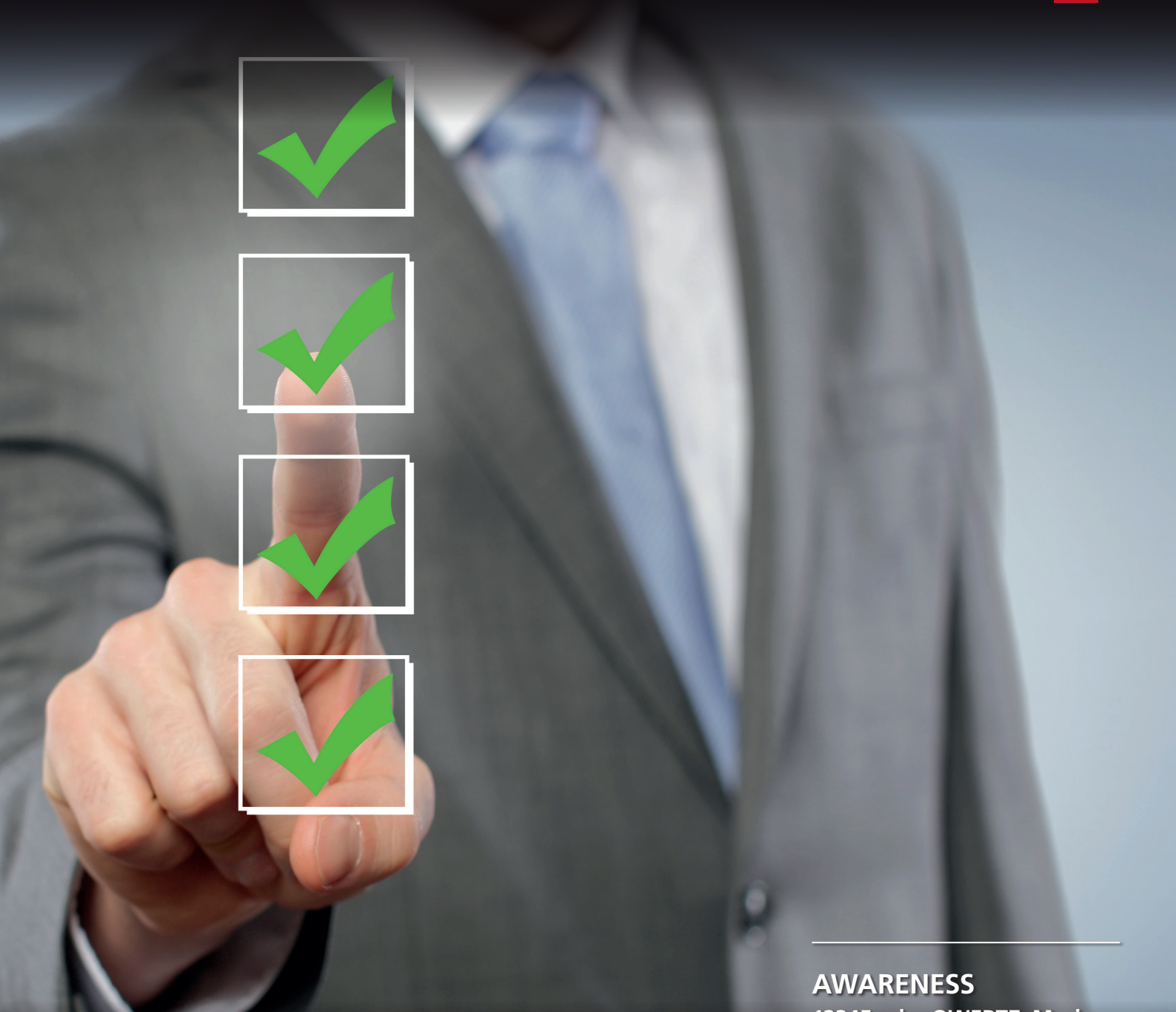
DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
APRIL 2026
Schweiz



SELBSTORGANISATION: SO KÖNNEN SIE STANDARDFÄLLE LEICHTER ERLEDIGEN

Reflektieren Sie sich

Liebe Leserin, lieber Leser,

kontinuierlich besser werden – das wollen viele Menschen, vielleicht auch Sie in Ihrer Rolle als Datenschutzberater. 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 Chefredaktor

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Zu Ihrem Onlinebereich:
https://kurzlink.ch/privacy

Expertenhotline:
https://kurzlink.ch/kontakt-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 Chefredaktor:
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
(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.

