DATENSCHUTZAKTUELL
FEB II 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

NEUES BSI-GESETZ IN KRAFT: DAS SOLLTEN SIE DAZU WISSEN

Sorgen Sie für positive Erfahrungen

Liebe Leserin, lieber Leser,

Datenschutz zählt bei vielen Menschen nicht gerade zu den Themen, die Begeisterungsstürme auslösen. Das ist vielleicht auch bei manchem Entscheider oder Projektverantwortlichen in Ihrem Unternehmen so.

Und dennoch können Sie viel dafür tun, dass alle den Datenschutz positiv wahrnehmen und nicht als notwendiges Übel. Sorgen Sie beispielsweise für positive Erfahrungen bei Ratsuchenden. Gestalten Sie Ihre Beratungen freundlich, praxisnah und lösungsorientiert. Zeigen Sie auf, wie man die Dinge richtig angeht und Probleme vermeidet. Findet man Sie und die Arbeit mit Ihnen gut, haben Sie viel erreicht.

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

Zu Ihrem Onlinebereich:!
https://www.privacyxperts.de/

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 | rcx_3; Seite 1: Adobe Stock | MQ-Illustrations

Erscheinungsweise: 26-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Die Neuerungen sind seit 6.12.2025 in Kraft.

Neues BSI-Gesetz in Kraft: Das sollten Sie dazu wissen

Schon seit einigen Monaten waren die NIS-2-Richtlinie der EU und das diesbezügliche deutsche Umsetzungsgesetz in aller Munde. Nachdem sich die deutschen Regelungen zur Stärkung der Cybersicherheit verzögerten, sind sie nun seit 6.12.2025 in Kraft. Weil auch Sie mit den Neuerungen in Berührung kommen können, sollten Sie dazu gut Bescheid wissen.

Was ist im Dezember 2025 in Kraft getreten?

Schon länger gibt es die NIS-2-Richtlinie der EU, die Richtlinie (EU) 2022/2555. Damit soll ein hohes gemeinsames Cybersicherheitsniveau in den Mitgliedstaaten geschaffen werden. Eine Richtlinie gibt jedoch nur die Mindeststandards vor. Die Mitgliedstaaten müssen die Vorgaben der Richtlinie in eigenen Gesetzen umsetzen. Umsetzungsfrist war bis Oktober 2024. Deutschland brauchte etwas länger, bis es das entsprechende „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" unter Dach und Fach hatte. Die letzten Hürden waren Anfang Dezember 2025 genommen, sodass die Regelungen am 6.12.2025 in Kraft getreten sind.

Welches Gesetz ist in Deutschland besonders betroffen?

Mit dem Umsetzungsgesetz wurden in Deutschland verschiedene Gesetze angepasst. Für Unternehmen dürfte in erster Linie das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI) und über die Sicherheit in der Informationstechnik von Einrichtungen", kurz BSI-Gesetz (BSIG), von Bedeutung sein. Dort sind nämlich die Anforderungen zu relevanten Maßnahmen im Bereich Cybersecurity im Unternehmensumfeld geregelt.

Welche Unternehmen müssen das BSIG einhalten?

Das hängt vor allem davon ab, ob man als wichtige oder besonders wichtige Einrichtung einzuordnen ist. Hier ist entscheidend, dass sich Ihr Unternehmen ganz genau die Anforderungen aus § 28 BSIG anschaut.

Auf den Punkt gebracht ist ein Unternehmen so einzustufen:

Besonders wichtige Einrichtungen (§ 28 Abs. 1 BSIG) sind

- natürliche oder juristische Personen, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und
- die einer der in der Anlage 1 BSIG bestimmten Einrichtungsarten zuzuordnen sind und
- die mindestens 250 Mitarbeiter beschäftigen oder
- einen Jahresumsatz von über 50 Mio. € und eine Jahresbilanzsumme von über 43 Mio. € haben.

Daneben sind bestimmte Einrichtungen generell als besonders wichtige Einrichtung eingestuft (§ 28 Abs. 1 Nr. 1–3 BSIG), etwa Betreiber kritischer Anlagen und große Betreiber öffentlicher Telekommunikationsnetze.

Wichtige Einrichtungen (§ 28 Abs. 2 BSIG) sind:

- natürliche oder juristische Personen, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und
- die einer der in den Anlagen 1 und 2 zum BSIG genannten Einrichtungsarten zuzuordnen sind und
- bei denen die für die Zuordnung relevante Geschäftstätigkeit nicht vernachlässigbar ist (§ 28 Abs. 3 BSIG) und
- die mindestens 50 Mitarbeiter beschäftigen oder
- einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mehr als 10 Mio. € haben.

Daneben können auch Vertrauensdiensteanbieter oder kleine Anbieter von öffentlich zugänglichen Telekommunikationsdiensten generell als wichtige Einrichtung gelten (§ 28 Abs. 2 Nr. 1 und 2 BSIG).

Auch indirekte Anwendbarkeit möglich

Unter Umständen ist Ihr Unternehmen Vertragspartner, Zulieferer oder Dienstleister einer verpflichteten Einrichtung. Dann kann es passieren, dass Ihr Unternehmen vertraglich verpflichtet wird, bestimmte Anforderungen zu erfüllen. Gerade wenn Ihr Unternehmen mit wichtigen und besonders wichtigen Einrichtungen zusammenarbeitet, sollte auch in Verträgen auf besondere oder zusätzliche Verpflichtungen im Bereich Cybersecurity geachtet werden. Verpflichtet sich Ihr Unternehmen zur Umsetzung von Anforderungen, ist es erst einmal vertraglich daran gebunden. Verträge sind zu erfüllen.

Was müssen betroffene Unternehmen tun?

Ist Ihr Unternehmen grundsätzlich als wichtige oder besonders wichtige Einrichtung anzusehen, ist eine weitere wichtige Prüfung nötig. Für bestimmte Einrichtungen gelten manche Vorgaben des BSIG nämlich nicht. Hier ist der Blick in § 28 Abs. 5–7 BSIG erforderlich. Beispielsweise Betreiber öffentlicher Telekommunikationsnetze oder Finanzunternehmen müssen manche Anforderungen nicht erfüllen.

