

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

OPTIMIERUNG

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

1-2

VIDEOÜBERWACHUNG

Alles dokumentiert? Schauen Sie, was Sie zur Videoüberwachung finden

3



Onlinebereich:
www.privacyxperts.de/login



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



PRIVACYXPERTS



„Die Gedanken sind (zoll-)frei“

Liebe Leserin, lieber Leser,

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

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

Viele Grüße

Andreas Würtz,
Rechtsanwalt und 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

Optimierung

Ständig den Datenschutz verbessern:
Setzen Sie dafür auf diese 7 Schritte
[Seiten 1–2](#)

Videoüberwachung

Alles dokumentiert? Schauen Sie, was
Sie zur Videoüberwachung finden
[Seite 3](#)

Datenverarbeitung

Ab in die Cloud!
Auf diese Datenschutzaspekte
sollten Sie hinweisen
[Seiten 4–5](#)

Know-how

Verpflichtungserklärung
noch zeitgemäß? Das sind
Ihre Argumente dafür
[Seite 6](#)

Fragen an die Redaktion

- ❓ **Kellerfund:** Was sollen wir mit alten Datenträgern machen?
- ❓ **Wie kann ich vorgehen, um eine Datenschutzorganisation vorzunehmen?**

[Seite 7](#)

Rechtsprechung

AG Lörrach: Beweisbilder
vom Nachbarn können gegen
die DSGVO verstoßen
[Seite 8](#)



Zum neuen Onlinebereich!
www.privacyxperts.de/login



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

Bildnachweise:

Titel: Adobe Stock | Gorodenkoff

Seite 1: Adobe Stock | magele-picture

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: Deinzer Grafik, Gartow

Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim

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.
© 2025 by VNR Verlag für die Deutsche Wirtschaft AG,
Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau,
Warschau



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

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

Verbessern ist immer eine gute Idee

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

Schritt 1: Analysieren Sie die Istsituation

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

- › Verarbeitungen personenbezogener Daten
- › Datenschutzprozesse
- › Regelwerke und Vorschriften
- › Stakeholder (z. B. Betroffene, Themenverantwortliche, Entscheider, Führungskräfte) und deren Interessen
- › bestehende Ressourcen
- › externe Einflussfaktoren

Schritt 2: Ermitteln Sie den Sollzustand

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

- › Umsetzung und Nachweis der Umsetzung der Grundsätze der Verarbeitung (Art. 5 DSGVO)
- › Umsetzungsmaßnahmen zur Einhaltung der DSGVO (Art. 24 Abs. 1 DSGVO)
- › risikoangemessene Schutzmaßnahmen (Art. 32 DSGVO)
- › vollständiges und aktuelles Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- › Einbindung und Unterstützung des Datenschutzbeauftragten (Art. 38 DSGVO)
- › geeignete Regelwerke und Prozesse

Schritt 3: Identifizieren Sie die Lücken

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

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

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



Ernten Sie erst einmal die „low hanging fruits“

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

Schritt 4: Klären Sie die Ursachen

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

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

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

Schritt 5: Entwickeln Sie die erforderlichen Maßnahmen

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

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

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

Schritt 6: Gestalten und begleiten Sie die Umsetzung

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

Schritt 7: Wiederholen Sie das Ganze regelmäßig

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

Alles dokumentiert? Schauen Sie, was Sie zur Videoüberwachung finden

Vielleicht setzt Ihr Unternehmen auf Videoüberwachung, um beispielsweise Gelände, Gebäude, Anlagen und Werte abzusichern. Klar, dass das datenschutzkonform passieren muss, sprich die Vorgaben der Datenschutz-Grundverordnung (DSGVO) gewahrt werden. Doch das Umsetzen ist nur die halbe Miete. Auch das Dokumentieren ist wichtig.

Darum sollten Sie die Dokumentation im Auge behalten

Die DSGVO kennt zahlreiche Rahmenbedingungen, die auch bei der Videoüberwachung eine Rolle spielen. Da wären beispielsweise die Grundsätze der Verarbeitung in Art. 5 Abs. 1 DSGVO. Doch auch Art. 5 Abs. 2 DSGVO ist wichtig, die Rechen-

schaftspflicht. Ihr Unternehmen muss belegen können, dass es bezüglich seiner Verarbeitungen die Vorgaben der DSGVO einhält. Und gerade bei der Videoüberwachung kann das schnell der Fall sein, etwa wenn sich jemand bei der Aufsicht beschwert. Prüfen Sie also, ob ein Konzept, ein Handbuch oder ein Ordner die nötigen Informationen enthält.

