



## SELBSTORGANISATION: SO KÖNNEN SIE STANDARDFÄLLE LEICHTER ERLEDIGEN

---

### AWARENESS

12345 oder QWERTZ: Machen Sie Schrottpasswörtern den Garaus 1-2

---

### DATENSCHUTZ-ORGANISATION

Beschwerden managen: Nutzen Sie diesen Erfassungsbogen 3

---





## Reflektieren Sie sich

Liebe Leserin, lieber Leser,

*kontinuierlich besser werden – das wollen viele Menschen, vielleicht auch Sie in Ihrer Rolle als Datenschutzbeauftragter. Denn wenn weniger Fehler passieren oder die Dinge leichter von der Hand gehen, macht auch das Arbeiten mehr Spaß.*

*Eine Maßnahme fürs Optimieren ist, dass Sie sich am besten kurz vor Feierabend zehn Minuten Zeit nehmen. Betrachten Sie Ihren Arbeitstag. Prüfen Sie kritisch, was gut lief und was nicht. Machen Sie aus, was Sie optimieren können und sollten. Arbeiten Sie dann in der nächsten Zeit genau an diesen Punkten. Nach und nach werden Sie so besser – ganz nebenbei.*

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.



**Zu Ihrem Onlinebereich:**  
<https://www.privacyxperts.de>



**Expertensprechstunde:**  
<https://t1p.de/andreas-wuertz>

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.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

## Impressum



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 | MK-Photo;  
Seite 1: Adobe Stock | Andrey Popov  
Erscheinungsweise: 26-mal pro Jahr  
E-Mail: kundendienst@privacyxperts.de  
Internet: [www.privacyxperts.de](http://www.privacyxperts.de)  
(bei Rückfragen bitte Kundennummer angeben)

## Inhalt

### Awareness

12345 oder QWERTZ: Machen Sie Schrottpasswörtern den Garaus  
Seiten 1–2

### Datenschutzmanagement

Beschwerden managen: Nutzen Sie diesen Erfassungsbogen  
Seite 3

### Datenschutzbeauftragter

So können Sie Standardfälle leichter erledigen  
Seiten 4–5

### Awareness

Bereiten Sie die Kollegen auf einen Besuch der Aufsicht vor  
Seite 6

### ❓ Fragen an die Redaktion

*Kann ich im Nebenjob Datenschutzbeauftragter sein?*  
Seite 7

*Verfahrensverzeichnis für jedermann: Brauchen wir das noch?*  
Seite 7

### Recht

*EuGH: Onlinemarktplatz ist für Fakeanzeigen verantwortlich*  
Seite 8



Machen Sie es Kriminellen so schwer wie möglich!

# 12345 oder QWERTZ: Machen Sie Schrottpasswörtern den Garaus

**Auch wenn der technische Fortschritt schon so manches überflüssig gemacht hat. Sie gibt es noch immer: Passwörter. Und die sind oftmals die erste Hürde, die Kriminelle überwinden müssen, um an schätzenswerte Daten heranzukommen. Umso wichtiger ist also, dass die Beschäftigten Ihres Unternehmens es den Kriminellen so schwer wie möglich machen.**

## Sehen Sie die Datenschutzrelevanz

Vielleicht denken Sie zunächst: „Warum sollte ich den Leuten sagen, warum sichere Passwörter wichtig sind? Da weiß doch eh jeder Bescheid.“ Doch einerseits können Sie sich nie so wirklich sicher sein, dass alle Mitarbeiter gleich gut Bescheid wissen. Andererseits lohnt es sich immer, wichtige Themen in den Mittelpunkt zu rücken und deren Bedeutung herauszustellen.

Machen Sie zudem Zweiflern immer klar: Passwörter sind wichtig. Denn sie können manchmal die entscheidende Schutzmaßnahme sein, um die Verarbeitung personenbezogener Daten sicher(er) zu machen. Und das ist ein wichtiges Ziel in der Datenschutz-Grundverordnung (DSGVO), wie Sie leicht an Art. 5 Abs. 1 Buchst. f DSGVO bzw. an Art. 32 DSGVO erkennen können.

## Machen Sie am 7.5.2026 gemeinsame Sache

Sie können den Beschäftigten Ihres Unternehmens beispielsweise per E-Mail einige wichtige Tipps rund um das Thema Passwort-

schutz geben. Dazu können Sie sich an folgendem Muster orientieren. Daneben können Sie auch eine größere Aktion am 7.5.2026 starten, dem „World Password Day“. Hier sollten Sie die Spezialisten der IT-Abteilung mit an Bord nehmen. Bauen Sie spezifische Tipps in Ihre E-Mail ein und geben Sie maßgeschneiderte Unterstützung. Flankierend können Sie auch eine gemeinsame kurze Infoveranstaltung oder eine virtuelle Fragestunde anbieten.



## Nutzen Sie den Austausch geschickt

**Sprechen Sie mit den Kollegen der IT-Abteilung, können Sie sich generell über die Umsetzung verschiedener Aspekte in Ihrem Unternehmen rund um das Thema austauschen. Fragen Sie beispielsweise gezielt nach Folgendem: Welche Maßnahmen zum Schutz von Benutzerkonten sind ergriffen? Welche Lösungen gibt es neben Passwörtern, um den Schutz noch zu steigern? Welche Passwortvorgaben gibt es, gerade für Systeme mit besonders schätzenswerten Informationen?**



## Muster: E-Mail zum Thema „Sichere Passwörter“

Liebe Kollegin, lieber Kollege,

Passwörter sind der digitale Schlüssel für eine besondere Schatzkiste in unserem Unternehmen. Die Rede ist vom DatenSCHATZ. Egal, ob es um die Daten von Kunden, Ihre persönlichen Informationen oder die Geschäftsgeheimnisse unseres Unternehmens geht: Passwörter sind ein wichtiger und manchmal auch entscheidender Schutz, um Sensibles sicher zu verwahren. Und seien Sie sich sicher: Schwache Passwörter sind nicht einfach nur eine schlechte Sache. Sie können Cyberkriminellen und Unbefugten Tür und Tor öffnen. Werden dann auch noch Daten gestohlen oder vernichtet, ist eines gewiss: Es droht nicht nur massiver Ärger. Wir können Kunden verlieren, etwa wenn diese das Vertrauen in unser Unternehmen verlieren.



