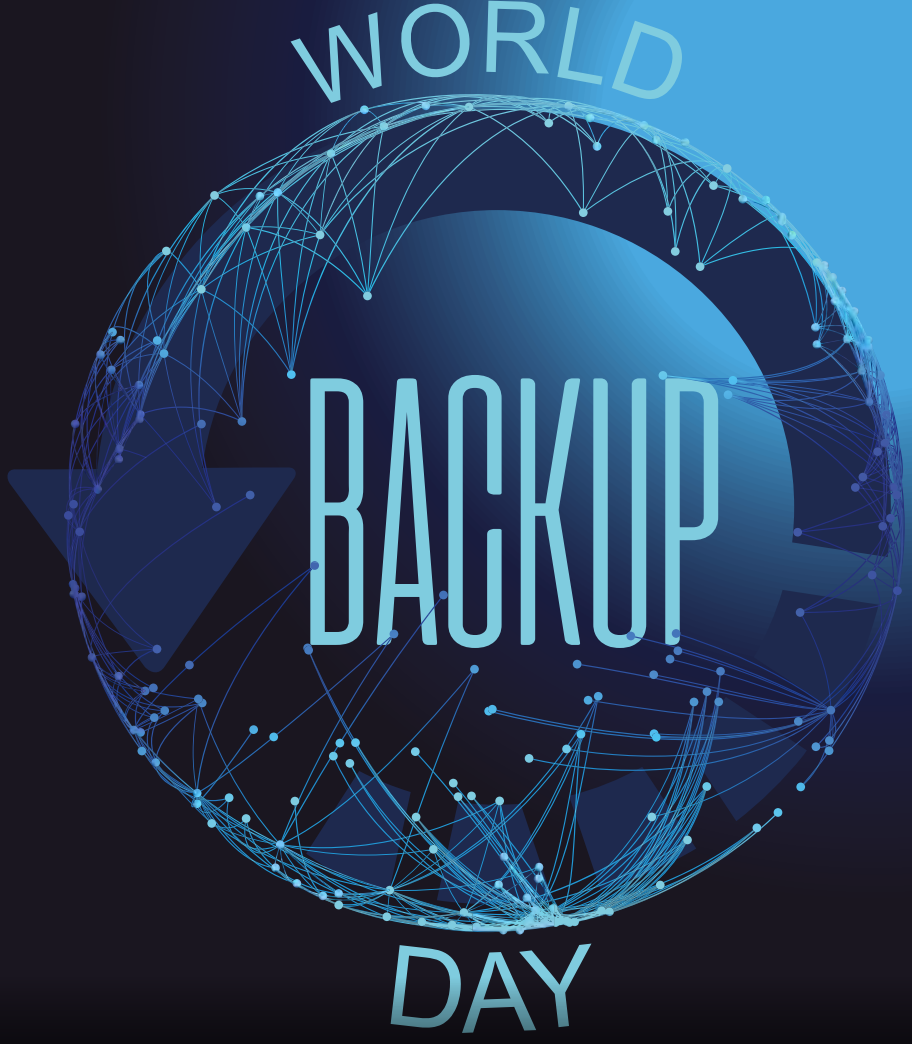
DATENSCHUTZAKTUELL
MÄR I 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH



31.3.2026: NUTZEN SIE GESCHICKT DEN „WORLD BACKUP DAY“

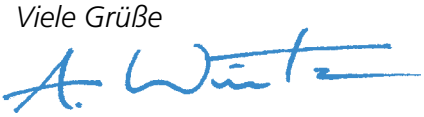
Denken Sie immer zwei Schritte weiter

Liebe Leserin, lieber Leser,

Sie kennen den Spruch „Wer A sagt, muss auch B sagen". Da ist viel Wahres dran, auch wenn Sie sich Ihre Rolle und Ihre Arbeit als Datenschutzbeauftragter vor Augen führen. Alles, was Sie beraten, bewerten oder entscheiden, hat Folgen, und zwar für Ihr Unternehmen, dessen Geschäftstätigkeit und die Beschäftigten.

Also ist es unerlässlich, dass Sie möglichst frühzeitig bedenken, welche Folgen Ihr Aktivwerden oder Ihre Entscheidungen haben können. Das bringt nicht nur allen Beteiligten etwas. Sie bewahren sich selbst davor, weniger professionell zu wirken, etwa wenn Sie Entscheidungen überdenken oder revidieren zu müssen.

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 | tubagusrachmat;
Seite 1: Adobe Stock | DoodleDaze

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.

Backups werden häufig vernachlässigt, sind aber enorm wichtig.

31.3.2026: Nutzen Sie geschickt den „World Backup Day“

Werden personenbezogene Daten verarbeitet, gibt es unzählige Herausforderungen. Manche kommen eher unscheinbar daher, etwa das Sichern von Daten. Doch Back-ups können für jedes Unternehmen überlebenswichtig sein. Nutzen Sie daher den anstehenden „World Backup Day“, um das Thema in den Fokus zu rücken.

Back-ups: die (Über-)Lebensversicherung schlechthin

Wenn es blöd läuft, kann so manches passieren, bei dem nur Back-ups eine wirkliche Chance auf Rettung bieten. Denken Sie etwa an Cyberkriminelle, die Systeme lahmlegen oder Daten verschlüsseln. Nur mit einem Back-up kann hier bald wieder weitergearbeitet werden. Doch es müssen keine Cyberkriminellen sein, um richtig große Probleme zu verursachen. Schon ein Stromausfall oder eine Spannungsspitze kann Datenträgern den Todesstoß versetzen. Gibt es kein Back-up der Daten, besteht oft nur eine geringe Chance, die Daten von den defekten Datenträgern vollständig zu retten. Zumindest wird die Wiederherstellung von Daten meist um ein Vielfaches teurer als ein rechtzeitig durchgeführtes Back-up.

