DATENSCHUTZAKTUELL Professional
MAI | 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

FERIENJOBBER UND AUSHILFEN: GEHEN SIE DAS THEMA SCHLAU AN

Wertschätzung geht auch nach oben

Liebe Leserin, lieber Leser,

sprechen Sie mit Personalprofis dazu, was Menschen bei der Arbeit motiviert, hören Sie ganz schnell dieses Schlagwort: Wertschätzung. Und bestimmt können auch Sie bestätigen, wie gut es tut, wenn Vorgesetzte oder Kollegen Lob aussprechen oder sich über die gute Zusammenarbeit freuen.

Und weil dem so ist, sollten Sie einmal überlegen, wen Sie vielleicht schon länger nicht mehr wertgeschätzt haben. Vielleicht ist das die Unternehmensleitung. Doch auch dort gibt es nur Menschen, die sich über ein paar wertschätzende Worte freuen. Probieren Sie es aus! Das wird garantiert nicht zu Ihrem Schaden sein.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

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

Inhalt

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
www.privacyxperts.de/kontaktformular/

Bildnachweise:
Titel: Adobe Stock | Racle Fotodesign
Seite 1: Adobe Stock | Daniel Ernst

Impressum

PRIVACYXPERTS

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

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

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

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn

Satz: Deinzer Grafik, Gartow

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

Erscheinungsweise: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Ferienjobber müssen Sie in Sachen Datenschutz an die Hand nehmen.

Ferienjobber und Aushilfen: Gehen Sie das Thema schlau an

Gerade wenn viele Mitarbeiter im Unternehmen in Urlaub sind oder wenn es vorübergehend Mehrbedarf an Arbeitskräften gibt, schlägt die Stunde für Aushilfen und Ferienjobber. Etwa bei Schülern und Studenten sind die vorübergehenden Tätigkeiten gern gesehen, um den Geldbeutel aufzupolstern. Doch es gibt hier auch im Datenschutz einiges zu beachten.

Gehen Sie die Sache schlau an

Wenn Sie sich des Themas „Aushilfen, Ferienjobber und Kurzzeitbeschäftigte" annehmen wollen, sollten Sie nicht Hals über Kopf in die Materie stolpern. Damit die Sache rund wird, können Sie auf die folgenden Tipps setzen:

Tipp 1: Sprechen Sie mit der Personalabteilung

Egal, ob Aushilfe, Mini- oder Ferienjobber, spätestens wenn es zu einem Arbeitsverhältnis kommen soll, ist die Personalabteilung involviert. Daher hat sie meist auch den umfassendsten Überblick darüber, was in Ihrem Unternehmen beispielsweise für die Pfingst- oder Sommerferien an kurzfristigen Beschäftigungen angedacht ist. Außerdem können Sie so schon frühzeitig in Erfahrung bringen, welche Tätigkeiten von den Kurzzeitbeschäftigten übernommen oder in welchen Bereichen sie eingesetzt werden sollen. Dann können Sie leicht Ihre nächsten Ansprechpartner ausmachen.

Tipp 2: Klären Sie die Rahmenbedingungen in den Einsatzbereichen

Gehen Sie auf die Kollegen in den betreffenden Bereichen zu und suchen Sie den Austausch in einem ersten Gespräch. Machen Sie von vorneherein klar, dass es Ihnen nicht um das Miesmachen einer guten Sache geht. Vielmehr wollen Sie mit Ihrer Beratung unterstützen, damit es zu keinen Problemen kommt. Natürlich liegt Ihr Fokus hier in erster Linie auf dem Schutz personenbezogener Daten.

Im Gespräch mit den Kollegen lassen Sie sich alle relevanten Informationen geben, etwa dazu:

- Wie viele Aushilfen oder Ferienjobber sollen für welchen Zeitraum eingesetzt werden?
- Welche Aufgaben werden von diesen erledigt?
- Inwieweit arbeiten die betreffenden Kurzzeitbeschäftigten mit personenbezogenen Daten?
- Wie schutzwürdig sind die Daten, mit denen die betreffenden Personen in Kontakt kommen?

Im Übrigen können Sie auf die abgedruckte Checkliste setzen. Damit stellen Sie im Gespräch sicher, dass Sie keine wichtigen Aspekte vergessen oder übersehen.

Tipp 3: Machen Sie relevante Risiken aus

Auf Basis der Informationen aus dem Austausch mit den Kollegen sollten Sie sich über mögliche Gefahren und die daraus resultierenden Risiken Gedanken machen. Dazu notieren Sie sich alles, was Ihnen an Gefahren in den Sinn kommt. Typischerweise denken Sie vielleicht an folgende Gefahren:

- Personenbezogene Daten werden ausgeplaudert, sprich an Unbefugte weitergegeben.
- Kurzzeitbeschäftigte entsorgen schutzwürdige Unterlagen im normalen Papiermüll.
- Es kommt zur Datenschutzpanne, weil Kriminelle mit einer Phishing-E-Mail Erfolg haben.

Bewerten Sie, wie groß ein denkbarer Schaden wäre und wie wahrscheinlich es ist, dass es zu einem Schaden kommt. Daraus ergibt sich dann das jeweilige Risiko. Um das Risiko zu eliminieren oder auf ein niedriges Niveau zu bringen, sind dann Gegenmaßnahmen erforderlich. Diese können technischer oder organisatorischer Natur sein. So kann beispielsweise der Zugriff auf bestimmte Daten technisch ausgeschlossen werden, etwa über die restriktive Vergabe von Berechtigungen. Organisatorisch können Regeln, Arbeitsanweisungen oder auch ein Training bzw. eine gute Betreuung viel zur Risikominimierung beitragen.

Tipp 4: Vermitteln Sie nötiges Wissen

Haben Sie generelle Risiken ausgemacht, etwa dass Kurzzeitbeschäftigte Cyberkriminellen auf den Leim gehen können, kann Folgendes sinnvoll sein: Sie stellen allgemeine Empfehlungen zum richtigen Verhalten zusammen. Dann sind etwa Aushilfen in der Lage, viele Gefahren rechtzeitig zu erkennen und das Richtige zu tun.