Jeder von uns hat es in der Hand und kann einen wichtigen Beitrag zum Schutz von Sensiblem leisten. Gestalten Sie Ihre Passwörter so, dass üble Zeitgenossen keine Chance haben. Dazu möchte ich Ihnen die folgenden Tipps an die Hand geben:

### **Tipp Nr. 1: Machen Sie es Kriminellen nicht leicht**

Nutzen Sie nichts als Passwort, auf das man bei Ihnen schließen könnte. So z. B. Namen von Ihnen, auch keine Spitznamen. Das gilt auch für Namen von Familienmitgliedern, Verwandten oder Freunden. Auch der Name Ihres Haustiers ist tabu. Diese Informationen können ggf. leicht über Suchmaschinen oder in Profilen in sozialen Netzwerken gefunden oder erschlossen werden. Manches lässt sich auch erraten.

Verwenden Sie auch nichts, was sich einfach in Büchern etwa Wörterbüchern oder Lexika finden lässt. Denn das in solchen Büchern Enthaltene kann von entsprechender Software durchprobiert werden. Das geht heutzutage ganz schnell. Wenn Sie unbedingt auf Begriffe setzen wollen, bauen Sie absichtlich Schreibfehler oder Dialekt mit ein. Je ungewöhnlicher, desto besser. Ein „Moi\_Schnuggelsche#06131“ legt für Kriminelle die Latte schon deutlich höher als ein „Autobahn123“.

### **Tipp Nr. 2: Länge schlägt Komplexität**

Viele Experten sind sich einig: Es kommt eher auf die Länge als auf die Komplexität eines Passworts an. Doch auch ein kurzes komplexes Passwort sollte mindestens acht Zeichen lang sein. Außerdem gilt für alle Passwörter: Es sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen bestehen. Besser ist es jedoch meist, wenn Sie Passwörter mit mindestens zwölf Zeichen wählen. Damit machen Sie Hackern das Leben zumindest schwerer.

### **Tipp Nr. 3: Setzen Sie auf kreative Merksätze**

Wollen Sie sich lange komplexe bzw. kryptische Passwörter merken, stehen Sie wie die meisten Menschen vor einer kniffligen Denksportaufgabe. Doch es geht auch ganz einfach, und zwar mit einem Kniff. Setzen Sie auf Liedzeilen, Aussagen oder Merksätze, an die Sie sich leicht erinnern können. Nehmen Sie die Anfangsbuchstaben, fügen Sie Ziffern und Sonderzeichen hinzu und bauen Sie Fehler ein. So wird aus dem Satz „Tanze Samba mit mir, tanze Samba die ganze Nacht“ das Passwort „T\$mMI@,t\$dgN@ch!“. Das funktioniert auch perfekt mit lustigen oder schrägen Merksätzen wie „Der dritte Himmel über Castrop-Rauxel hängt schon wieder voller Schinken!“, denn der wird zu „D3.Hü(C@S-RXL)hswv\$!“ . Oder wie wäre es mit Dialekt: „Hey Schnuggelsche Nummer 1? Schlotze ma ä Bembel?“ als „HSNr.1?Sm@B?“

### **Tipp Nr. 4: Jeder Account hat sein eigenes Passwort**

Vermeiden Sie Kettenreaktionen. Die kann es nämlich geben, wenn Sie für mehrere Konten ein und dasselbe Passwort nutzen und Kriminelle mit demselben Passwort auch anderswo leichtes Spiel haben. Um Kriminellen nicht mit einem Schlüssel alle Türen zu öffnen, sollten Sie auf Einzigartigkeit setzen: Jedes Konto erhält sein eigenes Passwort. Keines kommt mehrfach zum Einsatz.

### **Tipp Nr. 5: Aktivieren Sie eine Zwei-Faktor-Authentifizierung (2FA) oder Passkey**

Die Funktionsweise von 2FA ist schnell erklärt: Hier braucht man nicht nur das Passwort, sondern ein weiteres Sicherheitselement (z. B. einen an das Smartphone gesendeten Code). Nur wenn beides vorliegt, klappt es mit der Anmeldung. Besitzen Kriminelle nur ein Element, ist ein Zugriff ausgeschlossen. Daher: Setzen Sie auf 2FA, wo immer möglich und erst recht dort, wo es um Schützenswertes geht.

Alternativ können Sie auch auf Passkey setzen. Nutzen Sie dieses kryptografische Verfahren, können Sie sich auch ohne Passwort sicher anmelden. Damit das funktioniert, müssen Sie einerseits diese Anmeldevariante auf einer Webseite oder im Benutzerkonto aktivieren. Andererseits brauchen Sie z. B. ein Smartphone als zweiten Sicherheitsfaktor.

### **Tipp Nr. 6: Setzen Sie auf Ihren persönlichen Passworttresor**

Sie wollen oder können sich all die komplexen Passwörter nicht merken? Kein Problem! Setzen Sie auf die passende Software, sprich einen Passwortmanager oder Passworttresor. Hier können Sie all Ihre Passwörter sicher ablegen und ggf. neue generieren. Zudem sind die Passwörter durch Verschlüsselung geschützt. Merken müssen Sie sich nur ein einziges möglichst komplexes Passwort. Bitte bauen Sie jedoch allen Eventualitäten vor: Denken Sie auch an eine Sicherung Ihrer Passwortdatenbank.

Übrigens: Machen Sie doch mal den Qualitätscheck. So erkennen Sie mit der entsprechenden Funktion schnell, ob es bei Passwörtern Optimierungsbedarf gibt. Der kann bestehen, wenn Sie ein Passwort mehrfach verwenden oder wenn es einfach zu einfach ist.

### **Tipp Nr. 7: Seien Sie auf der Hut**

Kriminelle schlafen nicht und setzen alles daran, an Ihre Daten zu kommen. Daher ist wichtig: Haben Sie den Verdacht, dass etwa ein Passwort geknackt oder Unbefugte Kenntnis davon erlangt haben, sollten Sie es schnellstens ändern.

Außerdem: Gerne locken Kriminelle über gefälschte E-Mails oder SMS ihre Opfer in die Passwortfalle. Lassen Sie besondere Vorsicht walten, wenn man Sie zur Passwortänderung auffordert, obwohl Sie das nicht veranlasst haben. Nutzen Sie auf keinen Fall Links, die Sie nicht selbst herausgesucht haben. Schauen Sie immer zweimal hin und überlegen Sie gut: Kann das wirklich sein?

### **Sie haben Fragen? Melden Sie sich**

Wenn Sie Fragen rund um das Thema Passwortschutz haben, sind Sie hier an der richtigen Stelle. Bei technischen Aspekten wenden Sie sich an die IT-Abteilung. Steht der Datenschutz im Fokus, wenden Sie sich an den Datenschutzbeauftragten.

Danke für Ihre Unterstützung!

