DATENSCHUTZAKTUELL
JUL I 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

LEERLAUF IM SOMMER? DAS KÖNNEN SIE IN ANGRIFF NEHMEN

DATENSCHUTZ-BEAUFTRAGTER
Sind Sie überflüssig? Das sind 20 gute Gegenargumente 1–2

KNOW-HOW
Sie brauchen Software? So hat Ihre Auswahl Hand und Fuß 6

Setzen Sie auf Risikoorientierung

Liebe Leserin, lieber Leser,

wenn es Ihnen wie den meisten Datenschutzbeauftragten geht, haben Sie wahrscheinlich eher zu wenig als zu viel Zeit für die Wahrnehmung Ihrer Aufgaben. Oft lässt sich an dieser Situation auch nicht wirklich etwas ändern. Also müssen Sie das Beste daraus machen. Und das gelingt Ihnen, indem Sie sich an der Datenschutz-Grundverordnung orientieren.

Fordern Sie unbedingt mehr Unterstützung. Setzen Sie zugleich bei all Ihren Aufgaben auf Risikoorientierung. Gehen Sie immer zuerst die kritischsten Dinge an und kümmern Sie sich um weniger problematische Themen, wenn Sie die Zeit dazu finden.

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 im Unternehmen pragmatisch umsetzen lässt.

Inhalt

Datenschutzbeauftragter
Sind Sie überflüssig?
Das sind 20 gute Gegenargumente
Seiten 1–2

Produktiver beraten: So können
Sie vorgehen
Seite 3

Datenschutzorganisation
Leerlauf im Sommer? Das können
Sie in Angriff nehmen
Seiten 4–5

Know-how
Sie brauchen Software? So hat Ihre
Auswahl Hand und Fuß
Seite 6

Fragen an die Redaktion
Wie gehen wir mit dem Widerruf
der Einwilligung um?
Seite 7

Müssen unsere Datenschutzhinweise
akzeptiert werden?
Seite 7

Recht
Gehackte Altdaten führen nicht zu
Schadensersatz
Seite 8

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

Live-Talk:
https://t1p.de/live-talk

E-Mail-Beratung:
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 | PhotoSG; Seite 1: Adobe Stock | Jubayer

Erscheinungsweise: 36-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.

Bereiten Sie sich Ihre Argumente vor, wenn Ihr Arbeitgeber Sie für entbehrlich hält.

Sind Sie überflüssig? Das sind 20 gute Gegenargumente

Die Zeiten waren für den Datenschutz schon rosiger. Wo man auch hinschaut, wollen Politiker die Rahmenbedingungen verändern. Neben Sparaktionen bei Aufsichtsbehörden zieht man in Deutschland auch in Betracht, die Pflicht zur Benennung eines Datenschutzbeauftragten zu streichen. Bereiten Sie sich also am besten auf alle Eventualitäten vor.

Das steht an

Der Bund und die Länder in Deutschland haben sich das Thema Entbürokratisierung auf die Fahnen geschrieben. Ziel der „Föderalen Modernisierungsagenda" (https://t1p.de/3mhc3) ist es, gerade für Unternehmen bürokratische Pflichten zu streichen. Eine davon ist nach Ansicht der Politik die Regelung in § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG). Sollte diese Regelung tatsächlich gestrichen werden, dürfte für viele Unternehmen die nach dem BDSG geltende Vorgabe zur Benennung eines Datenschutzbeauftragten entfallen.

Keine Entlastung in Sicht

Was die Politik bei der Sache gerne verschweigt: Wirkliche Entlastung bedeutet das nicht. Die Datenschutz-Grundverordnung (DSGVO) gilt weiterhin in vollem Umfang. Und ggf. braucht das Unternehmen nach wie vor einen Datenschutzbeauftragten, eben auf Basis von Art. 37 DSGVO. Zudem: Weil das Unternehmen weiterhin voll den DSGVO-Anforderungen unterliegt, ist jemand mit Know-how und Erfahrung im Datenschutz erforderlich. Denn nur so hat die Umsetzung Hand und Fuß und Risiken werden wirklich minimiert.

Sie sind auch auf „freiwilliger Basis" wichtig

Vielleicht meint mancher in Ihrem Unternehmen, dass es ohne Sie als Datenschutzbeauftragter besser läuft und Datenschutz zum Kinderspiel wird. Bereiten Sie sich darauf vor, diesen Zahn ziehen zu müssen. Das gelingt Ihnen mit guten Argumenten. 20 Argumente finden Sie in dieser Checkliste. Gehen Sie die Punkte durch und finden Sie Beispiele aus Ihrer Tätigkeit. Dann sind Sie auch für schwierige Diskussionen über die Sinnhaftigkeit eines Datenschutzbeauftragten gut gerüstet.

Checkliste: Darum braucht Ihr Unternehmen Sie als Datenschutzbeauftragter

Darum werde ich als Datenschutzbeauftragter gebraucht	Hintergrund	Ihre Einfälle, Ideen, Beispiele
Mit meiner Beratung und meinen Kontrollen sichere ich die Compliance des Unternehmens.	› Jedes Unternehmen muss sich an Gesetze und Regelung halten, sprich compliant arbeiten. › Ohne Datenschutzbeauftragten kann es hier zu schweren Defiziten kommen, etwa wenn gegen die DSGVO verstoßen wird.	10 durchgeführte Audits, 6 gravierende Defizite behoben
Mit meiner Arbeit werden Bußgelder, Imageschäden und Umsatzeinbußen verhindert.	› Bußgelder können existenzbedrohend sein, auch wenn der Bußgeldrahmen des Art. 83 DSGVO nicht ausgeschöpft wird. › Wird schlechter Datenschutz publik, ist ein Imageschaden meist die Konsequenz. Zudem können Kunden ausbleiben oder abwandern.	Datenschutzpanne in 2025 führte aufgrund guter Datenschutzorganisation nur zu Verwarnung durch Datenschutzaufsicht.