Back-ups sind auch ein Datenschutzthema

Wahrscheinlich denken Sie hier zunächst daran, dass auch gesicherte Daten vor dem Zugriff Unbefugter geschützt sein müssen. Das ist richtig. Doch das ist nur das halbe Bild. Auch ein Back-up an sich ist eine Schutzmaßnahme im Sinne des Art. 32 Datenschutz-Grundverordnung. Schließlich ist durch risikoangemessene Schutzmaßnahmen auch das vom Gesetzgeber vorgegebene Ziel zu verfolgen, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Setzen Sie auf den Tag der Datensicherung

Der „World Backup Day“ am 31.3.2026 ist ein Geschenk für Sie. Schließlich können Sie ihn als Aufhänger nutzen, um die Beschäftigten auf das Thema Datensicherung aufmerksam zu machen. Dabei ist klar: Wenn es um das Vermitteln von Wissen geht, haben Sie immer zahlreiche Möglichkeiten:

- **E-Mail-Kampagne**
  Verschicken Sie am Jahrestag eine informative E-Mail, in der Sie auch einige besonders relevante Tipps geben. Für Ihren Entwurf können Sie sich an dem abgedruckten Muster orientieren. Ergänzen Sie die Tipps um solche, die speziell auf Ihr Unternehmen zugeschnitten sind. So können Sie auch auf geltende Vorgaben verweisen. Besonders nützlich können auch Links sein, die den Weg zu weiteren Informationen weisen.
- **Gemeinsame Aktivitäten mit der IT-Abteilung**
  Bei Back-ups kann es schnell sehr technisch werden. Gerade wenn Sie sich hier nicht bestens auskennen, sollten Sie mit der IT-Abteilung gemeinsame Sache machen. So können etwa Schulungen oder ein Infostand gemeinsam angeboten werden. Das bringt nicht nur zusätzliches Know-how. Sie ersparen sich auch einiges an Arbeit.
- **Virtuelle Schulungen und Trainings**
  Manches erklärt sich besser, wenn Sie es im Gespräch und anhand von praktischen Beispielen vermitteln. Zudem können sich viele Menschen mündlich viel besser ausdrücken als schriftlich. Das kann das Beantworten von Fragen erheblich erleichtern.
- **Materialien als Hilfe zur Selbsthilfe**
  Wie wäre es hier mit Anleitungen oder vertonten Präsentationen? Auch mit einer Checkliste können Sie viel Hilfestellung geben, um alles Relevante im Bereich Back-up zu bedenken oder zu prüfen. Bieten Sie flankierend an, bei aufkommenden Fragen mit Rat und Tat zur Seite zu stehen.

Muster: Informationsschreiben zum „World Backup Day 2026“

Heute ist „World Backup Day“ – leisten Sie Ihren Beitrag

Liebe Kolleginnen,
liebe Kollegen,

heute, am 31.3.2026, ist wieder „World Backup Day“, der internationale Tag der Datensicherung. Er erinnert uns daran, wie wichtig es ist, (wichtige) Daten und Informationen regelmäßig zu sichern. Denn bei Ihnen und unserem Unternehmen sollte sich nicht der in der IT-Welt gebräuchliche Spruch bewahrheiten: „No backup, no mercy“ – keine Datensicherung, kein Mitleid.

Darum sind Datensicherungen so wichtig

Klar ist natürlich: Daten auswählen und passend sichern ist mit Arbeit und Kosten verbunden. Doch der Aufwand lohnt sich immer. Denn Datensicherungen sind gerade in der heutigen Zeit eine Art Lebensversicherung für unser Unternehmen. Sie können der Rettungsanker sein, um weiter existieren zu können. Denn Back-ups sind unerlässlich gerade im Zusammenhang mit Folgendem:

Cyberangriffe: Kriminelle können Sicherheitslücken ausnutzen oder Schadsoftware einschleusen. Das Ziel: Daten werden verschlüsselt oder entwendet, um Lösegeld von unserem Unternehmen zu erpressen. Mit Back-ups minimieren wir dieses Risiko bzw. entschärfen das Druckmittel.

Technische Defekte: Alles hat eine begrenzte Lebenszeit. Wann etwa ein Datenträger das Zeitliche segnet, ist nicht wirklich vorhersehbar. Doch ist ein Datenträger kaputt, sind unter Umständen auch alle gespeicherten Daten futsch. Das kann ein großes und eventuell nicht mehr zu behebendes Problem sein.

Menschliches Versagen: Sie haben das vielleicht auch schon erlebt – ein falscher Klick und schon ist es passiert. Die Daten sind weg. Und das vielleicht für immer, wenn es keine Datensicherung gibt.

Schadensereignisse: Denken Sie hier gerade an Feuer und Wasser. Auch moderne Speichertechnik kann sensibel sein und damit nicht klarkommen. Eingedrungenes Wasser oder zu hohe Temperaturen können auch Daten killen.

Angemessene Datensicherheit: Datensicherungen sind auch unter Datenschutzaspekten wichtige Maßnahmen, um die Sicherheit der verarbeiteten Daten zu gewährleisten. Auch die Datenverfügbarkeit ist ein wichtiger Aspekt im Datenschutz. Dazu tragen Back-ups bei.

Achten Sie auf diese Back-up-Tipps

Sie meinen, Sie haben nichts, was gesichert werden müsste? Da liegen Sie garantiert falsch. Und weil es bei jedem sicherungswürdige Daten gibt, sollten Sie die folgenden Tipps rund um Back-ups beherzigen:

Finden Sie die relevanten Systeme und Daten

Schauen Sie sich in Ihrem Verantwortungsbereich, bei Ihrer Tätigkeit und in Ihrem Arbeitsumfeld um. Überlegen Sie kritisch: Welche Systeme oder Daten sind für das Unternehmen oder mich überlebenswichtig? Welche Informationen können im Fall der Fälle nicht oder nur mit erheblichem Aufwand oder Schwierigkeiten neu erstellt werden? Solche Informationen sollten regelmäßig gesichert werden.

Bewerten Sie gemeinsam die Notwendigkeit

Sprechen Sie mit Kollegen oder Vorgesetzten. Klären Sie nicht nur, wie deren Einschätzung bezüglich des generellen Sicherungsbedarfs ist. Besprechen Sie auch, für wie lange man realistisch auf bestimmte Informationen verzichten kann. Diese Einordnung ist wichtig, um eine passende Sicherungsmethode bzw. den passenden Rhythmus zu finden.

Sprechen Sie wegen der Methode mit den Profis

Was für den konkreten Fall in Sachen Back-up am besten passt und funktioniert, können Ihnen die Profis der IT-Abteilung sagen. Diese unterstützen Sie gerne dabei, leicht umsetzbare Back-up-Strategien zu entwickeln, damit Back-ups so gestaltet sind, dass sie mit minimalem Aufwand in Ihr Tagesgeschäft integriert werden können. Denn klar ist: Auch das Datensichern darf nicht auf die leichte Schulter genommen werden.