Hilfreich ist es auch, wenn Sie beispielsweise eine Präsentation bzw. Merkblätter mit Tipps und Handlungsempfehlungen für Vorgesetzte und Ansprechpartner erstellen. Einerseits können Sie diese für die Schulung der zukünftigen Vorgesetzten und Ansprechpartner der Aushilfen nutzen. Andererseits können Sie diese Medien für deren Schulungen oder Gespräche mit den Ferienjobbern bereitstellen. So gewährleisten Sie, dass die Informationsqualität für die Ferienjobber stimmt. Nichts wird vergessen oder falsch vermittelt.

Tipp 5: Beugen Sie selbst Pleiten, Pech und Pannen vor

Auch das kann eine gute Idee sein: Starten viele Ferienjobber oder Aushilfen zu einem Zeitpunkt, können auch Sie als Datenschutzbeauftragter zu einer kurzen Informationsveranstaltung einladen. Hier können Sie nicht nur wichtige Tipps und Hinweise zum richtigen Verhalten im Hinblick auf personenbezogene Daten geben. Sie machen sich zugleich auch bekannt. Das kann wichtig sein, wenn es Fragen zum Datenschutz gibt. Und man wird sich garantiert an Sie erinnern, wenn es unter Datenschutzaspekten brenzlig wird.

CHECKLISTE: Wichtige Datenschutz-Aspekte rund um Aushilfen und Ferienjobber

Aspekt	Darauf sollten Sie achten	Besprochen und geklärt?
In welchem Umfang werden Aushilfen oder Ferienjobber eingesetzt?	› Klären Sie hier die Anzahl und den zeitlichen Umfang des Einsatzes. Ist jemand nur eine Woche im Einsatz, bleibt wenig Zeit für das Vermitteln ggf. relevanter Verhaltensregeln mit Datenschutzbezug. › Gibt es viele Aushilfen, steigt auch der Betreuungsaufwand. Der muss ggf. auf mehrere Schultern verteilt werden.	☐ Ja ☐ Nein
Welche Aufgaben sollen sie wahrnehmen?	› Entscheidend ist zunächst der Einsatzbereich. Ein Ferienjobber in der Produktion hat unter Umständen kaum mit personenbezogenen Daten zu tun. Anders sieht es aus, wenn etwa eine Aushilfe beim Einscannen von Personalakten unterstützen soll. › Aus den Aufgaben können spezifische Gefahren resultieren. Denen muss ggf. durch technische oder organisatorische Maßnahmen begegnet werden.	☐ Ja ☐ Nein
Inwieweit arbeitet der Kurzzeitbeschäftigte mit personenbezogenen Daten?	› Haken Sie hier genau nach. Allgemeine Aussagen wie „Kundendaten“ sollten Sie nicht akzeptieren. Lassen Sie sich im Detail erklären, was gemeint ist. › Bewerten Sie auch die Schutzwürdigkeit der Informationen bzw. ob es sich um Daten nach Art. 9 Abs. 1 Datenschutz-Grundverordnung handelt, die eines besonderen Schutzes bedürfen.	☐ Ja ☐ Nein
Gibt es spezifische Verarbeitungen, bei denen die Aushilfe unterstützen soll?	› Unter Umständen soll ein Ferienjobber personenbezogene Daten in ein System eingeben. Hier ist nicht nur Können, sondern auch Zuverlässigkeit gefragt. › Handelt es sich um unternehmenskritische Verarbeitungen, sollten Sie klären, inwieweit die Erledigung der Arbeiten für Aushilfen überhaupt geeignet ist.	☐ Ja ☐ Nein
Wer in der Abteilung ist für die Betreuung der Ferienjobber zuständig?	› Lassen Sie sich Namen nennen, um diese Personen beispielsweise mit Informationen versorgen zu können. › Hinterfragen Sie, inwieweit die betreffende Person auch tatsächlich für Aushilfen greifbar ist, etwa wenn es um Fragen geht.	☐ Ja ☐ Nein
Wie soll der Kurzzeitmitarbeiter für richtiges Verhalten sensibilisiert werden?	› Besprechen Sie, was man abhängig von den Aufgaben wie vermitteln will. Neben Gesprächen sind auch Merkblätter oder Abteilungsregeln denkbar. › Klären Sie, inwieweit man die Aushilfen für besondere Gefahren sensibilisiert. Kann die Aushilfe E-Mails von extern erhalten, muss sie Bescheid wissen, wie man Phishing-E-Mails erkennt und richtig reagiert.	☐ Ja ☐ Nein
Welche Berechtigungen soll die Aushilfe erhalten?	› Lassen Sie sich dieses Thema insgesamt erläutern, und zwar nicht nur im Hinblick auf den Zugriff auf Daten. Auch der Zutritt sollte auf das für die Aufgabenwahrnehmung erforderliche Maß begrenzt sein. › Achten Sie darauf, dass es individuelle Benutzerkonten gibt. Multi-User-Kennungen sollten tabu sein.	☐ Ja ☐ Nein
Mit welchen Arbeitsmitteln wird die Aushilfe bzw. der Ferienjobber ausgestattet?	› Hier kann es erforderlich sein, dass dem Ferienjobber vermittelt wird, wie Computer & Co. genutzt werden dürfen. › Je nach Ausstattung kann es besondere Risiken geben, denen begegnet werden muss. Ein Notebook sollte verschlüsselt sein.	☐ Ja ☐ Nein
Inwieweit ist ein Arbeiten aus dem Homeoffice möglich?	› Soll das möglich sein, muss der Aushilfe bzw. dem Ferienjobber einiges vermittelt werden, etwa zur sicheren Einwahl in das Firmennetzwerk. Prüfen Sie, was man dem Ferienjobber wie erklären will. › Achten Sie darauf, dass das Thema Vertraulichkeit am heimischen Arbeitsplatz nicht vergessen wird. Vieles ist nämlich nicht für die Augen und Ohren von Angehörigen oder Mitbewohnern bestimmt.	☐ Ja ☐ Nein

Genaueres Hinschauen lohnt sich bei diesen 7 Hotspots

Als Profi im Datenschutz wissen Sie: Wenn Daten verloren gehen, z. B. durch Cyberangriffe, hat das oft schlimme Folgen für Betroffene, aber auch für das datenschutzrechtlich verantwortliche Unternehmen. Um das zu verhindern, ist es wichtig, Risiken für Datenverlust oder Datendiebstahl so gut wie möglich zu verringern. Dabei gibt es Hotspots, die gerne übersehen werden.