Bei mir sind Know-how und Erfahrung zur praktischen Umsetzung der DSGVO-Anforderungen gebündelt.	› Fachliches und rechtliches Wissen allein reicht nicht aus. Es braucht auch viel Know-how bei der praktischen Umsetzung der Anforderungen. › Langjährige Praxiserfahrung aus dem Unternehmen kann durch nichts ersetzt werden, weder durch eine Kanzlei noch durch KI.	
Ich vermittle Führungskräften und Mitarbeitern das nötige Datenschutzwissen.	› Sind alle bedarfsgerecht informiert und geschult, können Fehler und falsches Handeln vermieden werden. › Praxisnahe und auf den Bedarf zugeschnittene Schulungen gibt es nur von einem fähigen Datenschutzexperten.	
Neue Herausforderungen und neue Gefahren kann ich früh identifizieren.	› Eine frühzeitige Einbindung sorgt dafür, dass es keiner teuren Nachbesserungen im Datenschutz bedarf. › „Privacy by Design" wird als gesetzliche Pflicht nur mit einem Profi sachgerecht umgesetzt.	
Mit meinen Aktivitäten bleibt Datenschutz als Thema präsent.	› Mit mir gibt es kein „Aus den Augen, aus dem Sinn". › Mit Aktivitäten und regelmäßiger Kommunikation halte ich das Thema präsent und trage zur Umsetzung des Datenschutzes bei.	
Ich trage dazu bei, dass Betroffenenrechte ordnungsgemäß erfüllt werden.	› Betroffenenrechte sind ein komplexes Thema. Hier kann ohne Know-how viel falsch gemacht werden, was schnell zu Bußgeldern oder Schadensersatzforderungen führen kann. › Schon bei der Transparenzpflicht gibt es viele Stolperfallen. Mit meiner Unterstützung bleibt das Stolpern aus.	
Mit mir sinkt das Risiko für Datenpannen und Hackerangriffe.	› Awareness ist hier ein wichtiger Faktor, damit es nicht zu Vorfällen kommt. › Passiert doch etwas, trage ich dazu bei, dass der Schaden begrenzt bleibt und Meldepflichten ordnungsgemäß erfüllt werden.	
Beim Verzeichnis von Verarbeitungstätigkeiten sorge ich dafür, dass alles passt.	› Das Unternehmen muss seine Verarbeitungstätigkeiten dokumentieren. Passiert das nicht, kann ein Bußgeld drohen. › Ich unterstütze dabei, dass dieses „ungeliebte Thema" leicht von der Hand geht und dass inhaltlich alles passt.	
Ich sorge dafür, dass Risiken ordentlich beurteilt und sachgerecht behandelt werden.	› Risikoorientierung ist eine zentrale Datenschutzforderung. Dieser wird das Unternehmen mit mir leichter gerecht. › Gerade bei Schutzmaßnahmen achte ich darauf, dass den Risiken angemessen begegnet wird.	
Meine Arbeit sorgt dafür, dass Defizite frühzeitig erkannt werden.	› Es ist nötig, dass jemand im Datenschutz mit offenen Augen durchs Unternehmen geht. › Gibt es Gefahren, müssen diese ernst genommen werden. Ich adressiere den Handlungsbedarf.	
Dank meiner Unterstützung erfüllt das Unternehmen seine Rechenschaftspflicht.	› Vieles im Datenschutz muss das Unternehmen nachweisen können. Gelingt das nicht, kann auch das zu einem Bußgeld führen. › Nachvollziehbarkeit ist unerlässlich, vor allem wenn es um Rechtsgrundlage, Bewertungen und Maßnahmen geht.	
Ich begleite kompetent erforderliche Datenschutz-Folgenabschätzungen.	› Gerade beim Einsatz neuer Technologien (z. B. KI), systematischer Überwachung oder bei der Verarbeitung besonderer Kategorien personenbezogener Daten können solche besonderen Prüfungen erforderlich sein. › Damit die Folgenabschätzungen formell und inhaltlich passen, braucht es einen Spezialisten im Datenschutz.	
Bei Datenschutzfragen agiere ich unabhängig und weisungsfrei.	› Wer sich selbst kontrolliert, beurteilt die Dinge eher zu seinen Gunsten. Das kann im Datenschutz zum Problem werden. › Mit einem Datenschutzbeauftragten werden Bewertungen objektiviert.	
Ich trage zur risiko- und sachgerechten Weiterentwicklung der Datenschutzstrategie bei.	› Das Unternehmen muss auch im Datenschutz mit der Zeit gehen, etwa hinsichtlich der Umsetzungsstrategie. › Als jemand mit viel Know-how und Erfahrung kann der Datenschutzbeauftragte zu einer zielgerichteten Steuerung beitragen.	
Meine Existenz kann gut fürs Geschäft sein.	› Kunden ist der sichere Umgang mit ihren Daten wichtig. Sie schauen genau hin, wie Unternehmen das machen. › Geschäftspartner müssen ebenfalls Risiken minimieren. Warum sollten diese Datenschutzrisiken eingehen, weil der Vertragspartner beim Datenschutz spart?	
Ich bin Vertrauensperson für alle Beschäftigten in Datenschutzfragen.	› Mitarbeiter müssen Defizite und Probleme im Datenschutz ohne Sorge melden können. Hier ist ein Datenschutzbeauftragter idealer Ansprechpartner. › Ein Datenschutzbeauftragter kann zu einer positiven Fehlerkultur beitragen.	
Es wirkt bußgeldmindernd, dass es mich gibt.	› Bei der Bußgeldbemessung wird vieles berücksichtigt. Auch wie man es mit dem Datenschutz hält und diesen organisiert, kann ein relevanter Faktor sein. › Das Unternehmen muss immer alle Aspekte der DSGVO umsetzen. Das geht leichter und fehlerfreier mit einem Datenschutzbeauftragten.	
Ich koste weniger, als ich bringe.	› Den Datenschutzbeauftragten einsparen ist eine Milchmädchenrechnung. Pannen und Verstöße werden garantiert teuer. › Eingekaufte Ad-hoc-Beratungen sind oft aufwendiger und teurer als die dauerhafte Betreuung durch einen Datenschutzbeauftragten.	

