeben

Wenn es um das Bearbeiten von Personendaten geht, findet sich die Antwort für unsere europäischen Nachbarn nicht immer in der Datenschutz-Grundverordnung (DSGVO). Häufig sind Gerichte gefragt, etwa der deutsche Bundesgerichtshof (BGH). Und der musste klären, ob ein Verein die E-Mail-Adressen der Mitglieder an ein Mitglied herausgeben muss (Urteil vom 10.12.2025, Az. II ZR 132/24).

Der Sachverhalt

Das Mitglied (der spätere Kläger) eines Vereins war mit der Vereinsführung und dem Vorgehen der Vereinsspitze hinsichtlich des Verkaufs von Grundstücken nicht einverstanden, die dem Verein gehörten. Im Zuge einer Mitgliederversammlung wollte sich der Vereinsvorstand den Verkauf der besagten Grundstücke von den Vereinsmitgliedern absegnen lassen.

Der Kläger wollte zu diesem Vorhaben in Opposition treten. Um im Vorfeld der Versammlung Kontakt zu allen Vereinsmitgliedern aufnehmen und die Opposition organisieren zu können, verlangte der Kläger eine Liste mit den E-Mail-Adressen aller Vereinsmitglieder.

Verein verweigert E-Mail-Adressen

Der Aufforderung des Klägers wollte der Verein nicht nachkommen. Unter anderem wurde das damit begründet, dass man schon seit 2018 den Vereinsmitgliedern zusichere, dass die bei Vereinsbeitritt angegebene E-Mail-Adresse nur für einen Zweck genutzt werde. Der besteht darin, die Mitgliedschaft zu verwalten.

Verein fügt Einladung Schreiben bei

Der Verein lud zur Mitgliederversammlung. Mit der Einladung an die Mitglieder wurden Unterlagen für die Abstimmung per Briefwahl und auch ein Informationsschreiben der Initiative verschickt. Das hielt der Vorstand für ausreichend. Die Abstimmung fiel schliesslich zugunsten der Empfehlung des Vereinsvorstands aus und damit für den Verkauf der Grundstücke.

Mitglied klagt gegen Beschlüsse

Für den Kläger war die Sache nach der Abstimmung noch nicht erledigt. Er klagte vor dem Landgericht (LG). Seiner Ansicht nach waren verschiedene Beschlüsse der Mitgliederversammlung nichtig.

Zunächst entschied das LG gegen den Kläger. Vor dem Berufungsgericht sah die Sache anders aus. Das Oberlandesgericht (OLG) München gab dem Kläger recht. Die angefochtenen Beschlüsse der Mitgliederversammlung seien nichtig. Das insbesondere, weil dem Kläger im Vorfeld der Versammlung nicht die E-Mail-Adressen der Mitglieder überlassen wurden. Damit wäre gegen den Gleichbehandlungsgrundsatz und den Grundsatz der Chancengleichheit verstossen worden.

Gegen diese Entscheidung klagte nun der Verein und zog vor den BGH. Der urteilte wie die Vorinstanz.

So entschied der BGH

Der BGH bestätigte die Argumentation der Vorinstanz. Zu Recht ist das OLG davon ausgegangen, dass der Kläger die Herausgabe der E-Mail-Adressen fordern kann. Durch die Verweigerung der E-Mail-Adressen ist ein relevanter und zur Nichtigkeit der Versammlungsbeschlüsse führender Mangel entstanden. Der Kläger hat ein berechtigtes Interesse am Erhalt der E-Mail-Adressen, wenn er im Vorfeld einer Versammlung Kontakt zu den anderen Mitgliedern aufnehmen will, um auf deren Abstimmungsverhalten Einfluss zu nehmen. Dem steht auch nicht die DSGVO entgegen. Elementarer Bestandteil der Willensbildung in einem Verein ist das Zusammenwirken der Mitglieder. Ein berechtigtes Interesse ist anzunehmen, wenn die Kontaktaufnahme zu anderen Mitgliedern darauf abzielt, Bedenken gegen eine vom Vereinsvorstand beabsichtigte Entscheidung zur Kenntnis zu geben. Ein eventuelles Interesse anderer Mitglieder, nicht durch eine solche Kontaktaufnahme belästigt zu werden, tritt hinter dieses berechnete Interesse zurück. Dabei ist irrelevant, dass künftigen Mitgliedern zugesagt wurde, dass deren E-Mail-Adresse nur für die Mitgliedschaftsverwaltung verwendet wird.

Übermittlung ist Vertragserfüllung

Die Weitergabe der E-Mail-Adressen lässt sich auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO stützen. Auch der Beitritt zu einem Verein fällt unter den Vertragsbegriff. Dieser darf nicht zivilrechtlich verstanden werden, sondern datenschutzrechtlich und europaspezifisch. Der Auskunftsanspruch zur Durchsetzung der Mitgliedschaftsrechte des Klägers kann nur durch Übermittlung der E-Mail-Adressen erfüllt werden. Deshalb ist diese zur Vertragserfüllung erforderlich. Es gab auch keine mildereren Mittel. So musste der Kläger nicht nachfragen, ob die Mitglieder mit der Weitergabe ihrer E-Mail-Adresse einverstanden wären.

§

Das können Sie in der Schweiz folgern

Hier können wir die Wertung erkennen, die stets beim Datenschutz vorgenommen werden muss: Mit Datenschutz(zusagen) lässt sich nicht argumentieren, wenn berechnete Interessen vorrangig zu wahren sind. Im vorliegenden Fall liess sich die Übermittlung der E-Mail-Adressen zudem auf die Rechtsgrundlage „Vertragserfüllung“ (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO) stützen. Wichtig ist hier, dass der Begriff „Vertrag“ nicht im zivilrechtlichen Sinn verstanden werden darf.

„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

**IT- & INFORMATIONSSICHERHEIT UPDATE**

Ihr digitaler Praxisratgeber für mehr Schutz Ihrer betrieblichen Informationen

Schnelles Filtern der News, die Sie brauchen

Aus Fehlern anderer lernen

Praxisnahe (Video-)Anleitungen

Audit-Prüflisten

Schulungsmaterial

Interpretation der Gesetze und Richtlinien

Darum sollten Sie nicht auf das IT- & Informationssicherheit Update verzichten:

- Erhalten Sie alle 2 Wochen News, Praxistipps und Rechtsempfehlungen
- Sicherheitsmaßnahmen messbar machen, dank interaktiver Checklisten
- Arbeitshilfen im Onlinebereich sparen Zeit bei Schulungen, Richtlinien & Co.

Testen Sie das E-Magazin für mehr IT- und Informationssicherheit 1 Monat GRATIS





Innovatives e-Magazin

Cyber-Resilienz

Neu: Mit eigenen Themen

<http://bit.ly/IT-Info-Update>



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

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

Vorschau:

Schnelle Erstberatung gefälltig?
Setzen Sie auf diese Checkliste
7 Tipps, damit Sie die E-Mail-Flut beherrschen