Gilt Ihr Unternehmen jedoch als wichtige oder besonders wichtige Einrichtung und greifen die Ausnahmen nicht, müssen verschiedene Anforderungen erfüllt werden. Umzusetzen ist insbesondere Folgendes:

- **Risikomanagement**
  § 30 Abs. 1 BSIG gibt hier den Rahmen vor. Entsprechend verpflichtete Einrichtungen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen. Damit sollen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse vermieden und Auswirkungen von Sicherheitsvorfällen möglichst gering gehalten werden. Konkretere Anforderungen zu den nötigen Maßnahmen ergeben sich aus § 30 Abs. 2 BSIG.
- **Meldung von Vorfällen**
  Kommt es zu Sicherheitsvorfällen bei wichtigen oder besonders wichtigen Einrichtungen, müssen diese unverzüglich, jedoch je nach Umständen spätestens innerhalb 24 Stunden (Erstmeldung) oder 72 Stunden (Nachmeldung) nach Kenntniserlangung an die Behörde gemeldet werden. Die Anforderungen und Rahmenbedingungen hierzu, etwa zum Inhalt der Meldung, ergeben sich aus § 32 BSIG. Bei erheblichen Sicherheitsvorfällen müssen ggf. auch Kunden informiert werden (§ 35 BSIG).
- **Registrierung**
  Einrichtungen, die als besonders wichtige oder wichtige Einrichtung, eingestuft sind, müssen sich mit bestimmten Informationen beim Bundesamt registrieren (§§ 33, 34 BSIG).
- **Pflichten der Geschäftsleitung**
  § 38 BSIG legt fest, dass die Geschäftsführung eine Umsetzungspflicht in Sachen Risikomanagement (§ 30 BSIG) trifft und die Umsetzung überwachen muss. Zudem muss sie regelmäßig an Schulungen teilnehmen. Ferner steht fest: Für die Verletzung ihrer Pflichten für schuldhaft verursachte Schäden kann die Geschäftsleitung in Haftung genommen werden.
- **Nachweispflichten und Audits**
  Für Betreiber kritischer Anlagen besteht etwa die Pflicht zum Nachweis, dass die Anforderungen zum Risikomanagement erfüllt werden, und zwar alle drei Jahre (§ 39 Abs. 1 BSIG). Zudem können vom Bundesamt Audits und Prüfungen bei besonders wichtigen Einrichtungen angeordnet werden (§ 61 Abs. 1 BSIG).

Gibt es eine Übergangsfrist zur Umsetzung der Anforderungen?

Eine Übergangsfrist ist nicht vorgesehen. Das heißt also: Verpflichtete Unternehmen, sprich wichtige und besonders wichtige Einrichtungen, müssen seit dem 6.12.2025 die an sie gerichteten Anforderungen erfüllen. Zählt Ihr Unternehmen zu den verpflichteten Einrichtungen, ist schnelles Handeln oberstes Gebot. Das umfasst insbesondere folgende Aktivitäten:

- **Team zusammenstellen**
  So bewerten etwa Vertreter aus Unternehmensleitung, IT-Abteilung und anderen relevanten Bereichen, inwieweit man betroffen und was unverzüglich in die Wege zu leiten ist.
- **Know-how aufbauen oder beschaffen**
  Gerade wenn es um passende Maßnahmen zum Risikomanagement geht, ist viel praxisnahes Know-how gefragt. Das kann in Ihrem Unternehmen selbst aufgebaut werden, dauert aber. Eventuell muss das Wissen auch von externen Spezialisten kommen.
- **Maßnahmen schnellstens umsetzen**
  Weil es keine Übergangsfristen gibt, muss Ihr Unternehmen die notwendigen Maßnahmen schnell in Angriff nehmen und umsetzen. Das heißt einerseits schnell einer Registrierungspflicht nachkommen und andererseits die nötigen Schutzmaßnahmen in Angriff nehmen.

Wie teuer kann ein Verstoß werden?

Verpflichtete Unternehmen sollten die Sache nicht auf die leichte Schulter nehmen. Falls noch nicht geschehen, sollte bezüglich der Umsetzung keine Zeit verloren werden. Der Grund: § 65 BSIG sieht für zahlreiche Verstöße hohe Bußgelder vor. Die können bei Vorliegen der Voraussetzungen bis zu 10 Mio. € oder bis zu 2 % des Gesamtumsatzes liegen.

Welche Rolle spielen Datenschutz und Sie als Datenschutzbeauftragter?

Als Profi wissen Sie: Wenn es um die Verarbeitung personenbezogener Daten geht, gibt die Datenschutz-Grundverordnung (DSGVO) den Rahmen vor. Daran ändern auch die neuen Regelungen zur Stärkung der Cybersecurity nichts. Insofern ändert sich auch nichts an Ihrer Rolle oder an Ihren Aufgaben. Dabei ist jedoch wichtig: Sollen Sie auch im Bereich der neuen Vorgaben aus dem BSIG beraten, brauchen Sie nicht nur nötiges Fachwissen. Sie müssen es bei einem Beraten oder Empfehlen belassen. Es darf nämlich nicht dazu kommen, dass Sie im Zusammenhang mit der Verarbeitung personenbezogener Daten Entscheidungen treffen. Das kann nämlich schnell einen Interessenskonflikt verursachen. Und der muss vermieden werden (Art. 38 Abs. 6 Satz 2 DSGVO).

Mit Frage kalt erwischt worden? So schaffen Sie die Wende

Sie kennen das vielleicht: Sie sind mit dem Geschäftsführer in einem Termin oder jemand aus dem oberen Management spricht Sie zwischen Tür und Angel an. Er fragt Sie, wie eine bestimmte Sache einzuschätzen ist. Doch irgendwie haben Sie zum umrissenen Thema keinen blassen Schimmer. Doch das müssen Sie niemanden merken lassen. Seien Sie ganz Profi!