Produktiver beraten: So können Sie vorgehen

Geht es um Datenschutzfragen, sind Sie Ansprechpartner Nummer eins. Dass Sie hier Ihren Job möglichst gut erledigen wollen, ist bestimmt auch für Sie ein Anliegen. Mehr Effizienz und höhere Produktivität kommen nicht von selbst. Doch entsprechend besser zu werden ist machbar.

Soll eine Beratung produktiv verlaufen und am Ende eines Besprechungstermins ein gutes Ergebnis stehen, heißt es: planvoll vorgehen! Denn lassen Sie eine Beratung oder einen Termin einfach auf sich zukommen, kann das auch vertane Zeit sein. Das muss nicht sein. Orientieren Sie sich an den folgenden zehn Schritten:

Schritt 1: Machen Sie das Ziel aus

Das ist in mehrfacher Hinsicht wichtig. Geht es beispielsweise um einen Termin, zu dem man Sie eingeladen hat, sollten Sie vorab klären, worum es konkret gehen wird. Dabei ist nicht nur das Thema wichtig, damit Sie sich darauf einstellen können. Auch ist von großer Bedeutung, was man von Ihnen will. Klären Sie, ob es nur um einen ersten Austausch, eine Risikoeinschätzung, einen Lösungsvorschlag oder die Prüfung der datenschutzrechtlichen Rahmenbedingungen geht,

Daneben sollten Sie bei einem Vorhaben klären, was am Ende stehen soll. Meist wird es den Teilnehmern um eine bestimmte Verarbeitung oder eine diesbezügliche Vorgehensweise gehen. Wissen Sie, dass man bestimmte Daten für einen konkreten Zweck verarbeiten will, können Sie Ihre Beratung auf dieses Wunschziel ausrichten.

Schritt 2: Ermitteln Sie den Sachverhalt vollständig

Beschaffen Sie sich möglichst viele Informationen, damit Sie das ganze Bild haben. Denn je besser Sie den Sachverhalt kennen, desto besser und zielgerichteter können Sie Ihre Beratung gestalten. Das bringt zudem den Vorteil mit sich, dass Sie Ihre Kapazitäten punktgenau auf das fachlich Relevante konzentrieren können.

Schritt 3: Klären Sie Relevantes im Unternehmen

Gerade bei größeren Vorhaben kann noch vieles im Ideenstadium stecken. Ggf. müssen erst noch ein Projektteam zusammengestellt, zukünftige Strukturen geschaffen oder auch Technik beschafft werden. Zudem: Bei manchen Verarbeitungen kann auch das Thema Mitbestimmung eine große Rolle spielen. Gespräche mit dem Betriebsrat oder auch eine ggf. erforderliche Betriebsvereinbarung können Leitplanken für die Verarbeitung der personenbezogenen Daten vorgeben. Bringen Sie hier Licht ins Dunkel, kann Ihnen das anderswo manchen Prüfaufwand ersparen.

Schritt 4: Prüfen Sie, worauf es rechtlich ankommt

Identifizieren Sie die einschlägigen gesetzlichen Normen, sprich insbesondere welchen Rahmen die Datenschutz-Grundverordnung vorgibt. Lesen Sie sich gezielt ein. Setzen Sie hier idealerweise auf aktuelle Fachliteratur. Nutzen Sie am besten mehrere Gesetzeskommentare, um hier gleiche oder unterschiedliche Sichtweisen auszumachen.

Schritt 5: Suchen Sie Statements und Rechtsprechung

Nutzen Sie Veröffentlichungen von Datenschutzaufsichtsbehörden, Datenschutz- und Branchenverbänden, um deren Sichtweisen zu erkennen. Neben thematischen Veröffentlichungen und Tätigkeitsberichten sollten Sie auch nach Rechtsprechung Ausschau halten. Setzen Sie in diesem Zusammenhang auf KI, sollten Sie unbedingt die Ergebnisse verifizieren. KI halluziniert ab und an und reimt sich gerade bei Rechtsprechung gerne etwas zusammen.

Schritt 6: Bewerten Sie die Risiken

Bei allem, was man tut, gibt es Chancen und Risiken. Beim Verarbeiten personenbezogener Daten ist es unerlässlich, dass Sie hier genauer hinschauen. Klären Sie mit den Kollegen die Gefahren und die sich daraus ergebenden Risiken. Erst wenn man hier den Überblick hat, wird deutlich, wie groß die Dimension und die Auswirkungen einer Verarbeitung sind, etwa für Betroffene und für Ihr Unternehmen.

Schritt 7: Entwickeln Sie Lösungswege gemeinsam

Sie müssen nicht alles selbst machen. Setzen Sie sich mit den Kollegen zusammen, machen Sie ein Brainstorming und bewerten Sie mögliche Alternativen mit Pro- und Kontralisten.

Schritt 8: Sprechen Sie konkrete Empfehlungen aus

Wichtiger Teil Ihrer Beratung ist, dass Sie eine konkrete Einschätzung geben und den Kollegen eine Vorgehensweise empfehlen. Beziehen Sie hier mit ein, dass Ihr Vorschlag praktikabel sein muss.