Regeln sind wichtig

Nicht immer funktionieren Back-ups automatisch. Manchmal muss es eben manuell passieren. Ist das der Fall, sind Regeln unerlässlich. Legen Sie beispielsweise abteilungsintern fest, wer wann was wie wo zu sichern hat. Doch mindestens so wichtig wie die Regeln an sich ist deren Umsetzung. Liegt das in Ihrer Zuständigkeit, überlegen Sie, wie Sie sicherstellen können, dass Sie nötige Back-ups tatsächlich durchführen.

Setzen Sie auf die 3-2-1-Regel

Diese Regel hat sich in der Praxis bewährt und ist schnell erklärt: Wichtige Daten müssen unbedingt gesichert werden. Dazu sollte es drei Kopien der Daten als Sicherungen geben, eben die Originaldaten plus zwei Sicherungen. Die beiden Sicherungen sollten auf zwei unterschiedlichen Speichermedien abgelegt sein. Ein Speichermedium und damit eine Datenkopie sollte an einem anderen sicheren Ort aufbewahrt werden. Und sicher aufbewahren sollten Sie wörtlich nehmen. Achten Sie darauf, dass die Daten vor dem Zugriff Unbefugter geschützt sind. Dazu können auch das Verschlüsseln der Daten und das Wegschließen des Datenträgers zählen.

Denken Sie auch an Software

Nicht nur Daten können sicherungswürdig sein. Das kann auch für Software bzw. Installationsdateien gelten. Gerade wenn ältere Versionen gebraucht werden, etwa um Daten oder Dateiformate lesen zu können, sollten Sie auch hier das Back-up nicht vergessen.

Testen Sie den Zugriff und die Wiederherstellbarkeit

Die beste Datensicherung ist für die Tonne, wenn Sie Ihnen im Fall der Fälle nichts bringt. Probieren Sie daher aus, ob Sie problemlos auf gesicherte Informationen zugreifen können bzw. gesicherte Daten wiederherstellbar sind.

Haben Sie Fragen?

Die IT-Abteilung und ich als Datenschutzbeauftragter stehen Ihnen gerne zur Verfügung.

Ihr Max Mustermann

5 Praxistipps für die Altgeräteverwertung

Früher oder später ist es in jedem Unternehmen so weit: Bisherige Arbeitsmittel wie Computer, Notebooks oder Smartphones werden ausrangiert und durch modernere Geräte ersetzt. Grund dafür können neben dem technischen Fortschritt auch steuerrechtliche Abschreibungsmöglichkeiten sein. Doch bei der Sache darf nicht gelten: aus den Augen, aus dem Sinn. Denn der Datenschutz ist hier wichtig.

Verwertung bzw. Entsorgung darf nicht schieflaufen

Manchmal sind es eher die kleineren oder weniger präsenten Datenschutzthemen, die große Probleme verursachen können. So ist es, wenn Computer & Co. ausgetauscht werden. Dann liegt der Fokus auf den neuen Geräten. Um die ausrangierten Geräte macht man sich vielleicht weniger Gedanken. Das sollten Sie ändern. Beraten Sie frühzeitig, wenn ein größerer Austausch ansteht oder auch vorbeugend. Beherzigen Sie dabei diese Tipps:

Tipp Nr. 1: Bringen Sie Licht ins Dunkel

Gerade wenn viele Geräte mit Datenspeichern ausrangiert werden sollen, mit denen auch personenbezogene Daten verarbeitet wurden, sollten Sie mit den verantwortlichen Kollegen oder mit der Unternehmensleitung klären, welche Geräte ausrangiert werden. Idealerweise gibt es hierzu Listen mit weiteren Informationen, etwa zu Gerätetyp, bisherigem Einsatzart, Art und Umfang der Daten(träger)verschlüsselung.

Hatte man bislang nicht über das Löschen nachgedacht, sollten Sie klarmachen, dass das unerlässlich ist. Auch beim Löschen handelt es sich um eine Maßnahme, um die Sicherheit der Verarbeitung personenbezogener Daten im Sinne von Art. 32 Datenschutz-Grundverordnung (DSGVO) zu gewährleisten.

Gehen Sie lieber vom Personenbezug aus

Vielleicht hören Sie, dass mit dem Gerät keine personenbezogenen Daten verarbeitet wurden. Das können Sie meist in Zweifel ziehen. So gibt es bestimmt Benutzerkonten auf dem Gerät. Zudem zeigt die Erfahrung, dass Geräte meist nicht nur für den Zweck genutzt werden, für den sie gedacht sind. Auch wenn Datenträger verschlüsselt sind, entfällt nicht automatisch der Personenbezug.

Tipp Nr. 2: Sorgen Sie für Sensibilität

Unter Umständen stoßen Sie nicht unbedingt auf Verständnis, dass Geräte vor der Verwertung oder vor der Entsorgung „sauber" sein müssen. Führen Sie in diesen Fällen den betreffenden Kollegen vor Augen:

- **Daten dürfen nicht in falsche Hände geraten:** Gibt es personenbezogene Daten auf Geräten, müssen diese angemessen geschützt werden, etwa vor dem Zugriff und der Kenntnisnahme Unbefugter. Die Anforderungen des Art. 32 DSGVO zur Sicherheit der Verarbeitung gelten über den gesamten Lebenszyklus von Daten bzw. der diese verarbeitenden Technik, eben von Anfang bis Ende.
- **Auch Geschäftsgeheimnisse sind schützenswert:** Jedes Unternehmen hat etwas zu verbergen. Und selbst anscheinend Belangloses kann für Dritte oder die Konkurrenz von großem Wert sein. Schon allein zu wissen, wie Ihr Unternehmen arbeitet, kann für Wettbewerber von großem Wert sein.
- **Datenpannen sorgen für großen Ärger:** Erlangen Unbefugte Kenntnis von zu schützenden personenbezogenen Daten, liegt regelmäßig eine Datenpanne vor, die oft auch der Aufsichtsbehörde zu melden ist. Zudem können Schadensersatzforderungen von Betroffenen drohen. Auch das Image des Unternehmens kann tiefe Kratzer bekommen, weil amateurhaftes Vorgehen schnell viel Vertrauen zerstört.

Tipp Nr. 3: Auf den Schutzbedarf kommt es an

Wie viel Aufwand auch in Sachen Löschen von Datenträgern getrieben werden muss, hängt vor allem davon ab, wie schutzwürdig die damit verarbeiteten Daten sind. Sind die Daten nicht besonders schutzwürdig und war der Datenträger verschlüsselt, kann es ausreichen, den Datenträger einfach nur zu löschen. Ein Überschreiben der Daten ist nicht zwingend nötig. Anders sieht die Sache bei schutzwürdigeren Daten aus. Hier kann es sinnvoll sein, selbst verschlüsselte Daten ggf. sogar mehrfach zu überschreiben. Auch was die Anforderungen an eine Software oder einen Dienstleister angeht, sollten diese mit der Schutzwürdigkeit der Daten steigen.

