



WAS GIBT'S NEUES? KLÄREN SIE, WAS SICH IM UNTERNEHMEN VERÄNDERT

RISIKEN VORBEUGEN

Das Ende naht!
Heben Sie frühzeitig wegen
Windows 10 die Hand

1-2

DATENSCHUTZBERATER

Sie haben zu wenig Zeit für Ihren Job?
Beziffern Sie das Problem

3





Fragen Sie immer nach dem Warum

Liebe Leserin, lieber Leser,

vielen Menschen scheint es irgendwie in den Genen zu stecken. Auch wenn es um Personendaten geht, dürfte mancher eher „Jäger und Sammler“ sein. Zwar ist klar, dass man für das Bearbeiten eine Rechtsgrundlage braucht. Aber dass man nicht beliebig umfangreich Daten sammeln bzw. bearbeiten darf, wird ab und an übersehen.

Doch genau hier sollten Sie immer den Finger in die Wunde legen. Fragen Sie stets nach dem Warum und damit nach der Erforderlichkeit. Kann man Ihnen keinen nachvollziehbaren und berechtigten Grund liefern, fehlt es an der Erforderlichkeit. Ist die nicht gegeben, sind die Daten tabu.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz

Andreas Würtz ist Rechtsanwalt in Deutschland und verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Risiken vorbeugen

Das Ende naht! Heben Sie frühzeitig wegen Windows 10 die Hand
[Seiten 1–2](#)

Datenschutzberater

Sie haben zu wenig Zeit für Ihren Job? Beziffern Sie das Problem
[Seite 3](#)

Vorausschauend arbeiten

Was gibt's Neues? Klären Sie, was sich im Unternehmen verändert
[Seiten 4–5](#)

Soft Skills

Vertrauen ist die Grundlage für Ihre Arbeit: Nutzen Sie diese 7 Power-Tipps
[Seite 6](#)

Fragen an die Redaktion

- ❓ *Mitarbeiter fühlen sich beobachtet: Was können wir machen?*
- ❓ *Dienstleister liefert keine Infos fürs Verzeichnis: Können wir ihn zwingen?*

[Seite 7](#)

Urteil aus dem Ausland

LG Wiesbaden: Widerspruch gegen Verarbeitung bedarf besonderer Umstände
[Seite 8](#)



Expertensprechstunde:
www.privacyxperts.de/kontaktformular/

Bildnachweise:

Titel: Adobe Stock | sommart

Seite 1: Adobe Stock | Darius Murawski

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,
Meckenheim

Erscheinungsweise: 16-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



A problem has occurred with your PC and it needs to be restarted.
We just collect some error information and then restart for you.

85% complete

You can find more information about this problem and possible solutions on our website:

When you call a support agent, give them this information:
Stop code: 0x00000000

Es wird schon über Windows 12 spekuliert, Windows 10 hat ausgedient im Jahr 2025.

Das Ende naht! Heben Sie frühzeitig wegen Windows 10 die Hand

Manche Menschen fremdeln nach wie vor mit der aktuellen Version des Microsoft-Betriebssystems Windows 11. Vielleicht setzt man daher auch in Ihrem Unternehmen noch auf die Vorgängerversion Windows 10. Doch die Tage von Windows 10 sind gezählt. Ihr Unternehmen sollte sich den 14.10.2025 vormerken. Denn danach kann das alte Betriebssystem auch zum Datenschutzrisiko werden.

Das kommt auf Nutzer von Windows 10 zu

Jedes Unternehmen, das Software anbietet, weiss: Die Software auf aktuellem Stand zu halten und beispielsweise Sicherheitsupdates bereitzustellen, geht ins Geld. Und Zeit und Geld in Sicherheitsupdates zu investieren, kann für Anbieter schnell zu einem teuren und aufwendigen Unterfangen werden, gerade wenn es bereits ein Nachfolgeprodukt gibt. So ist es auch mit Microsofts Betriebssystem Windows 10. Das ist nicht nur schon etwas in die Jahre gekommen. Auch das Nachfolgeprodukt Windows 11 gibt es schon seit 2021. Insofern verwundert es also nicht, dass auch Microsoft nach und nach den Support für alte Betriebssysteme auslaufen lässt, nun eben auch für Windows 10.

Windows 11: Lassen Sie Ausreden nicht gelten

Wenn es um den Wechsel zu Windows 11 geht, haben manche Menschen schnell Ausreden zur Hand, warum das Ganze eben nicht machbar sein soll. Die folgenden „Gründe“ sollten Sie nicht akzeptieren:

› Kinderkrankheiten

Windows 11 ist schon lange nicht mehr neu. Kinderkrankheiten wie nicht funktionierende Software oder fehlende Treiber sind Geschichte. Auch nützliche Funktionen aus Windows 10, die zunächst in Windows 11 nicht enthalten waren, sind schon längst wieder zurück. Und klar ist auch: Ihr Unternehmen ist mit Windows 11 für längere Zeit auf der sicheren Seite. Ein Supportende ist derzeit nicht in Sicht.