 CHECKLISTE: Dokumentation der Videoüberwachung		
Thema	Das ist besonders relevant	Erledigt?
Übersicht bzw. Register	Stellen Sie Informationen in einem Ordner zusammen, sollten Sie dem nicht nur einen passenden Namen und ein Register geben. Mindestens genauso wichtig ist eine Versionierung. So sehen Sie auf einen Blick, wann das letzte Mal daran gearbeitet wurde.	☐ Ja ☐ Nein
Lageplan mit Kamerastandorten	Es sollte einen Grundstücks- bzw. Gebäudeplan geben, in dem die Kameras eingezeichnet sind. Achten Sie darauf, dass die Informationen auf einem Plan auch aussagekräftig sind. Gut ist es, wenn die Ausrichtung und der Erfassungsbereich der Kameras erkennbar sind. Außerdem kann der Kamerateyp angegeben werden (z. B. schwenkbar, zoombar, 360-Grad-Kamera, Dome-Kamera). Auch relevante Zusatzausstattung kann verzeichnet werden, etwa Infrarotscheinwerfer für eine verbesserte Nachtsicht.	☐ Ja ☐ Nein
Zweck und Rechtsgrundlagen für die jeweilige Kamera	Nur legitime Zwecke können verfolgt werden. Die Videoüberwachung darf also beispielsweise nicht gegen Grundrechte verstoßen. Das wäre etwa bei einer heimlichen Überwachung in Umkleiden der Fall. Zweck und Rechtsgrundlage müssen bei jeder Kamera geprüft werden und passen. Meist kommt vor allem das überwiegende berechnete Interesse (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO) in Betracht.	☐ Ja ☐ Nein
Einschlägige Betriebsvereinbarungen	Wird eine Videoüberwachung durchgeführt, gibt es meist auch eine Betriebsvereinbarung. Diese sollte im Bedarfsfall schnell zur Hand sein. Soll eine Betriebsvereinbarung die Verarbeitung datenschutzrechtlich erlauben, müssen die Standards der DSGVO eingehalten sein. Ein Unterschreiten ist nicht möglich. Insofern taugen alte Betriebsvereinbarungen oftmals nicht als Rechtsgrundlage.	☐ Ja ☐ Nein
Dokumentation der technischen Systeme	Hier sollte alles Relevante festgehalten sein, etwa zu Kameras, Auflösung, Speichersystemen oder Netzwerkanbindung. Mehr Informationen helfen Ihnen als Datenschutzbeauftragtem, dass Sie Ihrem Beratungs- und Kontrollauftrag nachkommen können.	☐ Ja ☐ Nein
Erfasste Bereiche und Bildausschnitte	Das lässt sich am besten mit einigen Screenshots darstellen. Je nach Kamerateyp können auch mehrere Bilder sinnvoll sein, etwa um die Zoomeinstellungen zu verdeutlichen. Denken Sie auch an die Bilder, auf denen ausgeblendete Bereiche zu sehen sind. Nur so ist etwa erkennbar, dass das Nachbargrundstück nicht überwacht wird.	☐ Ja ☐ Nein
Überwachungszeiten und Speicherfristen	Dazu sollte es klare Festlegungen geben. Hier spielt insbesondere der Zweck eine Rolle. Nur wenn eine Überwachung tatsächlich für die Zweckerreichung erforderlich ist, darf sie stattfinden. Ist der Zweck erreicht, wird in der Regel kein Recht mehr bestehen, die Daten weiter zu speichern. Sie müssen also gelöscht werden. Meist dürften 72 Stunden Speicherung ausreichen.	☐ Ja ☐ Nein
Zugriffs- und Auswertungsrechte	Achten Sie darauf, dass genau die Rollen festgelegt sind. Prüfen Sie zudem, ob die richtigen Personen den Rollen zugeordnet sind. Auch dabei gilt das Minimalprinzip.	☐ Ja ☐ Nein
Transparenzmaßnahmen	Hier geht es insbesondere um das Hinweisschild. Das sollte gut erkennbar auf die Videoüberwachung hinweisen. Achten Sie darauf, dass zumindest die Angaben nach Art. 13 Abs. 1 DSGVO enthalten sind. Die Informationen nach Art. 13 Abs. 2 DSGVO können etwa am Empfang hinterlegt oder auf eine Webseite gepackt werden.	☐ Ja ☐ Nein
Sicherheit der Verarbeitung	Es sollte konkret beschrieben werden, wie man den Anforderungen aus Art. 32 DSGVO gerecht wird. Hier ist zudem Risikoorientierung Pflicht, sprich, die Maßnahmen müssen risikoangemessen sein.	☐ Ja ☐ Nein
Arbeitsanweisungen und Prozesse	Denken Sie dabei an Prozesse zum Zugriff auf Daten. Diese sollten konkret festgeschrieben sein.	☐ Ja ☐ Nein
Verzeichnis von Verarbeitungstätigkeiten	Im Sinne der Übersichtlichkeit kann ggf. eine Eintragung ausreichen. Hier sollte allerdings auf detaillierte Informationen verwiesen werden. Achten Sie auf die Vollständigkeit und Aktualität der Angaben.	☐ Ja ☐ Nein