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 schützenswerte 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 Bearbeitung von Personendaten sicher(er) zu machen. Und das ist ein wichtiges Ziel des Bundesgesetzes über den Datenschutz (DSG), wie Sie leicht an Art. 8 Abs. 2 bzw. an Art. 7 Abs. 2 DSG 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 Passwortschutz 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 schützenswerten 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, gerne aus anderen Ländern: „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 Datenschutzberater.

Danke für Ihre Unterstützung!

Ihr

Theo Rettisch

Mit Frage kalt erwischt worden? So schaffen Sie die Wende

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

Niemand hat auf alles eine Antwort

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

Ihre Erfolgsformel: die Gegenfragen-Technik

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

Diese Gegenfragen funktionieren immer

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

Wie soll die Bearbeitung bzw. der Bearbeitungsprozess konkret aussehen?

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

Wer trägt die Verantwortung für das Ganze?

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

Für welchen Zweck sollen welche Daten bearbeitet werden?

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

Auf welcher Rechtsgrundlage soll die Bearbeitung basieren?

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

Liegt schon ein Konzept oder eine Projektbeschreibung vor?

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

Wer ist an der Bearbeitung beteiligt?

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

Inwieweit ist bereits eine Risikoanalyse erfolgt?

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

Liegen die Angaben für das Verzeichnis von Bearbeitungstätigkeiten vor?

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

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 Datenschutzberater nur zu gut. Und dennoch können Sie sich bei Standardfällen das Leben viel leichter machen.

Datenschutz ist wichtig für Betroffene. Und Sie als Datenschutzberater 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?
Schwerpunkte geschickt identifizieren		
Welche Fragen kommen immer wieder oder besonders häufig auf?	› 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?". › Setzen Sie auch auf ein Brainstorming. Denn unter Umständen haben Sie manches bei der Analyse von E-Mails & Co. nicht entdeckt. So z. B. kurze Beratungen oder die Beantwortung von Fragen in Besprechungen oder am Telefon.	○ Ja ○ Nein
Um welche Themen geht es schwerpunktmässig?	› Stellen Sie die Fragen und Themen nach Oberbegriffen zusammen. Bilden Sie beispielsweise Cluster zu Themen wie „Kundendatenschutz (z. B. Kundendatenbank, Werbung, Messestand)", „Beschäftigtendaten (z. B. Videoüberwachung, Homeoffice, Bewerbungsgespräche)", „Technisch-organisatorischer Datenschutz (z. B. Verschlüsselung, Risikoorientierung, Löschung)". › Erstellen Sie sich eine Rangliste der Schwerpunktthemen. Das ist wichtig, damit Sie leichter Prioritäten setzen können.	○ Ja ○ Nein
Wer stellt besonders häufig bestimmte Fragen?	› Klären Sie, welche Personengruppen welche Fragen stellen. › 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. › Fokussieren Sie später auf die jeweiligen Bedürfnisse der jeweiligen Zielgruppe. Das gilt gerade für die von Ihnen in Erwägung gezogenen Aktivitäten.	○ Ja ○ Nein
Warum kommen immer wieder die gleichen Fragen?	› 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. › 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. › Nutzen Sie jede Gelegenheit, Licht ins Dunkel zu bringen. Sprechen Sie dazu auch mit Fragenden bzw. Vertretern aus der Zielgruppe.	○ Ja ○ Nein
Welche Informationen werden bereitgestellt?	› 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. › 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. › 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.	○ Ja ○ Nein