7 Hotspots: Überprüfen Sie die gegenwärtige Lage

Passende technische und organisatorische Maßnahmen gewährleisten nicht nur Schutz und Sicherheit für personenbezogene Daten. Wichtig sind auch Regeln, Anweisungen und Prozesse. Aber oft gilt: Alles sieht gut aus, wenn man nur das Geschriebene betrachtet. Jedoch kommt es entscheidend darauf an, wie es in der Praxis umgesetzt wird.

Da bekanntlich Papier ziemlich geduldig ist, sollten Sie mit offenen Augen durchs Unternehmen gehen. Schauen Sie auch auf die Themen, die eigentlich passen müssten. Wie wäre es mit folgenden Hotspots:

Sie müssen sich nie rechtfertigen
Zwar sollen Sie bei der Wahrnehmung Ihrer Aufgaben risikoorientiert vorgehen, was Art. 39 Abs. 2 Datenschutz-Grundverordnung explizit vorsieht. Allerdings entscheiden Sie als Datenschutzbeauftragter eigenständig, wo Sie einmal genauer hinschauen und den Dingen auf den Grund gehen wollen. Hier brauchen Sie keine Erlaubnis.

ÜBERSICHT: 7 Hotspots für Ihre Prüfung

Hotspot	Das können Sie tun	In Ordnung?
Aushebeln von Sicherheitsmaßnahmen	› Prüfen Sie an Ihrem Computer, inwieweit Sie entsprechende Einstellungen selbst ändern können, etwa den Virenschutz deaktivieren. › Sprechen Sie mit der IT-Abteilung, über das Geräte-Management in Ihrem Unternehmen. So sollten Administrationsberechtigungen genauso eingeschränkt sein wie die Möglichkeit zur eigenmächtigen Installation von Software.	☐ Ja ☐ Nein
Einsatz von problematischer Technik bzw. Software	› Können Mitarbeiter selbst Software installieren, kann das nicht nur zu Lizenzproblemen führen, wenn etwa Programme nicht im kommerziellen Umfeld genutzt werden dürfen. Es bestehen auch Risiken für die Sicherheit, wenn die IT-Abteilung nicht weiß, was so installiert wird. › Besprechen Sie, inwieweit es eine Inventarisierung von Computern und Software gibt. Nur so lässt sich Handlungsbedarf erkennen, etwa bei veralteten Betriebssystemen.	☐ Ja ☐ Nein
Gefahren beim Datentransport bzw. -transfer	› Hier haben Sie vielfältige Ansatzpunkte, um Gefahren und Risiken für die Sicherheit von Daten auszumachen. Überlegen Sie, bei wem und auf welche Weise Daten von A nach B gehen. › Bei Datenträgern sollte nicht jeder alles nutzen können. Auch hier muss darauf geachtet werden, dass nur bekannte und freigegebene Datenträger genutzt werden, der Personenkreis begrenzt ist und die Sicherheit gewährleistet wird. › Verschlüsselung ist oft das Mittel der Wahl, wenn es um den Schutz vor unbefugtem Zugriff geht. Denken Sie hier an das WLAN, die Einwahlmöglichkeit ins Unternehmensnetzwerk, den Transport von Daten(trägern) oder die Eingabe von Daten auf der Webseite.	☐ Ja ☐ Nein
Nicht passende Berechtigungen	› Berechtigungen werden meist nicht komplett individuell vergeben. Vielmehr findet eine Zuordnung von Mitarbeitern zu bestimmten Rollen oder Berechtigungsgruppen statt. Hier können Sie auf Stichproben setzen und prüfen, inwieweit der Zuschnitt bzw. die Zuordnungen passen. › Orientieren Sie sich immer am „Need-to-know-Prinzip“. Hinterfragen Sie, ob der Grundsatz „Kenntnis, nur wenn erforderlich“ auch in der Praxis eingehalten wird.	☐ Ja ☐ Nein
Nutzung privater Arbeitsmittel	› Machen Sie aus, was wo für welchen Zweck zum Einsatz kommt. Denn private Geräte bergen immer Gefahren für den Datenschutz, schon allein wegen der nur eingeschränkten Beherrschbarkeit und Steuerbarkeit durch das Unternehmen. › Haben Sie ein Auge darauf, welche Regelungen im Unternehmen bestehen und inwieweit diese unter Datenschutzaspekten passen.	☐ Ja ☐ Nein
Unbedachte Weitergabe von Schützenswertem	› Halten Sie Ausschau nach Veröffentlichungen im Internet. Nicht selten finden sich dort auch Präsentationen oder andere Dokumente, die vertrauliche Informationen enthalten. Das kann auch durch Kooperationspartner passieren. Hier sollte Ihr Unternehmen alles daransetzen, dass die Informationen dort schnellstens verschwinden. › Bei Veranstaltungen sollten Sie in den Pausen einmal schauen, was an Sensiblem so alles auf den Tischen liegen bleibt. Nutzen Sie das, um direkt darauf hinzuweisen.	☐ Ja ☐ Nein
Stiefmütterliches Löschen von Daten	› Daten müssen gelöscht werden, wenn es für die Verarbeitung keine Berechtigung mehr gibt. Gerade auf Dateiablagen oder in Austauschordnern können Sie fündig werden. › Prüfen Sie, inwieweit es „vergessene“ Webseiten gibt. Ggf. sollten diese gelöscht werden.	☐ Ja ☐ Nein

Zukauf oder Verkauf von Unternehmen: Diese Punkte sollten Sie ansprechen

Zwar läuft es in Deutschland mit der Wirtschaft insgesamt gerade nicht so rund. Das muss jedoch nicht heißen, dass es allen Unternehmen schlecht geht. Insofern will Ihr Unternehmen womöglich weiter wachsen, und zwar auch durch den Zukauf eines anderen Unternehmens. Muss gespart werden, will man vielleicht einen Bereich loswerden. Beide Vorhaben sind für Sie von Interesse.