Ihr

Theo Rettisch

# Beschwerden managen: Nutzen Sie diesen Erfassungsbogen

Vielleicht hatte Ihr Unternehmen noch nie das Thema, aber vielleicht sind sie schon ein Standardthema. Die Rede ist von Beschwerden von Betroffenen bezüglich der Verarbeitung von personenbezogenen Daten. Wegschauen oder die Sache aussitzen sind keine Optionen. Vielmehr ist zügiges und professionelles Handeln angesagt.

## Wegducken geht nicht

Geht eine Beschwerde beispielsweise beim Kundenservice oder bei der Unternehmensleitung ein, wird man schnell auf Sie zukommen. Schließlich hofft man, dass Sie sich der Sache annehmen und alles Erforderliche in die Wege leiten. Dabei ist klar: Es ist eigent-

lich nicht Ihre Sache als Datenschutzbeauftragter, die Beschwerde bzw. das Anliegen des Betroffenen zu bearbeiten. Aber Sie können das Ganze managen oder koordinieren. Holen Sie dazu die zuständigen Kollegen an einen Tisch und starten Sie eine erste Bestandsaufnahme. Dazu können Sie unser Muster nutzen. Zudem stellen Sie damit sicher, dass Sie keine wichtigen Punkte vergessen.

## Muster: Formblatt Beschwerdemanagement



### Informationen zur Beschwerde

#### Beschwerdeführer:

Name, Vorname: \_\_\_\_\_ Anschrift/Kontaktinformationen: \_\_\_\_\_

Beschäftigter:  Ja  Nein  Kunde:  Ja  Nein  Lieferant/Sonstiger:  Ja  Nein

#### Beschwerde:

per:  Brief  E-Mail  Telefon  Sonstiges: \_\_\_\_\_ Empfänger bzw. empfangende Stelle: \_\_\_\_\_

Eingang im Unternehmen: \_\_.\_\_.2026 um \_\_.\_\_.Uhr Erstinformation des Datenschutzbeauftragten: \_\_.\_\_.2026

Frist: bis: \_\_.\_\_.2026  keine  Sonstiges: \_\_\_\_\_

Vorgebrachter Sachverhalt: \_\_\_\_\_

Als Betroffenenanfrage zu werten:  Nein  Ja, und zwar  Auskunft  Löschung  \_\_\_\_\_

Kritikalität der Angelegenheit: NIEDRIG >       < HOCH Im Fokus des Managements: NIEDRIG >      < HOCH

Datenschutzrelevanz: NIEDRIG >      < HOCH

### Prüfung der Angelegenheit

Aspekt	Hintergrund	Geprüft?
Sind wir als Unternehmen der richtige Adressat?	Prüfen Sie vorab, inwieweit Ihr Unternehmen überhaupt der richtige Adressat ist. Gerade in Konzernen wird gerne die Anfrage an den falschen Verantwortlichen gerichtet. Stellen Sie ggf. Rückfragen beim Beschwerdeführer.	<input type="radio"/> Ja <input type="radio"/> Nein
Wurde der Eingang bestätigt?	Das sollte zeitnah erfolgen, damit die betreffende Person weiß, dass man sich mit ihrem Anliegen auseinandersetzt. Das kann auch zur Entschärfung der Situation führen, gerade wenn die betreffende Person verärgert ist. Bei Betroffenenanfragen muss die Frist aus Art. 12 Abs. 3 Datenschutz-Grundverordnung (DSGVO) beachtet werden.	<input type="radio"/> Ja <input type="radio"/> Nein
Ist der Sachverhalt klar nachvollziehbar?	Es darf keine Zweifel geben, worum es dem Beschwerdeführer geht. Bei unklarer Interessenlage oder unklarer Beschreibung sollte das Anliegen zunächst mit dem Beschwerdeführer geklärt werden.	<input type="radio"/> Ja <input type="radio"/> Nein
Gibt es Auffälligkeiten bzw. Unstimmigkeiten?	Unter Umständen handelt es sich auch um eine „Fakeanfrage“, um Ihr Unternehmen zu beschäftigen. Eventuell hat man auch künstliche Intelligenz bemüht, um die eigene Position zu untermauern. Darauf können unpassende Argumente oder falsche Rechtsprechung hindeuten.	<input type="radio"/> Ja <input type="radio"/> Nein
Sind die zuständigen Stellen informiert?	Machen Sie aus, wer für die relevante Datenverarbeitung verantwortlich und zuständig ist. Laden Sie zum Gespräch und zur Festlegung von Maßnahmen bzw. zu nächsten Schritten ein.	<input type="radio"/> Ja <input type="radio"/> Nein
Ist die Unternehmensleitung einzubinden?	Je nach Beschwerde ist es sinnvoll, frühzeitig die Unternehmensleitung einzubinden. Sie trägt am Ende jede Entscheidung und ist für alles verantwortlich.	<input type="radio"/> Ja <input type="radio"/> Nein
Besteht ggf. eine Melde- bzw. Informationspflicht?	Geht es bei der Sache um eine Verletzung des Schutzes personenbezogener Daten, kann eine Meldung an die zuständige Aufsichtsbehörde erforderlich sein (Art. 33 DSGVO). Eventuell müssen auch mögliche weitere Betroffene informiert werden (Art. 34 DSGVO).	<input type="radio"/> Ja <input type="radio"/> Nein
Wie ist die Sache zu bewerten?	Ist die Beschwerde gerechtfertigt, sollte dieser abgeholfen werden. Dazu sind Maßnahmen nötig, die direkt eingeleitet werden müssen. Wichtig ist in diesem Zusammenhang, dass Aufgaben klar definiert und zugewiesen sind.	<input type="radio"/> Ja <input type="radio"/> Nein
Ist der Beschwerdeführer informiert worden?	Der Beschwerdeführer sollte über die Behandlung seiner Beschwerde informiert werden. Hatte er sich berechtigterweise beschwert, versteht sich eine Entschuldigung von selbst.	<input type="radio"/> Ja <input type="radio"/> Nein
Ist die Sache erledigt?	Klären Sie mit den Kollegen, inwieweit es noch eine Reaktion des Beschwerdeführers gab.	<input type="radio"/> Ja <input type="radio"/> Nein



# So können Sie Standardfälle leichter erledigen

**Vielleicht kennen Sie das: Irgendwie landen immer wieder die gleichen Fälle und gleichen Fragen auf Ihrem Schreibtisch. Dass Ablage P, sprich Papierkorb, nicht infrage kommt, wissen Sie als Datenschutzbeauftragter nur zu gut. Und dennoch können Sie sich bei Standardfällen das Leben viel leichter machen.**

Datenschutz ist wichtig für Betroffene. Und Sie als Datenschutzbeauftragter sind wichtig für Ihr Unternehmen. Schließlich helfen Sie dabei, dass Datenschutz ernst genommen wird und Pannen vermieden werden. Doch je besser Sie sind und je präsenter das Thema Datenschutz ist, desto mehr Arbeit landet auf Ihrem Schreibtisch. Dabei stellen auch Sie bestimmt fest: Es gibt Fragen, die immer wieder kommen. Auch manches Problem könnten die Fragenden selbst lösen. Sorgen Sie also für Entlastung. Gehen Sie es geschickt an, wird manche Frage zukünftig nicht mehr bei Ihnen landen. Das erledigen die Mitarbeiter dann in Eigenregie.