Tipp Nr. 4: Vorsicht bei Gerätespenden

Auch diese Idee ist weit verbreitet: Mit der ausrangierten Technik kann man noch Gutes tun. Aber: Ausrangierte Geräte sollten allenfalls blitzblank an soziale Einrichtungen, Schulen, Vereine oder Kindergärten gespendet werden. Ein vollständiges Löschen kann auch unter folgendem Aspekt wichtig sein: Lizenzen. Denn die will Ihr Unternehmen ggf. gerade nicht spenden oder die Lizenzen auf neu beschafften Geräten weiterhin nutzen.

Tipp Nr. 5: Achten Sie auf die Dokumentation

Je wichtiger es ist, dass richtig gelöscht wurde, desto wichtiger ist, dass Ihr Unternehmen die Löschung auch belegen kann. Professionelle Löschsoftware erstellt beispielsweise auch Löschprotokolle, aus denen alles Wesentliche hervorgeht. Auch beim Einsatz von Dienstleistern sollten Löschnachweise Standard sein.

Sind Ihre älteren Einschätzungen noch aktuell?

Die Zeit bleibt nicht stehen. Was vielleicht vor einigen Jahren noch „State of the Art" war, ist heute ein alter Hut. Das gilt auch für das Verarbeiten personenbezogener Daten und die damit im Zusammenhang stehende Technik. Ist auch Ihre Bewertung einer Verarbeitung schon in die Jahre gekommen, sollten Sie diese einmal auf den Prüfstand stellen.

Reviews sind wichtig

Es leuchtet schnell ein, dass ein Review, sprich eine Nachüberprüfung oder Nachbewertung, sinnvoll ist. Das vor allem, wenn Verarbeitungen personenbezogener Daten schon lange im Einsatz sind.

Dazu ein Beispiel: Sie haben vor Jahren eine Videoüberwachung datenschutzrechtlich unter die Lupe genommen und eventuell sogar eine Datenschutz-Folgenabschätzung nach Art. 35 Datenschutz-Grundverordnung (DSGVO) beratend begleitet.

Bei genauerem Hinsehen merken Sie schnell: die Zeit ist nicht stehen geblieben. Eventuell hat sich die Verarbeitung an sich verändert, weil Bereiche hinzugekommen oder weggefallen sind bzw. weil die Videoüberwachung technisch verändert wurde. Unter Umständen haben sich auch Gefahren und Risiken verändert, sodass Ihre Einschätzung anders ausfallen könnte. Dass das auch passieren kann, weil sich juristische Sichtweisen oder einschlägige Rechtsprechung ändern, liegt auf der Hand. Natürlich ist es auch Teil Ihrer Aufgaben, dass Sie (veränderte) Risiken erkennen und entsprechend darauf hinweisen bzw. beraten.

Oftmals ändert sich mehr, als man denkt

Auf den ersten Blick wirken Verarbeitungen personenbezogener Daten relativ statisch, sprich sie ändern sich kaum. Doch wenn Sie genauer hinschauen, können Sie gerade bei schon länger aktiven Verarbeitungen erhebliche Veränderungen erkennen. So z. B. im Zusammenhang mit Folgendem:

- **Zeitlicher Aspekt**
  Eine Bewertung haben Sie zu einem bestimmten Zeitpunkt vorgenommen. Inzwischen kann sich vieles verändert haben. Unter Umständen haben Sie manche durchgeführte Änderung überhaupt nicht mitbekommen. Die wurde einfach umgesetzt. Ihre Expertise als Datenschutzbeauftragter wurde nicht eingeholt.
- **Änderungen beim Sachverhalt**
  Nicht selten sehen Verarbeitungen mit der Zeit ganz anders aus. So können Anpassungen bei Betroffenengruppen oder verarbeiteten Daten vorgenommen werden. Auch interne Regelungen, Prozesse oder Verantwortlichkeiten können sich wesentlich ändern. Denken Sie vor diesem Hintergrund auch an Betriebsvereinbarungen, die eventuell spezielle Vorgaben machen, die auch auf den Datenschutz Auswirkungen haben können.
- **Veränderte rechtliche Rahmenbedingungen**
  Auch beim Recht bleibt die Zeit nicht stehen. Da wären nicht nur neue oder veränderte gesetzliche Rahmenbedingungen. Gerade Gerichte in Deutschland und auf EU-Ebene können dafür sorgen, dass manches heute anders zu sehen ist als zum Zeitpunkt Ihrer Bewertung.
- **Technischer Fortschritt**
  Denken Sie nur daran, dass heutzutage auch Software fast immer irgendetwas mit künstlicher Intelligenz zu tun hat. Zudem können neue Funktionalitäten auch neue Verarbeitungsmöglichkeiten eröffnen Das kann eine alte Verarbeitung erheblich verändern. Doch auch die Schutzmaßnahmen müssen mit der Zeit gehen.

Gehen Sie pragmatisch an die Sache ran

Eines ist klar: Sie können nicht alles auf den Prüfstand stellen. Dazu fehlen Ihnen die (zeitlichen) Kapazitäten. Also ist Risikoorientierung gefragt. Dazu können Sie sich an folgender Faustformel orientieren: Je kritischer eine Verarbeitung ist und je länger Ihre Bewertung zurückliegt, desto eher sollten Sie die Verarbeitung und Ihre Bewertung unter die Lupe nehmen. Für eine Prüfung können Sie auf folgende Checkliste setzen.