Ab in die Cloud! Auf diese Datenschutzaspekte sollten Sie hinweisen

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

Sie sind gefragt

Für Sie als Datenschutzbeauftragten ist klar: Sind personenbezogene Daten im Spiel, muss so manches bedacht werden, gerade an Vorgaben aus der Datenschutz-Grundverordnung (DSGVO). Das gilt besonders, wenn Datenverarbeitungen außerhalb des Unternehmens stattfinden sollen, etwa bei einem Dienstleister oder in der Cloud. Relevant sind immer die folgenden Aspekte:

- Grundsätze der Verarbeitung (Art. 5 Abs. 1 DSGVO).
- Sicherheit der Verarbeitung (Art. 32 DSGVO)
- Betroffenenrechte (Art. 12 ff. DSGVO)
- vertragliche Regelung der Datenverarbeitung (z. B. nach Art. 26 bzw. 28 DSGVO)
- angemessenes Datenschutzniveau bei Drittlandsbezug (Kapitel V der DSGVO)



Es gibt keine Automatismen

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



CHECKLISTE: Datenschutzaspekte bei Clouddiensten

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


CHECKLISTE: Datenschutzaspekte bei Clouddiensten

Wo findet die Verarbeitung der personenbezogenen Daten statt?	- Der Ort der Verarbeitung kann von erheblicher Bedeutung sein. Denn das muss nicht automatisch der Hauptsitz des Dienstleisters oder Anbieters sein. Eventuell findet die Verarbeitung in der EU statt, obwohl der Anbieter außerhalb der EU ansässig ist. - Hinterfragen Sie, ob tatsächlich die ganze Verarbeitung an einem Standort stattfindet. Ggf. kommen Subdienstleister zum Einsatz, die wiederum anderswo ansässig sein können. Das kann die Sache unter Datenschutzaspekten schwierig machen.	☐ Ja ☐ Nein
Welche Dienstleister oder Anbieter kommen in Betracht?	- Gerade im Zusammenhang mit der Auftragsverarbeitung muss Ihr Unternehmen beachten: Der Billigste ist nicht immer der Beste. - Klären Sie, welche Dienstleister in Betracht gezogen wurden.	☐ Ja ☐ Nein
Warum ist der ausgewählte Dienstleister bzw. Anbieter im Datenschutz als fähig und zuverlässig anzusehen?	- Das zielt darauf ab, dass Art. 28 DSGVO Ihrem Unternehmen auferlegt, nur mit qualifizierten Auftragsverarbeitern zu arbeiten. Die müssen hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO stattfindet. - Fordern Sie entsprechende Bewertungen ein. Gibt es diese nicht, sollten diese erstellt werden. Schließlich ist aufgrund der bestehenden Rechenschaftspflicht eine Nachweisbarkeit unerlässlich.	☐ Ja ☐ Nein
Wie steht es um die Sicherheit der Verarbeitung bzw. der Daten?	- Lassen Sie sich die Maßnahmen des Dienstleisters bzw. des Anbieters erläutern. - Fordern Sie Datenschutzkonzepte oder Zertifizierungen an. Prüfen Sie bei Zertifizierungen, was konkret zertifiziert wurde, wer zertifiziert hat und ob die Zertifizierung noch gültig ist. - Denken Sie auch an den Schutz drum herum. So z. B. für die Frage, wie die Daten zum Dienstleister kommen und wie Daten abgesichert werden, etwa durch ein Back-up.	☐ Ja ☐ Nein
Gibt es ein Datenschutzniveau, das für unsere Verarbeitung angemessen ist?	- Die (Standard-)Schutzmaßnahmen des Dienstleisters bzw. des Anbieters können auf dem Papier super klingen. Doch sie müssen ganz konkret zur Schutzwürdigkeit und zum Schutzbedarf Ihres Unternehmens und dessen Verarbeitung passen. - Die Risikoanalyse Ihres Unternehmens muss Maßstab für die Bewertung sein. Aussagen aus „Hochglanzbroschüren“ helfen nicht. Ihr Unternehmen ist und bleibt für die Verarbeitung verantwortlich.	☐ Ja ☐ Nein
Sind kritische oder problematische Subdienstleister im Einsatz?	- Gibt es diese angeblich nicht, sollten Sie genauer hinschauen. Meist können Dienstleister oder Anbieter die angebotene Leistung nicht ohne weitere Dienstleister erbringen. Haken Sie bezüglich einer Liste nach. Intransparenz kann zum großen Problem werden. - Gerade bei Subdienstleistern sollte auch unter dem Aspekt „Konkurrenz“ genau geprüft werden. Ein Konkurrent hätte ggf. Einblick in die Geschäftstätigkeit Ihres Unternehmens, selbst wenn Daten nicht vereinbarungswidrig verarbeitet werden.	☐ Ja ☐ Nein
Wie wird der Datenschutz vertraglich geregelt?	- Klären Sie, inwieweit es eine Vereinbarung geben soll und ob etwas verhandelbar ist. Läuft die Sache nach dem Motto „Friss oder stirb“ und kann Ihr Unternehmen nicht mitreden, sollten die entsprechenden Risiken bewertet werden. - Prüfen Sie, inwieweit die Vereinbarung zu den tatsächlichen Rollen der Beteiligten passt. Wird die falsche Vereinbarung geschlossen, kann Ärger vorprogrammiert sein, etwa auch mit der Datenschutzaufsicht. - Achten Sie auch auf das vereinbarte Recht. Zwar wird die Anwendung der DSGVO meist kein Thema sein. Anders kann es für die sonstigen Rahmenbedingungen aussehen.	☐ Ja ☐ Nein
Was passiert, wenn der Dienstleister oder die Cloud ausfällt?	- Hier sollten Sie das Thema „Business Continuity Management“ hinterfragen. Besprechen Sie, wie sichergestellt wird, dass man auch bei Problemen oder dem Ausfall des Dienstleisters bzw. Anbieters weiterarbeiten kann. Gibt es keine Überlegungen, kann das die Existenz des Unternehmens bedrohen. - Klären Sie zudem, auf welche Zwischen- und Notfälle man sich vorbereitet. Auch eine ausgefallene Internetverbindung kann zum Problem werden, wenn der Dienstleister oder Anbieter nicht mehr erreichbar ist.	☐ Ja ☐ Nein
Können wir schnell und unproblematisch Betroffenenrechte erfüllen?	- Ist Ihr Unternehmen Verantwortlicher, muss es den entsprechenden Verpflichtungen nachkommen können, und zwar grundsätzlich unverzüglich. Dabei muss ggf. auch der Dienstleister oder Anbieter unterstützen. Macht er das nicht, kann Ihr Unternehmen seine Pflichten nicht erfüllen. Ärger ist dann vorprogrammiert. - Haben Sie auch ein Auge auf den Umfang und eventuelle Kosten einer Unterstützung durch den Dienstleister. Ggf. können hier im Vertrag erhebliche Risiken lauern.	☐ Ja ☐ Nein
Wie soll die Einhaltung der Datenschutzstandards beim Dienstleister bzw. Anbieter überwacht werden?	- Wie detailliert man prüft, hängt insbesondere von der Schutzwürdigkeit der Daten ab. Ggf. reichen Zusicherungen aus. Unter Umständen ist jedoch eine Überprüfung der Schutzmaßnahmen vor Ort unerlässlich. - Lassen Sie sich die entsprechenden Planungen für Prüfungen vorlegen. Dabei muss den Risiken angemessen Rechnung getragen werden.	☐ Ja ☐ Nein



