DATENSCHUTZAKTUELL Professional
DEZ I 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

ERSTELLEN SIE JETZT IHREN TÄTIGKEITSBERICHT 2025

Bleiben Sie gelassen

Liebe Leserin, lieber Leser,

im Datenschutz kann es manchmal zugehen wie im „normalen" Leben auch: Es geht drunter und drüber und alles ist irgendwie Chaos. Oder manchmal scheint die linke Hand nicht zu wissen, was die rechte tut.

Finden Sie sich in einer solchen Situation wieder, heißt es vor allem: Ruhe bewahren. Betrachten Sie die Dinge mit etwas Abstand und sortieren Sie sich. Manchmal reichen schon einige Momente Ruhe aus, um wieder klarer zu sehen. Auch eine gute Portion Gelassenheit hilft Ihnen dabei, schwierige Situationen zu meistern.

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

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: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Looker_Studio; Seite 1: Adobe Stock | Duncan Andison

Erscheinungsweise: 26-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.

Ihre gute Beratung ist ein wichtiger Baustein für das Risikomanagement des Unternehmens.

Kein Hexenwerk: So vermeiden Sie Fehleinschätzungen mit links

Geht es um das Verarbeiten personenbezogener Daten, sind Sie Ansprechpartner Nummer eins. Schließlich kennen Sie sich am besten aus und verfügen über das meiste Know-how rund um personenbezogene Daten. Doch selbst viel Know-how schützt nicht vor Fehleinschätzungen. Diese sollten Sie jedoch im Interesse aller vermeiden.

Ihre Beratung ist entscheidend

Damit Datenschutz funktioniert und Verarbeitungen personenbezogener Daten im Einklang mit den Regeln der Datenschutz-Grundverordnung (DSGVO) erfolgen, kann entscheidend sein, dass Sie gut Ihren Aufgaben nachkommen. Nicht nur mit dem Kontrollieren der Umsetzung, sondern gerade mit dem Beraten in allen Datenschutzfragen tragen Sie dazu bei, dass man sich regelkonform verhält. Zugleich ist eine gute Beratung ein wichtiger Baustein für das Risikomanagement Ihres Unternehmens.

Doch leider sind die Fragen im Datenschutz meist nicht einfach und schnell zu beantworten, auch wenn man sich auf allen Seiten das noch so wünscht. Vielmehr müssen Sie professionell vorgehen und jeder Fehleinschätzung vorbeugen. Denn klar ist: Zwar muss eine Fehleinschätzung Ihrerseits nicht immer gleich zum Weltuntergang führen. Allerdings bedeutet jede Fehleinschätzung zusätzlichen Aufwand, und zwar für das Unternehmen, die Beschäftigten und Sie.

Beherzigen Sie einfache Grundregeln

Egal, ob es um eine Beratung oder eine Einschätzung geht. Fehleinschätzungen können Sie auch dadurch vorbeugen, dass Sie einfache Grundregeln befolgen und diese zum Standard Ihrer Arbeit machen. Bewahren Sie immer einen kühlen Kopf. Lassen Sie sich nicht zu vorschnellen Äußerungen, Bewertungen oder Entscheidungen hinreißen. Bleiben Sie objektiv und bewerten Sie erhaltene Informationen kritsch.

Setzen Sie auf diese Checkliste

Von Ihnen als Datenschutzbeauftragter werden vor allem zwei Dinge erwartet: Erstens müssen Sie über das nötige Know-how verfügen. Und zweitens sollen Sie dieses professionell anwenden. Damit Ihnen bei Ihrer Beratung keine Fehleinschätzungen unterlaufen, sollten Sie einfach die folgenden Tipps beherzigen. Bearbeiten Sie eine Frage zum Datenschutz, können Sie so immer gegenchecken, ob Sie alles umgesetzt haben.

Checkliste: Maßnahmen, mit denen Sie Fehleinschätzungen vermeiden

Ihre Maßnahme	Das sollten Sie beherzigen	Berücksichtigt?
Den Sachverhalt habe ich umfassend geklärt und erfasst?	› Dies ist entscheidend, damit Sie Fehleinschätzungen vermeiden können. Unklarheiten müssen ausgeräumt werden. Verlassen Sie sich nicht auf Vermutungen oder vage Aussagen. › Gehen Sie systematisch vor. Stellen Sie die W-Fragen: Wer? Was? Wann? Warum? Wie? › Fordern Sie im Zweifel eine schriftliche Schilderung des Sachverhalts ein. Ggf. können Sie Hilfestellung geben und mit den Kollegen den Sachverhalt gemeinsam aufbereiten und festhalten. › Um bei einem mündlich geschilderten Sachverhalt sicherzustellen, dass Sie alles richtig verstanden haben, sollten Sie den Sachverhalt in eigenen Worten wiederholen. Verschriftlichen Sie unbedingt das Gesagte.	○ Ja ○ Nein