Prüfen Sie generell in 5 Schritten

Damit Ihre Prüfung Hand und Fuß hat, machen Sie Folgendes:

- **Wählen Sie die richtigen Verarbeitungen aus**
  Hier können Sie auch stichprobenhaft bzw. nach dem Zufallsprinzip vorgehen. Besser ist jedoch meist: die ältesten und kritischsten Verarbeitungen zuerst zu prüfen.
- **Beschaffen Sie sich Informationen**
  Sowohl Informationen als Basis Ihrer ursprünglichen Bewertung als auch aktuelle Informationen sind unerlässlich. Denn nur so können Sie beurteilen, ob eine veränderte Situation vorliegt.
- **Machen Sie Ihren Check**
  Prüfen Sie umfassend, ob bezüglich Ihrer Bewertung der betreffenden Verarbeitung Anpassungsbedarf besteht, etwa weil sich Rahmenbedingungen verändert haben.
- **Dokumentieren Sie Ihre Prüfung**
  Halten Sie fest, was Sie geprüft und was Sie festgestellt haben. Dokumentieren Sie Ihren Review auch bei der betreffenden Verarbeitung, etwa im Verzeichnis von Verarbeitungstätigkeiten.
- **Bewerten Sie die Dinge neu**
  Gibt es erhebliche Abweichungen zur damaligen Situation, sollten Sie die Dinge neu bewerten. Muss dann etwas an der Verarbeitung geändert werden, adressieren Sie das bei den verantwortlichen Kollegen.

Checkliste: Review früherer Bewertungen des Datenschutzbeauftragten

Aspekt	Hintergrund	Geprüft und in Ordnung?
Sind die Einträge im Verzeichnis von Verarbeitungstätigkeiten vorhanden, vollständig und offensichtlich aktuell?	› Werfen Sie einen Blick ins Verzeichnis und prüfen Sie, ob die Angaben nach Art. 30 Abs. 1 DSGVO zu den Verarbeitungstätigkeiten stimmig sind. › Finden Sie Lücken vor oder erkennen Sie, dass etwas veraltet ist, sollten Sie die Verantwortlichen bitten, für ein entsprechendes Update zu sorgen.	○ Ja ○ Nein
Von wem und von wann stammt die Bewertung?	› Eventuell stammt die Bewertung von Ihnen. Unter Umständen haben Sie jedoch auf der Vorarbeit einer anderen Person oder Ihres Vorgängers aufgebaut. › Haben Sie sich auf die Einschätzung anderer verlassen, etwa weil Sie noch nicht genügend Know-how hatten, sollten Sie die übernommene Einschätzung kritisch hinterfragen. Ggf. sehen Sie die Dinge mit dem heutigen Know-how anders.	○ Ja ○ Nein
Auf welchen Unterlagen und Informationen basiert die Einschätzung?	› Prüfen Sie, inwieweit die damaligen Bewertungsgrundlagen noch vorhanden sind. Fehlen Informationen oder Unterlagen, sollte Sie das vorsichtig werden lassen. › Schauen Sie, inwieweit Sie eine vollständige Dokumentation Ihrer Entscheidungsfindung haben. Diese kann nötig sein, um die damaligen Erwägungen heute noch nachvollziehen zu können.	○ Ja ○ Nein
Welche beurteilungsrelevanten Rahmenbedingungen galten damals?	› Führen Sie sich die Rahmenbedingungen vor Augen. Gerade bei älteren Verarbeitungen können noch andere Maßstäbe angelegt worden sein. › Haben Sie nicht nur ein Auge auf rechtliche Rahmenbedingungen. Auch betriebliche Regeln oder Organisatorisches können in Ihre Einschätzung eingeflossen sein. Eventuell sieht die Welt heute anders aus.	○ Ja ○ Nein
Gibt es Veränderungen beim der Bewertung zugrunde liegenden Sachverhalt?	› Verschaffen Sie sich Klarheit darüber, inwieweit der damalige Sachverhalt auch heute unverändert zutrifft. › Prüfen Sie insbesondere, inwieweit Zielgruppen, Verarbeitungsmodalitäten und Verarbeitungsumfang noch passen. Ist hier manches anders, kann das auch eine Neubewertung der Sache erforderlich machen.	○ Ja ○ Nein
Passen die rechtlichen Rahmenbedingungen noch?	› Im Datenschutz tut sich immer viel. Schauen Sie, inwieweit Sie Ihre Bewertung auf die aktuell gültigen gesetzlichen Regelungen gestützt haben. › Bedenken Sie auch betriebliche Regelungen, etwa Betriebsvereinbarungen. Im Gegensatz zur Sichtweise früher müssen diese zwingend den Mindeststandard der DSGVO einhalten.	○ Ja ○ Nein
Gibt es Änderungen bei der technischen Umsetzung der Verarbeitung?	› Gerade bei schon lange aktiven Verarbeitungen kann es zwischenzeitlich zu erheblichen Anpassungen gekommen sein. › Sprechen Sie im Zweifel mit den Betreibern bzw. mit der IT-Abteilung und lassen Sie sich die Veränderungen und deren mögliche Auswirkungen auf die Verarbeitung erklären.	○ Ja ○ Nein
Inwieweit gibt es Veränderungen bei den an der Verarbeitung Beteiligten?	› Hier geht es nicht nur um die intern Beteiligten. Denken Sie auch an Dienstleister und Kooperationspartner, die bei der Verarbeitung unterstützen. Eventuell wurden auch Softwareanbieter ausgetauscht oder Verarbeitungen in die Cloud verlagert. Das kann eine Neueinordnung im Datenschutz nötig machen. › Gerade in Unternehmensgruppen und Konzernen gibt es oft Änderungen und Verlagerungen von Zuständigkeiten bzw. Aufgaben. Auch hier muss z. B. in Sachen Auftragsverarbeitung alles passen.	○ Ja ○ Nein
Hat sich die Gefahren- und Risikosituation verändert?	› Über die Zeit können sich Gefahren und die sich daraus ergebenden Risiken erheblich verändern. › Fordern Sie ggf. ein Update der entsprechenden Einschätzungen ein, damit Sie darauf Ihre Bewertung stützen können.	○ Ja ○ Nein
Liegen Veränderungen bei den technischen und organisatorischen Schutzmaßnahmen vor?	› Gerade wenn Gefahren und Risiken sich verändern, kann das zu nicht mehr angemessenen Maßnahmen führen. Hier kann eine Anpassung unerlässlich sein. › Haben Sie vor allem ein Auge auf den Aspekt „Stand der Technik". Der war vor längerer Zeit meist ein ganz anderer. Auch das kann Grund für eine neue Bewertung und für Nachbesserungen sein.	○ Ja ○ Nein
Sind die Grundsätze der Verarbeitung weiterhin gewahrt?	› Machen Sie auch hier den Check. Die Grundsätze gelten für alle Verarbeitungen personenbezogener Daten. Prüfen Sie, inwieweit gerade Rechtmäßigkeit, Zweckbindung und Datenminimierung eingehalten sind. › Haben Sie auch ein Auge auf die Rechenschaftspflicht. Die Einhaltung der Grundsätze muss Ihr Unternehmen auch belegen und nachweisen können.	○ Ja ○ Nein
Sind Anpassungen bei den Rechtsgrundlagen nötig?	› Schauen Sie, ob Rechtsgrundlagen noch passen. Hier kann es zwischenzeitlich erhebliche Veränderungen gegeben haben, etwa durch eine veränderte Rechtslage oder Rechtsprechung. › Gerade bei Einwilligungen sollten Sie genauer hinschauen. Gab es generelle Veränderungen bei der Verarbeitung oder zum Umfang der Verarbeitung, kann Anpassungsbedarf bestehen.	○ Ja ○ Nein
Ist die Umsetzung der Betroffenenrechte weiterhin gewährleistet?	› Machen Sie den Check zunächst hinsichtlich des Rechts auf Transparenz. Verändern sich Verarbeitungen, müssen ggf. auch die Transparenzinformationen, etwa nach Art. 13 DSGVO, angepasst werden. › Schauen Sie sich auch interne Regelungen, Zuständigkeiten oder Prozesse an. Eventuell passt hier manches nicht mehr. Den nötigen Veränderungs- und Anpassungsbedarf sollten Sie bei Ihrer Bewertung berücksichtigen.	○ Ja ○ Nein