Schritt 9: Unterstützen Sie die Umsetzung

Mit einer Beratung ist es meist nicht getan. Regelmäßige Folgetermine sind unerlässlich. Die sind auch wichtig, um den Fortschritt zu verfolgen. Zudem können Sie so frühzeitig erkennen, ob man irgendwo falsch abgebogen ist.

Schritt 10: Dokumentieren Sie Ihre Beratung

Halten Sie schriftlich fest, was Sie beraten haben, welche Entscheidungen getroffen wurden und wer was bis wann zu machen hat. Um auch später noch auskunftsfähig zu sein, sollten Sie Ihre Dokumentation für mindestens drei Jahre nach dem Verarbeitungsende aufbewahren.

Leerlauf im Sommer? Das können Sie in Angriff nehmen

Nicht jeder geht im Sommer in Urlaub. Vielleicht zählen auch Sie zu denjenigen, die die etwas ruhigere Zeit im Unternehmen genießen. Denn auch das kann ein „kleiner" Urlaub sein. Und Sie können in den ruhigeren Wochen mehr bewegen als Sie vielleicht denken.

Nutzen Sie die Zeit geschickt

Sind Sie im Unternehmen vor Ort, könnten Sie Däumchen drehen, wenn wenig los ist, weil irgendwie alle im Urlaub sind. Doch viel geschickter ist es, wenn Sie die ruhigeren Wochen nutzen, um Liegengebliebenes zu erledigen, klar Schiff zu machen oder kleinere Aktivitäten zu starten. Ideen, was Sie in Angriff nehmen können, finden Sie in der folgenden Checkliste.

Checkliste: Aktivitäten in den ruhigeren Sommermonaten

Das können Sie machen	Tipps zum Vorgehen	Erledigt?
Rund um Ihren Arbeitsplatz		
Machen Sie klar Schiff am Arbeitsplatz.	› Prüfen Sie selbstkritisch, wie gut Sie selber an Ihrem Arbeitsplatz das Clean-Desk-Prinzip einhalten. Machen Sie sich Gedanken, wo es etwas zu verbessern gibt. › Durchforsten Sie Ablagen, Rollcontainer und Schränke. Hier kann sich mit der Zeit so einiges ansammeln. › Arbeiten Sie bei Unterlagen am besten mit drei Stapeln oder Kisten. Packen Sie das, was Sie behalten wollen, in die erste Kiste. Was datenschutzkonform zu entsorgen ist, kommt in die zweite Kiste. Und in die dritte Kiste kommt das unbedenkliche Altpapier. › Klar Schiff machen ist nicht nur am Arbeitsplatz im Büro wichtig. Arbeiten Sie auch von zu Hause aus, sollten Sie auch diesen Arbeitsplatz genauer unter die Lupe nehmen.	○ Ja ○ Nein
Entrümpeln Sie Ihr E-Mail-Postfach.	› Machen Sie zunächst E-Mails ausfindig, die garantiert keine Relevanz mehr haben. Die betreffen oft Organisatorisches mit geringer Bedeutung für Ihre Arbeit. Das können Newsletter, Veranstaltungsinfos oder alte Speisepläne sein. › Arbeiten Sie mit einer geeigneten Ordnerstruktur im Postfach, um Abgelegtes später auf Anhieb wiederzufinden und nicht die oft unzureichende Suchfunktion nutzen zu müssen. › Wollen Sie Platz im Postfach sparen, können Sie auch E-Mails auslagern bzw. in PDFs umwandeln.	○ Ja ○ Nein
Bringen Sie Ordnung in Dokumentenablage und digitale Verzeichnisse.	› Prüfen Sie, inwieweit die bisherige Ordnerstruktur noch passt und Ihre Arbeit unterstützt. Macht sie Ihnen das Leben schwer, sollten Sie das schnellstens ändern. › Bewerten Sie Inhalte vor allem nach ihrer Relevanz und Aufbewahrungspflicht. Ist Letzteres entscheidend, sortieren Sie die Inhalte so, dass Sie sie für den Aufbewahrungszeitraum leicht finden. Das kann thematisch passieren, aber auch nach Jahren. › Prüfen Sie Ihr Notebook oder Ihr Smartphone auf lokal gespeicherte Daten, die Sie aufbewahren wollen. Verschieben oder kopieren Sie diese auf zentrale Datenablagen. › Achten Sie darauf, dass Ihre Daten regelmäßig gesichert werden. Klären Sie das Thema „Back-up".	○ Ja ○ Nein
Digitalisieren Sie Papierunterlagen.	› Relevante Unterlagen können Sie einscannen und in durchsuchbare PDF-Dateien umwandeln. › Überlegen Sie, ob Sie die Originale noch brauchen oder aufbewahren müssen. Ansonsten sollten Sie das Entsorgen erwägen.	○ Ja ○ Nein
Sortieren Sie veraltete Technik aus.	› Mit der Zeit kann sich so manches an veralteter Technik anhäufen. Schauen Sie gerade in Schränke oder Schubladen. Entsorgen Sie, was Sie nicht mehr brauchen oder was nicht mehr up to date ist. › Entsorgen Sie Geräte mit Datenspeichern nie unüberlegt. Sorgen Sie für eine sichere Löschung. Diese muss so erfolgen, dass Unbefugte auf die Daten keinen Zugriff nehmen können.	○ Ja ○ Nein
Checks und Prüfungen		
Führen Sie Clean-Desk-Begehungen durch.	› Statten Sie Großraumbüros gerade in Randzeiten einen Besuch ab. Prüfen Sie, inwieweit die Kollegen nichts Schützenswertes herumliegen lassen. Auch Computer sollten gesperrt sein. › Kritische Defizite sollten Sie direkt ansprechen. Bei weniger Schlimmem können Sie auch eine Haftnotiz mit einem Hinweis hinterlassen.	○ Ja ○ Nein