Die Rahmenbedingungen habe ich sorgfältig ermittelt?	› Fordern Sie nötige Informationen an, die Ihnen eine datenschutzrechtliche Einschätzung ermöglichen. Das sind beispielsweise die Informationen, die im Verzeichnis von Verarbeitungstätigkeiten enthalten sein müssen. Ferner sollten Sie Informationen zum Zweck, zu Datenarten, Empfänger, eingesetzter Technik oder zu Dienstleistern einfordern. › Hilfreich für das Verständnis sind auch Konzepte und Datenflussdiagramme. › Unter Umständen gibt es bereits kollektivrechtliche Vereinbarungen, etwa eine Betriebsvereinbarung. Diese kann erhebliche Auswirkungen auf Ihre Bewertung haben, etwa wenn dort bestimmte Verarbeitungsverbote enthalten sind.	○ Ja ○ Nein
Rechtliche Aspekte habe ich identifiziert?	› Man muss Ihnen sagen können, worauf man die Verarbeitung stützen will, sprich auf welcher Rechtsgrundlage die Verarbeitung basiert. › Nennt man Ihnen pauschal das „berechtigte Interesse", müssen Sie hier nachbohren. Erstens muss man hier konkret werden und zweitens muss später eine Interessenabwägung zugunsten des berechtigten Interesses ausfallen, damit sich die Verarbeitung auf Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO stützen lässt.	○ Ja ○ Nein
Ich habe Interpretationen, Sichtweisen und Meinungen recherchiert?	› Je eingriffsintensiver die Verarbeitung für das Persönlichkeitsrecht der Betroffenen ist, desto mehr Aufwand müssen Sie hier treiben. › Prüfen Sie nicht nur, was in Gesetzen steht. Mindestens genauso wichtig sind Fachbücher, Papiere von Aufsichtsbehörden und Rechtsprechung. › Auch eine Internetrecherche kann sinnvoll sein. Nutzen Sie künstliche Intelligenz (KI), kann auch das eine gute Informationsquelle sein. Aber Vorsicht: KI kann halluzinieren. Deshalb müssen Sie die Ergebnisse kritisch prüfen › Nutzen Sie möglichst viele voneinander unabhängige Quellen für Ihre Recherche. Auch bei Gesetzeskommentaren sollten Sie unbedingt auf mehrere aktuelle Werke setzen.	○ Ja ○ Nein
Vertretbare Positionen habe ich erarbeitet?	› Entwickeln Sie logische und rechtlich gut begründbare Meinungen zu den betreffenden Fragen Ihres Sachverhalts. › Gerade bei schwierigen Fragen kann eine Pro-und-Kontraliste der Entscheidungsfindung dienen und diese auch für später dokumentieren. › Was vertretbar ist, ist oft Ansichtssache. Hier kann es hilfreich sein, wenn Sie andere fragen, wie sie eine Sache sehen. Das können etwa Datenschutzprofis in anderen Unternehmen sein. Auch der Austausch bei Tagungen oder Fachveranstaltungen kann Ihr Meinungsbild verändern und Ihren Horizont erweitern.	○ Ja ○ Nein
Ich habe mir eine eigene Meinung gebildet?	› Setzen Sie hier einerseits auf Ihr Fachwissen und die bereits erarbeiteten Ergebnisse. Andererseits sollten Sie hier Ihre Erfahrungen einfließen lassen, etwa zur Praktikabilität oder Umsetzbarkeit in Ihrem Unternehmen. › Wahren Sie bei Ihrer Meinung Objektivität und Sachlichkeit. Beziehen Sie keine Position aus ideellen oder moralischen Erwägungen. › Achten Sie auf eine nachvollziehbare Begründung für Ihre Meinung. Vergessen Sie nicht, die tragenden Aspekte für Ihre Meinung zu dokumentieren.	○ Ja ○ Nein
Ich gehe risikoorientiert vor?	› Bei der Wahrnehmung Ihrer Aufgaben sollen Sie risikoorientiert vorgehen (Art. 39 Abs. 2 DSGVO). Das gilt auch für das Beraten. Bei unproblematischen Fragen brauchen Sie weniger intensiv prüfen. › Orientieren Sie sich an einem einfachen Prinzip: Je komplexer, riskanter oder eingriffsintensiver eine Verarbeitung ist, desto fundierter müssen Ihre Beratung und Ihre Prüfung ausfallen.	○ Ja ○ Nein
Ich habe andere relevante Stellen eingebunden?	› Vermeiden Sie Fehleinschätzungen bei Themen oder Aspekten, bei denen Sie sich nicht so gut auskennen und eher mit Vermutungen oder Annahmen arbeiten müssten. › Holen Sie andere Stellen im Unternehmen mit ins Boot. Das kann z. B. bei Fragen der technischen Umsetzung oder zum Stand der Technik bei Schutzmaßnahmen die IT-Abteilung sein.	○ Ja ○ Nein
Unsicherheiten oder Bedenken habe ich herausgearbeitet und formuliert?	› Gerade wenn es kompliziert wird oder man beispielsweise im Bereich KI rechtliches Neuland betritt, kann es Unsicherheiten geben. Diese sollten Sie klar formulieren. › Auch bei Bedenken ist wichtig, dass Sie diese klar formulieren. Achten Sie hier auf Sachlichkeit und vermeiden Sie ein Dramatisieren. Halten Sie Ihre Bedenken schriftlich fest.	○ Ja ○ Nein
Weitere Expertise habe ich hinzugezogen?	› Erkennen Sie, dass Sie in einem Bereich nicht über das nötige Wissen verfügen, hilft es nicht, wenn Sie einfach darüber hinweggehen. Gehen Sie offen damit um. › Raten Sie zur Einbindung von Experten. Das können interne Stellen sein, die über das nötige Spezialwissen verfügen. Ist das Wissen intern nicht verfügbar, sollten Sie zur Einbindung externer Spezialisten raten.	○ Ja ○ Nein
Ich habe mir Zeit für die Prüfung und Qualitätssicherung genommen?	› Bewertungen unter Stress und Druck vornehmen ist tödlich für eine gute Qualität. Nehmen Sie sich die Zeit, die Sie für eine fundierte Bewertung und Begründung brauchen. › Manche Prüfungen müssen reifen und gehen nicht auf die Schnelle. Wiederholen und durchdenken Sie Ihre Prüfung. Das beugt falschen Weichenstellungen und Denkfehlern vor.	○ Ja ○ Nein
Meine Prüfung und Empfehlung habe ich gut dokumentiert?	› Auch hier sollten Sie den risikobasierten Ansatz verfolgen. Ist etwas einfach zu lösen, kann die Dokumentation einfach ausfallen. Bei Schwierigem, Riskantem oder Kompliziertem sollte alles gut nachvollziehbar sein. › Am besten ist es, wenn Sie Ihr Vorgehen und die Entwicklung einer Bewertung bzw. Empfehlung schriftlich festhalten. Dann ist der Weg dorthin auch in Zukunft leicht nachvollziehbar.	○ Ja ○ Nein
Ich überlasse die Entscheidung anderen im Unternehmen?	› Formulieren Sie Ihre Bewertung oder Einschätzung immer als Empfehlung. Geben Sie dazu Ihre Einschätzung ab. Überlassen Sie jedoch das Entscheiden den verantwortlichen Stellen im Unternehmen. Das ist in letzter Konsequenz die Unternehmensleitung. › Dokumentieren Sie, wer wann welche Entscheidung getroffen hat. Hier kann es auch wichtig sein, dass die nächsten Schritte zur Umsetzung der Entscheidung festgehalten werden.	○ Ja ○ Nein

Wie Sie Zweifler vom Datenschutz überzeugen

Vielleicht kennen Sie auch in Ihrem Unternehmen die eine oder andere Person, die sich mit dem Datenschutz schwertut. Das ist umso problematischer, je weiter oben in der Hierarchie sie Zweifler oder gar Datenschutzverweigerer finden. Doch meist ist Hopfen und Malz noch nicht verloren. Überzeugen Sie im Datenschutz mit guten Argumenten.