› Kosten

Natürlich ist ein Wechsel zu einem neuen Betriebssystem mit Aufwand und Kosten verbunden. Allerdings ist der Wechsel von Windows 10 zu Windows 11 meist ohne Lizenzkosten möglich. Der Aufwand lässt sich so in Grenzen halten. Der Wechselassistent ermöglicht in aller Regel eine reibungslose Umstellung. Auch installierte Software muss nicht neu installiert werden. Allerdings ist ein Back-up immer wichtig, um auf der sicheren Seite zu sein.

Aber: Wechsel auf Windows 11 ist nicht immer möglich

Zwar ist ein Wechsel von Windows 10 auf Windows 11 unter Lizenzaspekten meist kostenlos möglich. Allerdings kann die bisherige Technik Ihrem Unternehmen einen Strich durch die Rechnung machen. Für Windows 11 müssen bestimmte Hardwarevoraussetzungen erfüllt sein. Gerade ältere Computer verfügen nicht über TPM 2.0, das „Trusted Platform Module“. Ist das nicht vorhanden, kann Windows 11 nicht installiert werden. Doch manchmal lohnt es sich, genauer hinzuschauen. Bei manchen Computern gibt es TPM, das ist jedoch deaktiviert. Kann TPM 2.0 etwa im BIOS des Computers aktiviert werden, ist eine wichtige Voraussetzung für den Wechsel zu Windows 11 erfüllt.

Ist das nun wirklich das Ende von Windows 10? Jein!

Stellt man Ihnen diese Frage, können Sie nur mit einem „Ja und Nein“ antworten. Ja, weil Microsoft den Support, sprich etwa die Bereitstellung von Sicherheitsupdates, zum 14.10.2025 auslaufen lässt. Insofern wird es standardmässig keinen Support mehr



geben. Nein, weil es weiterhin Möglichkeiten gibt, auch für Windows 10 Sicherheitsupdates zu erhalten, und zwar:

› ESU-Programm von Microsoft

Das Supportende von Windows 10 lässt sich quasi um drei Jahre nach hinten verschieben. Hierzu gibt es den Service „Windows 10 Extended Security Updates (ESU)“. Dabei handelt es sich um einen kostenpflichtigen Service für Privatpersonen und Unternehmen, bei dem Microsoft für die registrierten Computer weiterhin Sicherheitsupdates zur Verfügung stellt. Im ersten Jahr des ESU-Programms dürften die Kosten bei rund 60 € liegen. In den Folgejahren müssen Sie jedoch mit höheren Kosten pro Windows-Lizenz rechnen.

› Sicherheitsupdates von anderen Anbietern

Eventuell kann es für Ihre IT-Abteilung sinnvoll sein, nach Angeboten anderer Anbieter Ausschau zu halten. Die bieten ggf. Alternativen zum ESU-Programm von Microsoft an. Hier muss jedoch genau hingeschaut werden, etwa hinsichtlich des Serviceumfangs. Schliesslich müssen die Updates auch tatsächlich das bieten, was sie sollen: Sicherheit.

› Umstieg auf spezielle Windows-10-Lizenzen

Es gibt Windows-10-Lizenzen, die etwa für spezielle Anwendungsfälle gedacht sind. So z. B. „Windows 10 IoT Enterprise LTSC“. Solche Versionen sind in erster Linie für Terminalsysteme wie Geldautomaten oder Anzeigetafeln vorgesehen. Der Support und damit die Versorgung mit Sicherheitsupdates sind für diese Version beispielsweise bis Anfang 2032 vorgesehen. Ob eine solche Lizenz jedoch im Unternehmenseinsatz passt, hängt vom jeweiligen Anwendungsfall ab.

Ihr Unternehmen muss sich Gedanken machen

Einfach die Hände in den Schoss legen und hoffen, dass mit dem „alten“ Windows 10 auch nach dem Supportende alles gut gehen wird, ist nicht nur blauäugig. Vielmehr wäre es fahrlässig, das Problem nicht anzugehen. Schliesslich können fehlende Sicherheitsupdates beispielsweise Cyberkriminellen Tür und Tor öffnen. Gelingt es diesen, sich etwa über eine Sicherheitslücke Zugriff auf das Netzwerk Ihres Unternehmens zu verschaffen, gibt es für die Kriminellen meist kein Halten mehr. Sie nehmen alles mit oder verschlüsseln Daten, um dann „Lösegeld“ zu erpressen. Als wäre das nicht schon schlimm genug, kommt auch noch eine Datenschutzkomponente hinzu. Sind Personendaten betroffen, liegt in der Regel auch eine Verletzung der Sicherheit vor. Und das kann auch die Meldung gegenüber dem EDÖB und die Information der Betroffenen erforderlich machen (Art. 24 Bundesgesetz über den Datenschutz (DSG)). Auch finanzielle Schäden sind drin, etwa Lösegeldzahlungen, Bussgelder oder Schadensersatz für Betroffene. Zudem sind Imageschäden möglich. Bringen Sie also auch die folgenden Alternativen ins Spiel:

› Anschaffung neuer Geräte

Neue Computer sollten direkt mit Windows 11 ausgestattet sein und über eine entsprechende Lizenz verfügen. Der Vorteil hier: Ihr Unternehmen profitiert von Gewährleistungsansprüchen oder Garantien des Herstellers. Manche Hersteller bieten auch „Wechsel- oder Eintauschprämien“ an, sprich, es wird günstiger, wenn Ihr Unternehmen alte Geräte durch neue Computer ersetzt.

