DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
OKT 2025
Schweiz

AB IN DIE CLOUD! AUF DIESE DATENSCHUTZ-ASPEKTE SOLLTEN SIE HINWEISEN

„Die Gedanken sind (zoll-)frei“

Liebe Leserin, lieber Leser,

tagein, tagaus hört man: Zölle! Umso bedeutsamer ist in der heutigen Zeit das Zitat in der Überschrift, das etwa auch Martin Luther zugeschrieben wird. Allerdings geht die Sache wohl auf einen uralten römischen Rechtssatz zurück, wonach niemand für seine Gedanken bestraft wird.

So sollten Sie es auch bei Ihrer Arbeit als Datenschutzberater halten. Nehmen Sie niemandem seine Vorschläge oder Meinungen übel. Billigen Sie jedem das Recht freier Gedanken zu. Treten Sie diesen mit guten Argumenten gegenüber. Aber klar ist natürlich auch: Sie können dieses Recht genauso für sich selbst in Anspruch nehmen.

Viele Grüsse

Andreas Würtz,
Rechtsanwalt und Chefredaktor

Inhalt

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

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

Bildnachweise:
Titel: Adobe Stock | Gorodenkoff
Seite 1: Adobe Stock | magele-picture

Impressum

PRIVACYXPERTS

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

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

Der Datenschutz ist eine Dauerbaustelle.

Ständig den Datenschutz verbessern: Setzen Sie dafür auf diese 7 Schritte

Der Kölner Dom ist Ihnen bestimmt ein Begriff. Und bei dem ist es ähnlich wie beim Datenschutz. Ist man hinten mit den Baumassnahmen fertig, kann man vorn wieder anfangen. Auch der Datenschutz im Unternehmen ist eine Dauerbaustelle. Immer gibt es etwas neu zu planen, zu bauen, zu reparieren oder zu verbessern. Und gerade wenn Sie die Dinge verbessern wollen, sollten Sie geschickt vorgehen.

Verbessern ist immer eine gute Idee

Wenn Sie kurz darüber nachdenken, fallen Ihnen bestimmt einige Beispiele im Bereich Datenschutz ein, bei denen es in Ihrem Unternehmen nicht rundläuft. Doch warum es dabei belassen? Stellen Sie sich den Herausforderungen und machen Sie die Dinge besser. Das hilft dem Datenschutz, Ihrem Unternehmen und Ihnen. Um fortlaufend besser zu werden oder Verbesserungen zu implementieren, befolgen Sie einfach die folgenden 7 Schritte:

Schritt 1: Analysieren Sie die Istsituation

Wenn Sie die Datenschutzsituation im Unternehmen verbessern wollen, sollten Sie nicht einfach losmarschieren. Das birgt nämlich das Risiko, dass Sie in die falsche Richtung laufen, das Ziel aus den Augen verlieren oder irgendwann entnervt aufgeben. Sie müssen die Dinge von Grund auf planvoll angehen. Und hierfür ist zunächst erforderlich, dass Sie die Situation analysieren. Ermitteln Sie den Istzustand für alle relevanten Aspekte. Im Hinblick auf die Datenschutzsituation sollten Sie beispielsweise hier Licht ins Dunkel bringen:

- Bearbeitungen von Personendaten
- Datenschutzprozesse
- Regelwerke und Vorschriften
- Stakeholder (z. B. Betroffene, Themenverantwortliche, Entscheider, Führungskräfte) und deren Interessen
- bestehende Ressourcen
- externe Einflussfaktoren

Schritt 2: Ermitteln Sie den Sollzustand

Machen Sie sich zunächst Gedanken, was erreicht werden soll. So können Sie einen Idealzustand anstreben. Das ist aber unter Umständen nur erreichbar, wenn viel investiert wird, etwa auch Ihr Engagement, Ihre Zeit und Ihre Nerven. Besser ist es meist, wenn Sie zunächst auf einen guten Sollzustand hinarbeiten. Dazu prüfen Sie, was das Bundesgesetz über den Datenschutz (DSG) vorsieht. Suchen Sie beispielsweise in einem PDF einfach nach „Verantwortliche". So finden Sie schnell alle Regelungen, die an den Verantwortlichen adressiert sind, und können leicht die Pflichten ausmachen. Leiten Sie daraus ab, was nötig ist, damit es keine Probleme gibt. Denken Sie hier beispielsweise an die folgenden Aspekte:

- Umsetzung und Nachweis der Umsetzung der Grundsätze der Bearbeitung (Art. 6 DSG)
- Umsetzungsmassnahmen zur Einhaltung der DSGVO (Art. 7 Abs. 1 DSG)
- risikoangemessene Schutzmassnahmen (Art. 8 DSG)
- vollständiges und aktuelles Verzeichnis von Bearbeitungstätigkeiten (Art. 12 DSG)
- Einbindung und Unterstützung des Datenschutzberaters (Art. 10 DSG, Art. 23 Verordnung über den Datenschutz)
- geeignete Regelwerke und Prozesse

Schritt 3: Identifizieren Sie die Lücken

Das läuft neudeutsch unter dem Schlagwort „Gap-Analyse". Dabei handelt es sich einfach um den Abgleich zwischen Soll-

und Istzustand. Haben Sie die Lücken identifiziert, müssen Sie die damit in Zusammenhang stehenden Risiken ausmachen und bewerten. Das machen Sie einfach nach dem grundsätzlichen Prinzip „Schaden x Eintrittswahrscheinlichkeit = Risiko". Bewerten Sie diese Aspekte beispielsweise mit 1 für niedrig, 2 für mittel und 3 für hoch. Nach dem Multiplizieren haben Sie eine Rangfolge, was unter Risikoaspekten am ehesten angegangen werden sollte.

Übrigens: Damit Ihre späteren Aktivitäten noch zielgenauer werden und Sie Ihre Kapazitäten bestmöglich einsetzen, können Sie die Risiken auch noch priorisieren. Dazu bewerten Sie die Risiken nach Wichtigkeit und Dringlichkeit. Nutzen Sie auch hier die bekannte Bewertungssystematik: 1 für niedrig, 2 für mittel und 3 für hoch. Nach dem Multiplizieren sehen Sie direkt, was besonders wichtig und dringlich ist. Diesen Risiken sollten Sie die grösste Bedeutung beimessen und die grösste Aufmerksamkeit widmen.

Ernten Sie erst einmal die „low hanging fruits"
Bei aller Bewerterei sollten Sie eines nie aus den Augen verlieren: Manche Sachen sind mit wenig Aufwand ruckzuck erledigt. Diese „niedrig hängenden Früchte" sollten Sie als Erstes ernten. Denn damit können Sie nicht nur an manches schnell einen Haken machen. Sie haben positive Erlebnisse, die Sie auch bei den schwierigeren Dingen motivieren.