Niemand hat auf alles eine Antwort

Das ist einfach so – und das ist auch völlig in Ordnung. Egal ob Politiker, Manager oder Nobelpreisträger, es gibt immer Themen, bei denen man ins Schwimmen kommen kann oder bei denen fundiertes Wissen einfach Fehlanzeige ist. Warum also sollte das bei Ihnen und beim Datenschutz anders sein? Gerade weil Datenschutz komplex ist und auch eher banal erscheinende Fragen oft eine gründliche Recherche erfordern, müssen Sie sich keine Sorgen machen, wenn Sie auf Anhieb eben keine Antwort parat haben. Selbst die alten Hasen unter den Datenschutzbeauftragten können nicht jede Frage aus dem Stegreif beantworten. Und: Qualität braucht Zeit. Auch wenn manche meinen, dass Sie das lebende Datenschutzlexikon sind, ist es nur normal, wenn Sie nicht immer sofort eine Antwort parat haben. Denn qualifizierte Beratung braucht eben Zeit, etwa zum Nachdenken.

Ihre Erfolgsformel: die Gegenfragen-Technik

Unerwartete Fragen in größerer oder prominent besetzter Runde können für Sie eine große Herausforderung sein. Allerdings können Sie die Situation souverän meistern und müssen gerade nicht vorschnell etwas äußern, was Sie vielleicht später bereuen. Der Schlüssel zum Erfolg liegt einerseits darin, dass Sie zunächst Ruhe bewahren. Halten Sie inne und wenden Sie sich persönlich und freundlich an den Fragenden. Setzen Sie dann auf die Gegenfragen-Technik. Mit gezielten Gegenfragen können Sie nämlich Zeit gewinnen, wichtige Details in Erfahrung bringen und aktiv das Gespräch steuern.

Diese Gegenfragen funktionieren immer

Prägen Sie sich die folgenden Gegenfragen ein. Finden Sie sich in einer entsprechenden Situation wieder, werden Sie sich garantiert daran erinnern. Und Sie werden ganz schnell merken, wie erfolgreich Sie damit im Gespräch aus der Defensive in die Offensive kommen.

Wie soll die Verarbeitung bzw. der Verarbeitungsprozess konkret aussehen?

Lassen Sie sich das Vorhaben von A bis Z beschreiben. Das bedeutet nicht[M1] , dass Ihr Gesprächspartner bei Adam und Eva anfangen soll. Das kann eben auch bedeuten, dass erklärt werden soll, welche Daten bei wem für was beschafft werden sollen.

Wer trägt die Verantwortung für das Ganze?

Derjenige, der Sie fragt, ist unter Umständen nicht verantwortlich und verfügt gegebenenfalls dann auch nicht über alle Informationen. Sitzt der intern Verantwortliche nicht mit am Tisch, können Sie geschickt die weitere Diskussion vertagen. Schließlich sollte derjenige mit eingebunden sein, der über das Ob und Wie konkret entscheidet.

Für welchen Zweck sollen welche Daten verarbeitet werden?

Auch damit können Sie viel Zeit gewinnen. Denn oft kommen hier zunächst einfach nur Allgemeinplätze. Fragen Sie konkret nach, welches Ziel mit einer Verarbeitung bestimmter personenbezogener Informationen verfolgt wird. Wiederholen Sie das Ganze nochmals in eigenen Worten, gewinnen Sie nicht nur Zeit und stellen sicher, dass Sie alles richtig verstanden haben. Auch zeigen Sie Ihrem Gegenüber, dass Sie ihn und sein Anliegen ernst nehmen.

Auf welcher Rechtsgrundlage soll die Verarbeitung basieren?

Meist wird es auch hier schnell etwas dünn oder es wird einfach nur eine allgemeine Antwort präsentiert. Bei jeder Rechtsgrundlage können Sie nämlich nachbohren. Nennt man Ihnen beispielsweise die Einwilligung, können Sie nach dem konkreten Entwurf und den Umständen fragen.

Liegt schon ein Konzept oder eine Projektbeschreibung vor?

Gerade wenn es komplexer wird, geht es nicht ohne solche Beschreibungen. Je komplexer die Sache ist, desto eher wird man Verständnis haben, dass Sie nicht direkt eine Antwort präsentieren können. Vielmehr müssen Sie sich die Sache erst einmal anschauen. Erst dann können Sie konkrete Hinweise geben.

Wer ist an der Verarbeitung beteiligt?

Heutzutage wird vieles unter Einbindung von Dienstleistern erledigt. Ist das der Fall, können Sie die Zusammenarbeit hinterfragen. Fragen Sie etwa, ob der Dienstleister als Auftragsverarbeiter tätig werden soll und wie man die Sache regeln will.

Inwieweit ist bereits eine Risikoanalyse erfolgt?

Risikoangemessener Schutz ist ein tragendes Element des Datenschutzes. Nicht selten ist hier nichts an Analyse passiert, weil man vielleicht meint, dass Sie das machen. Spielen Sie den Ball zurück und fordern Sie eine entsprechende Analyse mit Ableitung der passenden Maßnahmen ein.

Liegen die Angaben für das Verzeichnis von Verarbeitungstätigkeiten vor?

Das ist die Frage schlechthin, um Zeit zu gewinnen bzw. eine Diskussion zu beenden. Denn meist beschäftigt sich niemand damit, die relevanten Informationen zusammenzustellen. Machen Sie klar, dass die Informationen für Ihre Beratung und Bewertung entscheidend sind.

Verarbeitungsverzeichnis: Machen Sie den Check

Das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ist vielleicht für manchen in Ihrem Unternehmen ein rotes Tuch. Und vielleicht sind auch Sie kein Freund der betreffenden Dokumentationspflicht. Doch wie dem auch sei: Es ist nicht nur Nachweis, sondern auch Arbeitsmittel für Sie. Grund genug also, dass Sie prüfen, ob alles passt.

Gehen Sie die Prüfung planvoll an

Das Verzeichnis von Verarbeitungstätigkeiten, gerne auch als Verfahrensverzeichnis oder Verarbeitungsverzeichnis bezeichnet, hat es in sich. Häufig passt es hier und da nicht so ganz oder Angaben sind falsch bzw. fehlen. Und weil das Verzeichnis eigentlich gar nicht von Ihnen zu führen, sondern Ihnen vom Verantwortlichen bereitzustellen ist, kann die Qualität dieses Arbeitsmittels fraglich sein. Doch das Verzeichnis ist ein wichtiges Arbeitsmittel für Sie: Denn damit können Sie leichter Risiken ausmachen, Schwerpunkte für Ihre Arbeit setzen und auch bei der Bearbeitung von Betroffenenrechten leichter unterstützen. Gehen Sie Ihre Prüfung planvoll an, indem Sie die folgenden Schritte umsetzen.