Machen Sie eine Tour durchs Unternehmen.	› Steuern Sie gezielt Orte an, an denen personenbezogene Daten zu finden sein können. Denken Sie an Besprechungsräume, Schwarze Bretter oder Kopierräume. Doch auch Technikräume oder Materiallager werden gerne genutzt, um etwas unterzubringen, was dort nichts verloren hat. › Schauen Sie sich auch einmal außerhalb der Gebäude um. Gibt es eine Videoüberwachung, können Sie die Standorte der Kameras prüfen. Haben Sie zudem ein Auge auf Veränderungen oder Neuerungen, von denen Sie noch nichts wissen. › Besuchen Sie Bereiche, in denen Sie bislang noch nicht waren. Vielleicht haben die doch mehr Datenschutzrelevanz, als Sie bisher angenommen haben.	○ Ja ○ Nein
Überprüfen Sie das Onlineangebot.	› Werfen Sie insbesondere einen Blick in die Datenschutzhinweise. Diese müssen das abdecken, was auf der Webseite passiert. Fehlt etwas, adressieren Sie das an die zuständigen Kollegen. › Auch ins Impressum kann sich ein Blick lohnen. Auch das muss vollständig und aktuell sein. Prüfen Sie insbesondere, ob die Angaben nach § 5 Digitale-Dienste-Gesetz vorhanden sind.	○ Ja ○ Nein
Nehmen Sie das Verzeichnis von Verarbeitungstätigkeiten unter die Lupe.	› Überprüfen Sie die Inhalte des Verzeichnisses einerseits auf Vollständigkeit. Hier müssen die Angaben für das jeweilige Verzeichnis nach Art. 30 Datenschutz-Grundverordnung (DSGVO) passen. Andererseits müssen die Angaben aktuell sein, sprich zur tatsächlich durchgeführten Verarbeitungstätigkeit passen. › Dokumentieren Sie, wo Sie Anpassungsbedarf entdeckt haben. Adressieren Sie die Aufgabe an die jeweils zuständigen Kollegen.	○ Ja ○ Nein
Aktualisieren Sie Muster, Unterlagen und Awareness-Materialien.	› Machen Sie den inhaltlichen Check. Haben Sie insbesondere ein Auge auf veraltete Informationen oder Gesetzesangaben. › Auch eine „Renovierung" kann sinnvoll sein. Gestaltungsvorschläge kann Ihnen auch Ihre Präsentationssoftware machen. Auch ein alter Inhalt kann so viel moderner wirken.	○ Ja ○ Nein
Unterziehen Sie das Datenschutzkonzept einem Check.	› Prüfen Sie, ob die Wege und Mittel zur Umsetzung des Datenschutzes noch zu Ihrem Unternehmen passen. Gab es beim Unternehmen Veränderungen, muss ggf. auch der Datenschutz verändert oder neu gedacht werden. › Starten Sie mit einem Blick in Strukturpläne, Pläne zur Unternehmensorganisation oder Organigramme. Ist etwas für Sie nicht nachvollziehbar, lassen Sie sich die Zusammenhänge erklären.	○ Ja ○ Nein
Prüfen Sie die Risikosituation des Unternehmens oder kritischer Verarbeitungen.	› Vieles im Datenschutz passiert risikoorientiert. So ist das Bewerten von Risiken Ausgangspunkt für die nötigen technischen und organisatorischen Schutzmaßnahmen. Wichtig ist also, dass die Bewertung der Risiken aktuell und zutreffend ist. › Schauen Sie gerade bei kritischen Verarbeitungen genauer hin. Das können Verarbeitungen sein, bei denen es um besondere Datenkategorien im Sinne von Art. 9 Abs. 1 DSGVO geht.	○ Ja ○ Nein
Identifizieren Sie Anpassungsbedarf bei Verträgen.	› Papier ist geduldig. Und nur weil etwas geregelt ist, muss es noch lange nicht so umgesetzt sein. Prüfen Sie also Vereinbarungen mit Datenschutzrelevanz, ob es hier Anpassungsbedarf gibt. › Gehen Sie risikoorientiert vor. Je problematischer oder risikobehafteter beispielsweise eine Auftragsverarbeitung ist, desto eher sollten Sie nach dem Rechten schauen.	○ Ja ○ Nein
Prüfen Sie die Eignung und die Aktualität von Notfall- und Krisenplänen.	› Legen Sie hier den Fokus auf Datenschutzrelevantes. Das können beispielsweise Pläne oder Verhaltensanweisungen für Datenpannen oder Angriffe von Cyberkriminellen sein. › Bewerten Sie kritisch die Praxistauglichkeit entsprechender Pläne. Nicht selten klaffen Theorie und Praxis weit auseinander.	○ Ja ○ Nein
Rund um Ihren Job		
Planen Sie Ihr zweites Halbjahr.	› Nutzen Sie die Zeit, um die nächsten Monate zu planen. Denken Sie etwa an Audits oder Schulungsmaßnahmen. › Haben Sie nicht nur ein Erledigungsdatum im Blick. Planen Sie auch den Weg dahin.	○ Ja ○ Nein
Checken Sie Budget und Ressourcen.	› Können Sie nicht aus dem Vollen schöpfen, ist ein Check unerlässlich, damit hier nichts aus dem Ruder läuft. › Klären Sie, inwieweit Sie für angedachte Aktivitäten auf entsprechende Ressourcen zurückgreifen können.	○ Ja ○ Nein
Bilden Sie sich weiter.	› Jeder Datenschutzbeauftragte hat mehr oder weniger große Wissenslücken. Machen Sie sich daran, diese etwas kleiner zu machen. › Haben Sie auch Soft Skills auf dem Radar. Fällt Ihnen manches leichter, haben Sie mehr Spaß im Job.	○ Ja ○ Nein
Sammeln Sie Themen für den Tätigkeitsbericht.	› Damit es am Jahresende weniger aufwendig wird, können Sie schon jetzt erste Themen zusammenstellen. › Notieren Sie nicht nur Ideen. Halten Sie unbedingt auch Fundstellen detailliert fest. Das erleichtert Ihnen das spätere Wiederfinden.	○ Ja ○ Nein
Pflegen Sie Kontakte.	› Statten Sie Kollegen einen Besuch ab. Lassen Sie dabei eventuell den Datenschutz einfach mal beiseite. Auch ein nicht fachlicher Austausch bringt Ihnen viel. › Sagen Sie dort Hallo, wo man Sie noch nie zu Gesicht bekommen hat. Ein kurzer Schwatz kann Berührungsängste abbauen.	○ Ja ○ Nein