Bringen Sie in Erfahrung, was man vorhat

Will Ihr Unternehmen wachsen und in diesem Zusammenhang ein anderes Unternehmen ganz oder in Teilen aufkaufen, muss vieles bedacht werden, und zwar gerade im Datenschutz. Nicht anders ist es, wenn Ihr Unternehmen ganz oder zum Teil verkauft werden soll. Damit Sie die Sache unter datenschutzrechtlichen Aspekten prüfen können, müssen Sie über die nötigen Informationen verfügen. Erfahren Sie also, dass es eine entsprechende Absicht gibt, sollten Sie sich einklinken. Denn nur wenn Sie eingebunden sind, können Sie vor allem Ihrem gesetzlichen Beratungsauftrag aus Art. 39 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) nachkommen.

Zeigen Sie die Rahmenbedingungen auf

Klar ist für Sie als Profi im Datenschutz: Wenn personenbezogene Daten verarbeitet werden, müssen insbesondere die Vorgaben der DSGVO beachtet werden. Da wären beispielsweise die Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO), die Pflicht zur Umsetzung erforderlicher Maßnahmen (Art. 24 Abs. 1 DSGVO), die Erfüllung von Betroffenenrechten (Art. 12 ff. DSGVO) sowie die Gewährleistung der Sicherheit durch passende Schutzmaßnahmen (Art. 32 DSGVO).

Soll ein Unternehmen oder sollen Teile hiervon gekauft oder verkauft werden, kommen jedoch einige Besonderheiten hinzu, die die zuständigen Kollegen nicht übersehen dürfen. So ist es nicht automatisch zulässig, dass personenbezogene Daten, etwa von Kunden, von Unternehmen A zu Unternehmen B wandern. Vielmehr kommt es darauf an, wie man bei der entsprechenden Transaktion vorgehen will. Zeigen Sie vor allem diese beiden Konstellationen auf:

› Share Deal

Bei dieser Vorgehensweise werden die Anteile am Unternehmen an ein anderes Unternehmen übertragen. Das kaufende Unternehmen wird also Rechtsnachfolger des gekauften Unternehmens. Damit gehen alle Rechte und Pflichten über. Bleibt der ursprüngliche Verantwortliche als solcher bestehen, gibt es auch keine Änderungen bei der Zulässigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten. Anders kann die Sache aussehen, wenn das aufgekaufte Unternehmen später in das kaufende Unternehmen integriert werden soll.

› Asset Deal

Hierbei wird nicht ein Unternehmen an sich verkauft, sondern nur einzelne Wirtschaftsgüter oder Werte, die sogenannten Assets. Denken Sie beispielsweise an eine App, die von einem Unternehmen an ein anderes verkauft werden soll, und zwar mit allem Drum und Dran, eben auch mit den Kundendaten. Hier muss genau geprüft werden, inwieweit eine Übertragung der Kundendaten zulässig ist.

Machen Sie es amtlich

Share Deal und Asset Deal sind komplexe Themen. Es müssen hier viele Konstellationen bedacht werden. Doch unter Umständen müssen Sie nicht lange suchen und sich erst recht nicht den Kopf zerbrechen. Setzen Sie auf einen relativ neuen Beschluss der Datenschutzkonferenz, des Abstimmungsgremiums der deutschen Datenschutzaufsichtsbehörden. Die Ausführungen zu „Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset Deals“ finden Sie hier: https://t1p.de/8s43k.

Begleiten Sie die Kollegen und das Vorhaben

Der Verkauf oder Kauf von Unternehmen oder auch nur Teilen ist meist eine längerfristige Sache, die umfassende Planung erfordert. Für Ihre Beratung der Kollegen können Sie auf die folgende Checkliste setzen:

CHECKLISTE: Aspekte beim Kauf oder Verkauf von Unternehmen oder Teilbereichen

Relevanter Aspekt	Das können Sie in Angriff nehmen	Besprochen und in Ordnung?
ZUKAUF eines Unternehmens(teils) oder Services		
Was genau soll zugekauft werden?	› Besprechen Sie das Vorhaben so konkret, dass Sie sich etwas darunter vorstellen können. Allgemeine Aussagen helfen nicht weiter und können später zum Problem werden. › Klären Sie, inwieweit man Ihnen relevante Hintergrundinformationen zur Verfügung stellen kann, damit Sie sich mit dem Vorhaben vertraut machen können.	☐ Ja ☐ Nein
Wo ist das andere Unternehmen ansässig?	› Das ist beispielsweise von Bedeutung, um rechtliche Rahmenbedingungen ausmachen zu können, gerade im Bereich Datenschutz. › In anderen Ländern können ganz andere Rahmenbedingungen bestehen. Bei der Umsetzung von EU-Standards zum Datenschutz kann das zu erheblichem Anpassungsaufwand führen.	☐ Ja ☐ Nein