Beugen Sie Frust vor

Je nach Größe des Unternehmens oder der Zahl und Komplexität der Verarbeitungstätigkeiten kann ein Check eine große Herausforderung sein. Daher: Sie sollten besser nicht alles auf einmal machen. Nehmen Sie sich beispielsweise vor, jeden Schritt in einer Woche zu erledigen. Dann kommen Sie auch ziemlich schnell zum Ziel, vermeiden aber, dass Sie sich überfordern und frustriert aufgeben.

So gestalten Sie Ihre Prüfung

Damit Ihre Prüfung Hand und Fuß hat, können Sie folgende Schritte abarbeiten:

Schritt 1: Bereiten Sie sich gut vor

- Eine gute Vorbereitung bedeutet, dass Sie sich zunächst mit Art. 30 DSGVO vertraut machen. Schauen Sie dazu in Gesetzeskommentare, um einen guten Überblick über die Rahmenbedingungen zu haben. Das kann für spätere Gespräche wichtig sein.
- Prüfen Sie, welche Vorgaben, Regelungen oder Prozesse es gibt, etwa damit die relevanten Informationen ihren Weg ins Verzeichnis finden. Gibt es noch keine Festlegung, etwa eine von der Unternehmensleitung freigegebene Arbeitsanweisung, sollten Sie das vielleicht als eine erste Maßnahme zügig angehen.
- Machen Sie ein Brainstorming: Überlegen Sie, was hat sich in letzter Zeit verändert, etwa zur Geschäftstätigkeit oder Organisation des Unternehmens. Auch neue oder veränderte Verarbeitungsprozesse sollten Sie notieren. Schreiben Sie alles auf, was Ihnen im Hinblick auf neue oder veränderte Verarbeitungen einfällt. Sortieren Sie später, was von Relevanz ist.
- Schauen Sie sich das aktuelle Verzeichnis an. Notieren Sie sich Auffälligkeiten, etwa offensichtliche Lücken oder Unvollständigkeiten. Auch dass das letzte Update schon lange her ist, ist eine wichtige Information.
- Bewerten Sie die Risikosituation. Das kann die Datenschutzsituation Ihres Unternehmens betreffen oder auch Verarbeitungstätigkeiten. Wo die größeren Risiken liegen, sollten Sie zuerst hinschauen und aktiv werden.

Schritt 2: Gehen Sie bei wichtigen Verarbeitungen ins Detail

Es ist unerlässlich, dass Sie sich zumindest die kritischen bzw. risikobehafteten Verarbeitungstätigkeiten genauer anschauen. Prüfen Sie hier nicht nur, ob etwa alle Angaben nach Art. 30 Abs. 1 DSGVO enthalten und aktuell sind. Schauen Sie insbesondere auch, inwieweit die vorgesehenen Schutzmaßnahmen noch zur aktuellen Risikosituation passen. Hier kann auch ein Blick in Sicherheitskonzepte nötig sein. Denn auch die sollten auf der Höhe der Zeit sein und den bestehenden Gefahren und Risiken angemessen Rechnung tragen.

Schritt 3: Sprechen Sie mit den Verantwortlichen

Gehen Sie hier nicht auf Konfrontation und vermeiden Sie Vorwürfe. Das ist Ihrer Sache nicht dienlich. Gibt es Unzulänglichkeiten, etwa weil Informationen veraltet sind oder fehlen, zeigen Sie auf, warum sich das ändern muss. Will man die Notwendigkeit nicht erkennen, sollten Sie das generelle „Unterstützungsproblem" mit der Unternehmensleitung besprechen.

Schritt 4: Fordern Sie aktuelle Informationen an

Machen Sie klar, dass man die nötigen Informationen für das Verzeichnis zügig bereitstellt. Verdeutlichen Sie, dass man Ihnen die Informationen liefern muss und es nicht Ihre Sache ist, sich die Informationen zu organisieren. Geben Sie beratende Unterstützung.

Schritt 5: Machen Sie den Vollständigkeits- und Plausibilitätscheck

Nur weil Sie etwas fordern, muss das nicht bedeuten, dass man dem auch wie gewünscht oder erforderlich nachkommt. Werden Informationen bereitgestellt oder in das Verzeichnis integriert, sollten Sie prüfen, ob das Verzeichnis damit rund ist. Prüfen Sie insbesondere, ob die gemachten Angaben passen können. Mit „Copy and Paste" will sich mancher Schlaumeier die Arbeit schnell vom Tisch schaffen. Das jedoch kann wiederum das Verzeichnis zu einem weniger guten oder unbrauchbaren Arbeitsmittel machen. Auch für diese Prüfung können Sie auf die folgende Checkliste setzen.

Checkliste: Passt das Verzeichnis von Verarbeitungstätigkeiten?