Verpflichtungserklärung noch zeitgemäß?

Das sind Ihre Argumente dafür

Bürokratieabbau ist wichtig, damit es mit der Wirtschaft wieder bergauf geht. Womöglich schaut man daher auch in Ihrem Unternehmen genauer hin und will Angestaubtes und Überflüssiges ausmachen. Vielleicht kommt man daher auch auf die seit jeher praktizierte „Verpflichtung der Mitarbeiter zum Datenschutz“ zu sprechen. Dieses Schriftstück kann man sich doch bestimmt sparen, oder?

Stellen Sie sich vor: Man fragt Sie, ob die Verpflichtungserklärung zum Datenschutz nicht etwas antiquiert sei. Schließlich verursachen die Einholung durch den Vorgesetzten, das Einscannen und Aufnehmen in die Personalakte einiges an Aufwand. Wollen Sie klarmachen, dass eine Verpflichtung der Mitarbeiter auf den Datenschutz weiterhin eine gute Sache ist, brauchen Sie gute Argumente. Mit diesen sieben Argumenten sollte Ihnen das Überzeugen leicht von der Hand gehen:

Argument 1: Mit einer Verpflichtungserklärung wird grundlegend sensibilisiert

Gerade wenn jemand seine Tätigkeit in unserem Unternehmen beginnt, ist es wichtig, dass er von Anfang an weiß, dass bestimmte Verhaltensweisen nicht in Ordnung sind. Das gilt erst recht für Azubis, Praktikanten und Aushilfen. Dass personenbezogene Daten des Unternehmens nicht für eigennützige Zwecke verwendet werden dürfen, sollte zwar jedem ohne Weiteres einleuchten. Jedoch kann man sich auch hier nie sicher sein. Daher ist es besser klar zu benennen, was in Ordnung ist und was nicht.