CHECKLISTE: Aspekte beim Kauf oder Verkauf von Unternehmen oder Teilbereichen

Relevanter Aspekt	Das können Sie in Angriff nehmen	Besprochen und in Ordnung?
Wie ist das andere Unternehmen organisiert?	› Lassen Sie sich Pläne und Organigramme zur Verfügung stellen. Achten Sie hier auf Aktualität und Vollständigkeit. › Aus der Struktur kann sich ablesen lassen, ob es im Datenschutz komplizierter werden kann. So z. B. bei Konzernen oder einem Unternehmen, das noch aus einem Verbund herausgelöst werden muss.	☐ Ja ☐ Nein
In welchen Ländern gibt es Niederlassungen?	› Klären Sie diese für Sie wichtige Frage. In anderen Ländern können spezifische Aspekte relevant sein, etwa zum lokalen Datenschutzrecht. › Lassen Sie sich eine Liste geben und markieren Sie sich, welche Standorte in der EU und welche außerhalb liegen. In der EU ist vieles einfacher, auch im Datenschutz.	☐ Ja ☐ Nein
In welchem Bereich ist das Unternehmen tätig?	› Die Tätigkeit kann Aufschluss darüber geben, inwieweit mit personenbezogenen Daten gearbeitet wird. › Ist man nur im Bereich Business-to-Business (B2B) tätig, heißt das nicht, dass es keine personenbezogenen Daten gibt. Gerne werden hierbei die Beschäftigten übersehen.	☐ Ja ☐ Nein
In welchem Umfang wird mit personenbezogenen Daten gearbeitet?	› Bitten Sie die Kollegen, Ihnen einen groben Überblick über die typischen Verarbeitungen zu geben. Hinterfragen Sie in diesem Zusammenhang auch, inwieweit es ein Verzeichnis von Verarbeitungstätigkeiten gibt, in das sie ggf. Einsicht nehmen können. › Klären Sie ferner, wie schutzwürdig die Daten sind und um welche Menge es sich handelt, etwa die Anzahl an Kunden und Beschäftigten.	☐ Ja ☐ Nein
Über welche Datenschutzorganisation verfügt das andere Unternehmen?	› Ist das andere Unternehmen hier schlecht aufgestellt, kann das für Ihr Unternehmen zur großen Herausforderung werden. Ggf. muss bei Adam und Eva angefangen werden. › Klären Sie, welche Regelungen zum Datenschutz bestehen und inwieweit es einen Datenschutzbeauftragten gibt.	☐ Ja ☐ Nein
VERKAUF eines Unternehmens(teils) oder Services		
Welcher Bereich, welche Produkte oder Services sollen verkauft werden?	› Bringen Sie in Erfahrung, was Ihr Unternehmen abspalten oder an ein anderes Unternehmen bzw. einen Investor verkaufen will. › Wird etwa ein Geschäftsbereich verkauft, sollten Sie frühzeitig klären, welche Standorte, Abteilungen bzw. Beschäftigte betroffen sein werden. Hier reichen auch erste grobe Informationen aus.	☐ Ja ☐ Nein
Wer steuert bei uns im Unternehmen die Abtrennung des zu verkaufenden Bereichs?	› Meist gibt es dazu ein Projektteam, weil viele relevante Ebenen zu betrachten sind. Denken Sie nicht nur an das, was verkauft werden soll. Meist sind auch andere Themen von Bedeutung, etwa Personal, IT, Patente, Steuern. › Gehen Sie mit den Kollegen in den Austausch und machen Sie deutlich, dass auch Datenschutz eine wichtige Rolle spielen dürfte.	☐ Ja ☐ Nein
Welche (Zeit-)Planung gibt es bereits?	› Das kann Ihnen Aufschluss darüber geben, wie konkret die ganze Sache schon ist. Insofern kann Ihnen das die Planung Ihrer Beratung erleichtern. › Ist die Sache schon konkreter, sollten Sie das Thema Datenschutz zügig auf die Agenda bringen.	☐ Ja ☐ Nein
Welche Systeme und Datenverarbeitungen sind betroffen?	› Egal, was verkauft wird, meist hat das Auswirkungen auf Systeme und Datenverarbeitungsverfahren. › Thematisieren Sie insbesondere Verarbeitungen personenbezogener Daten. Müssen Daten ausgelagert oder übertragen werden, muss das datenschutzkonform und sicher passieren.	☐ Ja ☐ Nein
Welche Auswirkungen gibt es auf Betroffene, z. B. Kunden?	› „Keine“ ist eine Antwort, die Sie mit den Kollegen diskutieren sollten. Werden Daten ggf. an den Käufer weitergegeben, muss hierfür eine Rechtsgrundlage gegeben sein. › Meist braucht es einiges an zeitlichem Vorlauf, um etwa die Übertragung von Daten vorzubereiten. So müssen ggf. Betroffene informiert, eine Widerspruchsfrist eingeräumt oder eine Einwilligung eingeholt werden.	☐ Ja ☐ Nein
Welche Informationen müssen Kaufinteressenten zur Verfügung gestellt werden?	› Keiner kauft gern die Katze im Sack. Insofern wird ein Kaufinteressent wissen wollen, worauf er sich einlässt. Das sollte aber möglichst ohne personenbezogene Daten passieren. › Sind personenbezogene Daten im Spiel, muss auf den Datenschutz geachtet werden. Auch muss es eine Rechtsgrundlage geben.	☐ Ja ☐ Nein
Wo sind potenzielle Käufer ansässig?	› Hier sollten Sie ein Auge auf Interessenten haben, die aus Sicht Ihres Unternehmens infrage kommen. › Werden Daten zur Verfügung gestellt, muss bei einem Interessenten aus einem Land ohne angemessenes Datenschutzniveau für dieses gesorgt werden.	☐ Ja ☐ Nein
Gibt es mit den Interessenten eine Vertraulichkeitsvereinbarung?	› Um die Vertraulichkeit zu gewährleisten, ist eine Vereinbarung unerlässlich. Klären Sie, inwieweit es ein Non-Disclosure-Agreement gibt. › Eine solche Vereinbarung ersetzt keine Vereinbarung zum Datenschutz, die ggf. bei einem Drittstaatentransfer erforderlich ist.	☐ Ja ☐ Nein

Alles in Ordnung bei Ihnen? Mit diesen Tipps sorgen Sie bei sich für Datenschutz

In Ihrem Unternehmen wird bestimmt viel mit personenbezogenen Daten gearbeitet, etwa mit Daten rund um die Beschäftigten. Natürlich muss dabei für die Einhaltung der Datenschutz-Grundverordnung und angemessenen Schutz gesorgt werden. Doch auch bei Ihnen als Datenschutzbeauftragtem gibt es viel Schützenswertes. Umso wichtiger ist, dass hier ebenfalls alles passt.

Beherzigen Sie diese einfachen Tipps

Das, was Sie anderen predigen, müssen Sie auch für sich selbst, Ihr Büro und die in Ihrer Verantwortung liegenden Daten einhalten. Um im Arbeitsalltag jederzeit einen guten Basisschutz zu gewährleisten, sollten Sie die folgenden Tipps umsetzen:

1. Tipp: Ihre Daten dürfen nicht irgendwo herumliegen

Als Datenschutzbeauftragter haben Sie viel mit sensiblen Informationen zu tun. Es ist wichtig, dass Sie Daten so ablegen, dass sie angemessen vor unbefugtem Zugriff geschützt sind. Insofern sollten Sie über eine Datenablage bzw. ein Laufwerk verfügen, auf das Sie und allenfalls einige wenige Administratoren Zugriff haben. Wenn das nicht ohnehin bereits geschehen ist, sollten Sie den Administratoren deutlich machen, dass sie allenfalls zu administrativen Zwecken auf die Dateiablage Zugriff nehmen dürfen, etwa um Berechtigungen zu vergeben und Datensicherungen durchzuführen. Kompetenzüberschreitungen können zu Ärger führen.