Geben Sie der internen Kommunikation einen Überblick

Gerade in größeren Unternehmen gibt es ganze Abteilungen, die sich um die interne Unternehmenskommunikation kümmern. Doch offen und transparent kommunizieren zu wollen bedeutet nicht, dass einfach alles erlaubt ist. Auch bei Mitarbeiterzeitung, Newsletter oder Intranet muss unter Datenschutzaspekten so manches bedacht werden.

Vermitteln Sie einige wichtige Punkte

Für die Kollegen in der internen Kommunikation steht vor allem im Vordergrund, gute und lesenswerte Artikel, Berichte oder Informationen bereitzustellen.

Dass es auch in Sachen Datenschutz und Persönlichkeitsrecht so einiges zu beachten gilt, hat man vielleicht nicht so wirklich auf dem Radar.

Daher ist wichtig: Vermitteln Sie bei Gelegenheit einige wichtige Aspekte. Auch wenn der eine oder andere Aspekt bereits bekannt sein sollte, schadet ein Austausch nie. Denn man lernt sich kennen und kommt über den Datenschutz ins Gespräch.

Machen Sie es sich einfach

Für ein Gespräch mit den Kollegen können Sie für sich die folgende Checkliste einsetzen. So stellen Sie sicher, dass Sie die wichtigsten Aspekte ansprechen und nichts Wichtiges vergessen. Alternative Idee: Sie können die Checkliste auch leicht anpassen und als Merkblatt bzw. als Selbstcheck an die Kollegen geben. Auch damit fördern Sie die Sensibilität, sprich Awareness.

Checkliste: Datenschutzthemen bei der internen Unternehmenskommunikation

Aspekt	Das können Sie erläutern	Besprochen
Veröffentlichungen sind meist auch ein Datenschutzthema.	› Die Arbeit der internen Kommunikation geht meist mit einer Verarbeitung personenbezogener Daten einher. Insofern sind in der Regel die Anforderungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) anwendbar. So z. B., wenn personenbezogene Daten zumindest teilweise elektronisch verarbeitet werden. › Hinzu kommen können auch andere Vorschriften, etwa im Zusammenhang mit Fotos und Videos das Kunsturhebergesetz (KUG oder KunstUrhG). Auch diese schützen das Persönlichkeitsrecht.	○ Ja ○ Nein
Anonymität hat Vorrang.	› Um Problemen mit dem Datenschutz oder im Zusammenhang mit dem Persönlichkeitsrecht aus dem Weg zu gehen, sollten Sie nach Möglichkeit auf Personenbezug verzichten. › Auch wenn keine Namen oder Bilder verwendet werden, kann man unter Umständen auf eine bestimmte Person schließen. Das kann zum Problem werden. Prüfen Sie immer, inwieweit auch ohne konkrete Informationen Rückschlüsse möglich sind.	○ Ja ○ Nein
Vorsicht bei privaten Informationen in Texten	› Haben Informationen keinen direkten geschäftlichen Bezug oder sind sie eher privater Natur, ist Vorsicht geboten. Meist gibt es für eine diesbezügliche Veröffentlichung nur eine Rechtsgrundlage: die Einwilligung der betreffenden Person. Gerade bei Beschäftigten heißt es hier jedoch Augen auf: Für Einwilligungen im Beschäftigungsverhältnis gelten besondere und strengere Anforderungen (§ 26 Abs. 2 BDSG). › Prüfen Sie kritisch, inwieweit private Informationen für die Aussage überhaupt von Relevanz sind. Steht das Private im Mittelpunkt, ist regelmäßig das Okay der betreffenden Person erforderlich.	○ Ja ○ Nein
Fotos können problematisch sein.	› Sollen Fotos veröffentlicht werden, auf denen Personen abgebildet sind, kann das unter Umständen auf ein überwiegendes berechtigtes Interesse gestützt werden. Hier heißt es jedoch, genau prüfen. In der Interessenabwägung müssen die Vorgaben des KUG berücksichtigt werden. › Greifen nicht insbesondere die Ausnahmen des § 23 KUG, ist die Einwilligung des Abgebildeten erforderlich (§ 22 KUG). Daher: Klären Sie unbedingt vor einer Veröffentlichung von Fotos oder Videos, inwieweit das zulässig ist.	○ Ja ○ Nein
Datenminimierung ist wichtig.	› Dabei handelt es sich um einen wichtigen Grundsatz der DSGVO. Verarbeiten Sie nur so viele persönliche Informationen wie nötig. Verzichten Sie auf nicht erforderliche bzw. überflüssige Informationen in Veröffentlichungen. › Typische Beispiele für oftmals nicht erforderliche Informationen sind hier Geburtstag, Familienstand oder Hobbys. Hierbei handelt es sich ohnehin eher um „private" Informationen, für deren Veröffentlichung es meist der Zustimmung der betreffenden Person bedarf.	○ Ja ○ Nein
Löschen Sie Veraltetes.	› Wenn es um personenbezogene Informationen geht, müssen diese irgendwann gelöscht werden. Meist ist dieser Zeitpunkt gekommen, wenn der Zweck der Verarbeitung erreicht ist. › Gerade im Zusammenhang mit veröffentlichten Bildern oder privaten Informationen kann der Zweck bei Ende des Beschäftigungsverhältnisses wegfallen, sodass Sie Entsprechendes löschen sollten, auch wenn es eine Einwilligung gibt.	○ Ja ○ Nein
Binden Sie den Datenschutzbeauftragten früh ein.	› Der Datenschutz und die gesetzlichen Rahmenbedingungen haben viele Facetten. Schnell kann hier etwas falsch gedeutet oder umgesetzt werden. › Haben Sie im Zusammenhang mit personenbezogenen Daten etwas vor oder gibt es Unklarheiten: nicht lange warten! Den Datenschutzbeauftragten einbinden.	○ Ja ○ Nein

Wie kann ich mit „Drückebergern“ bei Führungskräften umgehen?