Schritt 4: Klären Sie die Ursachen

Machen Sie ausfindig, warum es Lücken zwischen Soll und Ist gibt. Ein gut geeignetes und einfaches Mittel ist hier die 5-W-Methode, wobei das W für „Warum" oder englisch „Why" steht. Fragen Sie bis zu fünfmal nach dem Warum, um den tatsächlichen Ursachen auf die Schliche zu kommen.

Hier ein Beispiel: Bei der schriftlichen Verpflichtung zum Datenschutz rutschen immer einzelne Mitarbeiter durch. **Warum** passiert das? Weil Führungskräfte das vergessen. **Warum** passiert das? Weil dies nicht in der Eintrittscheckliste enthalten ist. **Warum** passiert das? Weil die Personalabteilung sich sperrt. **Warum** sperrt sie sich? Weil sie nicht von oben angewiesen wurde. **Warum** ist das so? Weil der Geschäftsführer nichts davon weiss und vom Datenschutzberater nicht gebeten wurde.

Betreiben Sie eine möglichst umfassende und gründliche Ursachensuche. Beschränken Sie sich dabei nicht nur auf Ihr Kernthema, den Datenschutz. Lassen Sie insbesondere organisatorische, prozessuale und systembezogene Aspekte nicht aussen vor.

Schritt 5: Entwickeln Sie die erforderlichen Massnahmen

Starten Sie hier mit einem Brainstorming. Meist gibt es nämlich verschiedene Ansätze, um ein Problem zu lösen. Eventuell ist es sinnvoll, wenn Sie hier auch Kollegen anderer Bereiche einbinden, wenn es Überschneidungen gibt. Werden beispielsweise Berechtigungen ausgeschiedener Mitarbeiter zu spät entzogen, sollten Sie die IT-Abteilung und ggf. auch die Personalabteilung mit ins Boot nehmen.

Versuchen Sie zudem, die Massnahmen nachhaltig zu gestalten, damit das Problem gelöst und die Situation dauerhaft verbessert wird. Dazu können Sie auf ein bewährtes Vorgehen setzen, den PDCA-Kreislauf. Die Abkürzung steht für verschiedene Schritte eines Zyklus:

- **PLAN:** Hier geht es darum, konkrete Massnahmen und Aktivitäten festzulegen. Das kann auch Regeln und konkrete Anweisungen umfassen. Idealerweise wird auch ein Zeitplan definiert.
- **DO:** Damit ist das Machen gemeint, sprich die Umsetzung der vorgesehenen Massnahmen und Aktivitäten. Hier sollte die Umsetzung so erfolgen, wie sie geplant wurde. Manchmal wird bereits hier schnell erkennbar, dass ein „guter Ansatz" in der Realität nicht machbar ist. Anpassungen sind dann unerlässlich.
- **CHECK:** Die Umsetzung und Wirksamkeit der Massnahmen und Aktivitäten müssen geprüft werden. Meist wird hier auch erst einmal die Umsetzung im Kleinen ausprobiert, bevor sie im ganzen Unternehmen geschieht. So vermeiden Sie, dass Hindernisse, Unzulänglichkeiten oder Probleme in der Praxis übersehen werden. Zudem sind Probleme im Kleinen leichter zu managen als bei einem grossen Roll-out.
- **ACT:** Hier geht es um eine Art Qualitätscheck des ganzen Prozesses: Wurde alles so umgesetzt, dass der neue Istzustand sich mit dem Sollzustand deckt? Ist das nicht der Fall, wird der Kreislauf neu gestartet. Defizite sollten unbedingt behoben werden.

Schritt 6: Gestalten und begleiten Sie die Umsetzung

Unter Umständen haben Sie bezüglich der Umsetzung der Massnahmen oder Aktivitäten eher eine begleitende Rolle. Schliesslich liegt die Verantwortung für Umsetzungsmassnahmen im Datenschutz in aller Regel beim Verantwortlichen und in der Folge bei den Führungskräften, Abteilungen und Mitarbeitern. Doch nicht selten wird man auf Ihre Unterstützung setzen. Schliesslich kennen Sie sich am besten mit allem rund um den Datenschutz aus. Stehen Sie also mit Rat und Tat zur Seite, schlagen Sie gleich zwei Fliegen mit einer Klappe. Sie unterstützen die Kollegen, damit diesen die Umsetzung gelingt. Und zugleich sorgen Sie dafür, dass dem Datenschutz besser entsprochen wird. Das wiederum erleichtert Ihnen Ihre Arbeit als Datenschutzberater.

Schritt 7: Wiederholen Sie das Ganze regelmässig

Bedenken Sie stets: Die Zeit bleibt nicht stehen. Gerade Situationen, Rahmenbedingungen, Risiken und Herausforderungen unterliegen ständiger Veränderung. Auch zeigt die Praxis immer wieder: Was heute funktioniert und perfekt zu sein scheint, kann sich morgen schon ganz anders darstellen. Hier können veränderte Strukturen im Unternehmen oder einfach nur die Bequemlichkeit von Mitarbeitern dazu führen, dass auch gute und durchdachte Massnahmen oder Prozesse nicht mehr funktionieren. Daher: Wiederholen Sie immer wieder diese Schritte, um im Datenschutz fortlaufend besser zu werden. Am besten klappt das, wenn Sie andere Stellen hierbei einbinden.

Besserer Datenschutz durch bessere Fehlerkultur? So können Sie das schaffen

Sie kennen den Spruch: Wo gehobelt wird, da fallen Späne. Klar, dass dort, wo gearbeitet wird, auch etwas schiefgehen kann. Passiert das beim Umgang mit Personendaten, kann ein „Kann ja mal passieren" die Probleme und den Schaden noch vergrössern. Um dem vorzubeugen, ist es wichtig, eine gute Fehlerkultur zu etablieren.

Fördern Sie, dass man aus Fehlern lernt

Als Datenschutzberater können Sie sich nicht um alles kümmern. Das geht schon einfach aus Kapazitätsgründen nicht. Umso wichtiger ist, dass Sie Hilfe zur Selbsthilfe leisten. Die kann beispielsweise auch darin bestehen, dass Sie zunächst einmal den Boden für eine gute Fehlerkultur bereiten. Denn nichts ist schlimmer, als Fehler nicht auch als Chance zu sehen und die Dinge zukünftig besser zu machen. Dazu können Sie beispielsweise auf das folgende Muster setzen:

Beugen Sie Angst und Misstrauen vor
Bedenken Sie stets, dass Sie als Datenschutzberater von vielen Beschäftigten auch als Autoritätsperson wahrgenommen werden. Vielleicht misstraut auch mancher dem Umstand, dass man sich vertrauensvoll an Sie wenden kann, und zwar auch, wenn mal etwas schiefgegangen ist oder falsch gemacht wurde. Daher ist wichtig: Machen Sie bei jeder Gelegenheit deutlich, dass man sich bei Fragen, Problemen oder Pannen im Datenschutz an Sie wenden kann.