Haben Sie Argumente immer griffbereit

Bestimmt nutzen Sie ein Notizbuch, etwa um in Besprechungen wichtige Punkte festhalten zu können. Doch nicht nur hierfür ist ein Notizbuch praktisch. Sie können es auch zum „Schweizer Messer" für Ihre Beratungsarbeit machen. Packen Sie sich Nützliches und Hilfreiches in Ihr Notizbuch. Das kann auch die folgende Liste mit Argumenten sein, die für einen gelebten Datenschutz sprechen. Finden Sie sich in einer entsprechenden Situation wieder, gehen Ihnen garantiert nie wieder die Argumente aus. Nutzen Sie einfach Ihren im Notizbuch abgelegten „Spickzettel".

Leisten Sie unentwegt Überzeugungsarbeit

Egal, ob Sie in Besprechungen sind oder in eher lockerer Runde das Gespräch auf den Datenschutz kommt. Nehmen Sie abwertende Äußerungen nicht einfach so hin und lassen Sie sie nicht unkommentiert im Raum stehen. Denn dann können sich falsche Ansichten festsetzen.

Checkliste: Ihre Argumente für gelebten Datenschutz

Ihr Argument	Das können Sie erläutern	Genutzt?
Die Konkurrenz schläft nicht.	› Datenschutz ist nicht nur für Ihr Unternehmen ein Thema. Es trifft alle Unternehmen und gerade auch die Konkurrenz. Ist diese im Datenschutz besser unterwegs als Ihr Unternehmen, kann das für Kunden der entscheidende Faktor sein. › Ein „Die Konkurrenz macht weniger im Datenschutz" sollten Sie nie gelten lassen. Sich im Falschen mit anderen zu messen kann gewaltig nach hinten losgehen. Es bringt auch nichts, damit zu argumentieren, wenn etwas schiefgeht oder Ärger mit der Datenschutzaufsicht droht.	○ Ja ○ Nein
Kunden reagieren sensibel auf fehlenden Datenschutz.	› Der Kunde ist König. Und er entscheidet letztendlich auch über den Erfolg Ihres Unternehmens. Erkennt er, dass seine Daten nicht sicher sind, wird er ggf. erst überhaupt nicht Kunde oder sucht schnellstmöglich das Weite. › Ernst gemeinter Datenschutz ist eine vertrauensbildende Maßnahme. Denn: Wer will Schützenswertes jemandem anvertrauen, der Schutz und Sicherheit auf die leichte Schulter nimmt? › Mit gutem Datenschutz schützt man auch die Reputation und das Image des Unternehmens.	○ Ja ○ Nein
Wir sind zu rechtskonformem Verhalten verpflichtet.	› Das magische Stichwort heißt hier „Compliance". Damit ist regelkonformes Verhalten gemeint. Jedes Unternehmen ist dazu verpflichtet. Werden Regeln ignoriert oder absichtlich übertreten, kann das auch für die Entscheider teuer werden. › Dass Compliance nie auf die leichte Schulter zu nehmen ist, zeigt sich immer wieder. Auch den einzelnen Mitarbeiter kann es empfindlich treffen. So können selbst „einfachen" Mitarbeitern arbeitsrechtliche Konsequenzen drohen. Auch Schadensersatzforderungen sind drin.	○ Ja ○ Nein
Datenschutz ist Teil des aktiven Risikomanagements.	› Jedes Unternehmen muss aktives Risikomanagement betreiben. Gefahren für das Unternehmen sind zu bewerten und Risiken sind abzuleiten. Diese müssen dann behandelt werden, etwa durch Gegenmaßnahmen. › Datenschutz ist Teil einer vorausschauenden Unternehmensführung. Probleme müssen frühzeitig erkannt werden, um rechtzeitig Lösungen zu etablieren. › Wird der Datenschutz vernachlässigt, steigt automatisch das Risiko, dass es zu Pannen, Datenschutzverstößen oder erfolgreichen Angriffen von Cyberkriminellen kommt.	○ Ja ○ Nein
Gelebter Datenschutz ist eine Investition in die Zukunft.	› Datenschutz kann zwar Aufwand und Kosten verursachen. Allerdings sind das keine verlorenen Investitionen. Im Gegenteil: Jeder in den Datenschutz investierte Euro zahlt sich aus, etwa in höherer Sicherheit, qualifizierteren Mitarbeitern und besseren Standards. › Wer an der falschen Ecke spart, zahlt am Ende drauf. Das gilt gerade im Datenschutz. Unzureichende Maßnahmen können große Schäden verursachen.	○ Ja ○ Nein
Datenschutz macht uns für Fachkräfte attraktiver.	› Jeder ist Betroffener, eben auch heutige und zukünftige Beschäftigte. Auch deren Interessen am effektiven Schutz personenbezogener Daten müssen ernst genommen werden. › Beschäftigtendaten sind nicht weniger schutzwürdig, nur weil es sich um Beschäftigte handelt. › Gerade im Kampf um Talente und Fachkräfte kann für diese entscheidend sein, wie ernst es das Unternehmen mit dem Datenschutz meint. Auch diese reagieren sensibel auf zu viel Sorglosigkeit.	○ Ja ○ Nein
Frühzeitige Berücksichtigung bedeutet Kosteneffizienz.	› Wird Datenschutz von Anfang an bedacht, etwa bereits in der Ideenphase, können Verarbeitungen datenschutzfreundlich gestaltet werden. Das kann Entwicklungs- und spätere Betriebskosten reduzieren. › Frühzeitig berücksichtigter Datenschutz vermeidet hohe Kosten, wenn spätere Umgestaltungen vermieden werden können, um Datenschutzvorschriften doch noch einzuhalten.	○ Ja ○ Nein

Erstellen Sie jetzt Ihren Tätigkeitsbericht 2025

Klar ist: Als Datenschutzbeauftragter sind Sie in erster Linie Berater in Datenschutzfragen und kontrollieren die Umsetzung der Anforderungen. Für die Umsetzung sind Sie nicht verantwortlich. Umso wichtiger ist, dass die Verantwortlichen wissen, wie es um den Datenschutz im Unternehmen steht. Geben Sie einen Überblick, und zwar mit Ihrem Tätigkeitsbericht.