Das können Sie prüfen	Das ist wichtig	Geprüft und in Ordnung?
Ist das Verzeichnis an sich verfügbar und nutzbar?	› Das Verzeichnis muss nicht von Ihnen geführt werden. Vielmehr ist es Ihnen bereitzustellen. Wird das so in Ihrem Unternehmen gehandhabt, sollten Sie leicht auf das Verzeichnis und die Inhalte zugreifen können. › Bewerten Sie auch die Praktikabilität und Übersichtlichkeit. Ein spezielles System muss es nicht sein. Geht es um wenige Verarbeitungstätigkeiten, kann auch das Führen einer Tabelle mit Standardsoftware völlig ausreichen.	○ Ja ○ Nein
Wann wurde das Verzeichnis erstellt und wann wurde es zuletzt aktualisiert?	› Schauen Sie auf das Datum der Ersterstellung. Ist das schon lange her, kann das darauf hindeuten, dass auch der Inhalt weniger stimmig oder insgesamt schon angestaubt ist. › Prüfen Sie die letzte Überprüfung des Verzeichnisses oder bestimmter Verarbeitungstätigkeiten. Gab es Neuerungen, aber kein danach liegendes Aktualisierungsdatum, passen die Informationen eventuell nicht mehr.	○ Ja ○ Nein
Von wem stammen die Inhalte?	› Hinterfragen Sie, wer die Informationen für das Verzeichnis bereitstellt. Das ist gerade dann wichtig, wenn Sie als Datenschutzbeauftragter eher nicht eingebunden sind. › Achten Sie auch darauf, inwieweit die bereitstellenden Personen über das nötige Wissen verfügen. Vieles ist auch beim Verzeichnis nicht selbsterklärend. Schnell sind dann Informationen falsch oder haben nicht die erforderliche Aussagekraft.	○ Ja ○ Nein
Welche Regelungen und Prozesse gibt es bezüglich des Verzeichnisses?	› Vorgaben und Prozesse können erheblich dazu beitragen, dass die Qualität des Verzeichnisses in Ordnung ist und die Inhalte passen. Prüfen Sie, inwieweit Regelungen vorhanden sind und praxisnah das Vorgehen beschreiben. › Gibt es keine Vorgaben oder Regelungen, sollten Sie das direkt auf Ihre To-do-Liste nehmen.	○ Ja ○ Nein
Wurden alle neuen oder erheblich veränderten Verarbeitungstätigkeiten aus 2025 aufgenommen?	› Haben Sie ein Brainstorming dazu gemacht, prüfen Sie, ob Sie alles von Ihnen Identifizierte im Verzeichnis wiederfinden. › Achten Sie darauf, dass die Informationen mit Beginn der Verarbeitung verfügbar sein müssen. Fehlende Verarbeitungstätigkeiten sollten Sie direkt anmahnen.	○ Ja ○ Nein
Sind alle bekannten Verarbeitungstätigkeiten enthalten?	› Schauen Sie sich insgesamt an, ob alle Ihnen bekannten Verarbeitungstätigkeiten abgedeckt sind. › Geben Sie ggf. Auszüge an verantwortliche Personen und bitten Sie um eine eventuell nötige Ergänzung der Eintragungen.	○ Ja ○ Nein
Sind alle sich aus Art. 30 Abs. 1 DSGVO ergebenden Pflichtangaben enthalten?	› Am besten Sie legen sich den Gesetzestext bereit. Gehen Sie die einzelnen Pflichtangaben durch. › Manchmal wird gerade bei den Zwecken oder den Datenkategorien „geschlampt". Achten Sie darauf, dass die Angaben konkret und aussagekräftig sind. › Stellen Sie Defizite fest, sprechen Sie die zuständigen Kollegen darauf an.	○ Ja ○ Nein
Gibt es Änderungen bei den Verarbeitungen an sich?	› Denken Sie hier an Veränderungen bei Verantwortlichkeiten oder bei strukturellen bzw. organisatorischen Aspekten. › Oft gibt es auch Vorgaben zur Verarbeitung oder den entsprechenden Prozessen. Eventuell können auch hier Veränderungen erhebliche Auswirkungen haben.	○ Ja ○ Nein
Sind die Schutzmaßnahmen noch aktuell und risikoangemessen?	› Die technischen und organisatorischen Schutzmaßnahmen im Sinne von Art. 32 DSGVO müssen risikoangemessen sein. Prüfen Sie, inwieweit sich Gefahren und Risiken verändert haben. Auch wenn sich der Stand der Technik ändert, kann es erforderlich sein, die Schutzmaßnahmen anzupassen. › Risikoanalyse und Schutzmaßnahmen sind grundsätzlich Sache des Verantwortlichen und damit der zuständigen Kollegen. Sie können sich auf das Beraten und Kontrollieren beschränken.	○ Ja ○ Nein
Passen die Löschfristen und sind sie in der Praxis umsetzbar?	› Bestehen Sie hier auf eine möglichst konkrete Festlegung. Ist diese zu schwammig, passiert in Sachen Löschen unter Umständen überhaupt nichts. › Damit das Löschen tatsächlich erfolgt, sind oft technische Maßnahmen oder organisatorische Regelungen nötig. Haben Sie auch hierauf ein Auge.	○ Ja ○ Nein
Sind die Angaben zu den Empfängern korrekt?	› Die Erfahrung zeigt, dass hier oft unsauber gearbeitet wird oder einfach ein „Keine" eingetragen wird. Meist ist das nicht zutreffend. Oft gibt es Stellen, die personenbezogene Daten erhalten. › Haben Sie besonders ein Auge auf Dienstleister und Dritte, die Daten erhalten können. Gerade Auftragsverarbeiter werden gerne vergessen. Auch das sind Empfänger im Sinne von Art. 4 Nr. 9 DSGVO.	○ Ja ○ Nein
Sind eventuelle Drittstaatentransfers zutreffend dokumentiert?	› Gibt es Datenübermittlungen in Drittstaaten, muss das im Verzeichnis festgehalten werden. So muss das betreffende Land konkret bezeichnet sein. › Prüfen Sie auch, ob dokumentiert ist, wie man für ein angemessenes Schutzniveau sorgt.	○ Ja ○ Nein
Sind Verweise und Verlinkungen noch aktuell?	› Damit das Verzeichnis noch übersichtlich bleibt, ist es sinnvoll, manches auszulagern. Denken Sie hier an Löschkonzepte, Regelwerke oder Beschreibungen der Schutzmaßnahmen. Achten Sie auch hier auf Aktualität. › Gibt es Links, sollten diese funktionieren. Ansonsten ist eine gute Beschreibung erforderlich, damit die betreffenden Dokumente leicht zu finden sind.	○ Ja ○ Nein

Warum sind Sie so wichtig? Das sind 7 starke Argumente

Die deutsche Politik will vielleicht bald Nägel mit Köpfen machen: Um angeblich die Unternehmen in Sachen Bürokratie zu entlasten, will man vielleicht auch die deutschen Sonderregeln zur Pflicht zur Benennung eines Datenschutzbeauftragten abschaffen. Dass man hier dem Datenschutz einen Bärendienst erweisen dürfte, liegt auf der Hand. Vielmehr sind Sie wichtig für Ihr Unternehmen und für den Datenschutz.

Weiß man eigentlich, was man an Ihnen hat?