MUSTER: Info-Schreiben „Fehler haben auch etwas Gutes"

Liebe Kolleginnen und Kollegen,

Sie kennen bestimmt den Spruch „Aus Schaden wird man klug". Der mag stimmen und hier und da seine Berechtigung haben. Allerdings ist ein Schaden ein schwacher Trost, gerade im Datenschutz. Schliesslich ist ein entstandener Schaden beim falschen Umgang mit personenbezogenen Daten oft ziemlich gross. Auch das Image unseres Unternehmens kann tiefe Kratzer davontragen. Also sollten wir uns alle an Folgendem orientieren: „Aus Fehlern wird man klug." Denn dann kommt es erst gar nicht zu weiteren Schäden.

Fehler können passieren
Seien wir ehrlich: Die Geschäfts- und Arbeitswelt wird immer herausfordernder. Auch der Umgang mit Personendaten ist komplex. Selbst wenn wir uns anstrengen und grosse Sorgfalt walten lassen, kann es passieren, dass etwas nicht optimal läuft oder schiefgeht.

Fehler sind wichtig
Natürlich liegt auf der Hand: Jeder Fehler im Umgang mit Personendaten ist ärgerlich. Doch die damit gemachte Erfahrung bietet zugleich die Chance, die Dinge in Zukunft besser zu machen. Manche Entwicklung hätte es nicht gegeben, wenn nicht etwas schiefgegangen wäre. Denken Sie nur an die gelben Klebezettel, die heutzutage in jedem Büro zu finden sind.

Helfen Sie, die Dinge besser zu machen
Sehen Sie beispielsweise, dass jemand Unterlagen mit schützenswertem Inhalt falsch entsorgt, sollten Sie nicht einfach wegschauen. Sprechen Sie den Kollegen an. Dabei ist wichtig: Schuldzuweisungen sind meist fehl am Platz. Fragen Sie lieber, ob sich der Kollege sicher ist, die richtige Vorgehensweise gewählt zu haben. Teilen Sie Ihre Sicht der Dinge. Erläutern Sie Ihre Einschätzung und geben Sie so Hilfestellung, das eigene Handeln zu überdenken.

Ausserdem ist wichtig: Sprechen Sie Fehler im Kollegenkreis oder in der Abteilung offen an. Dabei müssen Sie niemanden an den Pranger stellen. Wichtig ist vielmehr, dass alle über die Situation, das Problem und die passende Lösung informiert sind und sich dazu austauschen. Setzen Sie beispielsweise in der Diskussion auf ein „Ich habe kürzlich bemerkt, dass Unterlagen falsch entsorgt wurden. Das sollte vermieden werden, indem wir …".

Ihr Beitrag ist entscheidend
Gehen Sie offen mit Problemen und Fehlern um, leisten Sie Grosses: Sie tragen dazu bei, eine positive Fehlerkultur zu etablieren. Dabei ist klar: Werden Probleme oder Fehler frühzeitig erkannt, können sie auch schnell angegangen werden. Zugleich tragen Ihr Wissen und Ihre Erfahrungen dazu bei, dass sich Fehler nicht wiederholen. Und davon profitieren alle: das Unternehmen, die Beschäftigten und diejenigen, die uns ihre Daten anvertrauen.

Mein Versprechen an Sie
Auch mir als Datenschutzberater ist an einer guten Fehlerkultur gelegen. Es ist mir wichtig, dass alle mit Fehlern offen umgehen, gerade im Hinblick auf den Umgang mit Personendaten. Brauchen Sie Unterstützung oder Rat? Melden Sie sich bei mir. Haben Sie etwas falsch gemacht oder läuft etwas im Unternehmen schief? Lassen Sie uns darüber reden. Dabei ist klar: Vertraulichkeit ist bei mir garantiert.

Ihr Datenschutzberater

Sepp Tember

Ab in die Cloud! Auf diese Datenschutzaspekte sollten Sie hinweisen

Schon seit Jahren gibt es bei der Bearbeitung von Daten einen Trend: Viele Unternehmen machen immer weniger selbst und verlagern Bearbeitungen zu Dienstleistern ins Internet bzw. in die Cloud. Auf die Schnelle lassen sich hohe Kosten für die Beschaffung und den Betrieb von IT, Servern & Co. reduzieren. Doch wie so oft gilt auch hier: Wo Licht ist, da ist auch Schatten.

Sie sind gefragt

Für Sie als Datenschutzberater ist klar: Sind Personendaten im Spiel, muss so manches bedacht werden, gerade an Vorgaben aus dem Bundesgesetz über den Datenschutz (DSG). Das gilt besonders, wenn Datenbearbeitungen ausserhalb des Unternehmens stattfinden sollen, etwa bei einem Dienstleister oder in der Cloud. Relevant sind immer die folgenden Aspekte:

- Grundsätze der Bearbeitung (Art. 6 DSG).
- Sicherheit der Bearbeitung (Art. 8 DSG)
- Betroffenenrechte (Art. 25 ff. DSG)
- vertragliche Regelung der Datenbearbeitung (z. B. nach Art. 9 DSG)
- angemessenes Datenschutzniveau bei Drittlandsbezug (Artt. 14 bis 18 DSG)

Es gibt keine Automatismen

Soll eine bereits bestehende Bearbeitung bzw. die der Bearbeitung zugrunde liegende Technik an einen Dienstleister oder zu einem Anbieter in die Cloud ausgelagert werden, heisst das nicht, dass unter Datenschutzaspekten alles in Butter ist. Gerade wenn man meint, dass doch alles schon einmal geprüft wurde und im grünen Bereich wäre, müssen Sie die Hand heben. Machen Sie klar, dass eine zulässige Bearbeitung vor Ort im Unternehmen zwar datenschutzrechtlich in Ordnung sein kann. Dieselbe Bearbeitung kann jedoch ganz anderen Anforderungen unterliegen, wenn sie durch einen Dienstleister ausgeführt oder in die Cloud verlagert wird. Zudem muss vieles neu bewertet werden, etwa die möglichen Risiken. Damit Sie keinen wichtigen Aspekt übersehen, können Sie für Ihre Besprechung die folgende Checkliste verwenden:

CHECKLISTE: Datenschutzaspekte bei Clouddiensten

Aspekt	Hintergrund	Geprüft und in Ordnung?
Wie stellt sich der Gesamtprozess der Datenbearbeitung dar?	› Sie brauchen ein umfassendes Bild der Bearbeitung von Personendaten. Lassen Sie sich die Sache im Detail erklären und fordern Sie Konzepte, Übersichten und Diagramme an. › Klären Sie auch das Drumherum im Unternehmen, etwa Verantwortlichkeiten oder Entscheidungsträger bezüglich des Vorgehens. Manchmal ist es auch wichtig, den „Sponsor" zu kennen, weil oftmals hier die letzte Entscheidungsinstanz zu finden ist. › Prüfen Sie auch, inwieweit es tatsächlich um Personendaten geht.	☐ Ja ☐ Nein
Was hat man mit den Personendaten bzw. mit der Bearbeitung vor?	› Hinterfragen Sie die Motivation, warum man etwas an einer Bearbeitung ändern möchte oder warum diese bei einem Dienstleister oder in der Cloud stattfinden soll. › Orientieren Sie sich unter Datenschutzaspekten immer an dieser grundsätzlichen Frage: Wer will welche Personendaten zu welchem Zweck wie und wo bearbeiten? › Besprechen Sie auch das Thema Rechtsgrundlage. Hierzu müssen Sie wissen, was man konkret vorhat. Bei einer „normalen" Auftragsbearbeitung bedarf es keiner weiteren Rechtsgrundlage. Die Sache kann anders aussehen, wenn der Auftragsbearbeiter auch eigene Zwecke verfolgt, etwa ein KI-Training mit Kundendaten.	☐ Ja ☐ Nein
Wer ist heute daran beteiligt und wer soll es zukünftig sein?	› Lassen Sie sich am besten alle beteiligten Stellen im Unternehmen nennen. Meist ist das eben nicht nur die IT-Abteilung. › Durch eine Verlagerung zu einem Auftragsbearbeiter oder in die Cloud können sich die Beteiligten gegenüber der heutigen Situation ändern. Klären Sie, inwieweit das der Fall ist.	☐ Ja ☐ Nein
Welche datenschutzrechtliche Rolle haben die jeweiligen Beteiligten?	› Identifizieren Sie mit den Kollegen, wer welche Funktion oder Rolle bei einer Bearbeitung übernimmt. › Bedenken Sie auch: Geht es um eine Bearbeitung im Konzern, ist das wegen dieses „Konstrukts" nicht automatisch zulässig. Auch hier müssen die jeweiligen Rollen geprüft und die sich daraus ergebenden Verantwortlichkeiten bewertet werden.	☐ Ja ☐ Nein
Wo sind die Beteiligten ansässig und welchem Recht unterliegen sie?	› Lassen Sie sich genau nennen, mit wem Ihr Unternehmen zusammenarbeiten will. › Der Sitz und das relevante Recht können von Bedeutung sein, wenn der Dienstleister bzw. Anbieter in einem Drittstaat ohne anerkanntes Datenschutzniveau ansässig ist. Ggf. muss hier aufwendig für ein angemessenes Datenschutzniveau gesorgt werden. Das kann manchen Anbieter schnell weniger interessant werden lassen.	☐ Ja ☐ Nein

CHECKLISTE: Datenschutzaspekte bei Clouddiensten		
Wo findet die Bearbeitung der Personendaten statt?	› Der Ort der Bearbeitung kann von erheblicher Bedeutung sein. Denn das muss nicht automatisch der Hauptsitz des Dienstleisters oder Anbieters sein. Eventuell findet die Bearbeitung in der EU statt, obwohl der Anbieter ausserhalb der EU ansässig ist. › Hinterfragen Sie, ob tatsächlich die ganze Bearbeitung an einem Standort stattfindet. Ggf. kommen Subdienstleister zum Einsatz, die wiederum anderswo ansässig sein können. Das kann die Sache unter Datenschutzaspekten schwierig machen.	☐ Ja ☐ Nein
Welche Dienstleister oder Anbieter kommen in Betracht?	› Gerade im Zusammenhang mit der Auftragsbearbeitung muss Ihr Unternehmen beachten: Der Billigste ist nicht immer der Beste. › Klären Sie, welche Dienstleister in Betracht gezogen wurden.	☐ Ja ☐ Nein
Warum ist der ausgewählte Dienstleister bzw. Anbieter im Datenschutz als fähig und zuverlässig anzusehen?	› Das zielt darauf ab, dass Art. 9 DSG Ihrem Unternehmen auferlegt, nur mit qualifizierten Auftragsbearbeitern zu arbeiten. Die müssen hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Datensicherheit gewährleistet ist. › Fordern Sie entsprechende Bewertungen ein. Gibt es diese nicht, sollten diese erstellt werden. Schliesslich ist aufgrund der bestehenden Rechenschaftspflicht eine Nachweisbarkeit unerlässlich.	☐ Ja ☐ Nein
Wie steht es um die Sicherheit der Bearbeitung bzw. der Daten?	› Lassen Sie sich die Massnahmen des Dienstleisters bzw. des Anbieters erläutern. › Fordern Sie Datenschutzkonzepte oder Zertifizierungen an. Prüfen Sie bei Zertifizierungen, was konkret zertifiziert wurde, wer zertifiziert hat und ob die Zertifizierung noch gültig ist. › Denken Sie auch an den Schutz drum herum. So z. B. für die Frage, wie die Daten zum Dienstleister kommen und wie Daten abgesichert werden, etwa durch ein Back-up.	☐ Ja ☐ Nein
Gibt es ein Datenschutzniveau, das für unsere Bearbeitung angemessen ist?	› Die (Standard-)Schutzmassnahmen des Dienstleisters bzw. des Anbieters können auf dem Papier super klingen. Doch sie müssen ganz konkret zur Schutzwürdigkeit und zum Schutzbedarf Ihres Unternehmens und dessen Bearbeitung passen. › Die Risikoanalyse Ihres Unternehmens muss Massstab für die Bewertung sein. Aussagen aus „Hochglanzbroschüren“ helfen nicht. Ihr Unternehmen ist und bleibt für die Bearbeitung verantwortlich.	☐ Ja ☐ Nein
Sind kritische oder problematische Subdienstleister im Einsatz?	› Gibt es diese angeblich nicht, sollten Sie genauer hinschauen. Meist können Dienstleister oder Anbieter die angebotene Leistung nicht ohne weitere Dienstleister erbringen. Haken Sie bezüglich einer Liste nach. Intransparenz kann zum grossen Problem werden. › Gerade bei Subdienstleistern sollte auch unter dem Aspekt „Konkurrenz“ genau geprüft werden. Ein Konkurrent hätte ggf. Einblick in die Geschäftstätigkeit Ihres Unternehmens, selbst wenn Daten nicht vereinbarungswidrig bearbeitet werden.	☐ Ja ☐ Nein
Wie wird der Datenschutz vertraglich geregelt?	› Klären Sie, inwieweit es eine Vereinbarung geben soll und ob etwas verhandelbar ist. Läuft die Sache nach dem Motto „Friss oder stirb“ und kann Ihr Unternehmen nicht mitreden, sollten die entsprechenden Risiken bewertet werden. › Prüfen Sie, inwieweit die Vereinbarung zu den tatsächlichen Rollen der Beteiligten passt. Wird die falsche Vereinbarung geschlossen, kann Ärger vorprogrammiert sein, etwa auch mit der Datenschutzaufsicht. › Achten Sie auch auf das vereinbarte Recht. Zwar wird die Anwendung des DSG meist kein Thema sein. Anders kann es für die sonstigen Rahmenbedingungen aussehen.	☐ Ja ☐ Nein
Was passiert, wenn der Dienstleister oder die Cloud ausfällt?	› Hier sollten Sie das Thema „Business Continuity Management“ hinterfragen. Besprechen Sie, wie sichergestellt wird, dass man auch bei Problemen oder dem Ausfall des Dienstleisters bzw. Anbieters weiterarbeiten kann. Gibt es keine Überlegungen, kann das die Existenz des Unternehmens bedrohen. › Klären Sie zudem, auf welche Zwischen- und Notfälle man sich vorbereitet. Auch eine ausgefallene Internetverbindung kann zum Problem werden, wenn der Dienstleister oder Anbieter nicht mehr erreichbar ist.	☐ Ja ☐ Nein
Können wir schnell und unproblematisch Betroffenenrechte erfüllen?	› Ist Ihr Unternehmen Verantwortlicher, muss es den entsprechenden Verpflichtungen nachkommen können, und zwar grundsätzlich unverzüglich. Dabei muss ggf. auch der Dienstleister oder Anbieter unterstützen. Macht er das nicht, kann Ihr Unternehmen seine Pflichten nicht erfüllen. Ärger ist dann vorprogrammiert. › Haben Sie auch ein Auge auf den Umfang und eventuelle Kosten einer Unterstützung durch den Dienstleister. Ggf. können hier im Vertrag erhebliche Risiken lauern.	☐ Ja ☐ Nein
Wie soll die Einhaltung der Datenschutzstandards beim Dienstleister bzw. Anbieter überwacht werden?	› Wie detailliert man prüft, hängt insbesondere von der Schutzwürdigkeit der Daten ab. Ggf. reichen Zusicherungen aus. Unter Umständen ist jedoch eine Überprüfung der Schutzmassnahmen vor Ort unerlässlich. › Lassen Sie sich die entsprechenden Planungen für Prüfungen vorlegen. Dabei muss den Risiken angemessen Rechnung getragen werden.	☐ Ja ☐ Nein