So gehen Sie es an

Haben Sie für sich entschieden, dass Sie einen Tätigkeitsbericht für 2025 erstellen wollen, ist schon mal eine erste Hürde genommen. Und damit Sie nicht gleich wieder die Motivation verlieren, sollten Sie überlegt vorgehen. Denn haben Sie einen guten Plan, geht vieles leichter von der Hand und klappt wie am Schnürchen. Setzen Sie auf diese Schritte zur Erstellung Ihres Berichts:

Schritt 1: Sammeln Sie Informationen

Damit Sie ein Gespür dafür bekommen, was für 2025 berichtenswert sein könnte und welche Schwerpunkte Sie in Ihrem Bericht setzen sollten, brauchen Sie zunächst einen Überblick. Legen Sie sich einen Notizzettel bereit, um Ideen und Auffälligkeiten mit der jeweiligen Fundstelle zu notieren, und machen Sie dann Folgendes:

- Sichten Sie Ihr E-Mail-Postfach.
- Werten Sie den Kalender aus.
- Überfliegen Sie Ihre Beratungen.
- Schauen Sie in Auditprotokolle und Prüfberichte.
- Prüfen Sie Anfragen und Beschwerden sowie deren Status.
- Überblicken Sie Ihre Schulungs- und Awarenessaktivitäten.

Schritt 2: Führen Sie ein Brainstorming durch

Notieren Sie sich zu typischen Fragen alle Einfälle, Themen, Ereignisse oder Aktivitäten im Jahr 2025. Bewerten Sie noch nichts. Schreiben Sie alles auf, was Ihnen in den Sinn kommt. Typische Fragen für Ihr Brainstorming können sein:

- Welche Verarbeitungen waren neu in 2025?
- Wen bzw. welche Abteilungen habe ich beraten?
- Welche thematischen Schwerpunkte gab es bei der Beratung?
- Welche Projekte sind erwähnenswert?
- Welche Pannen oder Vorfälle gab es?
- Welche Awarenessaktionen habe ich durchgeführt?
- Welche Anfragen oder Beschwerden gab es?
- Welche Defizite sind zutage getreten?
- Welche Kennzahlen oder Statistiken sind nutzbar?

Daneben sind jedoch auch Impulsfragen wichtig, die Sie und Ihre Arbeit als Datenschutzbeauftragter betreffen. Schließlich soll ein Bericht auch unterstreichen, was Sie leisten und dass Sie Unterstützung brauchen. Denken Sie an folgende Fragen:

- Welche besonderen Erfolge sind erwähnenswert?
- Was verursachte bei mir besonderen Aufwand?
- Wo gab es Widerstände oder Konflikte?
- Was lief besonders gut?
- Wo gibt es Verbesserungsbedarf?

Schritt 3: Machen Sie das Berichtenswerte aus

Gehen Sie dann Ihre Einfälle durch. Bewerten Sie diese unter verschiedenen Aspekten. So z. B. was die Unternehmensleitung unbedingt wissen sollte. Auch sollten Sie die Einfälle dahin gehend bewerten, wie sehr sie von Bedeutung sind, damit die Unternehmensleitung angemessen mit Risiken umgehen und die nötigen Entscheidungen treffen kann.

Schritt 4: Clustern Sie die Themen

Hier können Sie das, was in den Bericht soll, thematisch gruppieren. Was zusammenpasst, sollte in einem aussagekräftigen Kapitel zu finden sein. Innerhalb der Kapitel sollten Sie die Themen weiter strukturieren. Hier haben Sie die Möglichkeit, chronologisch zu sortieren. Eventuell ist es jedoch besser, wenn Sie die Inhalte nach der Wichtigkeit ordnen.

Schritt 5: Wählen Sie die passende Form und den Umfang

Überlegen Sie, was Sie vermitteln, wen Sie erreichen wollen und wie das Ganze passieren soll. Die Darstellungsform ist nämlich meist eher zweitrangig. Viel wichtiger ist, dass Sie und Ihre Botschaft wahrgenommen werden. Klären Sie also für sich, was wohl am ehesten zu Ihrer Zielgruppe passt. So kann eine Präsentation, die Sie halten, auch bei wenigen Folien mehr bringen und nachhaltiger wirken als ein endloser Bericht, der schnell beiseitegelegt wird.

Schritt 6: Jetzt schreiben Sie

Egal, für welche Form Sie sich entscheiden: Halten Sie sich kurz, beschränken Sie sich auf das Wesentliche, formulieren Sie prägnant und verständlich und vermeiden Sie zu großen fachlichen Tiefgang. Schließlich wollen Manager über das Wichtige informiert sein. Mit dem „Fachkram" und den komplizierten Details will man sich meist nicht beschäftigen. Dafür hat man Sie, den Profi im Datenschutz.

Schritt 7: Prüfen Sie das Ergebnis

Kein Bericht ist beim ersten Wurf rund. Sie haben zunächst allenfalls eine Rohfassung. Drehen Sie mehrere Runden und schauen Sie, wo es besser, einfacher, verständlicher oder lesefreundlicher

werden muss. Und die Lesefreundlichkeit sollten Sie nie unterschätzen. Bauen Sie Bilder, Diagramme, Aufzählungen oder Statistiken ein. Damit können Sie nicht nur manche Botschaft transportieren. Sie lockern Ihren Bericht auch optisch auf.

Geben Sie nach Möglichkeit einer Vertrauensperson Ihren Bericht zum Gegenlesen. So werden ggf. Fehler und Unstimmigkeiten entdeckt, die Sie beheben sollten. Denn ein Bericht mit Fehlern wirkt schlichtweg weniger professionell.

Gliederung für Ihren Bericht gefällig? Setzen Sie diese Schwerpunkte

Hier müssen Sie nicht lange grübeln oder das Rad neu erfinden. Übernehmen Sie aus der folgenden Checkliste die Schwerpunkte oder Kapitel, die für Ihr Unternehmen und Ihre individuelle Situation passen.