Vielleicht sind Sie sich bezüglich der Antwort auf eine solche Frage nicht so ganz sicher. Und dann heißt es für Sie: Ändern Sie das schleunigst. Rühren Sie für den Datenschutz und für sich die Werbetrommel. Getreu dem Motto „Klappern gehört zum Handwerk" sollten Sie Marketing in eigener Sache betreiben. Damit können Sie nicht nur aufzeigen, wie wichtig ein Datenschutzbeauftragter für den Datenschutz und das Unternehmen ist. Sie können auch klarmachen, warum gerade Sie die richtige Besetzung für diese herausfordernde Position sind.

Setzen Sie auf die richtigen Argumente

Viele sehen den Datenschutz nur als Bremsklotz fürs Geschäft oder als großen Kostenfaktor. Doch das Positive wird oft nicht gesehen. Zeigen Sie also auf, was Sache ist. Machen Sie sich die folgenden Argumente zu eigen:

Argument Nr. 1: Sie sind der Garant für Datenschutz-Compliance

Compliance, sprich regelkonformes Verhalten, ist für jedes Unternehmen ein Muss. Und die Umsetzung des Compliancegebots steht auch für den Datenschutz nicht zur Debatte. Denn klar ist: Werden Regeln nicht eingehalten, kann das gerade im Datenschutz sehr teuer werden. Auch wenn Bußgelder vielleicht keine Millionenhöhe erreichen, gilt: Das Geld ist anderswo im Unternehmen viel besser investiert. Dass es nicht zu Bußgeldern kommt, liegt auch an Ihrer Arbeit als Datenschutzbeauftragter.

Argument Nr. 2: Sie schützen das Unternehmen vor teuren Fehltritten

Fehltritte sind nicht nur Verstöße, die in Bußgeldern enden. Schon bei der Planung und Umsetzung muss der Datenschutz mitgedacht werden. Macht man das nicht, sind spätere Reparaturmaßnahmen nicht nur aufwendig. Sie gehen meist auch richtig ins Geld. Sie sorgen mit Ihrer frühzeitigen und ergebnisorientierten Beratung dafür, dass man solche Fehltritte erst gar nicht macht.

Argument Nr. 3: Sie sichern Wettbewerbsfähigkeit und Umsatz

Will Ihr Unternehmen im Datenschutz sparen, kann das schnell nach hinten losgehen. Einerseits schläft die Konkurrenz nicht. Eventuell kann man bei Kunden, Bewerbern oder Geschäftspartnern mit umfassendem und funktionierendem Datenschutz punkten. Der kann gerade dann auf der Strecke bleiben, wenn sich niemand umfassend um den Datenschutz und die Einhaltung der geltenden Regeln kümmert. Und Teil eines funktionierenden Datenschutzes ist auch, dass sich jemand intensiv der Sache annimmt. Am besten eben ein Datenschutzbeauftragter.

Argument Nr. 4: Sie sind der zentrale Anlaufpunkt für geballtes Know-how

Auch wenn es keinen Datenschutzbeauftragten gäbe, müssten alle Regeln zum Datenschutz eingehalten werden. Um die gesetzlichen Anforderungen kommt nämlich niemand herum. Doch weil die Regeln nicht selbsterklärend sind und die Materie insgesamt ziemlich kompliziert ist, fährt ein Unternehmen besser, wenn es auf die Expertise eines Datenschutzbeauftragten setzen kann. Zudem wissen Beschäftigte, wo sie das relevante Know-how finden können, eben bei Ihnen.

Argument Nr. 5: Sie erkennen Gefahren und Risiken, bevor diese zum Problem werden

Sie halten nicht nur Ihr Wissen auf dem Laufenden. Sie beobachten auch, welche Gefahren und Risiken für Ihr Unternehmen von Relevanz sind. Zudem weisen Sie auf Probleme hin, bevor diese akut werden. Das ist ein ganz wichtiges Element im Bereich Risikovorsorge und Prävention. Das Bewerten, welche Risiken für Ihr Unternehmen konkret von Relevanz sind, schaffen nur Sie. Da sieht auch jede künstliche Intelligenz schnell alt aus.

Argument Nr. 6: Sie schützen Unternehmen und Management vor teuren Folgen

Das Unternehmen als Verantwortlicher und in der Folge die Geschäftsführung sind für die Einhaltung der Datenschutzvorschriften verantwortlich. Es muss nicht nur die Umsetzung sicherstellen, beispielsweise durch geeignete Spezialisten im Unternehmen. Es ist auch bezüglich der Umsetzung rechenschaftspflichtig und muss die Umsetzung nachweisen können. Nur mit Unterstützung eines Datenschutzbeauftragten kann das gelingen. Außerdem wichtig: Nimmt man es mit dem Datenschutz nicht so genau, kann es nicht nur für das Unternehmen teuer werden. Auch Geschäftsführer oder Manager können schnell in die Haftungsfalle tappen. Erleidet das Unternehmen durch Missmanagement im Datenschutz Schäden, muss unter Umständen die Unternehmensleitung den Kopf hinhalten.

Argument Nr. 7: Sie kosten viel weniger, als Sie für das Unternehmen bringen

Für Ihr Unternehmen steht auch im Datenschutz viel auf dem Spiel. So können Pannen und erfolgreiche Angriffe schnell die Existenz des Unternehmens bedrohen. Vor diesem Hintergrund sind die Kosten für Sie als Datenschutzbeauftragten eher ein kleiner Posten.

Muss ich mich an die Regelung der Betriebsvereinbarung halten?

FRAGE: Im von mir betreuten Unternehmen wurde ein neues System zur Zeiterfassung eingeführt. Dazu wurde auch eine Betriebsvereinbarung geschlossen. Hier war ich weder bei der Vorbereitung noch bei den Verhandlungen eingebunden. Nachdem die Vereinbarung veröffentlicht wurde, bin ich über eine Regelung gestolpert, die mich ärgert. So ist festgehalten, dass die datenschutzrechtliche Zulässigkeit des Systems von einer von mir durchgeführten Datenschutz-Folgenabschätzung abhängen soll, die positiv ausfällt. Die wäre jedoch aus meiner Sicht überhaupt nicht erforderlich. Ich frage mich in diesem Zusammenhang: Kann man das einfach so (mit mir) machen? Muss ich mich als Datenschutzbeauftragter an die Regelung der Betriebsvereinbarung halten?