Personendaten für den externen Auditor? Das können Sie empfehlen

Sie kennen den Spruch bestimmt: „Vertrauen ist gut, Kontrolle ist besser." Manchmal liegt deshalb ein Datenschutz-Audit an. Es ist für Unternehmen ein wichtigster Schritt, um die Einhaltung aller gesetzlichen Anforderungen zu überprüfen. Steht ein externes Audit ins Haus, müssen meist auch viele Informationen fliessen. Das kann auch ein Thema für Sie als Datenschützer sein. Besonders sensibel sind dabei Mitarbeiterdaten, die nicht in vollem Umfang preisgegeben werden dürfen. Hier sollten Sie immer beachten, in welchem Umfang und ob überhaupt eine Offenlegung notwendig ist. Sie sollten die Daten der Betroffenen schützen und zugleich die Anforderungen des Audits erfüllen.

Stellen Sie sich Folgendes vor:
Ihr Unternehmen wird von einer externen Prüfungsgesellschaft hinsichtlich der Umsetzung von mit einem anderen Unternehmen vereinbarten Qualitätsstandards geprüft. Dabei soll nicht nur das Qualitätsmanagement an sich unter die Lupe genommen werden; auch die Qualifikation der in diesem Bereich tätigen Beschäftigten wird hinterfragt. In einem Vorgespräch mit den Prüfern hat das Auditteam Ihres Unternehmens erfahren, dass man sich auch Arbeitsverträge, Stellenbeschreibungen und Qualifikationsnachweise ansehen will. Dazu sollen vorab entsprechende Unterlagen an die Prüfer geschickt werden. Ihre Kollegen wenden sich an Sie. Man ist sich unsicher, inwieweit das überhaupt mit dem Datenschutz vereinbar ist. Sie sollen Tipps geben, worauf man achten und wie man weiter vorgehen sollte.

So können Sie die Sache angehen

Am besten ist es, wenn Sie die Kollegen zu einem Termin einladen. Im Gespräch lassen sich viele Aspekte besser erörtern. Sie können Verständnisfragen stellen und auch die Kollegen können direkt nachhaken, falls ihnen etwas unklar bleibt. Erwähnen Sie beispielsweise die folgenden wichtigen Aspekte:

Die Rahmenbedingungen müssen geklärt werden

Entscheidend ist zunächst, dass die Kollegen möglichst gut Bescheid wissen. Wenn noch nicht geklärt, dann müssen beispielsweise das Auditziel und der Auditfokus ausgemacht werden. Dies ist dann meist auch der Zweck, der für eine Bearbeitung von Personendaten von besonderer Bedeutung ist. Daran bemisst sich, ob eine Bearbeitung von Personendaten rechtmässig und erforderlich ist.

In Erfahrung gebracht werden sollte auch, was konkret geprüft wird und welcher Nachweis von Ihrem Unternehmen gefordert wird. Hier sollte möglichst konkret nachgefragt werden. Werden etwa Arbeitsverträge gefordert, kann ggf. ein Muster ausreichen. Sollen abgeschlossene Verträge oder Qualifikationsnachweise (z. B. Zeugnisse) von Beschäftigten vorgelegt werden, ist die Frage entscheidend, welche Bestandteile dieser Unterlagen nicht benötigt werden. Diese brauchen dann auch nicht geliefert bzw. können entsprechend geschwärzt werden.

Anonymisierung ist das Mittel der Wahl

Ggf. reichen anonyme Nachweise aus. Das ist insofern eine tolle Sache, weil dann das Bundesgesetz für den Datenschutz (DSG) nicht greift. Eine Weitergabe anonymer Informationen ist unbedenklich. Aber: Es muss ausgeschlossen sein, dass der Auditor den Personenbezug herstellen kann. Insofern können auch pseudonyme Daten für den Auditor wie anonyme Daten wirken.

Kann er im Gegensatz zu Ihrem Unternehmen keine Zuordnung der Daten zu einer Person vornehmen, sind für ihn die Daten faktisch anonym. Das kann sich etwa günstig auf die Bewertung der Zulässigkeit einer Datenübermittlung auswirken.