2. Tipp: Setzen Sie auf Verschlüsselung

Eventuell zählen Sie zu den Datenschutzbeauftragten, die alle relevanten Informationen auf der lokalen Festplatte des Computers abspeichern. Das klingt erst mal sicher. Allerdings ist es das nicht wirklich. Auch wenn man für den einfachen Zugriff Ihr Anmeldepasswort bräuchte, ist das unter Umständen nur ein schwacher Schutz. Denn ohne Verschlüsselung haben Profis leichtes Spiel. Es gibt andere Wege, beispielsweise Daten auf der Festplatte ausfindig zu machen.

Also heißt es für Sie: Daten nur dann lokal ablegen, wenn eine Verschlüsselung einen unbefugten Zugriff unmöglich macht. Dazu haben Sie meist mehrere Möglichkeiten, die Sie ggf. mit der IT-Abteilung abklären sollten. So kann etwa bei Microsoft Windows mit der bordeigenen Verschlüsselung BitLocker eine gut funktionierende Verschlüsselung der Festplatte erfolgen. Alternativ nutzen Sie eine Software zur Erstellung eines verschlüsselten Datentresors, beispielsweise die Open-Source-Software VeraCrypt. Ist ein entsprechender Datentresor erstellt, können Sie nach Eingabe des Passworts Daten sicher ablegen.

Allerdings, wo Licht ist, ist auch Schatten. Bedenken Sie stets Folgendes: Erstens: Die beste Verschlüsselung bringt wenig, wenn Sie ein schlechtes Passwort verwenden. Und zweitens: Sie sollten darauf vorbereitet sein, dass es Probleme mit der Verschlüsselung gibt. So ist die sichere Aufbewahrung des Wiederherstellungsschlüssels für die BitLocker-Verschlüsselung genauso unerlässlich wie ein Back-up der enthaltenen Daten. Das sollte natürlich auch verschlüsselt sein.

Übrigens: Gehen Sie auf Nummer sicher. Denken Sie auch ans Verschlüsseln, wenn Sie mobile Datenträger nutzen. Bitlocker und VeraCrypt funktionieren auch mit externen Festplatten und USB-Sticks sehr gut.

3. Tipp: Ihre Passwörter müssen sicher sein

Sie wissen nur zu gut: Schlechte Passwörter sind eine große Hilfe für Unbefugte und Kriminelle. Daher müssen gerade Sie auf sichere Passwörter setzen, die Sie nicht mehrfach nutzen. Doch wenn Sie komplexe Passwörter verwenden, haben Sie ein Problem wie alle normalen Menschen. Die kann sich niemand merken.

Setzen Sie daher unbedingt auf einen Passwort-Safe, der Ihre Passwörter verschlüsselt speichert. Sie müssen sich dann nur ein sicheres Passwort für Ihren Passwort-Safe merken. Außerdem praktisch: Viele Lösungen enthalten Passwortgeneratoren. Dann geht Ihnen auch das Erstellen leicht von der Hand. Denken Sie aber auch hier an ein Back-up. Denn ein Datenverlust schmerzt hier besonders.

4. Tipp: Ein Back-up muss einfach sein

Auch als Datenschutzbeauftragter haben Sie unter Umständen äußerst wichtige Unterlagen. Und Cyberkriminelle machen auch vor Ihren Daten nicht halt. Es wird einfach alles verschlüsselt, um Lösegeld zu erpressen. Und gerade besonders Sensibles ist für Cyberkriminelle interessant, weil sich damit das Lösegeld nach oben schrauben lässt. Doch auch bei einer defekten Festplatte oder einem nicht bemerkten versehentlichen Löschen von Ordnern und Dateien ist ein Back-up Gold wert. Sprechen Sie mit der IT-Abteilung, inwieweit Ihre Daten gesichert werden. Ist das nicht der Fall, sollten Sie eine entsprechende Möglichkeit einfordern. Dabei ist wichtig: Das Back-up sollte regelmäßig erstellt und an einem sicheren Ort aufbewahrt werden. Eine Verschlüsselung kann ebenfalls sinnvoll sein.

5. Tipp: Entsorgen Sie datenschutzkonform

Egal, ob Sie Ordner auf Laufwerken oder Daten auf Ihrem Computer löschen wollen: Sind diese sensibel oder schützenswert, sollten Sie dafür sorgen, dass diese sicher gelöscht werden. Am besten Sie sprechen dazu mit der IT-Abteilung. Es gibt kleine Programme, mit denen Sie auch digitale Daten sicher „schreddern“ können. Die entsprechenden Speicherbereiche werden ggf. mehrfach mit generierten Daten überschrieben. Dann ist nichts mehr wiederherstellbar. Auch bei Computerfestplatten sollten Sie auf Nummer sicher gehen. Mit geeigneten Löschprogrammen werden die Speicherbereiche ein- oder mehrfach überschrieben.

Datenschutzanforderungen aus dem Ausland: Müssen wir die beachten?

FRAGE: Unser Unternehmen expandiert, und zwar insbesondere beim Onlineshop. Dieser ist auf unserer Webseite integriert und war bislang auf Deutschland als Markt beschränkt. Noch 2025 will man für die Produkte des Unternehmens neue Märkte erschließen, beispielsweise in den Niederlanden, Österreich und Dänemark. Was kann ich auf folgende Fragen antworten: Was müssen wir in dem Zusammenhang beachten bzw. welches Recht müssen wir umsetzen? Wie steht es beispielsweise mit Cookies? Müssen wir etwa Einwilligungen auf den jeweiligen Zielmarkt zuschneiden?

ANTWORT: Hierzu sollten Sie sich zunächst die geltenden Rahmenbedingungen vor Augen führen, und zwar einerseits im Hinblick auf den Datenschutz und andererseits auf den Umgang mit Cookies.

Zum Datenschutz an sich ist zu sagen: Der ist in der EU im Wesentlichen gleich. So wurde durch die Datenschutz-Grundverordnung (DSGVO) eine Harmonisierung vorgenommen, sodass überall in der EU die gleichen Rahmenbedingungen zum Verarbeiten personenbezogener Daten gelten. Insofern hat die DSGVO auch Anwendungsvorrang vor nationalen Regelungen. Nur in wenigen Bereichen sieht die DSGVO Spielräume für die Mitgliedstaaten vor, in denen diese Regelungen zum Datenschutz treffen können. Denken Sie hier etwa an das Thema Datenschutzbeauftragter oder den Umgang mit Beschäftigtendaten. Im Ergebnis heißt das: Bezüglich Ihres Shops und des damit einhergehenden Verarbeitens personenbezogener Daten muss sich Ihr Unternehmen in erster Linie an der DSGVO orientieren.