## Geben Sie Hilfe zur Selbsthilfe

Häufig ist es so, dass Menschen sich eigentlich selbst helfen wollen, bevor sie jemanden anderen fragen müssen. Arbeiten Sie also daran, dass man Sie bei Standardfällen erst gar nicht fragen muss. Bieten Sie also Hilfe zur Selbsthilfe. Das können Antworten auf häufige Fragen sein oder eben Merkblätter und Leitfäden. Damit Sie beim „Unter-die-Arme-Greifen“ das volle Potenzial ausschöpfen, setzen Sie auf den folgenden Fragenkatalog. So stellen Sie sicher, dass Ihr Ergebnis Hand und Fuß hat,



## Checkliste: Standardfälle leichter erledigen

Das sollten Sie klären	Das ist wichtig	Geprüft und erledigt?
<b>Schwerpunkte geschickt identifizieren</b>		
Welche Fragen kommen immer wieder oder besonders häufig auf?	<ul style="list-style-type: none"> <li>› Starten Sie zunächst mit einer Analyse. Prüfen Sie Ihr E-Mail-Postfach, Ihre Notizen, Protokolle oder Beratungsdokumente. Machen Sie eine einfache Strichliste nach dem Motto „Welches Thema kommt besonders häufig vor?“.</li> <li>› Setzen Sie auch auf ein Brainstorming. Denn unter Umständen haben Sie manches bei der Analyse von E-Mails &amp; Co. nicht entdeckt. So z. B. kurze Beratungen oder die Beantwortung von Fragen in Besprechungen oder am Telefon.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Um welche Themen geht es schwerpunktmäßig?	<ul style="list-style-type: none"> <li>› Stellen Sie die Fragen und Themen nach Oberbegriffen zusammen. Bilden Sie beispielsweise Cluster zu Themen wie „Kundendatenschutz (z. B. Kundendatenbank, Werbung, Messestand)“, „Beschäftigten-daten (z. B. Videoüberwachung, Homeoffice, Bewerbungsgespräche)“, „Technisch-organisatorischer Datenschutz (z. B. Verschlüsselung, Risikoorientierung, Löschung)“.</li> <li>› Erstellen Sie sich eine Rangliste der Schwerpunktthemen. Das ist wichtig, damit Sie leichter Prioritäten setzen können.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Wer stellt besonders häufig bestimmte Fragen?	<ul style="list-style-type: none"> <li>› Klären Sie, welche Personengruppen welche Fragen stellen.</li> <li>› Charakterisieren Sie für sich die betreffende Zielgruppe. So macht es einen großen Unterschied, ob es sich um Führungskräfte handelt, die etwas zu Mitarbeiterüberwachung fragen, oder einfache Beschäftigte.</li> <li>› Fokussieren Sie später auf die jeweiligen Bedürfnisse der jeweiligen Zielgruppe. Das gilt gerade für die von Ihnen in Erwägung gezogenen Aktivitäten.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Warum kommen immer wieder die gleichen Fragen?	<ul style="list-style-type: none"> <li>› Versuchen Sie, die Gründe und Ursachen auszumachen, weshalb Fragen aufkommen oder immer wieder die gleichen Fälle bei Ihnen auf dem Tisch landen. Typische Gründe können sein: Es gibt unklare oder fehlende Regeln bzw. Informationen, Informationen sind nicht auffindbar oder ohne klare Handlungsanweisung.</li> <li>› Versetzen Sie sich in die Situation anderer, etwa eines typischen Fragestellers. Gehen Sie damit auch kritisch mit sich selbst um. Eventuell liegt es an Ihnen, dass man Ihnen mehr Arbeit macht als nötig.</li> <li>› Nutzen Sie jede Gelegenheit, Licht ins Dunkel zu bringen. Sprechen Sie dazu auch mit Fragenden bzw. Vertretern aus der Zielgruppe.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Welche Informationen werden bereitgestellt?	<ul style="list-style-type: none"> <li>› Machen Sie auch einen „Kassensturz“ in Sachen vorhandener Informationen. Gibt es für bestimmte Themen nichts oder sind die Informationen irgendwo versteckt, kann sie auch niemand finden bzw. nutzen.</li> <li>› Klären Sie für sich, wer welche Informationen bereitstellen müsste. Weil Sie ja in erster Linie Berater in Datenschutzfragen sind, kann Ihre erste Aufgabe auch darin bestehen, dass Sie andere dabei unterstützen, ihren (Informations-)Auftrag wahrzunehmen.</li> <li>› Machen Sie die Probe aufs Exempel. Versuchen Sie, auf typische Fragen schnell selbst Informationen zu finden, etwa im Intranet. Dabei ist wichtig: Nur weil das Ihnen mit Ihrem Spezialwissen leicht von der Hand geht, muss das für andere nicht gelten. Machen Sie den Realitätscheck aus Perspektive des typischen Fragenden.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein

Handlungsbedarf ausmachen		
Wie hoch sind die Relevanz und Bedeutung bestimmter Themen?	<ul style="list-style-type: none"> <li>➤ Nur weil ein Thema oder eine Frage besonders oft kommt, muss das nicht bedeuten, dass Sie sich dem als Erstes widmen müssen.</li> <li>➤ Was weniger bedeutsam bzw. dringend ist, sollten Sie zwar nicht unter den Tisch fallen lassen. Gehen Sie es jedoch mit niedriger zeitlicher Priorität an.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Welche Risiken bestehen, wenn Sie sich nicht der Sache annehmen?	<ul style="list-style-type: none"> <li>➤ Hier sollten Sie verschiedene „Risikoperspektiven“ einnehmen. So z. B. die des Betroffenen, des Unternehmens und auch die des Datenschutzbeauftragten. Je nach Perspektive kann sich der Handlungsbedarf ganz anders darstellen.</li> <li>➤ Gehen Sie wie üblich bei Risikobewertungen vor. Machen Sie die mögliche Gefahr aus. Bewerten Sie dann die Eintrittswahrscheinlichkeit und die möglichen nachteiligen Konsequenzen mit 1 bis 3, eben für niedrig, mittel und hoch. Berechnen Sie eine Risikoziffer: Schadenshöhe (1 bis 3) × Wahrscheinlichkeit (1 bis 3) = Risiko (1 bis 9). Die hohen Risiken sollten als Erstes behandelt werden. Gehen Sie bei der Bearbeitung pragmatisch und praxisnah vor.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Ist eine einfache und zügige Umsetzung möglich?	<ul style="list-style-type: none"> <li>➤ Nehmen Sie bei den wichtigen Themen, diejenigen zuerst in Angriff, bei denen Sie schnell vorwärtskommen bzw. die Sie schnell erledigen können.</li> <li>➤ Identifizieren Sie vor allem Bremsklötze oder K.-o.-Kriterien. Auch wenn Themen wichtig sind, können diese nicht einfach oder schnell umsetzbar sein. Hier kann es sinnvoll sein, andere Strategien zu entwickeln.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Die passende Lösung finden		
Welche Maßnahme eignet sich besonders für den betreffenden Standardfall oder die Standardfrage?	<ul style="list-style-type: none"> <li>➤ Wählen Sie die passenden Lösungen aus Ihrem „Werkzeugkasten“.</li> <li>Typische Beispiele sind:</li> <li>➤ Regelungen und Prozessbeschreibungen</li> <li>➤ Themenseiten mit Erläuterungen im Intranet</li> <li>➤ thematische Listen mit Antworten auf häufig gestellte Fragen</li> <li>➤ Merkblätter und Checklisten</li> <li>➤ Anleitungen und Erklärvideos</li> <li>➤ Sprechstunden für individuelle Fragen</li> <li>➤ Oft sind Mischungen aus verschiedenen Lösungen am besten.</li> <li>➤ Die Qualität Ihrer Angebote steigt vor allem mit der Aktualität. Gibt es neue Informationen oder Hinweise, sollten diese zeitnah Einfluss in Ihr Angebot finden.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Wie können Beschäftigte befähigt werden, einfache Fragen selbst zu beantworten?	<ul style="list-style-type: none"> <li>➤ Werden Sie nach folgendem Motto aktiv: Der Köder muss dem Fisch schmecken und nicht dem Angler. Zielgruppenorientierung ist oberstes Gebot. So machen auch Sie sich das Leben und die Arbeit als Datenschutzbeauftragter leichter, wenn etwa bei komplizierten oder „Nerv-Themen“ endlich der Groschen fällt.</li> <li>➤ Klären Sie mit der Zielgruppe die Frage „Womit wäre Ihnen bei diesem Thema bzw. bei diesen Fragen in der Praxis am meisten geholfen?“. Gibt es nur spärliche Rückmeldung, geben Sie Beispiele. So zum Beispiel Checklisten, Leitfäden oder Anleitungen.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Wodurch wird sichergestellt, dass Informationen für die betreffende Zielgruppe leicht zu finden sind?	<ul style="list-style-type: none"> <li>➤ Vieles werden Sie ggf. im Intranet bereitstellen wollen. Hier ist entscheidend, dass Suchende schnell das Gesuchte finden. Setzen Sie daher auf eine gute und schlüssige Bezeichnung von Seiten, Dokumenten und Links.</li> <li>➤ Oft ist es für Suchende besonders hilfreich, wenn Sie eine ausführliche A-bis-Z-Liste bereitstellen. Die wird dann Anlaufstelle Nummer eins. Nehmen Sie in die Liste vor allem die Begriffe auf, die Zielgruppen am ehesten suchen dürften. Achten Sie zugleich dennoch darauf, dass Sie sich auf das Wesentliche konzentrieren und auf belanglose Themen verzichten.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Inwieweit ist sichergestellt, dass Informationen aktuell gehalten werden?	<ul style="list-style-type: none"> <li>➤ Egal, was Sie anbieten, es sollte aktuell gehalten sein. Denn veraltete Informationen sind nicht nur ärgerlich für den Nutzer. Schlimmstenfalls sorgen sie auch für Fehler oder falsches Verhalten.</li> <li>➤ Versehen Sie nach Möglichkeit alles Veröffentlichte mit einer Versionsnummer und einem Bearbeitungsdatum. Das hilft nicht nur Nutzern, die Aktualität einzuschätzen. Auch Sie erkennen auf einen Blick, was schon etwas in die Jahre gekommen ist.</li> <li>➤ Prüfen Sie gerade bei Intranetangeboten regelmäßig, ob Seiten und Links funktionieren. Tote Links sind meist mehr als nur bloßes Ärgernis. Sie können Suchende frustrieren und dazu führen, dass diese ihre Suche aufgeben.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Wie werden die angedachten Maßnahmen kommuniziert?	<ul style="list-style-type: none"> <li>➤ Nicht nur gute Informationen, Dokumente oder unterstützende Maßnahmen sind wichtig. Mindestens genauso wichtig ist, dass Sie diese kommunizieren. Gut geeignet sind Newsletter, die Sie beispielsweise einmal im Quartal verschicken. Hier können Sie nicht nur aktuelle Themen ansprechen. Sie können auch auf Intranetangebote und Schulungen hinweisen.</li> <li>➤ Wollen Sie Schulungen oder Sprechstunden anbieten, sollten Sie nicht nur mehrere Termine zur Auswahl bereithalten. Geben Sie die Termine auch frühzeitig bekannt, damit möglichst viele Interessierte die Teilnahme ermöglichen können.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
An die Umsetzung machen		
Liegt ein Plan für die Umsetzung vor?	<ul style="list-style-type: none"> <li>➤ Überlegen Sie, was Sie in die Wege leiten und umsetzen müssen, um ein gutes Ergebnis zu erzielen.</li> <li>➤ Denken Sie auch immer über Alternativen nach. Manchmal muss man eben Abstriche am Ergebnis machen oder einen anderen Weg einschlagen.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein
Wer bzw. welche Ressourcen werden für die Umsetzung benötigt?	<ul style="list-style-type: none"> <li>➤ Für dies oder jenes brauchen Sie die Unterstützung anderer Kollegen. Sprechen Sie diese frühzeitig an.</li> <li>➤ Sind Kosten unvermeidbar, sollten Sie die Deckung vorab klären. Denn leider gilt so oft: ohne Moos nix los.</li> </ul>	<input type="radio"/> Ja <input type="radio"/> Nein

# Bereiten Sie die Kollegen auf einen Besuch der Aufsicht vor

Wenn es im Datenschutz in Ihrem Unternehmen gerade nicht so rundläuft oder Ihr Unternehmen in die Schlagzeilen geraten ist, kann eines passieren: Mitarbeiter der zuständigen Datenschutzaufsichtsbehörde stehen vor der Tür. Und die sind nicht für ein Kaffeekränzchen gekommen. Die wollen Ihrem Unternehmen auf den Zahn fühlen.