ANTWORT: Führen Sie sich zunächst einige wichtige Rahmenbedingungen vor Augen:

- Das erwähnte Zeiterfassungssystem wird dafür genutzt, die Leistung bzw. das Verhalten von Arbeitnehmern zu kontrollieren. Insofern besteht ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG). Die Rahmenbedingungen zum Einsatz einer solchen technischen Einrichtung verhandeln Arbeitgeber und Betriebsrat miteinander. Ergebnis des Mitbestimmungsprozesses sind Regelungen auf Betriebsebene, die in einer Betriebsvereinbarung festgehalten sind.
- Gibt es gemeinsame Beschlüsse, etwa eine Betriebsvereinbarung, ist es grundsätzlich Sache des Arbeitgebers, diese Beschlüsse umzusetzen. Das ergibt sich aus § 77 Abs. 1 Satz 1 BetrVG. Zudem wirken Betriebsvereinbarungen unmittelbar und zwingend (§ 77 Abs. 4 Satz 1 BetrVG). So kann ein Arbeitnehmer etwa die Nutzung eines vereinbarten Systems nicht einfach ablehnen.
- Als Datenschutzbeauftragter sind Sie unabhängig. Das bedeutet insbesondere, dass Ihnen niemand vorschreiben kann und darf, wie Sie Ihre Aufgaben wahrzunehmen haben und wie Sie einen Sachverhalt beurteilen. Ihre Weisungsfreiheit ergibt sich aus Art. 38 Abs. 3 Satz 1 Datenschutz-Grundverordnung (DSGVO). Insofern kann man mit einer Regelung in einer Betriebsvereinbarung auch nicht vorschreiben, was Sie wie zu prüfen haben. Außerdem ist hier wichtig: Eine Datenschutz-Folgenabschätzung ist Sache des Verantwortlichen. Sie können diese nicht machen, sondern dabei nur beraten (Art. 35 Abs. 2, Art. 39 Abs. 1 Buchst. c DSGVO).
- Eine Datenschutz-Folgenabschätzung ist in bestimmten Fällen durchzuführen, etwa wenn ein Fall des Art. 35 Abs. 1 DSGVO gegeben ist. Bei der Zeiterfassung könnte ein entsprechender Fall vorliegen, wenn biometrische Merkmale genutzt werden sollen (Art. 35 Abs. 3 Buchst. b DSGVO). Ansonsten ist eine Zeiterfassung üblicherweise nicht mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden. Auch dürfte kein Fall der sogenannten Muss-Liste der deutschen Datenschutzaufsichtsbehörde vorliegen. Das heißt in der Folge: Es wird wahrscheinlich tatsächlich keiner Datenschutz-Folgenabschätzung bedürfen.

Mehr Mitarbeiter im Unternehmen: Habe ich jetzt Kündigungsschutz?

FRAGE: Ich bin auf freiwilliger Basis als Datenschutzbeauftragter ernannt. Nun hat sich die Mitarbeiterzahl deutlich auf über 20 erhöht. Da wir ein IT-Unternehmen sind, arbeiten auch alle mit personenbezogenen Daten. Hat das zur Folge, dass ich nun besonderen Kündigungsschutz genieße?

ANTWORT: Wird eine Benennung eines Datenschutzbeauftragten verpflichtend, greifen für den ernannten Datenschutzbeauftragten auch die Besonderheiten, etwa der besondere Kündigungsschutz nach § 38 Abs. 2, § 6 Abs. 4 Bundesdatenschutzgesetz. Damit Sie auf der sicheren Seite wären, müsste ggf. Ihre Benennung erneuert werden. Ob das aber strategisch klug ist, müssen Sie selbst beurteilen. Aktuell sind Sie freiwillig benannt. Weisen Sie auf die Sache hin, könnte Folgendes passieren: Man könnte die Benennung beenden und jemand anderen zum Datenschutzbeauftragten machen. Insofern kann es schlauer sein, erst einmal wie gehabt weiterzumachen und sich erst auf den Kündigungsschutz zu berufen, wenn es wirklich nötig wäre. Ggf. lässt sich dann argumentieren, dass aus der freiwilligen Benennung eine Pflichtbenennung wurde.

Übrigens: Prüfen Sie, ob Sie als Datenschutzbeauftragter bei der Datenschutzaufsicht gemeldet sind. Ist das der Fall, kann das dafür sprechen, dass Ihnen beim Überschreiten der Beschäftigtenzahl für eine Pflichtbenennung auch die entsprechenden Rechte zustehen.

VG Berlin: keine gemeinsame Verantwortung bei Lettershop

In Sachen Briefwerbung setzen Unternehmen oft auf das Lettershop-Verfahren. Dabei wird etwa eine Agentur beauftragt, die vom Auftraggeber vorbereitete Werbung an die nur der Agentur bekannten Adressen der Zielgruppe zu schicken. Was datenschutzrechtlich „sauber" klingt, kann dennoch zu Ärger führen, wie ein Urteil des Verwaltungsgerichts (VG) Berlin vom 14.10.2025 (Az. 1 K 74/24) zeigt.

Das führte zum Rechtsstreit

Ein Berliner Theater wollte vor Weihnachten 2021 Werbung für sein Angebot machen. Die Werbung sollte per Post erfolgen und sich an eine zahlungskräftigere Zielgruppe richten. Hierzu beauftragte das Theater einen Adresshändler. Dieser sollte das Versenden von vorbereiteter Werbung im Lettershop-Verfahren übernehmen. Das Theater stellte das Werbeschreiben bereit und wählte die Zielgruppenmerkmale. Der Adresshändler selektierte entsprechend den Wünschen des Theaters die Empfängeradressen in seinem Bestand. Im Dezember wurde die Werbung per Post verschickt.

Diese erhielt auch eine Frau in Berlin, die bislang keinerlei Bezug zum Theater hatte. Der Vater der Frau, ihr Betreuer, beschwerte sich im Januar 2022 bei der Datenschutzaufsichtsbehörde. Nachdem die Behörde das Theater mehrfach anhörte, erging am 19.1.2024 ein Bescheid gegenüber dem Theater. Darin verwarnte die Behörde das Theater wegen verschiedener Verstöße gegen die Datenschutz-Grundverordnung (DSGVO). So läge keine Rechtsgrundlage für die Verarbeitung der Adressdaten vor. Außerdem wäre gegen die Informationspflicht nach Art. 14 DSGVO sowie gegen die Vorgaben zur gemeinsamen Verantwortung nach Art. 26 Abs. 1 und Abs 2 Satz 2 DSGVO verstoßen worden. Denn nach Ansicht der Behörde läge eine gemeinsame Verantwortung zwischen Theater und Adresshändler vor.