FRAGE: Ich biete für Führungskräfte Schulungen zum Datenschutz an. Nachdem ich nun viele Führungskräfte geschult habe, fällt mir auf, dass es einige „Drückeberger“ gibt. Die sagen kurzfristig ihre Teilnahme wieder ab oder erscheinen einfach nicht. Da es hier auch einige Mitglieder der Geschäftsleitung gibt, denen es immer wieder nicht möglich ist, teilzunehmen, frage ich mich: Wie soll ich mit solchen „Drückebergern“ umgehen?

ANTWORT: Jedermann leuchtet ein: Wer mit personenbezogenen Daten zu tun hat, der muss zumindest über grundlegendes Know-how verfügen. Um auch wenig verfügbare Beschäftigte in Ihrem Unternehmen mit dem nötigen Wissen zu versorgen, können Sie Folgendes machen:

- **Verdeutlichen Sie den Betreffenden die Erforderlichkeit**
  Gerade Führungskräfte und Unternehmenslenker tragen große Verantwortung im Datenschutz. So verantworten sie intern oft nicht nur die Verfahren, Technik oder Prozesse, mit denen personenbezogene Daten verarbeitet werden. Sie sind auch dafür verantwortlich, dass die ihnen disziplinarisch zugeordneten Beschäftigten regelkonform und sorgsam mit personenbezogenen Daten umgehen. Kommt es hier zu Fehlverhalten, kann das auch für die betreffende Führungskraft ernste Konsequenzen haben.
- **Zeigen Sie auf, wer über die Teilnahme entschieden hat**
  Hat die Unternehmensleitung entschieden, dass die Führungskräfte an einer von Ihnen angebotenen Schulung teilnehmen müssen, ist das nicht unbedingt überall angekommen. Machen Sie klar, dass ganz oben die entsprechende Entscheidung gefallen ist. Die Teilnahme ist auch unter Risikoaspekten geboten. Schließlich muss die Unternehmensleitung dafür Sorge tragen, dass Risiken für das Unternehmen angemessen begegnet wird. Und ein Risiko ist auch, dass Führungskräfte und Beschäftigte gegen den Datenschutz verstoßen.
- **Klären Sie darüber auf, welche Folgen ein Fernbleiben haben kann**
  Hier müssen Sie niemandem mit Bußgeldern & Co. drohen. Machen Sie aber deutlich, dass Sie irgendwann der Unternehmensleitung Bericht erstatten müssen, inwieweit alle Führungskräfte an Ihren Schulungen teilgenommen haben. Dann müssen Sie Ross und Reiter benennen. Sie müssen offenlegen, wer es terminlich nie geschafft hat. Und das kann unschöne Konsequenzen für diejenigen haben, die eine Teilnahme bislang umgangen haben. Zumindest ein ernstes Gespräch mit dem Chef dürfte drin sein. Und hier kann man im Ergebnis eigentlich nur schlecht aussehen.
- **Terminfindungsprobleme: Drehen Sie den Spieß um**
  Sie können nach Rücksprache mit der Unternehmensleitung über deren Assistenz einen Termin mit den „Härtefällen“ koordinieren lassen. Unter Umständen wird man hier einen Termin eher möglich machen, weil das Vorzimmer des Chefs doch meist großen Eindruck hinterlässt. Alternativ können Sie die betreffenden Führungskräfte bitten, sich untereinander abzustimmen und Ihnen einen Termin vorzuschlagen.

Muss ich in Datenschutzhinweisen genannt werden?

FRAGE: Eine Kanzlei hat für die neue App unseres Unternehmens Datenschutzhinweise erstellt. Darin tauche auch ich als Datenschutzbeauftragter mit Namen und persönlicher E-Mail-Adresse auf. Nach meiner Rückfrage hieß es, dass das so sein müsse. Ich bezweifle das. Muss ich wirklich persönlich genannt werden?

ANTWORT: Bei der Erhebung personenbezogener Daten müssen bestimmte Informationen gegeben werden. Dazu zählen nach Art. 13 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO) auch die Kontaktdaten des Datenschutzbeauftragten. Nun kommt das Aber: Auch eine namentliche Nennung des Datenschutzbeauftragten wäre eine Verarbeitung personenbezogener Daten. Dazu besteht jedoch keine Pflicht. Die DSGVO fordert nur Kontaktdaten, keine namentliche Nennung. Also reichen allgemeine Kontaktdaten aus. Das sind etwa die Firmenanschrift mit „Datenschutzbeauftragter“ und eine auf die Funktion bezogene E-Mail-Adresse, z. B. „datenschutzbeauftragter@musterladen-abc.xyz“. Weiteres Argument gegen die Angabe Ihres konkreten Namens: Weil in Art. 13 DSGVO keine namentliche Nennung gefordert ist, wäre eine Veröffentlichung konkreter persönlicher Informationen ein Verstoß gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO). Es fehlt an der Erforderlichkeit.

Erben können für Verstorbene keine Rechte geltend machen

Die Datenschutz-Grundverordnung (DSGVO) gilt grundsätzlich nur für lebende natürliche Personen. Doch wie sieht die Sache aus, wenn Erben Rechte für einen verstorbenen Betroffenen geltend machen, etwa als Beschwerde bei der Aufsicht? Damit hat sich das Oberverwaltungsgericht (OVG) Rheinland-Pfalz beschäftigt (Urteil vom 28.11.2025, Az. 10 A 11059/23.OVG).

Der Sachverhalt

Eine Frau, die spätere Klägerin, war mit einer anderen Frau verheiratet. Die Ehepartnerin war an Krebs erkrankt. Im Rahmen der Behandlung wurde Ende 2019 ein Institut mit der Analyse von Gewebe beauftragt. Die diesbezügliche Rechnung des Instituts wurde beglichen. Der Befundbericht wurde auch an einen beratenden Onkologen übermittelt. Anfang 2020 kam es zu ergänzenden Beratungsleistungen durch diesen Onkologen. Dieser stellte der Patientin hierfür im eigenen Namen eine Rechnung. Im Juni 2020 verstarb die erkrankte Frau. Alleinerbin war die Klägerin.