Argument 2: Wir verdeutlichen den Stellenwert des Datenschutzes

Mit einer Verpflichtung machen wir klar, dass Datenschutz kein „Gedöns“ ist. Der richtige Umgang mit personenbezogenen Daten ist wichtig und unser Unternehmen hat sich den Datenschutz auf die Fahne geschrieben. Der Anspruch ist hoch und jeder muss dem gerecht werden.

Argument 3: Eine Verpflichtung schafft Verantwortungsbewusstsein

Durch eine schriftliche und vom Mitarbeiter zu unterzeichnende Verpflichtungserklärung erzeugen wir Verantwortungsbewusstsein. Es wird dem Verpflichteten klar, dass er selbst etwas zu tun hat und auch er seinen Beitrag leisten muss, um Daten angemessen zu schützen. Kommt es zu Verstößen, die der betreffende Mitarbeiter zu verantworten hat, muss er die entsprechenden Konsequenzen tragen.

Argument 4: Wir setzen eine wichtige organisatorische Maßnahme um

Zwar ist eine Verpflichtung selbst nicht ausdrücklich in der Datenschutz-Grundverordnung (DSGVO) geregelt, sprich, es gibt viel Spielraum bezüglich Ob und Wie. Allerdings handelt es sich bei der Verpflichtung um eine organisatorische Maßnahme im Sinne von Art. 24 Abs. 1 DSGVO. Mit dieser stellen wir sicher, dass den Anforderungen der DSGVO im Unterneh-

men entsprochen wird. Auch kann die Verpflichtung als eine grundlegende Weisung im Sinne von Art. 32 Abs. 4 DSGVO bzw. Art. 29 DSGVO angesehen werden. Dadurch wird sichergestellt, dass Mitarbeiter personenbezogene Daten nur im Rahmen des Zulässigen verarbeiten und insbesondere eigenmächtiges Handeln unterbunden wird.

Argument 5: Wir investieren in die Prävention von Fehlverhalten

Mit der Verpflichtung beugen wir Fehlverhalten vor. Ist klar, was erlaubt ist bzw. was passiert, wenn gegen Regeln verstoßen wird, haben Mitarbeiter eine gute Orientierung, um sich richtig zu verhalten. Den meisten Mitarbeitern ist daran gelegen, Ärger aus dem Weg zu gehen. Und der kann drohen, wenn gegen den Datenschutz verstoßen wird, beispielsweise auch vonseiten der Datenschutzaufsicht.

Argument 6: Wir können interessierten Dritten die Sensibilisierung nachweisen

Als Unternehmen sind wir gegenüber der Datenschutzaufsicht rechenschaftspflichtig, beispielsweise nach Art. 5 Abs. 2 DSGVO. Viele weitere Regelungen der DSGVO sehen ausdrücklich vor, dass wir den Nachweis für die wirksame Umsetzung der Anforderungen oder geeigneter bzw. risikoangemessener Maßnahmen erbringen können müssen. Mit einer schriftlichen Verpflichtung können wir grundlegende Weisungen zum Datenschutz nachweisen, deren Kenntnisnahme der Mitarbeiter bestätigt hat. Zudem können Vertragspartner oder Auftraggeber einer Auftragsverarbeitung entsprechende Belege grundlegender Weisungen fordern.

Argument 7: Wir haben im Fall der Fälle etwas in der Hand

Verstößt ein Mitarbeiter gravierend gegen den Datenschutz, kann etwa in einem arbeitsgerichtlichen Verfahren die Vorlage einer vom Mitarbeiter unterzeichneten Verpflichtungserklärung entscheidend sein. Schließlich kann dann niemand behaupten, er hätte von seiner Pflicht nichts gewusst, sorgsam mit personenbezogenen Daten umzugehen. Durch Vorlage des Schriftstücks können wir eine solche Schutzbehauptung sofort entkräften.



Das Ob steht außer Frage, über das Wie lässt sich reden

Eine schriftliche Verpflichtung ist eine Möglichkeit. Aber vielleicht sind andere Ansätze für Ihr Unternehmen die bessere Lösung. Denkbar ist auch, dass die Inhalte in einer Schulung vermittelt werden.

Kellerfund: Was sollen wir mit alten Datenträgern machen?

FRAGE: Unser Unternehmen hat ein Gebäude übernommen. Das gehörte früher einem Unternehmen, das schon vor langer Zeit insolvent gegangen ist. Bei einer Begehung wurden in einem Kellerraum Archivkisten entdeckt. Diese enthalten verschiedene Datenträger, die wohl zur Datenspeicherung genutzt wurden, so z. B. Musikkassetten, Disketten und Videobänder. Die Datenträger sind teilweise beschriftet, etwa mit „Videoüberwachung“, „Datensicherung Personalabrechnung“. Wir haben nun überhaupt keine technische Möglichkeit, die Datenträger zu prüfen. Einfach entsorgen geht ja wohl nicht, da ggf. auch personenbezogene Daten – wenn auch nicht unsere – in falsche Hände geraten könnten. Haben Sie einen Vorschlag, was wir mit den alten Datenträgern machen sollen?