Handlungsbedarf ausmachen		
Wie hoch sind die Relevanz und Bedeutung bestimmter Themen?	› Nur weil ein Thema oder eine Frage besonders oft kommt, muss das nicht bedeuten, dass Sie sich dem als Erstes widmen müssen. › Was weniger bedeutsam bzw. dringend ist, sollten Sie zwar nicht unter den Tisch fallen lassen. Gehen Sie es jedoch mit niedriger zeitlicher Priorität an.	○ Ja ○ Nein
Welche Risiken bestehen, wenn Sie sich nicht der Sache annehmen?	› Hier sollten Sie verschiedene „Risikoperspektiven" einnehmen. So z. B. die des Betroffenen, des Unternehmens und auch die des Datenschutzberaters. Je nach Perspektive kann sich der Handlungsbedarf ganz anders darstellen. › 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.	○ Ja ○ Nein
Ist eine einfache und zügige Umsetzung möglich?	› Nehmen Sie bei den wichtigen Themen, diejenigen zuerst in Angriff, bei denen Sie schnell vorwärtskommen bzw. die Sie schnell erledigen können. › 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.	○ Ja ○ Nein
Die passende Lösung finden		
Welche Massnahme eignet sich besonders für den betreffenden Standardfall oder die Standardfrage?	› Wählen Sie die passenden Lösungen aus Ihrem „Werkzeugkasten". Typische Beispiele sind: › Regelungen und Prozessbeschreibungen › Themenseiten mit Erläuterungen im Intranet › thematische Listen mit Antworten auf häufig gestellte Fragen › Merkblätter und Checklisten › Anleitungen und Erklärvideos › Sprechstunden für individuelle Fragen › Oft sind Mischungen aus verschiedenen Lösungen am besten. › Die Qualität Ihrer Angebote steigt vor allem mit der Aktualität. Gibt es neue Informationen oder Hinweise, sollten diese zeitnah Einfluss in Ihr Angebot finden.	○ Ja ○ Nein
Wie können Beschäftigte befähigt werden, einfache Fragen selbst zu beantworten?	› 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 Datenschutzberater leichter, wenn etwa bei komplizierten oder „Nerv-Themen" endlich der Groschen fällt. › 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.	○ Ja ○ Nein
Wodurch wird sichergestellt, dass Informationen für die betreffende Zielgruppe leicht zu finden sind?	› 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. › 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.	○ Ja ○ Nein
Inwieweit ist sichergestellt, dass Informationen aktuell gehalten werden?	› 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. › 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. › 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.	○ Ja ○ Nein
Wie werden die angedachten Massnahmen kommuniziert?	› 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. › 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.	○ Ja ○ Nein
An die Umsetzung machen		
Liegt ein Plan für die Umsetzung vor?	› Überlegen Sie, was Sie in die Wege leiten und umsetzen müssen, um ein gutes Ergebnis zu erzielen. › Denken Sie auch immer über Alternativen nach. Manchmal muss man eben Abstriche am Ergebnis machen oder einen anderen Weg einschlagen.	○ Ja ○ Nein
Wer bzw. welche Ressourcen werden für die Umsetzung benötigt?	› Für dies oder jenes brauchen Sie die Unterstützung anderer Kollegen. Sprechen Sie diese frühzeitig an. › Sind Kosten unvermeidbar, sollten Sie die Deckung vorab klären. Denn leider gilt so oft: ohne Moos nix los.	○ Ja ○ Nein

Warum sind Sie so wichtig? Das sind 7 starke Argumente

Das Schweizer Datenschutzrecht kennt keine so weitgehende Pflicht zur Benennung eines Datenschutzberaters wie manche EU-Staaten, doch zeigt die Praxis: Eine klar benannte fachliche Ansprechperson für Datenschutzfragen erleichtert nicht nur die Einhaltung der gesetzlichen Vorgaben, sondern stärkt auch Vertrauen bei Kunden, Mitarbeitenden und Behörden. Das sind gute Gründe, die eigene Position sich selbst aber auch gegenüber der Unternehmensleitung vor Augen zu führen.

Weiss man eigentlich, was man an Ihnen hat?

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

Setzen Sie auf die richtigen Argumente

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

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

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

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

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

Argument Nr. 3: Sie sichern Wettbewerbsfähigkeit und Umsatz

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

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

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

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

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

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

Das Unternehmen als Verantwortlicher und in der Folge die Geschäftsführung sind für die Einhaltung der Datenschutzvorschriften verantwortlich. Es muss nicht nur die Umsetzung sicherstellen, beispielsweise durch geeignete Spezialisten im Unternehmen. Es ist auch bezüglich der Umsetzung rechenschaftspflichtig und muss die Umsetzung nachweisen können. Nur mit Unterstützung eines Datenschutzberaters kann das gelingen.

Ausserdem wichtig: Nimmt man es mit dem Datenschutz nicht so genau, kann es nicht nur für das Unternehmen teuer werden. Auch Geschäftsführer oder Manager können schnell in die Haftungsfalle tappen. Erleidet das Unternehmen durch Missmanagement im Datenschutz Schäden, muss unter Umständen die Unternehmensleitung den Kopf hinhalten.

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

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

Wie geht man am besten mit unterschiedlichen Auffassungen um?