Auch die DSGVO kann tückisch sein

Allerdings müssen Sie auch bezüglich der DSGVO-Umsetzung einiges im Hinblick auf neue Zielmärkte bedenken. So muss Ihr Unternehmen etwa die Datenschutzinformationen nach Art. 13 DSGVO in der Sprache zur Verfügung stellen, die Betroffene im Zielmarkt verstehen. Also sind verschiedene Sprachversionen unerlässlich. Nichts anderes gilt für Einwilligungen, die Ihr Unternehmen etwa als Rechtsgrundlage für die Verarbeitung personenbezogener Daten nutzen will. Hier muss der Betroffene nachvollziehen können, was mit seinen personenbezogenen Daten passiert. Das ist ihm in der Regel in der im Zielmarkt üblichen Sprache möglich.

Bei Cookies gilt nationales Recht

Beim Thema Cookies sieht die Sache anders aus. Ausgangsbasis ist die sogenannte Cookie-Richtlinie, die die Mitgliedstaaten in nationales Recht umgesetzt haben. Zwar sollte auch hier mit der ePrivacy-Verordnung eine europaweite Vereinheitlichung gelten. Doch die ePrivacy-Verordnung wird es nicht geben. Das Vorhaben wurde im Februar 2025 von der EU-Kommission beerdigt. Das hat zur Folge: Ein Unternehmen wird regelmäßig die Anforderungen zu Cookies des jeweiligen Zielmarkts umsetzen müssen. In Deutschland finden Sie die entsprechenden Vorgaben im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

In anderen Mitgliedstaaten gibt es ähnliche gesetzliche Vorschriften. Für Cookies heißt das also: Ihr Unternehmen muss diese so gestalten, dass diese für den Zielmarkt passen und den dort geltenden Anforderungen entsprechen.

Alles eine Frage des Risikos
Als Profi wissen Sie: Die DSGVO, aber auch nationale Vorschriften lassen sich vielfältig interpretieren. Kein Wunder also, dass Aufsichtsbehörden manches sehr unterschiedlich auslegen. Es besteht also ein gewisses Risiko, dass eine Aufsichtsbehörde im jeweiligen Zielmarkt bestimmte Anforderungen an die Umsetzung der einschlägigen Vorschriften macht. Nicht anders ist es mit den Gerichten. Will man also keinen Ärger riskieren, kann eine Prüfung durch Spezialisten vor Ort sinnvoll sein, etwa einen Rechtsanwalt im Zielmarkt. In Anbetracht möglicher Strafen ist das auf jeden Fall gut investiertes Geld.

Keine Ankreuzbox bei Einwilligung: Geht das so in Ordnung?

FRAGE: Ich soll eine Einwilligungserklärung auf einem Papierformular prüfen. Mir liegt ein Entwurf vor, bei dem neben dem Einwilligungstext „Ich willige ein, dass …“ kein Ankreuzfeld vorgesehen ist. Geht das so in Ordnung?

ANTWORT: Grundsätzlich reicht es aus, wenn ein Einwilligungstext durch den Betroffenen bestätigt wird, meist eben durch seine Unterschrift. Eine Box für ein Kreuz ist nicht zwingend erforderlich. Ein solches Wahlfeld kann jedoch sinnvoll sein, wenn dem Betroffenen mehrere Optionen angeboten werden. So z. B. ob eine E-Mail-Adresse an einen Lieferdienst zur Ankündigung der Lieferung weitergegeben werden darf und ob der Betroffene Werbung per Post erhalten möchte. Durch ein entsprechendes Kreuz bringt er dann seinen Willen zum Ausdruck. Wichtig zum Schluss: Kreuze dürfen nicht vorab gesetzt sein. Bei Einwilligungen ist das Aktivwerden des Betroffenen erforderlich.

Verwirrung wegen OLG-Urteils: Sind verschlüsselte E-Mails nun Pflicht?

Als Datenschützer wissen Sie: Verschlüsselung ist die Maßnahme schlechthin, wenn Sie Daten vor unbefugter Kenntnisnahme schützen wollen. Doch in der Praxis, gerade bei E-Mails, ist das Verschlüsseln noch lange nicht Standard. Und das kann für Unternehmen zum Problem werden, wie ein Urteil des Oberlandesgerichts (OLG) Schleswig-Holstein vom 18.12.2024 (Az. 12 U 9/24) zeigt.

Der Sachverhalt in Kürze

Ein Unternehmer, der spätere Kläger, erbrachte im Rahmen eines Werkvertrags Bauleistungen gegenüber einem Verbraucher, dem späteren Beklagten. Schließlich stellte der Unternehmer eine Schlussrechnung, die sich auf rund 15.000 € belief. Die Rechnung schickte er als Anhang per E-Mail an den Kunden. Was in diesem Zusammenhang genau passierte, ist unklar: Auf jeden Fall wurden die Bankdaten in der Rechnung von einem Dritten in krimineller Absicht manipuliert. Die Folge: Der Kunde zahlte durch händisch ausgefüllten Überweisungsträger den Betrag auf das von den Kriminellen angegebene Konto.

Der Unternehmer forderte von seinem Kunden weiterhin die Zahlung des Betrags von 15.000 €. Der meinte jedoch, dass er nicht zur Zahlung verpflichtet wäre, weil er für die Überweisung auf das falsche Konto nicht verantwortlich sei.

Unternehmen klagt auf Zahlung

Die Sache landete in erster Instanz beim Landgericht (LG). Das urteilte, dass nur dann eine Erfüllung der Forderung gegeben ist, wenn der zu leistende Betrag auf einem Konto des Klägers eingegangen ist. Die Manipulation der Rechnung wäre auch keine Verletzung einer vertraglichen Nebenpflicht, die der Unternehmer zu verantworten hätte. Insofern bestehe auch kein Schadensersatzanspruch für den Kunden. Nach Ansicht des LG hätte die vom Unternehmen eingesetzte Transport-Layer-Security-Verschlüsselung (TLS-Verschlüsselung) als Schutzmaßnahme für den Versand der E-Mail ausgereicht. Selbst wenn man theoretisch einen Schadensersatzanspruch beim Kunden sehen würde, müsste dieser wegen eines Mitverschuldens erheblich gekürzt werden. Der Kunde gab sich mit dieser Niederlage nicht zufrieden und zog vor das OLG. Und zwar mit Erfolg.