Erbin beschwert sich

Die Klägerin wandte sich im Februar 2022 an die Datenschutzaufsichtsbehörde. Aus ihrer Sicht war die Übermittlung der Daten ihrer verstorbenen Frau vom Institut an den Onkologen nicht in Ordnung. Die Aufsichtsbehörde sah darin jedoch kein Problem. Vielmehr ging man davon aus, dass die Verarbeitung im Rahmen der Tätigkeit des Onkologen zulässig war. Ferner seien das Tätigwerden des Arztes und die Kenntnisnahme der personenbezogenen Daten von einer Einwilligung gedeckt. Ob eine gesonderte Abrechnung zulässig war, wäre keine Frage des Datenschutzes.

Im weiteren Schriftwechsel machte die Klägerin auch einen Verstoß gegen die Informationspflichten aus Art. 13 DSGVO geltend. Doch auch hierfür sah die Aufsicht keine Anhaltspunkte. Also beendete die Behörde Ende Oktober 2022 das Beschwerdeverfahren.

Gericht soll die Sache klären

Die Erbin zog vor das Verwaltungsgericht (VG). Ihrer Ansicht nach könne sie die zu Lebzeiten ihrer Ehefrau entstandenen Datenschutzrechte wahrnehmen. Diese wären Teil des digitalen Nachlasses. Es gehe um eine Verarbeitung, die zu Lebzeiten der Ehefrau stattgefunden habe. Diese sei unzulässig gewesen. Insofern wäre auch der Bescheid der Aufsichtsbehörde zur Beendigung des Beschwerdeverfahrens rechtswidrig. Das VG sah die Sache anders und wies die Klage ab. Die Klägerin wäre selbst nicht von der infrage stehenden Verarbeitung personenbezogener Daten betroffen gewesen. Als Erbin könne sie keine Datenschutzrechte für die verstorbene Ehefrau geltend machen. Doch die Erbin klagte vor dem OVG als Berufungsinstanz, und zwar erfolglos.

So entschied das OVG

Die Klage ist unbegründet. Für die Erbin bestand kein Recht nach Art. 77 Abs. 1 DSGVO, für die verstorbene Ehefrau eine Datenschutzbeschwerde einzureichen und hieraus Rechte geltend zu machen.

Generell besteht für eine betroffene Person ein Beschwerderecht nach Art. 77 Abs. 1 DSGVO, und zwar bezüglich der sie betreffenden personenbezogenen Daten. Insofern ist auch eine Deckungsgleichheit zwischen der betroffenen und der in den Daten beschriebenen Person erforderlich. Im Umkehrschluss ist nicht betroffene Person, wer durch die betreffenden Daten nicht identifiziert oder identifizierbar ist. Vorliegend bezieht sich die Beschwerde nicht auf die Verarbeitung der eigenen personenbezogenen Daten, sondern auf diejenigen der verstorbenen Ehefrau.

Beschwerderecht geht unter

Als Erbin kann die Klägerin nicht das Beschwerderecht aus Art. 77 Abs. 1 DSGVO wahrnehmen. Sie ist nicht nach § 1922 Bürgerliches Gesetzbuch in die Betroffenenstellung der Verstorbenen eingetreten. Beim Recht auf Beschwerde handelt es sich um eine nicht übergangsfähige Rechtsposition. Insofern geht das Beschwerderecht als höchstpersönliches Recht mit dem Tod der betroffenen Person unter. Zudem zielt die DSGVO nur auf den Schutz lebender natürlicher Personen ab. Diese Begrenzung der DSGVO wird ausdrücklich durch Erwägungsgrund 27 Satz 1 klargestellt.

Andere Rechtsprinzipien greifen nicht

Für eine erweiternde Auslegung des Art. 77 DSGVO, des Begriffs des Betroffenen sowie für eine analoge Anwendung der Regelung besteht kein Raum. Auch können keine rechtlichen Erwägungen zum digitalen Nachlass herangezogen werden. Das gilt ferner für die Aspekte des postmortalen Persönlichkeitsrechts. Zudem kann sich die Klägerin auch nicht auf den postmortalen Sozialdatenschutz berufen. Bei den die Verstorbene betreffenden Daten handelt es sich nicht um Sozialdaten im Sinne von § 67 Abs. 2 Sozialgesetzbuch X. Im Übrigen sind medizinische Daten nicht allgemein als Sozialdaten anzusehen.

§

Das können Sie aus dem Urteil folgern

Die DSGVO gilt nur für lebende natürliche Personen. Mit dem Tod enden auch die Rechte, die sich für den Betroffenen aus der DSGVO ergeben. So vor allem die Betroffenenrechte und das Recht auf Beschwerde. Insofern können Erben auch nicht mehr die Erfüllung von Rechten von Verstorbenen fordern, etwa das Recht auf Auskunft oder Löschung.

Die digitale Lösung für Ihre Pflichtschulungen

Arbeitssicherheit & Datenschutz

Schützen Sie Ihr Unternehmen vor Datenskandalen, hohen Strafzahlungen und Arbeitsunfällen, indem Sie geprüfte Schulungsunterlagen für Präsenz-, Online- oder E-Learning-Einheiten nutzen, den Lernfortschritt über kompakte Dashboards auf Mitarbeiter- oder Gruppenebene überwachen und Schulungen standortübergreifend zentral verwalten.

Testen Sie skillsforwork kostenlos

Compliance & ESG

Mit jährlich aktualisierbaren, individuell anpassbaren E-Learnings zu Compliance-, ESG- & KI-Compliance-Themen sensibilisieren Sie Ihre Mitarbeitenden wirksam durch alltagsnahe, interaktive Lerninhalte und sichern zugleich eine lückenlose Dokumentation des Lernfortschritts.

Cyber Security

Wirksame Awareness-Schulungen und individuell anpassbaren Phishing-Simulationen sensibilisieren Ihre Mitarbeitenden nachhaltig, während monatliche Reports Ihnen jederzeit einen klaren Überblick über das Sicherheitslevel Ihres Unternehmens geben.

skillsforwork

PRIVACYXPERTS

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

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

Vorschau:

Frühjahrsputz: Starten Sie Ihre Mitarbeiteraktion

BGH: Ihr Unternehmen haftet für Auftragsverarbeiter