› Beschaffung gebrauchter Geräte

Nicht immer müssen es neue Geräte sein. Denkbar ist auch, gebrauchte Computer zu beschaffen, etwa aus Unternehmensauflösungen oder Insolvenzen.

› Isolierter Betrieb

Funktioniert eine bestimmte Software mit Windows 11 nicht mehr, kann man über Folgendes nachdenken: Der Computer wird so betrieben, dass er keine Verbindung zum Internet hat. Wenn ein Computer keine Verbindung zum Internet hat, können Hacker nicht von aussen auf Daten zugreifen und auf diesem Weg keine Sicherheitslücken ausgenutzt werden. Im Übrigen sollte es hier ein spezielles Sicherheitskonzept geben, um Risiken angemessen zu begegnen.

› Wechsel auf ein anderes Betriebssystem

Ob der Wechsel auf ein anderes Betriebssystem, etwa Linux, sinnvoll ist, hängt von vielen Faktoren ab. So braucht es hierfür nicht nur spezielle Kenntnisse. Auch ist meist andere Software nötig.

Sprechen Sie mit den richtigen Leuten

Sprechen Sie mit den Kollegen der IT-Abteilung, inwieweit das Supportende von Windows 10 für Ihr Unternehmen noch ein Thema ist. Ggf. hat man bereits alle relevanten Geräte und Systeme umgestellt. Ist das nicht der Fall, sollten Sie sich erläutern lassen, wie man mit dem Thema umgehen will. Machen Sie in diesem Zusammenhang auch die Dimension für den Datenschutz deutlich.

Beissen Sie bei Ihrer ersten Anlaufstelle auf Granit und will man das Thema ignorieren oder aussitzen, sollten Sie bei Gelegenheit mit der Unternehmensleitung sprechen. Machen Sie die aus Ihrer Sicht bestehenden Risiken und den Handlungsbedarf deutlich.



Sie müssen nichts entscheiden

Veraltete Betriebssysteme sind immer ein Sicherheits- und Datenschutzrisiko. Doch als Datenschutzberater liegt es nicht in Ihrer Verantwortung, die richtigen Weichen zu stellen, damit die entsprechenden Risiken reduziert oder ausgeschaltet werden. Vielmehr ist es an Ihnen, die Hand zu heben und im Rahmen Ihres Beratungsauftrags (Art. 10 Abs. 2 Buchst. a DSGVO) auf die Risikosituation aufmerksam zu machen. Handeln müssen andere.

Nicht nur Betriebssysteme im Fokus haben

Generell können Sie bei Ihrem Gespräch hinterfragen, wie es um das Management der IT-Lebenszyklen steht. Dabei ist es wichtig, auch die Hardware auf dem Radar zu haben, weil eben Technik nicht ewig hält. Ausserdem muss nicht nur bei Betriebssystemen, sondern auch bei der Software auf den Lebenszyklus geachtet werden. Das Datum für das Supportende von Windows 10 beispielsweise, der 14.10.2025, ist auch der Stichtag für das Supportende mancher Softwareprodukte von Microsoft. Setzt Ihr Unternehmen etwa Microsoft Office 2016 oder 2019 ein, ist auch hier ein Wechsel unumgänglich. Welche Software noch aus dem Support fällt, erfahren Sie hier: <https://t1p.de/vbntn>.

Sie haben zu wenig Zeit für Ihren Job?

Beziffern Sie das Problem

Wer seine Arbeit als Datenschutzberater gut machen will, braucht nicht nur Know-how und die passende Arbeitsausstattung. Meist ist der entscheidende Faktor, dass Sie ausreichend Zeit für Ihre Aufgaben zur Verfügung haben. Ist diese zu knapp bemessen, kann irgendwann auch das Priorisieren von Aufgaben keine Lösung mehr sein. Sie brauchen einfach mehr Zeit.

Mehr Zeit für Ihre Aufgaben im Datenschutz können Sie sich nicht einfach selbst nehmen. Hier müssen Sie mit Ihrem Vorgesetzten und/oder mit der Unternehmensleitung sprechen. Doch etwa im Gespräch mit der Unternehmensleitung einfach nur zu sagen, dass Sie mehr Zeit brauchen, ist meist nicht überzeugend. Schliesslich muss man ggf. die von Ihnen sonst noch wahrgenommenen Aufgaben auf andere Schultern verteilen. Und ausserdem sollten Sie eine Antwort liefern können, wenn man von Ihnen wissen will, wie viel mehr an Zeit Sie denn brauchen. Ihre Antwort finden Sie in drei Schritten:

Schritt 1: Stellen Sie zusammen, was Sie machen

Zunächst sollten Sie mit einem Brainstorming starten, sprich einer Ideensammlung. Überlegen Sie, was Sie alles an Aufgaben oder Erledigungen übernommen haben. Ferner sollten Sie notieren, was aus Ihrer Sicht 2025 an Herausforderungen auf Sie zukommen dürfte. Schreiben Sie auch das auf, was allenfalls indirekt mit dem Datenschutz zu tun hat. Das können auch Besprechungen oder Managementtagungen sein, über die Sie sich mit Informationen versorgen und die Sie zum Netzwerken nutzen.