Eine Rechtsgrundlage ist unerlässlich

Sollen Personendaten weitergegeben werden, muss es hierfür eine Erlaubnis geben. Manchmal lässt sich die Weitergabe von Personendaten auf eine gesetzliche Pflicht stützen. Oft wird damit jedoch ein berechtigtes Interesse verfolgt. Dieses Interesse muss dann die Interessen der Betroffenen überwiegen (Art. 31 Abs. 1 DSG).

Ausserdem ist wichtig: Liegt eine Bearbeitung für einen anderen als den ursprünglichen Zweck vor (beispielsweise der Auditor fordert die Vorlage eines Arbeitsvertrags oder von Qualifikationsnachweisen), muss das mit Art. 6 Abs. 3 DSG vereinbar sein. Der Zweckbindungsgrundsatz ist verletzt, wenn die betroffene Person dies berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann.

Die Grundsätze der Bearbeitung müssen beachtet werden

Legen Sie hier den Schwerpunkt auf das Grundprinzip der Verhältnismässigkeit (Art. 6 Abs. 2 DSG). Folgende Frage, die sich am Need-to.know-Prinzip orientiert, bringt den Verhältnismässigkeitsgrundsatz auf den Punkt: Ist diese Information für das verfolgte Ziel wirklich erforderlich?

Im Übrigen sollten auch für einen Prüfer vor Ort Zutritts- und Zugriffsrechte auf das erforderliche Mass beschränkt sein.

Bei Sensiblem: unbedingt das Vieraugenprinzip umsetzen

Auch bei Personendaten gibt es viel Sensibles. Bevor hiervon etwas weitergegeben wird, sollten die kompetenten Personen die Sache bewerten. Bei Personendaten sollte man Sie als Datenschutzberaer einbinden. So lässt sich leichter sicherstellen, dass Rechtsgrundlage, Datenumfang und Datensicherheit gewährleistet sind. Auch wird vermieden, dass andere relevante Aspekte übersehen werden, etwa das Schaffen der nötigen Transparenz.

Wie nutze ich das Schulungsbudget für 2025 jetzt noch am effizientesten?

FRAGE: Als Datenschutzberater habe ich vom neuen Geschäftsführer kurzfristig für 2025 noch ein Qualifizierungsbudget von 3.500 Franken bekommen. Im Gegensatz zu früher kann ich vollkommen selbst entscheiden, wie ich das Budget für meine fachliche Qualifikation einsetze. Zuerst kam mir der Gedanke, dass ich an einer Tagung oder einer Zertifizierung für Datenschutzbeauftragte teilnehme. Dann jedoch hatte ich die Idee, dass ich das Geld doch lieber in Fachliteratur, etwa neue Fachbücher, weitere Fachzeitschriften oder Gesetzeskommentare, investieren könnte. Was meinen Sie: Was fange ich am besten mit dem Geld an?

ANTWORT: Zunächst dürfte wichtig sein, dass Sie noch einige Rahmenbedingungen klären. Denn diese können entscheidend sein, wie Sie das zur Verfügung stehende Geld einsetzen. Denken Sie beispielsweise an Folgendes:

- Klären Sie, inwieweit das für 2025 vorgesehene Budget eine einmalige Sache ist. Gibt es im nächsten Jahr kein Budget, kann das Ihre Entscheidung erheblich beeinflussen. Bringen Sie in Erfahrung, ob nicht genutztes Budget ins nächste Jahr übertragen werden kann.
- Auch sollten Sie in Erfahrung bringen, was Sie alles aus dem Qualifizierungsbudget finanzieren dürfen. Eventuell ist es tatsächlich nur für Fachveranstaltungen gedacht. Dann wäre etwa Fachliteratur nicht umfasst. Auch ein Training zu Soft Skills, etwa zur Arbeitsorganisation oder zum Zeitmanagement, wäre dann nicht drin.
- Im Hinblick auf Fachliteratur sollten Sie klären, inwieweit es hierfür ein spezielles Budget gibt. Können Sie das auf andere Weise finanzieren, bleibt Ihnen das ganze Budget für die fachliche Weiterbildung.

Entscheidende Frage: Was bringt Ihnen am meisten?

Haben Sie die Rahmenbedingungen geklärt, sollten Sie Folgendes machen: Bewerten Sie für sich, was für Sie und Ihre Arbeit den grössten Mehrwert bringt. Wollen Sie sich mit anderen Datenschutzberatern austauschen, kann eine Fachtagung sinnvoll sein. Unter Umständen ist hier Ihr Budget jedoch sehr schnell aufgebraucht. Schliesslich kostet nicht nur die Veranstaltung Geld. Sie müssen auch an die Anreise und Ihre Übernachtung denken. Wollen Sie hier sparen, können Sie an vielen Stellschrauben drehen. So können Sie eine kostengünstige Veranstaltung besuchen oder bei einem Datenschutzverband oder einer Aufsichtsbehörde eine kostenfreie Veranstaltung besuchen. Eventuell reicht Ihnen auch eine virtuelle Teilnahme aus, wenn es Ihnen um fachliche Informationen geht. Dann können Sie sich die Reise- und Übernachtungskosten sparen.

Auch das Kombinieren verschiedener Bedarfe können Sie in Erwägung ziehen. Sparen Sie bei der Veranstaltung, haben Sie unter Umständen mehr Budget für Fachliteratur. Die kann gerade dann sinnvoll sein, wenn Sie komplexere Sachverhalte bewerten müssen. Denn Antworten auf ganz spezielle Fragen finden Sie oft eher in Fachliteratur, Gesetzeskommentaren oder Fachzeitschriften.

Nicht zuletzt sollten Sie überlegen, was Ihnen persönlich etwas bringt bzw. was Ihnen das Arbeitsleben leichter macht. Unter Umständen bringt Ihnen ein Sprachkurs, bei dem Sie Ihr sprachliches Ausdrucksvermögen in einer Fremdsprache verbessern, mehr als eine Veranstaltung zum Datenschutz, bei der die Themen für Sie bzw. Ihre Arbeit nur von geringer Bedeutung sind.

Mehrere Datenschutzberater in der Unternehmensgruppe: Ist das zulässig?

FRAGE: Ich bin Datenschutzberater in einem Unternehmen, bei dem einige Teile ab 2026 in mehrere rechtlich selbstständige Unternehmen ausgegliedert werden. Alle Unternehmen sollen dann eine Unternehmensgruppe bilden. In den neuen Unternehmen soll es einen Datenschutzberater geben. Wie ich gehört habe, soll das ggf. nicht ich sein. Daher meine Frage: Ist das zulässig? Kann ich die Ernennung irgendwie erzwingen?

ANTWORT: Art. 10 Abs. 1 Bundesgesetz über den Datenschutz sieht vor, dass ein Datenschutzberater oder eine Datenschutzberaterin ernannt werden kann. Demzufolge können Sie nichts erzwingen.