## Verfallen Sie nicht in Panik

Grundsätzlich braucht eine Aufsichtsbehörde keinen konkreten Anlass für eine Prüfung, und zwar auch nicht für eine Prüfung vor Ort. Das heißt aber nicht, dass Sie als Datenschutzbeauftragter bzw. Ihr Unternehmen Sorge haben müssen, dass schon morgen die Mitarbeiter der Datenschutzaufsicht vor der Tür stehen und alles genau unter die Lupe nehmen.

Meist wird eine Aufsichtsbehörde gestuft vorgehen. Denn Prüfungen sind auch eine Kapazitätsfrage, sodass eine Aufsichtsbehörde entsprechend sach- und risikoorientiert vorgehen muss. Folgende Szenarien sind denkbar:

- Gibt es etwa eine Beschwerde eines Betroffenen oder soll generell der Branche Ihres Unternehmens auf die Finger geschaut werden, wird man meist eher auf einen Fragenkatalog setzen. Den sollte Ihr Unternehmen ernst nehmen und rechtzeitig sowie vollständig beantworten.
- Ignoriert Ihr Unternehmen den Fragenkatalog der Aufsicht, deuten die Antworten oder andere Gründe darauf hin, dass im Datenschutz so einiges im Argen liegt, steigt die Wahrscheinlichkeit, dass man bei Ihrem Unternehmen vorstellig wird.
- Ziemlich sicher ist ein Besuch der Aufsichtsbehörde, wenn es zu gravierenden Verstößen kommt oder wenn Verstöße offensichtlich sind. Letzteres kann auch der Fall sein, wenn ein Prüfer beim Vorbeifahren erkennt, dass die Videoüberwachung Ihres Unternehmens offensichtlich auf den öffentlichen Bereich ausgerichtet ist.

## Bereiten Sie die Kollegen auf den Fall der Fälle vor

Damit etwa die Unternehmensleitung, deren Assistenz, der Empfang oder andere zuständige Kollegen nicht gleich ins erstbeste Fettnäpfchen treten, sollten Sie bei Gelegenheit die betreffenden Personen informieren. Geben Sie beispielsweise die folgenden sieben Tipps:

### **Tipp Nr. 1: Bitte nicht generell den Zutritt verweigern**

Die Vertreter der Datenschutzaufsichtsbehörde dürfen für ihre Kontrollen Grundstücke und Geschäftsräume betreten. Außerdem ist Zugang zu allen Datenverarbeitungsanlagen und -geräten zu gewähren. Das sieht § 40 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) vor. Nur außerhalb der üblichen Betriebs- und Geschäftszeiten könnte man den Zutritt verweigern, wie sich aus §§ 40 Abs. 5 Satz 3, § 16 Abs. 4 Satz 2 BDSG ergibt. Wird ansonsten der Zutritt verweigert, kann das schon der erste Schritt Richtung Bußgeld sein.

### **Tipp Nr. 2: Schnellstens die richtigen Personen informieren**

Damit nichts anbrennen kann, sollten sofort die entscheidenden Personen informiert werden. Das sind die Unternehmensleitung, der IT-Leiter und der Datenschutzbeauftragte. Sind diese nicht vor Ort, müssen sie telefonisch über den Besuch der Aufsicht informiert werden.

### **Tipp Nr. 3: Unbedingt klären: Ist sicher, wer vor einem steht?**

Verlangen Sie unbedingt nach dem Dienstaussweis. Bestehen irgendwelche Zweifel, sollten Sie sich die Echtheit der Person bzw. des Besuchs durch die Aufsichtsbehörde bestätigen lassen. Hier genügt meist ein Anruf. Nutzen Sie die Nummer, die auf der Webseite der Aufsichtsbehörde veröffentlicht ist.

### **Tipp Nr. 4: Die Prüfer sollten gut betreut werden**

Am besten werden die Prüfer in einen Besprechungsraum gebracht und um etwas Geduld gebeten. In der Zwischenzeit werden die Unternehmensleitung und zuständige Kollegen informiert. Ein Kaffee oder ein Getränk sollte unbedingt angeboten werden. Das hat auch einen strategischen Hintergedanken: Die Wartezeit kommt einem weniger lang vor.

### **Tipp Nr. 5: Kooperation anstatt Konfrontation**

Generell sollten alle Beteiligten im Unternehmen auf Kooperation setzen. Damit ist man selbst dann gut beraten, wenn Verstöße offensichtlich sind und ein Bußgeld droht. Denn Kooperation und Zusammenarbeit können das Bußgeld reduzieren. Außerdem: Die Behörde sitzt im Zweifel immer am längeren Hebel.

### **Tipp Nr. 6: Auskünfte geben nur die zuständigen Kollegen**

Fragen beantworten sollten nur die fachlich zuständigen Kollegen. Denn solide und fundierte Antworten zeugen nicht nur von Professionalität. Es wird auch vermieden, dass man sich mit falschen Aussagen oder unzutreffenden Mutmaßungen in die Bredouille bringt. Außerdem versteht sich von selbst: bitte bei der Wahrheit bleiben. Lügen rächen sich früher oder später.

Doch auch für die zuständigen Kollegen ist wichtig: Es wird nur auf das geantwortet, was gefragt wurde. So sollte weder freimütig geplaudert werden, noch sollten mehr als die erforderlichen Informationen gegeben werden. Schließlich wäre es zu blöd, wenn man sich als Unternehmen um Kopf und Kragen redet.

### **Tipp Nr. 7: Wichtige Informationen sollten griffbereit sein**

Wichtige Informationen sollten aktuell und verfügbar sein. So z. B. das Verzeichnis von Verarbeitungstätigkeiten. Alles, was bereitgestellt werden muss, sollte vorzeigbar sein. Auch bei Prüfungen gibt es meist keine zweite Chance für einen ersten Eindruck.

# Kann ich im Nebenjob Datenschutzbeauftragter sein?

**FRAGE:** Ich bin angestellter Datenschutzbeauftragter. In der Freizeit bin ich in einem Verein aktiv. Dieser hat mich nun gefragt, ob ich nicht für den Verein die Funktion des Datenschutzbeauftragten übernehmen kann. Prinzipiell würde ich das gerne machen, zumal ich mir damit auf Minijob-Basis einige Euro dazuverdienen könnte. Nun gehen mir viele Fragen durch den Kopf: Geht das mit der Nebentätigkeit als Datenschutzbeauftragter überhaupt? Muss ich mir die Zustimmung meines Arbeitgebers holen? Kann mir der Arbeitgeber diese Zustimmung verweigern?