FRAGE: Das von mir als Datenschutzberaterin betreute Unternehmen ist oft als IT-Dienstleister tätig. Dass hier Art. 9 Bundesgesetz über den Datenschutz (DSG) gilt und es einer Vereinbarung zur Auftragsbearbeitung bedarf, liegt auf der Hand. Unser Datenschutzkonzept ist Teil zahlreicher Verträge mit Auftraggebern. Die Datenschutzberaterin eines potenziellen Auftraggebers hat dieses Konzept als nicht ausreichend bewertet. Ich sehe das als Datenschutzberaterin ganz anders. Allerdings könnte nun das Geschäft mit dem neuen Auftraggeber platzen, wenn nicht dessen Anforderungen entsprochen wird. Wie geht man mit dieser kniffligen Situation am besten um?

ANTWORT: Wichtig ist zunächst, dass Ihr Unternehmen das Gespräch mit dem Auftraggeber sucht, um die Situation zu besprechen und Möglichkeiten auszuloten, wie man doch noch zusammenkommen kann. Dazu kann es eine gute Idee sein, wenn Sie sich mit der Datenschutzberaterin des Auftraggebers austauschen. Sie sollten verstehen und nachvollziehen können, welche Aspekte, Einschätzungen und Feststellungen zu ihrer Einschätzung führten. Unter Umständen sind die Gründe gerechtfertigt.

Daneben ist natürlich Folgendes wichtig: Auch bei der Festlegung der technischen und organisatorischen Schutzmassnahmen herrscht quasi Vertragsfreiheit. Es ist also zwischen Verantwortlichem und Auftragsbearbeiter „verhandelbar", welche Massnahmen im konkreten Fall umzusetzen sind.

Dabei gibt es auch für Ihr Unternehmen mehrere Optionen. Es kann die gewünschten Schutzmassnahmen umsetzen und die anfallenden Kosten in seine Vergütung einpreisen. Alternativ kann Ihr Unternehmen die aus seiner Sicht angemessenen Schutzmassnahmen anbieten und dem Vertragspartner die Entscheidung überlassen, ob diese für seine konkrete Bearbeitung ausreichend und risikoangemessen sind. Will dieser die angebotenen Massnahmen nicht akzeptieren, kommt das Geschäft nicht zustande. Das kann für Ihr Unternehmen die vorzugswürdige Option sein, wenn es ein sehr starres Datenschutzkonzept verfolgt und für Kunden nur in sehr begrenztem Umfang davon abweichen kann. Denn jedes Abweichen kann die Dienstleistung verteuern, etwa durch Prozesse, die individuell gestaltet sind und nicht mehr von der Stange.

Tauschen Sie sich aus

Sprechen Sie mit der Datenschutzberaterin. Eventuell können Sie sie von Ihrer Auffassung überzeugen. Doch auch wenn Sie erkennen, dass Sie falsch lagen, wäre das kein Beinbruch. Machen Sie den zuständigen Kollegen klar, dass Sie in diesem Fall an Ihrer bisherigen Einschätzung nicht mehr festhalten können, und diskutieren Sie die Auswirkungen auf Ihr Unternehmen. Müssen Anpassungen vorgenommen werden, etwa am Datenschutzkonzept, ist das etwas, an dem kein Weg vorbeiführt. Schliesslich müssen die Schutzmassnahmen nach Art. 7 und 8 DSG passen.

Muss ich in Datenschutzhinweisen genannt werden?

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

ANTWORT: Bei der Erhebung von Personendaten müssen bestimmte Informationen gegeben werden, damit Betroffene wissen, wohin sie sich wenden können. Dazu zählen nach Art. 10 Abs. 3 Buchst. d Bundesgesetz über den Datenschutz (DSG) auch die Kontaktdaten des Datenschutzberaters.

Jedoch: Auch eine namentliche Nennung des Datenschutzberaters wäre eine Bearbeitung von Personendaten. Dazu besteht keine Pflicht. Das DSG fordert nur Kontaktdaten, keine namentliche Nennung.

Also reichen allgemeine Kontaktdaten aus. Das sind etwa die Firmenanschrift mit „Datenschutzberater" und eine auf die Funktion bezogene E-Mail-Adresse, z. B. „datenschutzberater@musterladen-abc.xyz".

Weiteres Argument gegen die Angabe Ihres konkreten Namens: Weil in Art. 10 DSG keine namentliche Nennung gefordert ist, wäre eine Veröffentlichung konkreter persönlicher Informationen ein Verstoss gegen den Grundsatz der Verhältnismässigkeit (Art. 6 Abs. 2 DSG).