ANTWORT: In Betracht kommen verschiedene Möglichkeiten. Bringen Sie beispielsweise folgende ins Spiel:

- **Rechtsnachfolger finden:** Eventuell lässt sich ausfindig machen, ob es für die insolvente Firma einen Nachfolger gab. Ein Rechtsnachfolger bzw. ein Käufer des insolventen Unternehmens tritt regelmäßig auch die datenschutzrechtliche Nachfolge an und wird so zum Verantwortlichen. Insofern wäre es dann dessen Aufgabe, die Datenträger zu sichten und ggf. datenschutzkonform zu entsorgen.
- **Mit Datenschutzaufsicht abstimmen:** Sie können auch eine Kontaktaufnahme zur Datenschutzaufsichtsbehörde empfehlen. In Abstimmung mit der Behörde kann dann entschieden werden, wie weiter vorzugehen ist. Ggf. hat man dort auch mehr Möglichkeiten, etwas Licht ins Dunkel zu bringen. Das kann sowohl bezüglich der Rechtsnachfolge der Fall sein als auch hinsichtlich der Sichtungsmöglichkeiten der Datenträger.
- **Datenschutzkonforme Entsorgung:** Lässt sich niemand mehr ausfindig machen, der für die Datenträger verantwortlich ist, sollte Ihr Unternehmen dennoch auf Nummer sicher gehen. Die Datenträger sollten so entsorgt werden,

dass ein Zugriff auf möglicherweise personenbezogene Daten ausgeschlossen ist. Gerät nämlich Ihr Unternehmen wegen der Entsorgung in die Schlagzeilen, kann das schnell am Image kratzen. In Betracht kommen folgende Lösungen:

- **Dienstleister beauftragen:** Für das Entsorgen von Datenträgern gibt es zahlreiche Dienstleister. Hier kann ggf. ein Fall der Auftragsverarbeitung vorliegen (Art. 28 Datenschutz-Grundverordnung).
- **Thermische Vernichtung:** Hier kann es sinnvoll sein, mit dem Betreiber einer Müllverbrennungsanlage Kontakt aufzunehmen. Ggf. lassen sich die Kartons mit den Datenträgern direkt der Müllverbrennung zuführen, so dass die Datenträger und die womöglich enthaltenen personenbezogenen Daten sicher vernichtet sind.
- **Selbst Hand anlegen:** Handelt es sich nicht um große Mengen, kann auch der Gang in die Werkstatt oder ein Baumarktbesuch beim Finden der passenden Lösung helfen. So können beispielsweise Disketten problemlos mit einem Bolzenschneider oder einem Hebelschneider so zerlegt werden, dass ein Wiederherstellen und Lesen des Datenträgers ausgeschlossen sind.

Wie kann ich vorgehen, um eine Datenschutzorganisation vorzunehmen?

FRAGE: Ich möchte gern bei uns im Unternehmen eine Datenschutzorganisation mit Strukturen und Prozessen einführen. Haben Sie einige Tipps für mich, wie ich hier am besten vorgehen kann?

ANTWORT: Am besten ist es, wenn Sie sich an den folgenden Tipps orientieren:

- **Starten Sie mit einer Bedarfsanalyse:** Schauen Sie, was nötig ist, damit der Datenschutz besser organisiert wird bzw. leichter oder effektiv umgesetzt werden kann. Denken Sie darüber nach, was es braucht, etwa Regelwerke, Funktionen, Unterstützung oder Prozesse.
- **Überlegen Sie, was Sie erreichen wollen:** Lassen Sie Ihre Interessen nicht außen vor. Der zukünftige Zustand muss auch Ihnen die Arbeit leichter machen.
- **Machen Sie eine Bestandsaufnahme:** Prüfen Sie, was es bereits gibt und worauf Sie aufbauen können.
- **Leiten Sie nötige Maßnahmen ab:** Arbeiten Sie heraus, was es an nötigen Umsetzungsmaßnahmen braucht.
- **Planen Sie kurz-, mittel- und langfristig:** Gehen Sie in kleineren Arbeitspaketen vor. Das hilft dabei, das Ziel zu erreichen, ohne dass die Organisation, Sie und die unterstützenden Kollegen überfordert werden.
- **Stimmen Sie Ihr Vorhaben ab:** Holen Sie Bereiche ab, die von Ihrem Vorhaben betroffen sind oder einen Beitrag leisten müssen. Stimmen Sie Ihre Vorschläge ab.
- **Stellen Sie Ihre Idee der Leitung vor:** Nur wenn es hier grünes Licht gibt, kann die ganze Sache ins Rollen gebracht werden. Zeigen Sie die Vorteile auf. Verschweigen Sie aber nicht die entstehenden Aufwände.