**ANTWORT:** Prinzipiell dürfte einer Nebentätigkeit nichts entgegenstehen. Allerdings sollten Sie in erster Linie auf folgende Aspekte achten:

➤ **Datenschutzbeauftragter geht auch im Nebenjob**

Generell kann die Tätigkeit als Datenschutzbeauftragter auch im Nebenjob ausgeübt werden. Doch auch hier ist wichtig, dass ein Datenschutzbeauftragter über das nötige Wissen verfügt, um seine Aufgaben wahrnehmen zu können. Das fordert letztendlich auch Art. 37 Abs. 5 Datenschutz-Grundverordnung. Daneben muss man Sie mit den erforderlichen (zeitlichen) Ressourcen ausstatten. Kein Problem ist in der Regel, wenn Sie beim Verein auf Minijob-Basis tätig werden. Denn dann gelten auch im Hinblick auf die Sozialversicherung und Steuern vereinfachte Rahmenbedingungen.

➤ **Schauen Sie in Ihren Arbeitsvertrag**

Bezüglich Ihrer Haupttätigkeit im Unternehmen, sollten Sie zunächst einen Blick in Ihren Arbeitsvertrag werfen. Unter Umständen gibt es dort Festlegungen zu Nebentätigkeiten oder bestimmte Informationspflichten gegenüber dem Arbeitgeber. Diese sollten Sie einhalten, um nicht gegen den Arbeitsvertrag und damit Ihre Pflichten als Arbeitnehmer

zu verstoßen. Ein Verstoß kann zumindest eine Abmahnung rechtfertigen.

- **Prüfen Sie, welche betrieblichen Festlegungen es gibt**  
Möglicherweise gibt es spezifische Festlegungen im Unternehmen zum Thema Nebentätigkeiten. So kann es einen Informations- und Genehmigungsprozess geben. Der ist in vielen Fällen eher Formsache. Schließlich hat auch ein Arbeitgeber nur begrenzte Möglichkeiten zu argumentieren, dass die Nebentätigkeit eines Arbeitnehmers seine Interessen verletzt. Letzteres wäre beispielsweise der Fall, wenn Sie Ruhezeiten nicht einhalten könnten oder mit Ihrer Tätigkeit in Konkurrenz zum Arbeitgeber treten würden. Diese Fälle dürften bei Ihnen eher nicht gegeben sein.
- **Sprechen Sie mit der Personalabteilung**  
Wird ein Antrag abgelehnt oder stellt man sich gegen eine Nebentätigkeit, sollten Sie zunächst das Gespräch suchen. Meist sind Sie hier bei der Personalabteilung an der richtigen Adresse. Häufig lassen sich hier auch Missverständnisse aufklären und Befürchtungen aus dem Weg räumen. Will man sich nicht umstimmen lassen, können Sie auch mit dem Betriebsrat sprechen. Der kann Sie als Ihr Interessenvertreter unterstützen.

# Verfahrensverzeichnis für jedermann: Brauchen wir das noch?

**FRAGE:** Kürzlich haben wir unser Onlineangebot geprüft. Dabei wurden auch einige „Leichen“ entdeckt. Auf einer schon in die Jahre gekommenen Webseite gab es nicht nur Datenschutzhinweise. Darin war auch ein „Verfahrensverzeichnis für jedermann“. Irgendwie bin ich dazu in der Datenschutz-Grundverordnung (DSGVO) nicht fündig geworden. Können Sie etwas Licht ins Dunkel bringen? Was hat es mit dem Verzeichnis auf sich? Und brauchen wir das noch?

**ANTWORT:** Das Wichtigste vorweg: Ihr Unternehmen braucht das „Verzeichnis für jedermann“ nicht mehr. Das kann bedenkenlos entsorgt werden. Was es damit auf sich hat, ist schnell erklärt: So etwas wie das heutige Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO gab es schon vor der DSGVO, und zwar bis Mai 2018 im früheren Bundesdatenschutzgesetz (BDSG-alt). Das war das interne Verfahrensverzeichnis, welches

dem Datenschutzbeauftragten mit den Angaben nach § 4e Satz 1 BDSG-alt zur Verfügung zu stellen war. Die meisten Angaben aus diesem Verzeichnis musste der Datenschutzbeauftragte auf Anfrage jedermann in geeigneter Weise verfügbar machen. Je nach Unternehmen gab es mehr oder weniger solcher Anfragen. Der Einfachheit halber veröffentlichten manche Unternehmen das „Verzeichnis für jedermann“ auf der Webseite.



# EuGH: Onlinemarktplatz ist für Fakeanzeigen verantwortlich

Wenn es um die Verantwortung nach der Datenschutz-Grundverordnung (DSGVO) geht, ist vieles nicht so eindeutig, wie es auf den ersten Blick erscheint. So hat sich der Europäische Gerichtshof (EuGH) mit der Verantwortung eines Kleinanzeigenportals beschäftigt, bei dem eine rufschädigende Anzeige veröffentlicht wurde (Urteil vom 2.12.2025, Rs. C-492/23).

## Das führte zur Vorabentscheidung des EuGH

Der Betreiber (spätere Beklagte) eines Onlinemarktplatzes in Rumänien bot an, auf seiner Seite Kleinanzeigen zu veröffentlichen. Das machte auch eine unbekannte Person. Diese veröffentlichte zu einer Frau, der späteren Klägerin, eine Anzeige. In dieser wurden Bilder veröffentlicht und unter Angabe ihrer Telefonnummer sexuelle Dienstleistungen angeboten. All das traf nicht zu und geschah ohne Kenntnis und Zustimmung der Frau. Als die Frau auf die Anzeige angesprochen wurde, wandte sie sich an das Portal. Dieses reagierte sofort und entfernte die Anzeige. Allerdings kopierten zwischenzeitlich andere Internetseiten die Anzeige und veröffentlichten diese ebenfalls. Dort blieb die Anzeige auch weiterhin veröffentlicht.