SG Dresden: Gelöscht ist nur, wenn tatsächlich gelöscht ist

Als Datenschutzprofi wissen Sie: Personendaten müssen irgendwann gelöscht werden. Doch was ist, wenn das technisch nicht geht? Unter anderem damit beschäftigte sich das Sozialgericht (SG) der deutschen Stadt Dresden in einem Urteil vom 22.10.2025 (Az. S 15 SF 304/24 DS).

Der Sachverhalt

Eine Frau, die spätere Klägerin, war bei einer Migrationsberatungsstelle tätig. Dort unterstützte sie ausländische Mitbürger bei der Beantragung von Leistungen beim Jobcenter, dem späteren Beklagten. In den Systemen des Jobcenters war die Klägerin auch mit einem eigenen Datensatz gespeichert, weil sie früher Anträge für sich selbst stellte. Enthalten waren z. B. ihr Name und ihre Privatanschrift.

Nun passierte Folgendes: Die Klägerin unterstützte eine Mitbürgerin, eine sogenannte Klientin, bei der Beantragung von Leistungen. Dazu legte sie eine Schweigepflichtentbindung vor und erbat vom Jobcenter Informationen. Das Jobcenter sah die Klägerin nun als Bevollmächtigte dieser Klientin an. In der Folge wurden in der Akte der Klientin auch die bereits vorhandenen Stammdaten der Klägerin hinterlegt, sprich insbesondere ihr Name und ihre Privatadresse. Anstatt an die dienstliche Adresse schickte das Jobcenter die angefragten Informationen zur Klientin an die Privatanschrift der Klägerin und nicht an die dienstliche Postanschrift.

Die Klägerin meldete sich beim Jobcenter und beanstandete eine Datenschutzverletzung. Zudem beantragte sie die Löschung ihrer Privatadresse und persönlicher Informationen aus der Akte.

Jobcenter lehnt Löschung ab

Gegen diesen Bescheid legte die Klägerin Widerspruch ein. Zwar räumte das Jobcenter eine Datenschutzverletzung ein. Allerdings habe man die fehlerhafte Datenverknüpfung der Adressen behoben. Ferner wären die Datenblätter mit den privaten Adressdaten in der elektronischen Akte der Klientin ausgeblendet worden, sodass etwa eine unrechtmässige Kenntnisnahme ausgeschlossen sei. Mehr als ein Ausblenden sei technisch nicht möglich.

Die Frau akzeptierte das nicht. Sie klagte vor dem SG gegen den Ablehnungs- und den Widerspruchsbescheid. Dort bekam sie teilweise recht, allerdings erhielt sie insbesondere den geltend gemachten Schadensersatz in Höhe von 200 € nicht zugesprochen.

So urteilte das SG

Die angefochtenen Bescheide waren rechtswidrig. Allerdings nur, soweit die Löschung der Privatadresse der Klägerin aus der Akte der Klientin abgelehnt wurde. Die Klägerin hat einen Anspruch auf Löschung der Privatadresse nach Art. 17 Abs. 1 Buchst. d Datenschutz-Grundverordnung (DSGVO). Hinsichtlich des Namens besteht jedoch kein Anspruch auf Löschung. Eine unrechtmässige Verarbeitung durch das Jobcenter gab es nur hinsichtlich der Privatadresse der Klägerin. Diesbezüglich gab es für das Jobcenter keine Rechtsgrundlage. Insbesondere gab es kein Einverständnis für eine Verwendung der Privatadresse. Die Verwendung ihres Namens, etwa im Zusammenhang mit der Zusendung von Informationen der Klientin an die dienstliche Adresse, wäre hingegen zulässig. Aus Sicht des Gerichts liegt hierfür eine Einwilligung vor, die nicht widerrufen wurde. Zudem ist der Name der Klägerin im Zusammenhang mit einem Auskunftsanspruch bezüglich Leistungen des Jobcenters verarbeitet worden. Insofern steht einer Löschung Art. 17 Abs. 3 Buchst. b Variante 2 DSGVO entgegen.