Zu „Was mache ich alles?“ könnten folgende Punkte gehören:

- › Beratung im Datenschutz
- › Unterstützung bei Projekten
- › Audits und Prüfungen im Datenschutz
- › Unterstützung beim Verzeichnis von Bearbeitungstätigkeiten
- › Awarenessaktionen
- › Hilfestellung bei Betroffenenanfragen
- › Unterstützung bei Datenpannen
- › an Besprechungen teilnehmen, Protokolle erstellen

Auch wenn in einem Brainstorming einiges zusammenkommt, sollten Sie schauen, was Sie sonst noch so alles machen. Werfen Sie insbesondere einen Blick in Ihr E-Mail-Postfach und den Kalender. Doch auch ein Blick in Projektpläne oder die Geschäftsziele kann einiges zutage fördern, was Ihnen nicht auf Anhieb eingefallen ist.

Schritt 2: Bewerten Sie den Zeitaufwand

Ist eine Liste der Aufgaben erstellt, ist das schon mal die halbe Miete. Nun brauchen Sie noch Zahlen, denn erst dadurch wird Ihr Aufwand messbar. Hierzu haben Sie mehrere Möglichkeiten: Muss es schnell gehen, können Sie die Aufwände schätzen. Besser ist es, wenn Sie nachvollziehbar erklären können, wie Sie auf eine Zahl gekommen sind. Listen Sie also einige Stichpunkte auf, die den Aufwand belegen. Alternativ können Sie auch eine Arbeits- oder Aufwandsstatistik führen.



BEISPIEL: Aufwandsstatistik

Aufgabe/Erledigung	Arbeitsstunden 01.2025	Arbeitsstunden 02.2025
Beratung im Datenschutz	18	16
Unterstützung Projekt „Vernetzte Produkte“	6	6
Teilnahme Arbeitsgruppe „Künstliche Intelligenz“	3	3
Begleitung Anfrage durch Datenschutzaufsicht	16	8
Beratung bei Audit durch Firma XYZ	5	20
Unterstützung bei Betroffenenanfragen	10	8
Awarenessaktivitäten	8	16
E-Mail-Anfragen	25	20
Besprechungen mit der Unternehmensleitung	5	5
Weiterbildung	4	4
Dokumentation	5	5
Gesamt	105	111

Schritt 3: Geben Sie dem Istaufwand eine Zahl

Vielleicht denken Sie zunächst auch: Die Stundenanzahl in der obigen Statistik ist doch gar nicht so hoch. Doch das ist nur auf den ersten Blick der Fall. Setzen Sie die Zahlen ins Verhältnis, sieht die Sache schnell anders aus. Dazu folgendes Beispiel: Arbeiten Sie im Kanton Freiburg, hat das Jahr 2025 bei einer Arbeitswoche von Montag bis Freitag 251 Arbeitstage. Davon ziehen Sie Ihren Urlaub ab, beispielsweise 30 Tage. Damit sind 221 Arbeitstage übrig. Der Januar 2025 hatte 22 Arbeitstage. Beträgt die tägliche Arbeitszeit 8 Stunden, wären das für Januar 2025 176 Stunden Gesamtarbeitszeit. Hätten Sie 105 Stunden für die Datenschutzarbeit verwendet, wären das immerhin rund 60 % der gesamten Arbeitszeit. Für Februar 2025 mit 20 Arbeitstagen wären es rund 69 %.

Stehen Ihnen eigentlich nur 50 % Ihrer gesamten Arbeitszeit für Datenschutzaufgaben zur Verfügung, drängt sich ein Schluss auf: Sie brauchen mehr Zeit zur Wahrnehmung Ihrer Aufgaben bzw. Ihre sonstigen Aufgaben kommen zu kurz. Das kann weder im Interesse des Unternehmens bzw. des Datenschutzes noch Ihrer sonstigen Aufgaben sein. Es muss also eine Lösung gefunden werden, wie Sie allem gerecht werden können.



Was gibt's Neues? Klären Sie, was sich im Unternehmen verändert

Der Wandel hat Beständigkeit. Egal, ob aufgrund veränderter Rahmenbedingungen oder weil sich das „Business“ Ihres Unternehmens ändert: Vieles, was passiert, kann auch Auswirkungen auf den Datenschutz haben. Und damit auch auf Ihre Tätigkeit als Datenschutzberater.