AG Lörrach: Beweisbilder vom Nachbarn können gegen die DSGVO verstoßen

Vielleicht kennen Sie auch den einen oder anderen Fall, bei dem es zwischen Nachbarn nicht wirklich harmonisch zugeht. Da werden auch gerne mal Kameras gezückt, um Verstöße des Nachbarn zu dokumentieren und beispielsweise für einen Rechtsstreit zu verwenden. Doch das kann auch wegen der Datenschutz-Grundverordnung (DSGVO) nach hinten losgehen. Das zeigt ein Urteil des Amtsgerichts (AG) Lörrach vom 3.3.2025, Az. 3 C 1099/24.

Das führte zum Rechtsstreit

In einem als ausschließliches Wohngebiet ausgewiesenen Ortsteil waren auch zwei Männer wohnhaft. Diese wohnten als Nachbarn nebeneinander in einer Straße. Der spätere Kläger wohnte in Nummer 21, der spätere Beklagte in Nummer 19. In diesem reinen Wohngebiet waren gewerbliche Tätigkeiten verboten. Der Kläger war in der Firma seiner Eltern angestellt, einem Hausmeisterdienst.

Nun kam es zu Folgendem: Der Beklagte fühlte sich durch Aktivitäten auf dem Grundstück des Klägers gestört. Seiner Auffassung nach ging dieser einer gewerblichen Tätigkeit nach. Das machte er beispielsweise daran fest, dass mit einigem Lärm und unter Beteiligung weiterer Angestellter der Eltern des Klägers Gartenmaschinen aus einem Firmenfahrzeug aus- und eingeladen wurden.

Nachdem ein klärendes Gespräch aus Sicht des Beklagten keine Besserung brachte, wollte dieser dem gewerblichen Treiben auf dem Nachbargrundstück behördlich den Garaus machen. Nachdem ihm wohl auch sein Anwalt dazu riet, machte der Beklagte im Zeitraum von Februar 2024 bis Januar 2025 zahlreiche Fotos und auch ein Video. Diese Aufnahmen sollten die unzulässige gewerbliche Tätigkeit des Klägers belegen.

Nachbar zieht vor Gericht

Von den Aufnahmen erfuhr auch der Kläger. Er sah sich in seinem Persönlichkeitsrecht unzulässig beeinträchtigt. Alle Aufnahmen würden ihn bei privaten Tätigkeiten zeigen. Also klagte er vor dem AG. Dort forderte er Auskunft über die gefertigten Videos, die Löschung der Bilder und Videos sowie einen Nachweis der Löschung. Außerdem sollte der Beklagte zur Unterlassung verurteilt werden.

Die Beklagtenseite sah die Sache ganz anders. Weil der Kläger bezüglich der unzulässigen Ausübung einer Gewerbetätigkeit keine Einsicht gezeigt hätte, werde mit dem Anfertigen der Bilder und Videos ein berechtigtes Interesse verfolgt. Zudem sei das AG das falsche Gericht. Wegen des Streitwerts von 10.000 € wäre das Landgericht zuständig.

So entschied das AG

Nach Ansicht des Gerichts ist die Klage vor dem AG zulässig. Es ist für die Klage zuständig, weil es den Streitwert nur auf 4.500 € schätzt. Ein höherer Streitwert wäre unangemessen, weil es hier nur um die Einschränkung der Privatsphäre durch eine einzelne Person geht und ein Bezug zur Öffentlichkeit fehlt.

Die Klage ist auch weitgehend begründet. So hat der Kläger einen Auskunftsanspruch. Dieser ergibt sich aus Art. 15 Abs. 1 DSGVO. Dieser wurde auch hinsichtlich der Videoaufnahme erfüllt, weil diese im Schriftsatz des Anwalts inhaltlich beschrieben wurde. Ein weitergehender Anspruch, etwa auf Kopie, wurde vom Kläger nicht geltend gemacht.

Personenbezug ist entscheidend

Es besteht für den Kläger auch ein Anspruch auf Löschung der Bilder und Videos nach Art. 17 Abs. 1 Buchst. d DSGVO. Die DSGVO greift. Es handelt sich um personenbezogene Daten. Die Bilder und Videos sollen Beweis Zwecken dienen, sodass eine rein persönliche Tätigkeit des Beklagten nicht vorliegt. Auch ist der Beklagte Verantwortlicher nach Art. 4 Nr. 7 DSGVO. Er hat die personenbezogenen Daten selbst verarbeitet sowie über Zweck und Mittel entschieden. Dass er dies auf Anraten seines Anwalts machte, ist unbeachtlich.