Wollen Sie erreichen, dass Sie für alle Unternehmen benannt werden, bedarf es hier unter Umständen einer Entscheidung der Leitung der Unternehmensgruppe. Und hier müssen Sie vielleicht Überzeugungsarbeit leisten. Ein gemeinsamer Datenschutzberater kann diverse Vorteile bringen.

Diese Vorteile hat die gemeinsame Sache

So z. B., dass innerhalb der Unternehmensgruppe im Datenschutz eine einheitliche Linie verfolgt wird, etwa in Sachen Beratung oder Kontrollen. Auch kann das Kosten sparen, da mehrere Datenschutzberater ggf. zu höheren Ausgaben führen. Das betrifft nicht nur das Gehalt, sondern auch die Kosten für Aus- und Weiterbildung. Ausserdem gibt es kein Hin und Her, wenn mehrere Datenschutzberater unterschiedlicher Meinung sind.

BGH zu negativer Bewertung: Portal muss Bewertenden nicht offenbaren

Wenn sich die Wege von Unternehmen und Mitarbeitern trennen, passiert das nicht immer im Guten. Gerade wenn Mitarbeiter unzufrieden sind, machen sie vielleicht in entsprechenden Bewertungsportalen ihrem Ärger Luft. Kein Wunder, dass mancher Arbeitgeber ein Problem mit der aus seiner Sicht unzutreffenden Bewertung hat. Doch muss ein solches Portal dann offenlegen, wer eine Negativbewertung vorgenommen hat? Der Bundesgerichtshof (BGH), das höchste deutsche Zivilgericht, meint, es kommt auf den Einzelfall an (BGH, Beschluss vom 11.3.2025, Az. VI ZB 79/23).

Das führte zum Rechtsstreit

Eine Rechtsanwaltskanzlei stritt vor Gericht wegen einer aus ihrer Sicht negativen Arbeitgeberbewertung mit dem Betreiber des Portals. Dort hatte ein Nutzer die Kanzlei als Arbeitgeber bewertet, womit diese nicht gut wegkam. So bewertete der Nutzer den Aspekt „Vorgesetztenverhalten" mit nur einem Stern. Daneben beschrieb er das Verhalten des Managements gegenüber aktiven Mitarbeitern, etwa dass diese durch Abwesenheit glänzten und die Angestellten anhielten, schnell so viel Geld wie möglich zu machen. Dann gab es noch eine für den Rechtsstreit besonders relevante Aussage. So äusserte der Nutzer, dass er es als Krönung ansehe, dass ausgeschiedene Mitarbeiter ausstehendes Gehalt bzw. die Erteilung von Arbeitszeugnissen gerichtlich durchsetzen müssten. Tatsächlich gab es jedoch nur einen ehemaligen Mitarbeiter, bei dem dies zutraf.

Kanzlei will Auskunft zum Nutzer

Die bewertete Kanzlei erfuhr von der negativen Beurteilung als Arbeitgeber. Allerdings wollte die Kanzlei diese Bewertung nicht hinnehmen. Aus ihrer Sicht gab es unwahre Behauptungen. Es hätte gerade keine Vielzahl von ehemaligen Mitarbeitern gegeben, die ihre Ansprüche einklagten. Also wollte die Kanzlei vom Betreiber des Portals Auskunft über den Nutzer, der die betreffende Bewertung verfasst hatte. Diesem Offenlegungsanspruch nach § 21 Abs. 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) kam der Betreiber des Portals jedoch nicht nach. Also klagte die Kanzlei zunächst vor dem Landgericht. Als das Gericht den Anspruch ablehnte, zog man vor das Oberlandesgericht. Doch auch hier blieb der Erfolg aus. Also setzte die Kanzlei bezüglich des Auskunftsanspruchs auf eine Rechtsbeschwerde vor dem BGH. Aber auch dort blieb der Kanzlei der Sieg verwehrt.

So urteilte der BGH

Nach Ansicht der Richter ist das Portal nicht verpflichtet, eine Auskunft über die Bestandsdaten des Nutzers der betreffenden Bewertung zu erteilen. Die Voraussetzungen des § 21 Abs. 2 TDDDG liegen nicht vor.

Ein Auskunftsanspruch gegenüber dem Anbieter eines digitalen Dienstes besteht, wenn dies erforderlich ist, um zivilrechtliche Ansprüche durchzusetzen. Hierbei müssen die Inhalte etwa den Tatbestand der Beleidigung, der üblen Nachrede oder der Verleumdung nach §§ 185 bis 187 Strafgesetzbuch (StGB) erfüllen. An einem solchen rechtswidrigen Inhalt im Sinne von § 21 Abs. 2 TDDDG fehlt es jedoch.

Äusserung ist zulässige Meinung

Die Äusserung ist nicht als Tatsachenbehauptung einzuordnen, sondern als Werturteil. Für Tatsachenbehauptungen ist wesentlich, dass sich deren Richtigkeit beweisen lässt. Bei Werturteilen steht jedoch das Stellungnehmen oder Dafürhalten im Vordergrund, sodass sich diese nicht als wahr oder unwahr einstufen lassen. Bei einer Äusserung können sich Tatsachenbehauptung und Werturteil vermengen. Steht hier das Wertende oder Meinen im Vordergrund, ist die Äusserung vom Grundrecht auf freie Meinungsäusserung aus Art. 5 Abs. 1 Satz 1 Grundgesetz geschützt.