Sie brauchen Software? So hat Ihre Auswahl Hand und Fuß

Als Datenschutzbeauftragter arbeiten Sie viel mit dem Computer. Egal, ob Sie eine Präsentation erstellen oder bei der Zusammenstellung von Unterlagen für eine Betroffenenauskunft unterstützen: Mit der passenden Software können Sie sich das Leben erleichtern, produktiver sein und viel schneller zu besseren Ergebnissen kommen. Doch vorab sollten Sie so einiges klären.

Bedenken Sie stets Ihre Rolle

Einfach mal ein Programm herunterladen, mit dem man bequem unzählige Dateien umbenennen kann, ist ziemlich verlockend. Das umso mehr, wenn das Programm direkt ausführbar und als Open-Source-Software sogar gratis ist. Doch Sie dürfen als Datenschutzbeauftragter nicht Wasser predigen und Wein trinken. Sie müssen sich an die üblichen Regeln halten, wenn es um die Beschaffung und den Einsatz von Software geht. Außerdem: Gerade Sie als Datenschutzbeauftragter sind in einer Vorbildfunktion. Sie müssen darauf achten, dass alles passt und insbesondere den Anforderungen zu Datenschutz und Datensicherheit entsprochen wird. Bevor Sie also einen Download starten, sollten Sie sich mit einigen wichtigen Aspekten beschäftigen. Nutzen Sie dazu die folgende Checkliste. Die können Sie auch verwenden, wenn Sie Kollegen entsprechend beraten sollen.

Checkliste: Software-Auswahl und Beschaffung

Das sollten Sie prüfen	Hintergrund	Geklärt, geprüft und in Ordnung?
Machen Sie aus, was Sie wirklich brauchen.	› Machen Sie sich bewusst, was Sie wirklich brauchen. Unter Umständen reicht eine einfachere Software vollkommen aus, wenn die benötigten Funktionen auch in der „Sparversion" enthalten sind. › Lassen Sie sich nicht von „Marketingversprechen" beeindrucken. Funktionen, die Sie nicht brauchen, haben für Sie selbst gerade keine Funktion. › Visualisieren Sie, was Sie brauchen. Machen Sie eine Liste mit „Muss"-, „Soll"- und „Kann"-Funktionen.	○ Ja ○ Nein
Vergleichen Sie Software, Versionen und Editionen.	› Manchmal reicht eine Basis- oder Standard-Version vollkommen aus. Die Professional-Version kann zwar mehr, nicht selten wird aber das nicht wirklich gebraucht. › Auch können Vorversionen in Betracht kommen, wenn diese weiter mit Updates versorgt werden. Eventuell muss es gerade nicht das Neueste sein. Manchmal sind ältere Versionen in Sachen Funktionalität oder Umfang sogar die bessere Wahl.	○ Ja ○ Nein
Nehmen Sie Lizenz- und Abomodelle unter die Lupe.	› Brauchen Sie eine Software nur sporadisch, kann ein kurzfristig kündbares Abo eine gute Wahl sein. › Seien Sie mit „lebenslangen" Lizenzen vorsichtig. Die wirken günstig. Aber wollen Sie für immer bei dieser Version bleiben?	○ Ja ○ Nein
Haben Sie ein Auge auf den Datenschutz.	› Nehmen Sie den Anbieter unter die Lupe, etwa die Webseite, die Datenschutzhinweise und seine Haltung zum Datenschutz insgesamt. › Prüfen Sie, inwieweit die Software zu Datenschutzproblemen führen kann. Werden personenbezogene Daten verarbeitet, müssen auch Sie so einiges bedenken. Achten Sie insbesondere auf die Grundsätze aus Art. 5 Abs. 1 Datenschutz-Grundverordnung. › Legen Sie Ihren Fokus auf risikoangemessene Schutzmaßnahmen. › Gerade wenn personenbezogene Daten in der Cloud liegen oder verarbeitet werden sollen, müssen ggf. Vereinbarungen zur Auftragsverarbeitung geschlossen werden. Prüfen Sie zudem, inwieweit es zu Drittstaatentransfers kommt, was zusätzlichen Regelungsbedarf mit sich bringt. › Geben Sie nach Möglichkeit lokaler Software bzw. Verarbeitungen den Vorrang, sprich, alles passiert auf Ihrem Computer. Damit vermeiden Sie manchen Regelungsaufwand. Zudem haben Sie mehr Kontrolle darüber, was passiert. Außerdem können Sie den Schutz vor Cyberkriminellen besser steuern. › Prüfen Sie, inwieweit Einträge ins Verzeichnis von Verarbeitungstätigkeiten erforderlich sind.	○ Ja ○ Nein
Klären Sie mit der IT-Abteilung die Rahmenbedingungen.	› Klären Sie die Beschaffungsmöglichkeiten und ggf. bereits vorhandene Lizenzen. Eventuell bestehen Volumenlizenzen oder Sie können zurückgegebene Lizenzen nutzen. › Besprechen Sie, wie eine Sicherheitsprüfung bzw. wie die Installation durch die IT-Abteilung erfolgen kann.	○ Ja ○ Nein
Lassen Sie die Software von Profis installieren.	› Im Unternehmensumfeld kann so manches komplizierter sein, als man es sich zunächst vorstellt. Damit Ihr Gerät und andere Software auch nach einer Installation der neuen Software noch funktioniert, sollten Sie das Installieren von Software den Kollegen der IT-Abteilung überlassen. › Sichern Sie oder die IT-Kollegen die Installationsdateien. Nur wenn Sie diese haben, ist eine spätere Neuinstallation auch dann kein Problem, wenn die Version nicht mehr im Internet abrufbar ist.	○ Ja ○ Nein
Stellen Sie Updates und Back-ups sicher.	› Sprechen Sie mit der IT-Abteilung ab, wie Aktualisierungen vorgenommen werden und wer hier aktiv werden muss. › Auch wenn Sie Daten in der Cloud haben, sollten Sie dennoch ein Back-up erstellen, eben für den Fall der Fälle.	○ Ja ○ Nein