Darum sollten Sie auf die Jagd nach Änderungen gehen

Als Datenschutzberater haben Sie einen gesetzlichen Arbeitsauftrag zu erfüllen. Dieser ergibt sich aus Art. 10 Abs. 2 Bundesgesetz über den Datenschutz (DSG). Er umfasst z. B., dass Sie informieren, beraten und auf Gefahren bzw. Risiken hinweisen. Für Ihren Erfolg ist es entscheidend, dass Sie einerseits risikoorientiert und andererseits vorausschauend arbeiten.

Und gerade im Frühjahr tut sich in den meisten Unternehmen so einiges. So kommt es zu Veränderungen, die offensichtlich Datenschutzrelevanz haben, beispielsweise eine neue Bearbeitung oder den Einsatz eines neuen IT-Dienstleisters. Doch es gibt auch viele sonstige Veränderungen, bei denen erst bei genauerem Hinschauen klar wird, dass auch sie von Bedeutung für den Schutz von Personendaten sind. Denken Sie z. B. an folgende Änderungen:

› Es gibt neue Geschäftsführer

Auf den ersten Blick ändert sich nur die Leitung des Unternehmens. Doch die Änderung ist auch unter Datenschutzaspekten weitreichend. Einerseits ändert sich damit der „Kopf“ des Verantwortlichen im Sinne von Art. 5 Buchst. j DSG. Und dieser kann den zukünftigen Datenschutz erheblich beeinflussen. Neue Geschäftsstrategien können ganz neue Herausforderungen im Datenschutz mit sich bringen. Auch kann eine neue Unternehmensleitung in Sachen Datenschutz ganz anders ticken als die bisherige.

› Ihr Unternehmen arbeitet anders

Zum Jahreswechsel ist es eventuell auch dazu gekommen, dass Ihr Unternehmen sich neu aufgestellt hat, die Geschäftstätigkeit geändert oder eine Abteilung verlagert bzw. geschlossen wurde. Eventuell will die Geschäftsführung auch das Geschäft ausweiten, vielleicht sogar in einem anderen Land. In all diesen Fällen sind viele Datenschutzaspekte zu berücksichtigen.

› Es gibt neue Herausforderungen

Die Ursachen können verschieden sein. Eventuell will Ihr Unternehmen mehr mit künstlicher Intelligenz arbeiten, etwa im Kundenmanagement. Hier können schnell datenschutzrechtliche Fragen zu betrachten sein. Doch auch Cyberkriminelle schlafen nicht. Hier kann Ihr Unternehmen ganz plötzlich vor nie gekannten Herausforderungen stehen, etwa um die Folgen eines erfolgreichen Angriffs wieder in den Griff zu bekommen.

Gehen Sie schlau vor

Planvolles Vorgehen ist immer schlau. Denn so setzen Sie Ihre Ressourcen punktgenau ein. Um für den Datenschutz und Ihre Arbeit relevante Änderungen auszumachen und alles Nötige in die Wege zu leiten, sollten Sie Schritt für Schritt vorgehen.

Schritt 1: Überlegen Sie, wo sich wahrscheinlich etwas ändern wird

Das Stichwort lautet hier: Brainstorming. Notieren Sie sich alle Einfälle, die Ihnen hinsichtlich Änderungen im Unternehmen in den Sinn kommen. Gehen Sie hier zunächst sehr allgemein an die Sache heran, sprich, Ihre Einstiegsfrage lautet tatsächlich: Wo ändert sich etwas im Unternehmen? Notieren Sie alle Einfälle und prüfen Sie erst später, inwieweit die Einfälle direkt oder indirekt auch Auswirkungen auf den Datenschutz oder Ihre Tätigkeit haben. Damit Ihre Einfälle sprudeln, können Sie auch auf die hier abgedruckte Checkliste setzen.

Schritt 2: Sprechen Sie mit relevanten Personen

Es gibt Stellen im Unternehmen, die Ihnen meist schnell sagen können, was sich ändert. So kann die Unternehmensleitung oder das Business Development sagen, ob es Änderungen bei der Geschäftsstrategie oder beim oberen Management gibt. Hinsichtlich neuer Produkte oder Services können Sie mit der Entwicklung sprechen. Geht es um die Bearbeitung von Daten an sich, sind Sie bei der IT-Abteilung an der richtigen Adresse.

Schritt 3: Ziehen Sie die entsprechenden Schlüsse

Analysieren Sie die erhaltenen Informationen und prüfen Sie, inwieweit diese Relevanz für den Umgang mit Personendaten haben. Auch für Ihre Arbeit sollten Sie ableiten, welche Konsequenzen die Veränderungen haben. Das kann beispielsweise auch mehr Unterstützungsbedarf vonseiten des Unternehmens bedeuten, etwa mehr Budget und Kapazitäten. Unter Umständen müssen Sie sich aber auch qualifizieren, um bei neuen Herausforderungen angemessen unterstützen zu können.