Checkliste: Mögliche Schwerpunkte Ihres Tätigkeitsberichts

Schwerpunkt, Kapitel	Das können Sie darstellen oder berichten	Enthalten?
Management-Summary	› Stellen Sie eine kurze Zusammenfassung als Einleitung Ihrem Bericht voran. So ist auch derjenige gut informiert, der nicht den kompletten Bericht durchsehen will. › Achten Sie darauf, dass alle Ihre Kernbotschaften enthalten sind. Nehmen Sie unbedingt auf, was Sie vermitteln wollen und was hängen bleiben soll.	○ Ja ○ Nein
Datenschutzorganisation	› Stellen Sie dar, wie der Datenschutz in Ihrem Unternehmen organisiert und strukturiert ist. › Hier können Sie mit Zahlen meist sehr gut verdeutlichen, wie sehr Sie eingespannt sind.	○ Ja ○ Nein
Aktuelle Situation und Entwicklungen im Datenschutz	› Geben Sie einen generellen Überblick über die für Ihr Unternehmen geltenden Rahmenbedingungen. Wichtig sind auch Besonderheiten, die sich aus der Geschäftstätigkeit oder Struktur des Unternehmens ergeben können. › Erläutern Sie, welche Veränderungen es extern und intern gegeben hat. › Hatten veränderte rechtliche Rahmenbedingungen (z. B. Äußerungen von Aufsichtsbehörden, Rechtsprechung) Auswirkungen, sollten Sie diese kurz darstellen.	○ Ja ○ Nein
Besondere Risiken	› Hier können Sie die Risiken erwähnen, die im Berichtszeitraum 2025 besonders im Fokus standen. › Denken Sie an Risiken, die von extern kommen (z. B. Cyberkriminelle). Wichtig sind aber auch interne Risiken (etwa zu geringe Awareness bei Führungskräften) oder Risiken aus der Geschäftstätigkeit (z. B. Einbindung von IT-Dienstleistern). › Gibt es Gegenmaßnahmen, sollten Sie auch diese kurz darstellen.	○ Ja ○ Nein
Bedeutende Beratungen	› Zeigen Sie auf, welche Beratungen Ihrerseits von großer Bedeutung für das Unternehmen bzw. für Sie als Datenschutzbeauftragten waren. › Erwähnen Sie auch Beratungen, die besonders herausfordernd oder aufwandsintensiv waren. Eventuell mussten hierfür andere Aufgaben oder Vorhaben zurückgestellt werden.	○ Ja ○ Nein
Durchgeführte Kontrollen, Prüfungen und Audits	› Listen Sie auf, wie viele Kontrollen Sie durchgeführt haben und wie viele Abweichungen Sie festgestellt haben. Hier können Sie auch abstufen, und zwar nach geringen, mittleren oder gravierenden Mängeln. › Stellen Sie dar, was Sie thematisch geprüft haben und welche Erkenntnisse Sie gewonnen haben. Defizite sollten Sie als solche auch konkret benennen.	○ Ja ○ Nein
Durchgeführte Schulungen und Awarenessaktionen	› Auch hier können Sie zunächst mit Zahlen einen guten Überblick geben. Nennen Sie die Anzahl der Veranstaltungen und die Teilnehmerzahl. › Erläutern Sie, welche Angebote Sie gemacht haben, etwa virtuelle Trainings, und wie diese angenommen wurden. › Haben Sie positives Feedback erhalten, können Sie auch das hier unterbringen.	○ Ja ○ Nein
Pannen und Vorfälle	› Berichten Sie über das, was schiefgegangen ist und welche konkreten Folgen dies hatte. › Erläutern Sie auch, wie man vorgegangen ist, um die Panne zu beheben bzw. den Vorfall zu managen. Erwähnen Sie auch, wie Sie dabei unterstützt haben.	○ Ja ○ Nein
Anfragen, Beschwerden und Betroffenenrechte	› Nennen Sie die Zahl der entsprechenden Vorgänge. › Gehen Sie detaillierter auf Vorgänge ein, die kompliziert waren oder viel Aufwand verursacht haben. › Gibt es Verbesserungsbedarf bei der Bearbeitung, sollten Sie diesen adressieren.	○ Ja ○ Nein
Künftige Herausforderungen	› Zeigen Sie auf, vor welchen Herausforderungen Ihr Unternehmen in nächster Zeit stehen wird. Bewerten Sie insbesondere das, was bereits jetzt absehbar ist. Das können auch Veränderungen beim Business, bei der Unternehmensorganisation oder in der IT sein. › Fokussieren Sie hier vor allem auf Datenschutzrelevantes. Dabei können jedoch gerade typische Zukunftsthemen wie künstliche Intelligenz oder Cybersecurityanforderungen rund um die NIS-2-Richtlinie der EU auch von großer Bedeutung sein.	○ Ja ○ Nein
Ausblick für 2026	› Erläutern Sie, was in naher Zukunft für Ihr Unternehmen von großer Bedeutung sein wird. Meist steht nämlich schon fest, was Ihr Unternehmen im kommenden Jahr vorhat. Das kann Auswirkungen auf den Datenschutz im Unternehmen haben. › Geben Sie zudem einen Ausblick darauf, worauf Sie sich im kommenden Jahr besonders konzentrieren wollen. Das können etwa spezielle Awarenessmaßnahmen oder Kontrollschwerpunkte sein. Erläutern Sie ggf. die Schwerpunktsetzung auf Basis der betreffenden Risiken.	○ Ja ○ Nein
Handlungsempfehlungen des Datenschutzbeauftragten	› Machen Sie klar, wo Entscheidungen der Leitung nötig sind, etwa um die Datenschutzsituation im Unternehmen zu verbessern. › Sprechen Sie konkrete Empfehlungen aus. › Damit Sie gut arbeiten können und Datenschutz im Unternehmen funktioniert, brauchen Sie die nötige Unterstützung. Ist mehr Unterstützung nötig, sollten Sie das hier adressieren.	○ Ja ○ Nein

Entlarven Sie 5 Mythen rund um den Datenschutz

Datenschutz ist ein komplexes Thema. Kein Wunder, dass es hier und da falsche Vorstellungen davon gibt oder mancher Mythos besteht. Solchen Mythen können auch Sie begegnen. Dann heißt es für Sie: den Mythos entzaubern. Bei fünf typischen Mythen gelingt Ihnen das mit den folgenden Informationen:

Mythos Nr. 1: Der Datenschutzbeauftragte ist für die Einhaltung des Datenschutzes verantwortlich

Zwar hält sich dieser Mythos noch immer, und zwar gerade bei denen, die die Verantwortung für den Datenschutz loswerden wollen, etwa Geschäftsführer. Gerne wird dem Datenschutzbeauftragten die Verantwortung zumindest sprachlich zugewiesen. Allerdings ist die rechtliche Realität eine ganz andere: Dazu lohnt zunächst der Blick in die Datenschutz-Grundverordnung (DSGVO). Die meisten Pflichten treffen den Verantwortlichen bzw. den Auftragsverarbeiter. Überfliegen Sie einfach einmal die Regelungen, etwa zu den Grundsätzen (Art. 5 DSGVO), zu den Betroffenenrechten (Art. 12 ff. DSGVO) oder zur Sicherheit der Verarbeitung (Art. 32 DSGVO). Dass die Umsetzungsverantwortung Sache des Verantwortlichen und nicht des Datenschutzbeauftragten ist, erkennen Sie erst recht an Art. 24 DSGVO.

Übrigens: Sollte man Ihnen nicht glauben, können Sie es quasi „amtlich" begründen. Auch die Datenschutzaufsichtsbehörden in der EU sind der Auffassung, dass den Datenschutzbeauftragten keine Umsetzungsverantwortung trifft. Insbesondere ist er nicht verantwortlich, wenn das Unternehmen Datenschutzanforderungen nicht erfüllt. Die entsprechende Aussage finden Sie im Arbeitspapier 243 auf den Seiten des Europäischen Datenschutzausschusses unter https://t1p.de/z42w2.

Mythos Nr. 2: Kommt es zu einem Bußgeld, muss der Datenschutzbeauftragte dafür geradestehen

Das ist vom Grundsatz her falsch. Das Bußgeld richtet sich immer an den Verantwortlichen. Das ist z. B. das Unternehmen, bei dem ein interner Datenschutzbeauftragter angestellt ist. Der Verantwortliche entscheidet allein oder gemeinsam mit anderen über Zwecke und Mittel einer Verarbeitung personenbezogener Daten (Art. 4 Nr. 7 DSGVO). Dem Unternehmen wird grundsätzlich auch Fehlverhalten von Beschäftigten zugerechnet.

Mythos Nr. 3: Wenn der Datenschutzbeauftragte etwas falsch beurteilt, haftet er voll dafür

Der Mythos kann dann tatsächlich zutreffen, wenn es sich um einen externen Datenschutzbeauftragten handelt. Zwischen Unternehmen und externem Datenschutzbeauftragten gilt normales Vertragsrecht. Erbringt der externe Datenschutzbeauftragte nicht die geschuldete Leistung oder verursacht er Schäden, muss er diese ersetzen. Beim internen Datenschutzbeauftragten sieht die Sache ganz anders aus. Hier greifen die Grundsätze zur Arbeitnehmerhaftung. Kommt es beim Arbeitgeber zu einem Schaden, den der Datenschutzbeauftragte zu verantworten hätte, müsste dieser nur bei Vorsatz und grober Fahrlässigkeit voll haften und Schadensersatz leisten. Bei mittlerer Fahrlässigkeit kommt es nur zur anteiligen Haftung, wobei viele Aspekte auf Arbeitgeberseite zu berücksichtigen sind. Hat dieser nicht angemessen unterstützt oder den Datenschutzbeauftragten überfordert (z. B. trotz fehlender juristischer Ausbildung komplexe Rechtsfragen klären lassen), kann das den Haftungsanteil des Datenschutzbeauftragten erheblich reduzieren. Bei leichter Fahrlässigkeit, etwa einem Versehen, muss der Arbeitgeber den Schaden allein tragen.

Mythos Nr. 4: Der Betriebsrat darf im Datenschutz mitreden

Viele meinen, dass der Betriebsrat im Rahmen der sogenannten erzwingbaren Mitbestimmung auch in Datenschutzfragen mitreden darf, und zwar im Rahmen von § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG). Doch das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG bei der Einführung von technischen Einrichtungen erfasst gerade nicht den Datenschutz insgesamt. Das urteilen auch Arbeitsgerichte so, beispielsweise das Landesarbeitsgericht Hessen (Beschluss vom 5.12.2024, Az. 5 TaBV 4/24).

Auch ansonsten ergeben sich aus dem BetrVG keine generellen Mitspracherechte beim Datenschutz. Zwar hat der Betriebsrat einen allgemeinen Überwachungsauftrag (§ 80 Abs. 1 BetrVG), der sich auch auf die Gesetze zum Datenschutz erstrecken kann. Allerdings kann er hier nichts in Sachen Umsetzung einfordern. Den Datenschutz umzusetzen ist Sache des Arbeitgebers, sprich des Unternehmens.

Mythos Nr. 5: Betroffene können immer Schadensersatz fordern

Bei zahlreichen Verstößen kann ein Betroffener ohnehin nichts für sich geltend machen. So z. B. wenn das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) nicht geführt oder eine Datenpanne nicht rechtzeitig der Aufsicht gemeldet wird (Art. 33 DSGVO). Das sind eher formelle Anforderungen ohne Bedeutung für den Betroffenen. Denkbar ist Schadensersatz nach Art. 82 DSGVO nur, wenn drei Voraussetzungen vorliegen: Erstens:

Es muss ein DSGVO-Verstoß vorliegen. Zweitens: Es muss einen materiellen bzw. immateriellen Schaden geben. Drittens: Zwischen Verstoß und Schaden muss ein Ursachenzusammenhang bestehen. Der Betroffene muss das Vorliegen dieser drei Voraussetzungen nachweisen. Erst dann ist ein Schadensersatzanspruch tatsächlich möglich.

Können wir uns in Sachen Auskunft an den Betroffenen „freikaufen“?

FRAGE: Wir rätseln, wie wir mit speziellen Betroffenenanfragen umgehen sollen. Manche Kunden beschweren sich über von uns verkaufte Produkte, manchmal auch nach Ablauf der Gewährleistung. Sie sind wohl so über die Ablehnung eines Austauschs des Produkts verärgert, dass sie ihren Anspruch aus Art 15 Datenschutz-Grundverordnung (DSGVO) geltend machen. Die Erfüllung jeder Betroffenenanfrage ist bei uns mit viel Rechercheaufwand verbunden. Daher stellt sich uns die Frage: Wäre es möglich, dass wir dem Betroffenen Ersatz zukommen lassen und fragen, ob sich damit auch sein Datenschutzanliegen erledigt hat?