Rechtsgrundlage fehlt

Es liegt keine Erlaubnis zur Verarbeitung vor, auch nicht nach Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO. Zwar besteht ein berechtigtes Interesse, eine unzulässige Grundstücksnutzung zu dokumentieren. Allerdings besteht keine Erforderlichkeit vor dem Hintergrund des Prinzips der Datenminimierung. Eine Ablichtung von Personen ist nicht erforderlich, um einen eventuellen Verstoß zu dokumentieren. Im Übrigen ist keines der Bilder geeignet, eine gewerbliche Tätigkeit des Klägers zu belegen. Hierfür hatte der Kläger schlüssige und nachvollziehbare Erklärungen für eine private Tätigkeit.

Löschen reicht aus

Zwar hat der Kläger einen Anspruch auf Löschung. Einen Nachweis kann er jedoch nicht verlangen. Art. 5 Abs. 2 DSGVO enthält nur eine abstrakte Rechenschaftspflicht und keinen Anspruch für den Kläger. Im Übrigen zielt Löschen auf ein rückstandsloses Löschen ab. Ein Nachweis, was gelöscht wurde, würde dem widersprechen. Weil der Kläger die Löschung verlangen kann, besteht auch ein Unterlassungsanspruch für die Zukunft.



Das können Sie mit der Entscheidung anfangen

Das Urteil ist ideal, um etwa eine Schulung aufzulockern und die Teilnehmer an einige grundlegende Datenschutzaspekte heranzuführen, etwa die Grundsätze der Verarbeitung oder die Anwendbarkeit der DSGVO. Im Übrigen können Sie folgern: Löschen muss nicht inhaltlich anhand der Daten dokumentiert werden. Es reicht aus, es zu tun.

PROFITIEREN SIE VON DEN DIGITALEN ARBEITSHILFEN



PRIVACYXPERTS – neuer Onlinebereich



Den gesamten Inhalt von „Datenschutz aktuell“
stellen wir Ihnen auch online zur Verfügung.
Schauen sie einfach unter www.privacyxperts.de



QR-Code scannen
und loslegen!



Ihre Vorteile im Überblick:

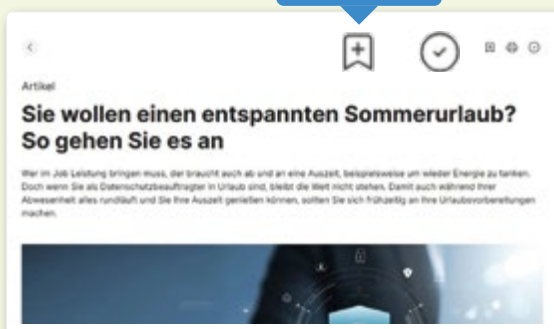
Ihr Onlinebereich bietet Ihnen alle Ausgaben und Beiträge auf einen Klick sowie zahlreiche Muster und Vorlagen zum praktischen Sofort-Download.

Alle Inhalte auf einen Blick!

Lassen Sie sich alle bisher erschienenen Ausgaben online anzeigen. Wählen Sie die gewünschten Inhalte – Ausgaben, Beiträge und Muster-Vorlagen. Laden Sie sich diese herunter oder lesen und nutzen Sie sie gleich online.



Merken



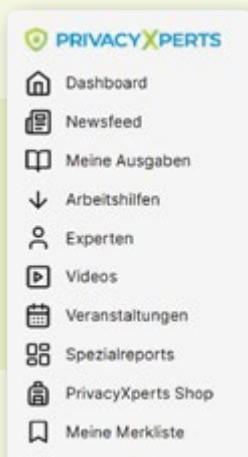
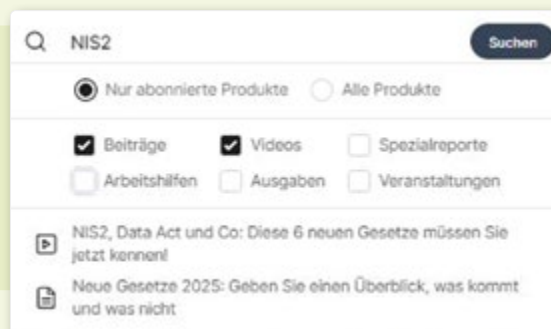
Tipp:

Setzen Sie die für Sie wichtigsten Ausgaben, Beiträge und Arbeitshilfen auf Ihre Merkliste. So haben Sie Ihre TOP-Themen immer schnell im Blick.

Praktische Suchfunktion!

Sie suchen nach etwas Bestimmtem – beispielsweise Informationen über das Thema NIS2?

Geben Sie Ihren Suchbegriff in das Suchfeld ein und wählen Sie das gewünschte Format.



Erkunden Sie Ihren Onlinebereich ...

... und entdecken Sie viele weitere, nützliche, hilfreiche und interessante Inhalte und Inklusivleistungen, die Ihren Fachratgeber optimal ergänzen. Viel Erfolg!



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:

Personelle Änderungsmitteilungen: Das sollten Sie prüfen
Gut aufgestellt im Datenschutz? Machen Sie den Check