Schritt 4: Adressieren Sie den nötigen Handlungsbedarf

Zwar kann der auch bei Ihnen liegen. Doch meist wird es darauf hinauslaufen, dass Sie sich auf Ihren Beratungsauftrag beschränken müssen. Schliesslich dürfen Sie nichts übernehmen, was Sache des Verantwortlichen ist und beispielsweise das Ob und Wie der Bearbeitung von Personendaten betrifft. Haben Sie Handlungsbedarf ausgemacht, sollten Sie diesen möglichst schnell gegenüber den zuständigen Kollegen adressieren.

Schritt 5: Begleiten Sie die Aktivitäten

Sind die nötigen Aktivitäten adressiert, sollten Sie denjenigen mit Rat und Tat zur Seite stehen, die das Ganze umsetzen müssen. Beraten Sie so, dass Sie nach Möglichkeit die Interessen des Datenschutzes und Ihres Unternehmens in Ausgleich bringen.



CHECKLISTE: Typische Veränderungen im Unternehmen



Typische Aspekte	Das können Sie in Erfahrung bringen	Geprüft und geklärt?
Unternehmen		
Gibt es Veränderungen in der Unternehmensleitung?	› Klären Sie, inwieweit personelle Änderungen bei der Geschäftsleitung vorgesehen sind. Wichtig sind auch Änderungen, die sich abzeichnen, etwa wenn jemand in den Ruhestand geht. › Gibt es mehrere Geschäftsführer, kann es auch Änderungen beim Zuschnitt der Verantwortungsbereiche geben. Das kann Auswirkungen darauf haben, wen Sie im Fall der Fälle ansprechen müssen, wenn Sie Handlungs- oder Unterstützungsbedarf aufzeigen bzw. einfordern wollen.	☐ Ja ☐ Nein
Inwieweit ändern sich Strukturen bzw. diesbezügliche Leitungen?	› Halten Sie Ausschau nach neuen Verantwortlichkeiten. Gerade wenn neue Führungskräfte von extern hinzukommen, kann das Anlass für Sie sein, das Gespräch zu suchen und über den Datenschutz im Unternehmen zu informieren. › Nicht nur das Management ganz oben ist für Sie wichtig. Denken Sie auch an das obere und mittlere Management. Hier können sich veränderte Zuschnitte erheblich auf den Datenschutz und dessen Umsetzung auswirken.	☐ Ja ☐ Nein
Kommt es zu rechtlichen Änderungen bezüglich des Unternehmens?	› Bringen Sie in Erfahrung, welche Absichten es hier gibt. Eventuell will man ein anderes Unternehmen hinzukaufen. Egal, ob dieses weiterhin eigenständig bleiben soll oder ob man es in das bestehende Unternehmen integrieren will, es wird viele Fragen zum Datenschutz geben. So z. B. wenn Personendaten ausgetauscht werden sollen. › Denken Sie auch daran, dass ggf. das Unternehmen verkleinert werden soll. Möglicherweise will man einen Teil ausgliedern oder verkaufen. Auch hier können viele datenschutzrelevante Aspekte zu betrachten sein.	☐ Ja ☐ Nein
Geschäftstätigkeit		
Welche Veränderungen sind im „Business“ vorgesehen?	› Sprechen Sie mit den relevanten Kollegen, was man kurz-, mittel- und langfristig beabsichtigt. Will man neue Märkte erschliessen, können datenschutzrechtliche Besonderheiten zu beachten sein. › Eventuell will man auch das Geschäft mit neuen Produkten oder Services ausweiten, ggf. mit Funktionalitäten im Bereich künstliche Intelligenz. Hier ist eine frühzeitige Einbindung erforderlich, damit Sie unter Datenschutzaspekten gut unterstützen können.	☐ Ja ☐ Nein
Welche Kooperationen sind vorgesehen?	› Möglicherweise will Ihr Unternehmen mit einem anderen Unternehmen zusammenarbeiten. Hier kommt es eventuell auch zum Austausch von Personendaten. › Relevant kann auch der Aspekt sein, mit wem man die Zusammenarbeit beenden will. Auch das kann unter Datenschutzaspekten zum grösseren Projekt werden.	☐ Ja ☐ Nein
Bearbeitungen		
Welche neuen grösseren Bearbeitungen sind beabsichtigt?	› Klären Sie, welche neuen Bearbeitungen auf der Agenda stehen, und lassen Sie sich diese grob beschreiben. Guten Aufschluss gibt schon eine einfache Frage: Wer hat mit welchen Personendaten was vor und wie wird das umgesetzt? › Verdeutlichen Sie, dass Ihre Beratung unerlässlich ist, wenn Personendaten im Spiel sind. Entscheidend ist, dass Sie möglichst früh eingebunden werden.	☐ Ja ☐ Nein
Sind Neuerungen bei Systemen und Technologien angedacht?	› Eventuell bleiben Bearbeitungen an sich unverändert, jedoch gestaltet sich vieles im Hintergrund um. Das kann auch auf den Datenschutz Auswirkungen haben, etwa wenn sich Schutzmassnahmen ändern. › Bringen Sie neue Technologien ins Spiel, insbesondere künstliche Intelligenz. Fragen Sie in anderen Abteilungen nach, was diesbezüglich angedacht ist. Auch hier muss vieles im Datenschutz beachtet werden, weil das DSGVO unverändert gilt.	☐ Ja ☐ Nein
Gibt es Änderungen bei Dienstleistern?	› Hier kann es für Sie relevante Umgestaltungen geben, wenn sich beispielsweise Services ändern. Klären Sie, inwieweit etwa angepasste Services auch den Datenschutz beeinträchtigen. › Veränderungen führen oftmals dazu, dass auch Vereinbarungen im Datenschutz neu geschlossen oder bestehende angepasst werden müssen. Stichworte sind hier: Auftragsbearbeitung, gemeinsame Verantwortung und Drittstaatenbezug.	☐ Ja ☐ Nein
Datenschutzorganisation		
Gibt es Veränderungen, die die Datenschutzorganisation betreffen?	› Werden Sie von anderen Abteilungen unterstützt, können Veränderungen dort auch die Ihnen zukommende Unterstützung beeinträchtigen. › Haben Sie Mitarbeiter, sollten Sie auch hier ein Auge darauf haben, inwieweit sich Änderungen abzeichnen, was Sie vor ganz neue Herausforderungen stellen kann.	☐ Ja ☐ Nein