ANTWORT: In solchen wie von Ihnen geschilderten Fällen kann tatsächlich der Eindruck entstehen, dass es einem wohl verärgerten Kunden eher darum geht, es Ihrem Unternehmen heimzuzahlen. Es soll spüren, was es davon hat, dass man nicht aus Kulanz ein Produkt ersetzt hat. Allerdings sollten Sie in Sachen Betroffenenrechte immer bedenken: Grundsätzlich kommt es nicht auf die Motivation für die Geltendmachung der Betroffenenrechte an. Jedermann kann jederzeit bei jedem Verantwortlichen sein Recht auf Auskunft geltend machen. Es ist nicht einmal erforderlich, dass ein Verantwortlicher bislang in einer Beziehung zu einem Betroffenen stand.

Eine Auskunft kann allerdings verweigert werden, wenn die Geltendmachung rechtsmissbräuchlich ist, sprich es sich um einen offenkundig unbegründeten Antrag handelt oder dieser einen exzessiven Charakter hat (Art. 12 Abs. 5 Satz 2 DSGVO). Das Problem im konkreten Fall kann hier sein, dass Ihr Unternehmen den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen müsste. Vorliegend hat der Betroffene gerade nicht geäußert, dass er seinen Auskunftsanspruch geltend machen wird, wenn er kein Ersatzprodukt bekommt. Insofern dürfte es mit dem Nachweis schwierig werden.

Nachfrage kann sinnvoll sein

Unter Umständen ist es tatsächlich eine Frage der Kosten und des Aufwands, wie Ihr Unternehmen mit solchen Fällen umgehen will. Denn es kann sein, dass es einem verärgerten Kunden eher nicht um den Datenschutz geht, sondern um sein Produkt. Ein Produkttausch könnte mit deutlich niedrigeren Kosten verbunden sein, als sie bei einer Bearbeitung der Auskunft entstehen. Rein wirtschaftlich betrachtet, kann es Sinn ergeben, wenn Ihr Unternehmen dem Kunden einen Produkttausch anbietet und nachfragt, inwieweit er weiterhin Auskunft wünscht. Unter Umständen verzichtet er auf die Auskunft. Hält er jedoch daran fest, muss Ihr Unternehmen die Auskunft liefern.

Hafte ich für falsche Englischübersetzungen?

FRAGE: In unserem Unternehmen will man zukünftig auf Englisch als Geschäftssprache setzen. Dazu sollen alle Bereiche E-Mails, Bewertungen oder Stellungnahmen nur noch in Englisch verfassen. Zwar beherrsche ich die englische Sprache einigermaßen. Allerdings habe ich als Datenschutzbeauftragter dennoch Bedenken, beispielsweise meine Einschätzungen, Bewertungen und Empfehlungen nur noch in Englisch zu verfassen. Hafte ich für „Übersetzungsfehler“?

ANTWORT: Bezüglich einer möglichen Haftung brauchen Sie sich in aller Regel keine Sorgen zu machen. Einerseits schafft das Unternehmen selbst die Gefahr bzw. das Risiko, dass Nichtmuttersprachler bei englischen Sprachfassungen Fehler machen und etwas falsch ausdrücken. Schließlich ist nach wie vor Englisch kein Standard in Deutschland und erst recht keine Amtssprache.

Andererseits werden Fehler, die Sie machen, grundsätzlich dem Unternehmen zugerechnet. Kommt es zu Schäden, greifen die Grundsätze zur Arbeitnehmerhaftung, weil Sie trotz Ihrer Funktion als Datenschutzbeauftragter ganz normaler Arbeitnehmer sind. Insofern gilt: Sie haften als Arbeitnehmer nur für Schäden voll, wenn Sie vorsätzlich oder grob fahrlässig den Schaden verursacht haben. Bei leichter Fahrlässigkeit, etwa einem Versehen, haften Sie überhaupt nicht. Bei mittlerer Fahrlässigkeit muss genau geprüft werden, wer welchen Anteil an der Schadensursache hat. Hier hat nämlich der Arbeitgeber durch die Sprachvorgabe das Risiko von Fehlern erhöht. Insofern müsste er auch Gegenmaßnahmen zur Reduzierung des Risikos ergriffen haben. Hat er das nicht gemacht, dürfte das zu seinen Lasten gehen. Insofern dürfte auch bei mittlerer Fahrlässigkeit die Haftung fehlerhafte Übersetzungen voll beim Unternehmen liegen.

OLG Frankfurt: E-Mail-Adresse ist für Zugfahrt nicht nötig

Rechtsgrundlagen sind oft essenziell, damit eine Verarbeitung personenbezogener Daten erlaubt ist. Doch die Datenschutz-Grundverordnung (DSGVO) sieht gerade bei Einwilligung & Co. viele Anforderungen vor, die für eine Wirksamkeit zu erfüllen sind. Freiwilligkeit und Erforderlichkeit sind entscheidend, wie ein Urteil des Oberlandesgerichts (OLG) Frankfurt vom 10.7.2025 (Az. 6 UKl 14/24) zeigt.

Das führte zum Rechtsstreit

Die Bahn nutzte verschiedene Vertriebswege für den Verkauf von Tickets für Bahnfahrten. Vergünstigte Spartickets waren nur mit Kundenkonto über das Internet bzw. in einer App erhältlich. Später waren die Tickets auch am Schalter zu kaufen. Doch hier war für die Ausstellung eines Tickets die Angabe einer E-Mail-Adresse bzw. einer Mobiltelefonnummer erforderlich. Dorthin wurde ein Code geschickt, mit dem das Ticket in die App geladen werden konnte. Wollte man keine E-Mail-Adresse oder Mobiltelefonnummer angeben, blieb nur der Kauf nicht vergünstigter Tickets beispielsweise am Fahrscheinautomaten.