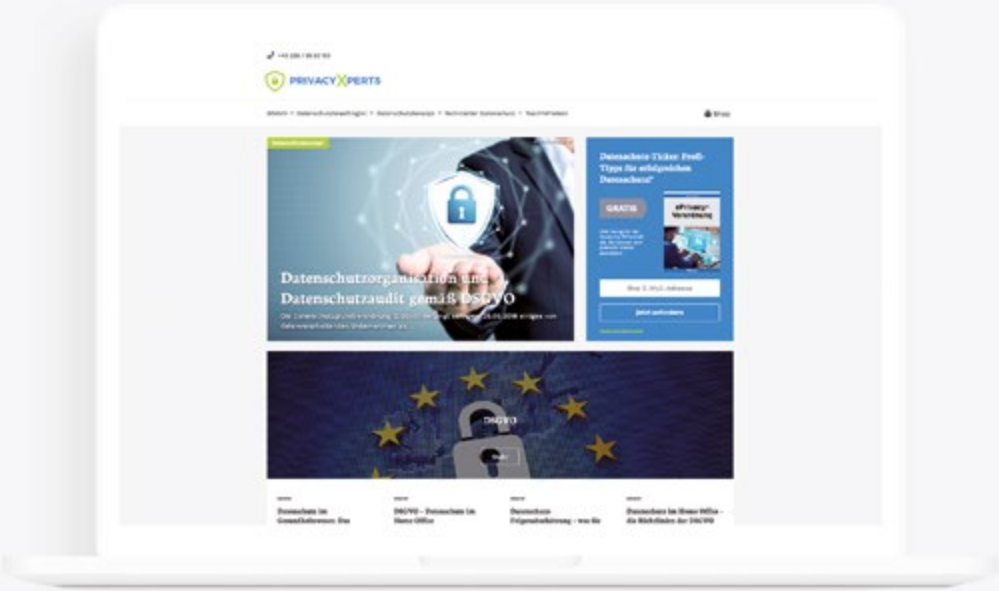
Mit der Äusserung wurde auch nicht der Tatbestand der Beleidigung nach § 185 StGB erfüllt. Für die Annahme einer Beleidigung muss eine Abwägung der Beeinträchtigungen erfolgen, die den betroffenen Rechtsgütern drohen. Im konkreten Fall muss die Meinungsfreiheit des Nutzers gegen den sozialen Geltungsanspruch als Teil des allgemeinen Persönlichkeitsrechts der Kanzlei abgewogen werden. Allerdings muss hier das allgemeine Persönlichkeitsrecht hinter die Meinungsfreiheit des Nutzers zurücktreten. So gab es tatsächlich einen Fall in der Vergangenheit, in dem ein ehemaliger Mitarbeiter Gehaltszahlungen und Zeugnisansprüche gegenüber der Kanzlei gerichtlich geltend machte. Insofern muss die Äusserung als zulässige Kritik des Nutzers am Verhalten der Kanzlei als Arbeitgeber angesehen werden.

§

So ziehen Sie in der Schweiz Nutzen aus der Entscheidung

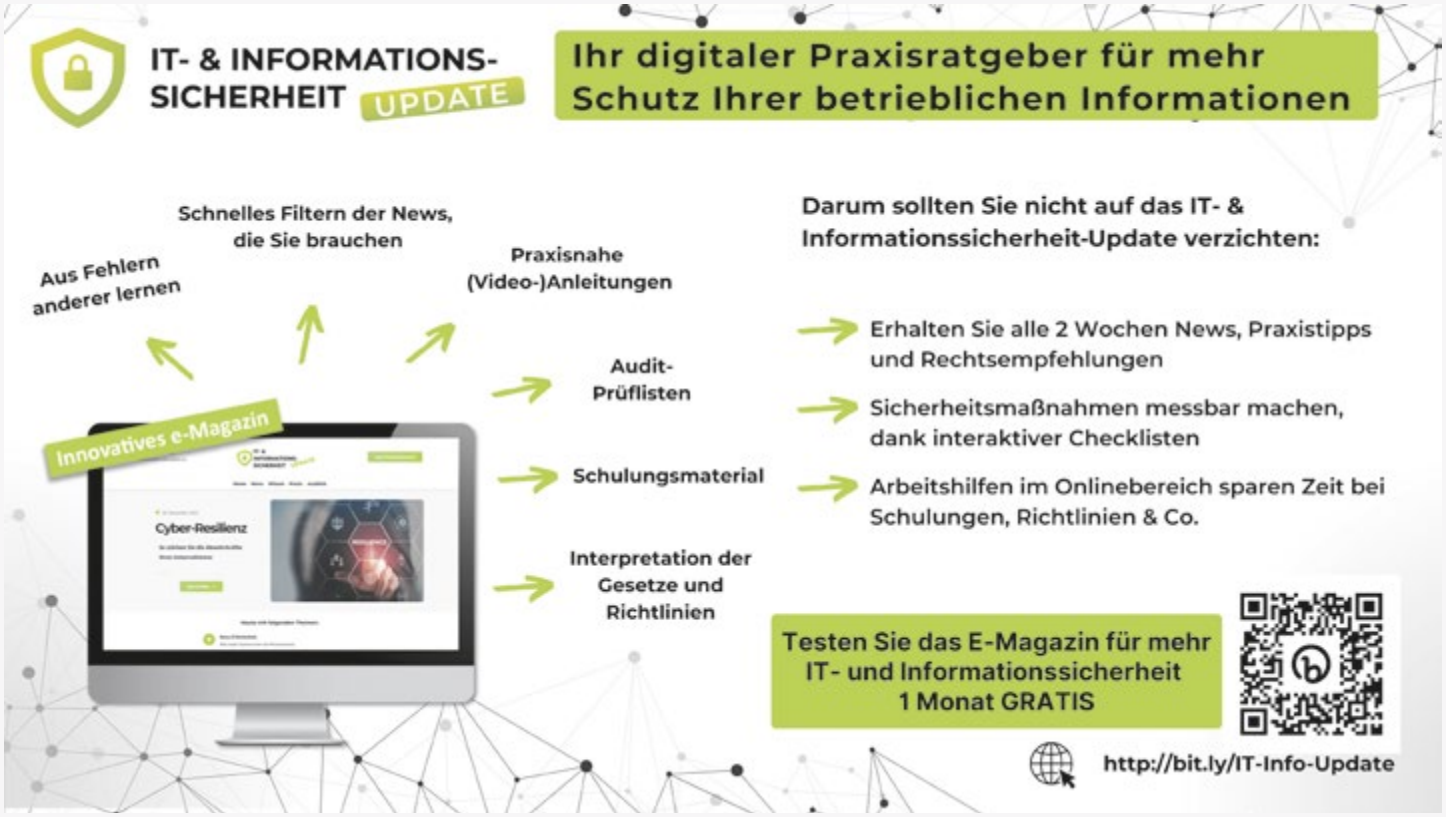
- Im konkreten Fall lag keine strafrechtlich relevante Äusserung vor, sondern nur eine Meinung. Insofern gab es auch keinen Anspruch auf Offenlegung des betreffenden Nutzers nach § 21 TDDDG. Datenschutzrechtlich betrachtet gilt daher: Mit § 21 TDDDG besteht eine Spezialvorschrift zur Herausgabe von Informationen. Sind die Anforderungen nicht erfüllt, muss eine Offenlegung unterbleiben. Diese kann auch nicht auf sonstige Rechtsgrundlagen gestützt werden, z. B. das überwiegende berechtigte Interesse des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung).
- Erinnern Sie sich an das Urteil, wenn Sie einmal eine Aussage oder Bewertung dahin gehend bewerten sollen, ob es sich noch um eine Meinung handelt oder um eine unzulässige Äusserung (z. B. falsche Tatsachenbehauptung oder Schmähkritik). Es wird im Detail ausgeführt, worauf man bei der Bewertung einer Äusserung abstellen muss.

„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:

Unbekanntes Risiko Schatten-IT: Bringen Sie Licht ins Dunkel
Das sind die typischen Hotspots fehlender Schutzmassnahmen

PRIVACYXPERTS

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

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