Vertrauen ist die Grundlage für Ihre Arbeit: Nutzen Sie diese 7 Power-Tipps

Bestimmt wollen Sie als Datenschutzberater Ihren Aufgaben bestmöglich gerecht werden. Doch wie erfolgreich Sie sind und wie gut der Datenschutz im Unternehmen angenommen und umgesetzt wird, hängt auch davon ab, wie gut man mit Ihnen zusammenarbeitet. Dass die Zusammenarbeit gut funktioniert, haben auch Sie in den Händen. Schaffen Sie mit diesen sieben Tipps zunächst eine solide Vertrauensbasis:

Power-Tipp 1: Reflektieren Sie sich und Ihre Arbeit

Setzen Sie sich zunächst einmal kritisch mit sich und Ihrer Arbeit auseinander. Denken Sie etwa über Ihr Auftreten in Beratungssituationen, Besprechungen oder schwierigen Gesprächen nach. Wagen Sie in diesem Zusammenhang den Perspektivwechsel und prüfen Sie kritisch, wie Sie zuletzt etwa bei Teilnehmern oder Gesprächspartnern angekommen sein dürfen. Seien Sie hier unbedingt ehrlich zu sich selbst. Kommen Sie zu dem Ergebnis, dass das nicht gerade eine Glanzleistung war, sollten Sie überlegen, wie Sie es in Zukunft besser machen können. Geben Sie sich hier einige gute Vorsätze und versuchen Sie, sich bei kommenden Terminen daran zu halten.

Im Übrigen kann es eine „Offenbarung“ sein, wenn Sie Ihr Auftreten und Ihre Aussenwirkung von Kollegen bewerten lassen, denen Sie vertrauen können. Deren Hinweise sind Gold wert. Auch wenn mancher Hinweis zunächst schmerzt: Zeigen Sie sich dankbar für die ehrliche Einschätzung. Die bringt Sie garantiert weiter.

Power-Tipp 2: Setzen Sie auf vertrauensbildende Werte

Wollen Sie Vertrauen bei anderen aufbauen, sollten Sie sich zunächst fragen, was Ihnen wichtig ist, um eine Person als vertrauenswürdig anzusehen. Bestimmt fallen Ihnen Werte wie Zuverlässigkeit, Verbindlichkeit, Ehrlichkeit, Respekt und Wertschätzung ein. Und schon weil Ihnen diese Werte wichtig sind, sollten Sie davon ausgehen, dass das bei anderen Menschen nicht viel anders sein dürfte. Insofern ist wichtig: Setzen Sie alles daran, diese Werte in Ihr (Arbeits-)Leben zu integrieren. Achten Sie darauf, dass sie Ihr Handeln prägen. Denn das ist Ihre Visitenkarte, mit der Sie sich empfehlen.

Power-Tipp 3: Geben Sie Gesprächen stets den Vorrang

Egal, ob man Ihnen per Messenger eine Nachricht schickt, Ihnen eine E-Mail zukommen lässt oder Ihnen auf den Anrufbeantworter spricht: Vermeiden Sie es nach Möglichkeit, lang und breit per E-Mail oder Messenger zu antworten. Denn hier lauern viele Fallen. So kann man das, was für Sie klar zum Ausdruck kommt, ganz anders oder missverstehen. Ausserdem können sich leicht Tipp- und Rechtschreibfehler einschleichen, gerade wenn Sie per Messenger antworten wollen.

Übrigens: Wenn Ihnen Stil und Respekt wichtig sind, sollten Sie bei schriftlichen Reaktionen nicht zu locker werden. Insbesondere sollten Sie stets auf eine angemessene Anrede achten. Zu lockere Sprache kann den Wert des Gesagten herabsetzen oder den Eindruck erwecken, dass Ihnen die Sache nicht wichtig genug ist.