So entschied das OLG

Es besteht kein Anspruch des Unternehmers auf erneute Zahlung der 15.000 € gegenüber dem Kunden. Zwar führt die gutgläubige Überweisung des Kunden auf das falsche Konto nicht zur Erfüllung des Anspruchs gegenüber dem Unternehmer. Allerdings hat der Kunde gegenüber dem Unternehmen einen Schadensersatzanspruch in Höhe des überwiesenen Betrags.

Der Ersatzanspruch des Kunden ergibt sich aus Art. 82 Datenschutz-Grundverordnung (DSGVO). Hierbei handelt es sich um einen direkten deliktischen Schadensersatzanspruch mit einer Verschuldensvermutung. Allerdings kann der Verantwortliche einen Entlastungsbeweis antreten. Die Voraussetzungen des Art. 82 DSGVO sind erfüllt. Es gibt eine Verarbeitung personenbezogener Daten unter Verstoß gegen die DSGVO. Ferner liegt beim Kunden ein Schaden vor. Außerdem besteht ein Ursachenzusammenhang zwischen der rechtswidrigen Verarbeitung und dem Schaden.

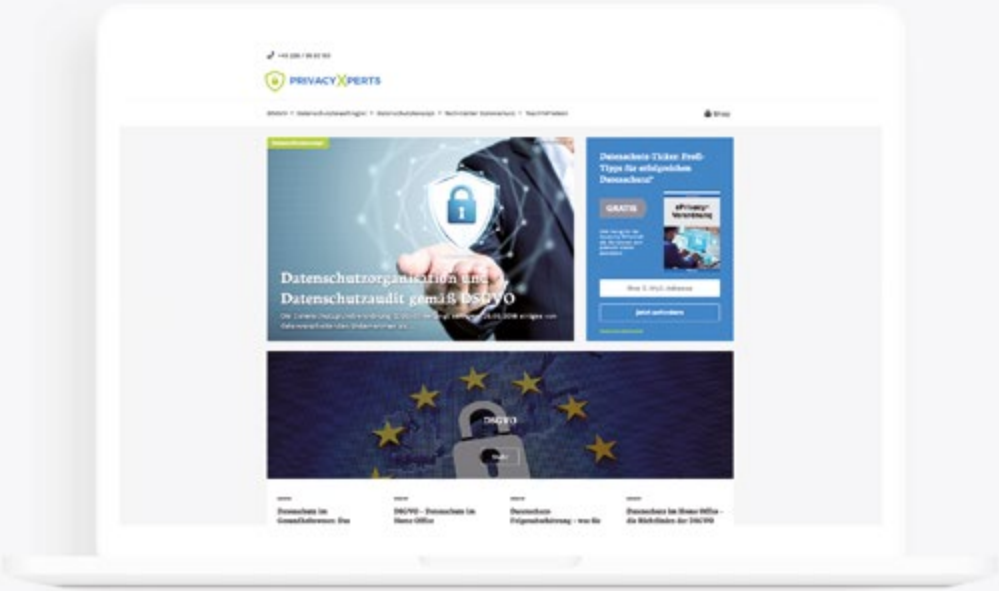
Nur Ende-zu-Ende-Verschlüsselung ist risikoangemessen

Der Verstoß gegen die DSGVO ergibt sich nicht automatisch daraus, dass Unbefugte auf Daten zugegriffen haben. Die Schutzmaßnahmen im Sinne von Art. 24 und 32 DSGVO können dennoch geeignet sein. Allerdings muss der Verantwortliche aufgrund seiner Rechenschaftspflicht nachweisen, dass die Maßnahmen geeignet waren, um den erforderlichen Schutz zu bieten. Davon war das OLG nicht überzeugt. Insbesondere hielt es eine TLS-Verschlüsselung nicht für ausreichend. Vielmehr wäre eine Ende-zu-Ende-Verschlüsselung erforderlich gewesen. Das vor allem, weil hier durch das Verfälschen der Rechnung ein hohes finanzielles Risiko bestand. Kann ein Unternehmen diesen Standard nicht umsetzen, kann es Rechnungen per Post verschicken.

So können Sie das Urteil einordnen

- Aus dem Urteil ergibt sich keine Pflicht, alle E-Mails zu verschlüsseln. Die Richter hielten im konkreten Fall die Verschlüsselung für erforderlich, weil im Zusammenhang mit der Verarbeitung personenbezogener Daten (E-Mail) die Manipulation der Bankdaten zu einem hohen Schaden geführt hat.
- Es handelt sich zwar um die Entscheidung eines Obergerichts. Allerdings können andere Ober- oder Bundesgerichte anders urteilen. Im konkreten Fall wird es aber keine Überprüfung durch den Bundesgerichtshof geben, da keine Revision eingelegt wurde.
- Manche IT-Experten und Juristen halten die Entscheidung für „verunglückt". Viele relevante Aspekte, etwa wo es genau zur Manipulation kam, wurden nicht ermittelt. Auch sprechen die Richter nur von Verschlüsselung als sichere Möglichkeit, wobei ggf. das Signieren einer E-Mail bzw. eines PDF-Anhangs die bessere Lösung wäre. Dann wäre eine Veränderung bzw. Manipulation für den Empfänger erkennbar.
- Die Entscheidung macht deutlich: Verantwortliche sind im Zweifel in der Beweispflicht, dass sie alles unternommen haben, um die DSGVO und insbesondere die Sicherheit der Verarbeitung zu gewährleisten. Können sie das nicht, geht das unter Umständen voll zu ihren Lasten.
- Ob Ihr Unternehmen nun auf Verschlüsselung beim Rechnungsversand an Verbraucher setzt, ist eine Frage des (Schadens-)Risikos.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter www.privacyxperts.de/shop

Vorschau:

Daten auf Abwegen: Das sind Ihre Optionen
Ihr Termin mit dem Chef: Das müssen Sie vorbereiten

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

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