Theater wehrt sich

Diese behördliche Verwarnung wollte das Theater nicht akzeptieren. Am 23.2.2024 klagte es vor dem VG Berlin. Aus seiner Sicht war ihm nichts vorzuwerfen. Insbesondere wäre es nicht für die Verarbeitung verantwortlich. Man habe nur Zielgruppenvorgaben gemacht. Auf die Verarbeitung der personenbezogenen Daten hätte man keinen Einfluss gehabt. Eine Rechtsgrundlage für die Werbung läge vor, nämlich Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO. Das Gericht urteilte, und zwar zugunsten des Theaters. Die Verwarnung der Datenschutzaufsichtsbehörde wurde aufgehoben.

So begründete das VG sein Urteil

Die Verwarnung der Datenschutzaufsicht ist rechtswidrig und verletzt das Theater in seinen Rechten. Auf das Vorliegen einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten kommt es vorliegend nicht an. Das Theater wäre der falsche Adressat der Verwarnung. Es war nämlich mit dem Adresshändler nicht gemeinsam Verantwortlicher im Sinne von Art. 4 Nr. 7, Art. 26 Abs. 1 Satz 1 DSGVO.

Das Verwenden der Adressdaten für das Werbeschreiben ist eine Verarbeitung, die der DSGVO unterliegt. Allerdings lag keine gemeinsame Verantwortung vor. Hierzu wäre es erforderlich, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen. Zwar können die Beteiligten in verschiedenen Phasen und in unterschiedlichem Ausmaß eingebunden sein. Auch muss nicht jeder der Beteiligten Zugang zu den betreffenden personenbezogenen Daten haben. Allerdings ist vor allem die jüngere Rechtsprechung des Europäischen Gerichtshofs (EuGH) so zu deuten: Für die Annahme einer gemeinsamen Verantwortung kommt es auf die tatsächlich im Eigeninteresse erfolgende Einflussnahme auf die Entscheidung über die Zwecke und Mittel der Verarbeitung an.

Voraussetzungen nicht erfüllt

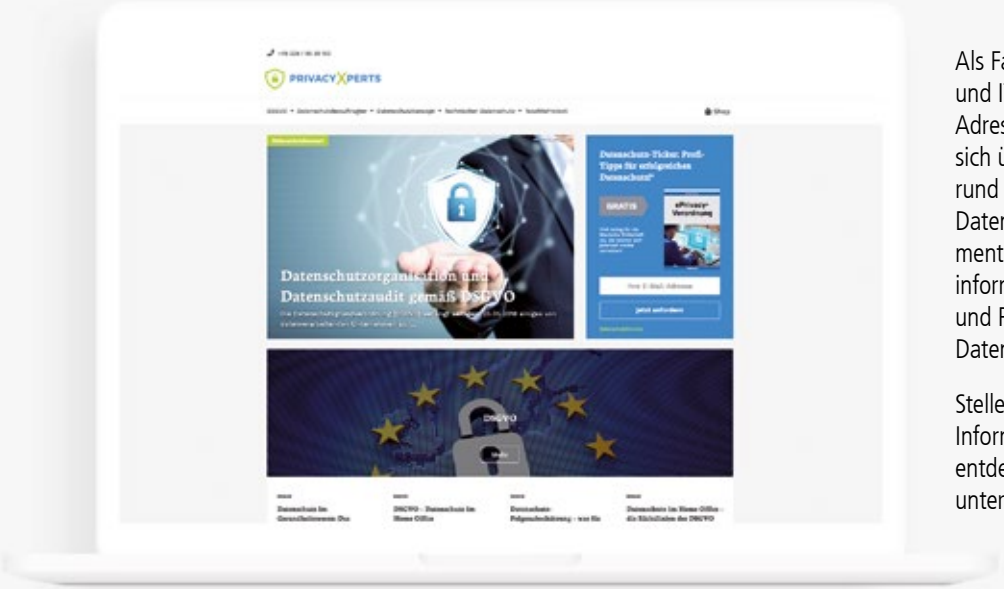
Das Theater hatte zwar im Eigeninteresse Einfluss auf die Zwecke der Verarbeitung durch den Adresshändler genommen, etwa weil es mit der Werbung wirtschaftliche Interessen verfolgte. Allerdings hatte das Theater keinen Einfluss auf die Mittel der Verarbeitung. Es gab für es keine Möglichkeit, auf die Ausgestaltung der Prozesse beim Adresshändler Einfluss zu nehmen. Das Festlegen einer Zielgruppe reicht insofern nicht aus. Es hätte eine über die Erteilung des Auftrags hinausgehende organisatorisch konzeptionelle Mitwirkung an der Datenverarbeitung geben müssen.

§

Diese Schlüsse können Sie aus dem Urteil ziehen

Datenschutzaufsichtsbehörden müssen mit ihrer Sicht der Dinge nicht immer richtigliegen. Das gilt gerade, wenn es um schwierig zu fassende Aspekte des Datenschutzrechts geht, wie vorliegend die Voraussetzungen einer gemeinsamen Verantwortung im Sinne von Art. 26 DSGVO. Zudem wird deutlich: Auch wenn es eigentlich nur um eine Verwarnung der Aufsichtsbehörde ging, kann es nötig sein, sich dagegen zu wehren. Das ist z. B. der Fall, wenn damit das wirtschaftliche Handeln Ihres Unternehmens beeinträchtigt wird. Übrigens: An die Entscheidung sollten Sie sich erinnern, wenn „gemeinsame Verantwortung" einmal Thema bei Ihrem Unternehmen ist. Das Gericht begründet seine Entscheidung auch ausführlich mit der Rechtsprechung des EuGH. Insofern können Sie sich einen schnellen und umfassenden Überblick verschaffen, worauf es bei der gemeinsamen Verantwortung ankommt.

„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**

Schnell und effektiv Mitarbeiter schulen!

Jetzt Mitarbeiterinformation bestellen

https://t1p.de/gmxhs

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