Wie gehen wir mit dem Widerruf der Einwilligung um?

FRAGE: Wir verschicken bei uns einen E-Mail-Newsletter an Interessenten. Die Einwilligung wird im Double-Opt-in-Verfahren dokumentiert. Nun passierte Folgendes: Ein Abonnent teilte per E-Mail mit, dass er seine Einwilligung widerrufe. Außerdem forderte er, dass alle seine personenbezogenen Daten gelöscht werden. Wir haben den Abonnenten gebeten, dass er doch den Abmeldelink im Newsletter nutzen möge. Das hat er nicht gemacht und auch nicht auf unsere E-Mail reagiert. Wie gehen wir nun mit der Sache um? Sollen wir die Daten wie gewünscht trotzdem löschen?

ANTWORT: Bewerten Sie einerseits den Widerruf der Newsletter-Einwilligung und andererseits den Wunsch nach Löschung.

So sieht es mit dem Widerruf der Einwilligung aus:

- Das Verarbeiten der personenbezogenen Informationen zum Newsletter-Versand hatte Ihr Unternehmen auf die Einwilligung gestützt. Wird sie widerrufen, entfällt fortan die Berechtigung für die Verarbeitung der betreffenden Daten.
- Bezüglich des Widerrufs darf Ihr Unternehmen keine besonderen Hürden aufbauen. Genau eine solche Hürde könnte man im Verweis auf die Abmeldemöglichkeit in einem E-Mail-Newsletter sehen. Hat er nämlich einen solchen nicht mehr, wird es auch mit dem Abmelden schwierig. Also sollte Ihr Unternehmen den Kunden vom Newsletter abmelden bzw. die E-Mail-Adresse aus der Liste löschen.
- Aus dem Umstand, dass der Kunde auf die E-Mail nicht reagiert hat, kann Ihr Unternehmen nichts herleiten. Im Ergebnis muss also der Widerruf der Einwilligung – unverzüglich – umgesetzt werden. Die betreffenden Daten sind aus einer Empfängerdatenbank zu löschen.

Bezüglich des Löschens der Daten an sich gilt Folgendes:

- Hier müssen Sie prüfen, welche personenbezogenen Daten Ihr Unternehmen zum Betroffenen verarbeitet.
- Im nächsten Schritt muss bewertet werden, inwieweit eine Löschung möglich ist. Unter Umständen bestehen jedoch Gründe nach Art. 17 Abs. 3 Datenschutz-Grundverordnung (DSGVO), etwa gesetzliche Aufbewahrungspflichten, sodass das Löschen unterbleiben muss.
- Daneben ist wichtig, dass Ihr Unternehmen die Einwilligung des Abonnenten des Newsletters nicht löscht. Denn die belegt, mit welchem Wortlaut diese wann abgegeben und wann sie widerrufen wurde. Ihr Unternehmen muss nämlich nachweisen können, dass bisherige Newsletter rechtmäßig auf Basis einer wirksam erklärten Einwilligung verschickt wurden (Art. 7 Abs. 1 DSGVO).

Informieren Sie den Betroffenen

Wichtig ist, dass Ihr Unternehmen unverzüglich den Wunsch des Betroffenen umsetzt und ihn über den Umgang Ihres Unternehmens mit seinem Anliegen informiert. Dazu zählt nicht nur, dass man den Widerruf umgesetzt hat. Ihr Unternehmen muss auch dazu informieren, dass es die Einwilligung nicht löschen kann und aus Nachweisgründen weiter vorhalten wird.

Allerdings kann Ihr Unternehmen die E-Mail-Adresse aus einer Empfängerliste für künftige Newsletter löschen.

Müssen unsere Datenschutzhinweise akzeptiert werden?

FRAGE: Bei uns müssen bei einer Bestellung im Onlineshop Datenschutzhinweise akzeptiert werden, sprich, ein entsprechendes Häkchen muss gesetzt werden. Ein Mitarbeiter meinte nun, dass das falsch sei. Stimmt das?

ANTWORT: Zwar kann man bei fast allen Rechtsthemen unterschiedlicher Auffassung sein. Aber der Mitarbeiter hat recht. Akzeptiert werden müssen beispielsweise Allgemeine Geschäftsbedingungen, damit diese Teil des (Kauf-)Vertrags zwischen den Vertragspartnern werden.

Datenschutzhinweise gehen jedoch auf eine gesetzliche Informationspflicht zurück, sprich Art. 13 Datenschutz-Grundverordnung. Und hier muss nichts akzeptiert oder als „gelesen" bestätigt werden.

Das bedeutet also: Ein Akzeptieren mittels Setzens eines Häkchens ist nicht nötig. Es reicht vollkommen aus, wenn ein Kunde darauf hingewiesen wird, dass er sich über die Verarbeitung seiner Daten in den Datenschutzhinweisen informieren kann und wie er dorthin findet, etwa über einen Link.