Verbraucherschützer klagen

Zwar hat die Bahn die Praxis geändert, sodass ein Erwerb von Spartickets am Schalter auch ohne Angabe einer E-Mail-Adresse oder Mobiltelefonnummer möglich ist. Das hielt jedoch den Dachverband von 16 Verbraucherzentralen nicht davon ab, die Bahn nach dem Unterlassungsklagengesetz (UKlaG) zu verklagen. Aus Sicht der Verbraucherschützer war die Verarbeitung der personenbezogenen Daten im Zusammenhang mit den Spartickets, sprich eine Angabe von E-Mail-Adresse oder Mobiltelefonnummer am Schalter, für die Erbringung der Beförderungsleistung nicht erforderlich.

Das OLG Frankfurt sah das im Ergebnis genauso. Es verurteilte die Bahn zur Unterlassung. Die Bahn darf also nicht E-Mail-Adressen oder Mobiltelefonnummern von Verbrauchern im Zusammenhang mit dem Verkauf von Spartickets verarbeiten, wenn gleichzeitig nicht vergünstigte Tickets ohne Angaben gekauft werden können und keine Kaufmöglichkeit der vergünstigten Tickets ohne Angabe von E-Mail-Adresse bzw. Mobiltelefonnummer besteht.

So entschieden die OLG-Richter

Den Verbraucherschützern steht ein Unterlassungsanspruch aus § 2 Abs. 1, Abs. 2 Nr. 13 UKlaG in Verbindung mit Art. 5 Abs. 1 Buchst. a DSGVO zu. Die im Zusammenhang mit dem Erwerb von Spartickets zwingende Angabe von E-Mail-Adresse bzw. Mobiltelefonnummer führte zu einer Datenverarbeitung. Diese war nicht rechtmäßig.

Rechtsgrundlagen fehlen

Es liegt keine Einwilligung in die Verarbeitung personenbezogener Daten vor (Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO). Entscheidend für die Wirksamkeit einer Einwilligung ist der Aspekt der Freiwilligkeit. Der Betroffene muss eine echte und freie Wahl haben. Er muss die Einwilligung ohne Nachteile verweigern oder zurückziehen können.

Aus Art. 7 Abs. 4 DSGVO (sogenanntes Koppelungsverbot) ergibt sich, dass eine Einwilligung unfreiwillig erteilt sein kann, wenn die Erfüllung eines Vertrags von einer Einwilligung in eine Verarbeitung abhängig gemacht wird, die für die Vertragserfüllung nicht erforderlich ist. Es fehlt gerade dann an der Freiwilligkeit, wenn dem Betroffenen faktisch nur eine bestimmte Entscheidung bleibt, um die vertragliche Leistung zu erhalten. Dass ein Betroffener eine echte Wahl hat, muss der Verantwortliche nachweisen. Voraussetzung hierfür ist, dass dem Betroffenen tatsächlich eine gleichwertige Alternative ohne Datenpreisgabe angeboten wurde. Hierbei muss auch eine marktbeherrschende Stellung berücksichtigt werden.

Vorliegend wurde die Vertragserfüllung von einer Einwilligung abhängig gemacht, und zwar für eine Verarbeitung, die für die Vertragserfüllung nicht erforderlich war. Eine Beförderung ist auch ohne diese Informationen möglich. Eine Verweigerung der Einwilligung war nicht möglich, ohne Nachteile zu erleiden.

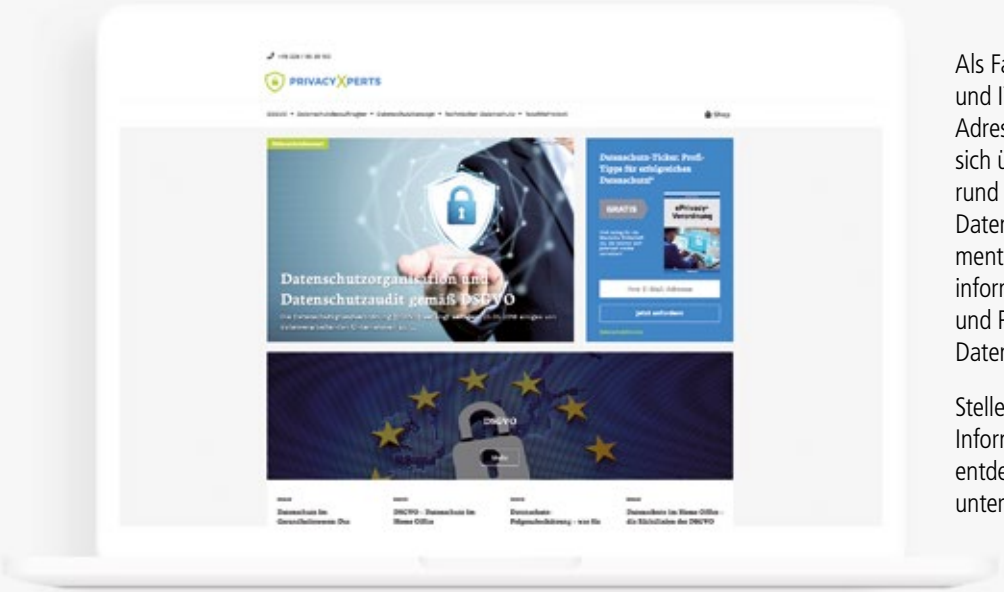
Auch ist die Verarbeitung nicht zur Vertragserfüllung (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO) erforderlich. Hierfür hätte sie für den konkreten Vertragszweck notwendig sein müssen. Ein Nützlichsein reicht nicht aus. Die Leistung kann auch ohne digitale Tickets erbracht werden.

Zudem scheidet als Rechtsgrundlage das überwiegende berechtigte Interesse (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO) aus. Hier fehlt es an der Erforderlichkeit. Zwar mag bestmögliche Effizienz ein berechtigtes Interesse sein. Allerdings lässt sich das Ziel auch mit anderen Mitteln erreichen, die weniger in die Rechte der Betroffenen eingreifen. Es hätte auch für die Spartickets ein Weg gewählt werden müssen, der mit dem geringsten Maß an personenbezogenen Daten auskommt.

§ Das können Sie aus der Entscheidung folgern

Rechtsgrundlagen müssen genau geprüft werden. Nur weil etwas aus Sicht des Verantwortlichen besonders praktisch oder wirtschaftlich ist, heißt das noch nicht, dass es datenschutzrechtlich zulässig ist. Es kommt häufig entscheidend auf die Erforderlichkeit an. Auch das Koppelungsverbot ist nicht zu unterschätzen.

„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**

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