Ausblenden ist kein Löschen

Zwar ist Löschen in der DSGVO nicht definiert. Allerdings ist darunter der Entzug des Personenbezugs zu verstehen, sodass es faktisch unmöglich ist, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen. Die personenbezogenen Daten dürfen nicht mehr Teil der Datenverarbeitung sein, was unumkehrbar sichergestellt sein muss. Ein Ausblenden führt jedoch nicht zu einem Löschen. Die Daten sind vorhanden, auch wenn sie nicht sichtbar sind. An der Irreversibilität fehlt es, wenn ein Wiedereinblenden möglich ist. Dass ein Programm technisch nicht löschen kann, führt nicht dazu, dass ein Ausblenden dem Löschen gleichkommt. Es muss vielmehr technisch dafür gesorgt werden, dass geltende Gesetze und Betroffenenrechte umgesetzt werden können.

Keinen Schaden nachgewiesen

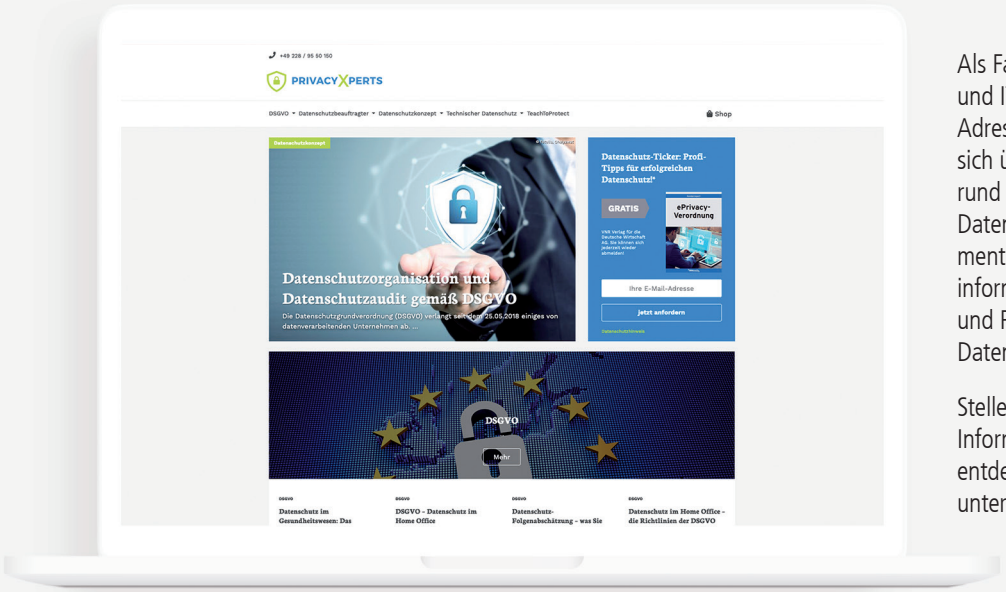
Ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO besteht nicht. Zwar gibt es hier einen Datenschutzverstoss. Allerdings ist der Klägerin kein konkreter Schaden entstanden. In diesem Zusammenhang hätte die Klägerin den Zusammenhang mit dem Verstoss nachweisen müssen. Zudem reicht ein rein hypothetisches Risiko für einen Datenmissbrauch nicht aus. Hier hatten Dritte die betreffenden Daten gerade nicht zur Kenntnis genommen.

§

Das können Sie aus der Entscheidung folgern

Die Entscheidung macht klar, dass Löschen nur Löschen ist, wenn der Personenbezug bei Daten irreversibel entfernt wird. Eine spätere Zuordnung von Informationen darf tatsächlich nicht mehr möglich sein. Dass ein System oder eine Software keine Löschung vorsieht, ist kein Grund, um dem Löschanspruch nicht nachzukommen. In einem solchen Fall muss die entsprechende Funktion nachgerüstet oder es muss eine andere Software beschafft werden. Das dürfte auch in der Schweiz so sein.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter **www.privacyxperts.de/shop**

MITARBEITERINFORMATION CYBERSICHERHEIT

- ✓ **zeitsparend und wirksam** für Cybergefahren und Informationssicherheit sensibilisieren
- ✓ die **wichtigsten Informationen griffbereit** und mit **praktischen Checklisten** direkt umsetzbar
- ✓ **perfekt für neue Mitarbeiterinnen und Mitarbeiter, um** schnell die relevantesten Themen zu schulen

JETZT STAFFELRABATT SICHERN

JETZT NEU

Bestellen Sie direkt hier: https://t1p.de/MitarbeiterinformationCybersicherheit

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: kurzlink.ch/privacy

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

Vorschau:

Know-how:
5 Praxistipps für die Altgeräteverwertungen

Sind Ihre älteren Einschätzungen noch aktuell?