Gehackte Altdaten führen nicht zu Schadensersatz

Für jeden Arbeitgeber ist es das Schreckensszenario schlechthin: Ein Mitarbeiter fällt auf Cyberkriminelle herein, installiert Malware und Unmengen an Daten werden gestohlen, eben auch zu Beschäftigten. Doch das muss nicht dazu führen, dass etwa ehemalige Beschäftigte Schadensersatz vom Unternehmen fordern können (Urteil des Hessischen Landesarbeitsgerichts (LAG) vom 10.2.2026, Az. 12 SLa 709/25).

Der Sachverhalt

Ein Mann, der spätere Kläger, war bis zum November 2020 bei einem Unternehmen eines Konzerns, dem späteren Beklagten, beschäftigt. Dieser Konzern wurde im Sommer 2022 Opfer eines Angriffs von Cyberkriminellen. Dabei wurden rund 40 Terabyte Daten kopiert, darunter auch Daten zu Beschäftigten. Erfolgreich waren die Cyberkriminellen, weil ein Beschäftigter verbotswidrig private Software updatete. Dieses Update enthielt einen Trojaner.

Hacker fordern Millionen

Die Hacker erpressten nach dem Datendiebstahl den Konzern. Sie forderten 50 Mio. Dollar Lösegeld, damit die Daten nicht im Darknet zum Verkauf angeboten würden. Der Konzern ging nicht darauf ein. Die Hacker veröffentlichten im Darknet eine Liste der zum Kauf stehenden Daten, allerdings nicht die Dateien selbst.

Konzern meldet Datenpanne

Der Konzern informierte zunächst die Datenschutzaufsichtsbehörde über den Vorfall nach Art. 33 Datenschutz-Grundverordnung (DSGVO). Zudem startete der Konzern eine Überwachung des Darknets, ob betreffende Dateien oder Daten auftauchen würden. Die zuständige Aufsichtsbehörde prüfte die Sache. Sie kam zum Ergebnis, dass es an den Sicherheitsmaßnahmen des Konzerns nichts zu beanstanden gäbe. Insofern sah die Datenschutzaufsicht auch vom Ergreifen von Maßnahmen ab. Insbesondere wurde kein Bußgeldverfahren eingeleitet.

Ehemaliger Beschäftigter fordert Schadensersatz

Das Unternehmen informierte die Beschäftigten und auch den Kläger im November 2023 über den Datendiebstahl. Nach Ansicht des Klägers war es aufgrund mangelhafter Schutzmaßnahmen zum Datendiebstahl gekommen. Mit dem Kopieren der ihn betreffenden Daten durch die Hacker habe er einen Kontrollverlust erlitten. Dieser hätte bei ihm Sorgen und Ängste bezüglich eines Missbrauchs seiner Daten hervorgerufen. Ferner hätte das Unternehmen im Zusammenhang mit dem Datenklau auch gegen andere Vorschriften der DSGVO verstoßen. Deshalb machte er einen immateriellen Schadensersatz vor dem Arbeitsgericht von mindestens 3.000 € geltend. Doch das Arbeitsgericht sah keinen entsprechenden Ersatzanspruch. Weil er das Urteil nicht hinnehmen wollte, zog der Mann vor das LAG. Doch auch hier blieb der juristische Erfolg aus.

So entschied das LAG

Die Vorinstanz hat zutreffend geurteilt und die Klage des ehemaligen Beschäftigten zu Recht abgewiesen. Die Klage ist nämlich unbegründet.

Zwar kann nach Art. 82 Abs. 1 DSGVO materieller wie immaterieller Schaden wegen eines Verstoßes gegen die DSGVO zu ersetzen sein. Hier sind die Voraussetzungen für einen Schadensersatzanspruch aber nicht gegeben. Um diesen bejahen zu können, sind drei Merkmale zu erfüllen:

1. Es muss ein Verstoß gegen die DSGVO gegeben sein,
2. ein Schaden muss vorliegen und
3. es muss ein Ursachenzusammenhang zwischen Verstoß und Schaden bestehen.

Das Vorliegen dieser Voraussetzungen muss derjenige nachweisen, der Schadensersatz fordert.

Immaterieller Schaden ist nicht gegeben

Es fehlte schon am schlüssigen Vortrag eines DSGVO-Verstoßes. Der Kläger konnte weder sagen, welche Daten konkret betroffen waren. Noch ist das Vorliegen eines Schadens belegt. Zwar können Befürchtungen eines Datenmissbrauchs ein Schaden sein. Allerdings reicht hier ein rein hypothetisches Risiko nicht aus. Insbesondere sind Befürchtungen eines Missbrauchs unbegründet, weil die betreffenden Daten teilweise schon zum Zeitpunkt der Entwendung in 2022 veraltet waren.

Verstöße gegen DSGVO nicht belegt

Auch ein geltend gemachter materieller Schaden im Hinblick auf eine Verletzung von Art. 6, 12 bis 14, 33, 34 sowie 35 DSGVO war abzulehnen. Auch hier fehlt es an einem schlüssigen Vortrag zum Ursachenzusammenhang zwischen dem behaupteten DSGVO-Verstoß und dem beanspruchten Schaden.

§

Das können Sie aus dem Urteil folgern

Auch wenn Hacker Daten entwenden, ist das an sich noch lange nicht ausreichend, um als Betroffener Schadensersatz fordern zu können. Vor allem kann sich ein Betroffener nicht pauschal auf einen Kontrollverlust oder Missbrauchsängste bezüglich der entwendeten Daten berufen. Das muss der Betroffene konkret darlegen.

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:

Phishing und Co.: Steigern Sie die Awareness
Wie sicher sind eigentlich Ihre Daten?