## Frau verklagt Betreiber

Aus ihrer Sicht war durch die Anzeige gegen ihr Recht am eigenen Bild, ihren Schutz der Ehre, des guten Rufs und des Privatlebens verstoßen worden, ebenso gegen die DSGVO. In erster Instanz war die Frau erfolgreich. Das Gericht sprach ihr Schadensersatz in Höhe von 7.000 € zu. Der Betreiber ging in Berufung und das mit Erfolg. Die Klägerin gab sich mit dem ablehnenden Berufungsurteil nicht zufrieden. Sie legte Rechtsmittel ein. Das nun zuständige Gericht legte dem EuGH mehrere Fragen zur Auslegung der DSGVO vor. In seinem Urteil beantworten die Richter des EuGH die Fragen, sodass nun die Rechtsmittelinstanz in Rumänien die Sache entscheiden kann.

## So entschieden die Richter

Mit der Veröffentlichung der Anzeige ist es zu einer Verarbeitung personenbezogener Daten gekommen. Es geht um besondere Kategorien von Daten, für die nach Art. 9 Abs. 1 DSGVO besondere Schutzregeln gelten. Schließlich betreffen die Informationen das Sexualleben bzw. die sexuelle Orientierung einer natürlichen Person. Dass die Informationen falsch sind, ist für diese Einordnung unbeachtlich.

## Betreiber ist Verantwortlicher

Als Verantwortlicher ist anzusehen, wer aus Eigeninteresse auf eine Verarbeitung personenbezogener Daten Einfluss nimmt. Insofern wirkt er an der Entscheidung über Zwecke und Mittel mit. Dabei können auch mehrere Verantwortliche gemeinsam Verantwortliche sein. Gemeinsame Entscheidungen über Zwecke und Mittel der Verarbeitung sind zwingend nicht erforderlich. Es können auch sich ergänzende Entscheidungen sein.

Vorliegend hat der Betreiber die Anzeigen auf seinem Marktplatz nicht nur für inserierende Nutzer, sondern auch aus kommerziellem Eigeninteresse veröffentlicht. Also hat er auf den Zweck der Verarbeitung Einfluss genommen. Ferner wirkte der Betreiber mit der Bereitstellung des Marktplatzes an der Festlegung der Mittel mit.

## DSGVO-Pflichten müssen erfüllt werden

Bei der Verarbeitung personenbezogener Daten hat ein Verantwortlicher die Grundsätze aus Art. 5 Abs. 1 DSGVO einzuhalten. Die Einhaltung muss er nachweisen können (Art. 5 Abs. 2 DSGVO). In der Folge bedeutet das insbesondere: Ein Verantwortlicher ist nach Art. 24 bis 26 DSGVO verpflichtet, geeignete Maßnahmen zu ergreifen, um Anzeigen mit sensiblen Inhalt zu identifizieren. Schon bei der Konzeption einer Verarbeitung ist das zu berücksichtigen. Ferner muss ein Anbieter prüfen, ob ein inserierender Nutzer auch die Person ist, um die es bei der Anzeige mit sensiblen Daten geht. Kann er beispielsweise nicht nachweisen, dass die von der Anzeige betroffene Person in die Veröffentlichung ihrer sensiblen Daten eingewilligt hat, muss der Betreiber eine Veröffentlichung verweigern.

## Kontrollverlust muss vermieden werden

Ein Verantwortlicher muss im Zusammenhang mit der Veröffentlichung sensibler Daten im Zusammenhang mit Art. 32 DSGVO diejenigen technischen und organisatorischen Maßnahmen treffen, die einen Verlust der Kontrolle über diese Daten verhindern. Das bedeutet auch, dass das Kopieren einer Anzeige so weit wie möglich zu blockieren ist und eine weitere unrechtmäßige Veröffentlichung auf anderen Webseiten unterbunden werden muss.

## §

### Das können Sie aus dem Urteil folgern

Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist Ihr Unternehmen, wenn es mit einer Verarbeitung Eigeninteressen verfolgt, etwa mit der Verarbeitung Geld verdienen will. Auch wenn andere Verantwortliche beteiligt sind, kann es sich seiner Verantwortung nicht entziehen. Es reicht aus, wenn es über Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt oder die Entscheidung hierüber beeinflusst. Die Einstufung als Verantwortlicher führt dazu, dass viele Pflichten zu erfüllen sind, etwa die Grundsätze nach Art. 5 Abs. 1 DSGVO. Das gilt bereits bei der Konzeption, wie sich aus Art. 24 und 25 DSGVO ergibt.

# Datenschutz aktuell Live Talk:

## Gratis-Webinar

**Austausch, Aktualität, fachliche Tiefe für alle mit Aufgaben im Datenschutz**



am letzten  
**Freitag**  
jeden Monats



um  
**16:30 Uhr**  
60 Minuten

Moderator & Fachexperte  
**Andreas Würtz**



### Warum am Live Talk teilnehmen?

Neue Leitlinien, geplante Gesetzesänderungen, behördliche Anforderungen und praxisnahe Umsetzungsfragen stellen Datenschutzverantwortliche regelmäßig vor neue Herausforderungen. Oft bleiben dabei konkrete Fragen offen – oder es fehlt die Gelegenheit, Themen direkt mit einem Experten zu besprechen.

Der **Datenschutz aktuell Live Talk** ist aufgrund seines digitalen Formats bequem von überall erreichbar. Im Mittelpunkt steht ein **vertraulicher**,

**fachlicher Austausch** zu aktuellen Schwerpunktthemen aus Datenschutzrecht und Datenschutzpraxis.

Die Veranstaltung wird **nicht aufgezeichnet**. So entsteht ein geschützter Rahmen, in dem auch sensible Fragestellungen offen angesprochen werden können. Sie entscheiden selbst, wie aktiv Sie teilnehmen möchten: **Bringen Sie Ihre Fragen ein oder hören Sie einfach zu** – ganz nach Ihrem Bedarf und ganz wie Sie mögen.

*Der Live Talk ist bewusst kein klassisches Webinar mit Frontalvortrag, sondern ein dialogorientiertes Format, das auf Austausch, Aktualität und fachliche Tiefe setzt.*

*Ich freue mich auf Ihre Teilnahme!*

Ihr Moderator & Fachexperte **Andreas Würtz**

Rechtsanwalt | Datenschutzexperte

Chefredakteur des Fachratgebers „Datenschutz aktuell“

Jetzt zum  
nächsten  
Live-Talk  
anmelden:



[t1p.de/live-talk](https://t1p.de/live-talk)



Telefon: 02 28 95 50 150  
Fax: 02 28 36 96 480  
E-Mail: [kundendienst@privacyxperts.de](mailto:kundendienst@privacyxperts.de)  
Internet: [www.privacyxperts.de](http://www.privacyxperts.de)

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

## Vorschau:

Mitarbeiter als Aushängeschild:  
Prüfen Sie diese Punkte  
Interner Datenschutzcheck:  
So instruieren Sie die Kollegen