Power-Tipp 4: Wagen Sie den Perspektivwechsel

Bedenken Sie stets, dass nicht immer alles offensichtlich sein muss und Sie häufig nicht direkt erkennen können, warum jemand das sagt, was er sagt, oder das macht, was er macht. Wechseln Sie in die Perspektive der betreffenden Person und versuchen Sie, die Gründe auszumachen, warum man beispielsweise in einer bestimmten Situation aggressiv reagierte. Unter Umständen erkennen Sie so, dass das der Situation geschuldet war oder die betreffende Person entsprechend auftreten musste, um ihr Gesicht zu wahren.

Ein Perspektivwechsel bringt Ihnen auch immer etwas, wenn Sie hinterfragen, wie Ihr Handeln bei anderen ankommt. Eventuell erkennen Sie, dass man Ihr Handeln leicht in den falschen Hals bekommen kann. Und seien Sie sich sicher: Können Sie die Lage anderer nachvollziehen, kann das Ihr Handeln positiv beeinflussen. Und das hilft auch Ihrem Gegenüber.

Power-Tipp 5: Keine Überraschungen – Berechenbarkeit zählt

Vermeiden Sie unbedingt, dass man sich über Ihr Verhalten ärgert, etwa weil Sie A sagen, aber B machen. Solche „bösen Überraschungen“ sind Gift für jedes Vertrauen. Müssen Sie eine Meinung oder Ihr Handeln ändern, sollten Sie das möglichst langfristig einleiten und Ihre Beweggründe erläutern. Versteht man Sie und ziehen Sie Menschen in Ihr Vertrauen, wird das wertgeschätzt.

Power-Tipp 6: Helfen Sie anderen

Hilfsbereitschaft zahlt sich immer aus. Das merken Sie zwar unter Umständen nicht sofort. Allerdings hat gewährte Unterstützung immer Depotwirkung. Sie verbessern Ihre Chancen, dass man Ihnen hilft, wenn Sie entsprechend Unterstützung brauchen.

Daher: Helfen Sie, auch wenn man Sie nicht dazu auffordert, eventuell auch bei einer Angelegenheit, die nicht zu Ihrem Kernthema Datenschutz gehört. Nehmen Sie Kollegen in Schutz, wenn diese Schutz verdient haben. Lassen Sie sie nicht alt aussehen, auch wenn sie etwas falsch gemacht haben.

Power-Tipp 7: Humor öffnet viele Türen

Datenschutz ist zwar eine ernste Sache, doch auch wiederum nicht so ernst, dass man nicht manches mit Humor nehmen könnte. Machen Sie ab und zu einen Scherz und nehmen Sie den Datenschutz nicht zu wichtig. Das zeigt, dass auch Sie ein „normaler Mensch“ sind, und fördert das Vertrauen.

Mitarbeiter fühlen sich beobachtet: Was können wir machen?

FRAGE: Unser Unternehmen hat mit einem anderen Unternehmen einen gemeinsamen Parkplatz. Weil es dort nachts immer wieder zu Beschädigungen und Aufbrüchen von Firmenfahrzeugen des Nachbarunternehmens kam, hat man in Abstimmung mit unserer Unternehmensleitung eine Videoüberwachung installiert. Gegenüber sind mehrere Kameras montiert, die auf den Parkplatz ausgerichtet sind und nur nachts in Betrieb sein sollen. Nun liegen jedoch einige Beschwerden von Mitarbeitern unseres Unternehmens wegen dieser Videoüberwachung vor. Die betreffenden Personen haben Büros mit Fenstern und fühlen sich durch die Videoüberwachung bei der Arbeit beobachtet und überwacht. Unsere Unternehmensleitung unterstützt die Videoüberwachung des Nachbarn, weil man sich schon rein von der optischen Wirkung her einen Sicherheitsgewinn verspricht. Daher fragte man nun bei mir als Datenschutzberater nach, was wir in dieser Situation machen können.

ANTWORT: Grundsätzlich ist wichtig, dass seitens des Verantwortlichen, sprich des benachbarten Unternehmens, die Videoüberwachung so gestaltet wird, dass sie im Einklang mit dem Datenschutz steht. Dabei kann Ihr Unternehmen natürlich Hilfestellung geben.

Zunächst ist umfassende Transparenz gegenüber den betreffenden Mitarbeitern wichtig. Ist für diese nachvollziehbar, dass eine Videoüberwachung nur ausserhalb der Arbeitszeiten bzw. nachts stattfindet, können deren Bedenken eventuell schon ausgeräumt werden. Ferner bietet es sich an, einen Vor-Ort-Termin beim Nachbarunternehmen zu machen und beispielsweise den von den Kameras gelieferten Bildausschnitt in Augenschein zu nehmen. Werden etwa Bereiche verpixelt oder ausgeblendet, dann fehlen die entsprechenden Bildinformationen. Eine Überwachung ist nicht möglich.

In diesem Zusammenhang kann es auch hilfreich sein, wenn der für das andere Unternehmen zuständige Datenschutzberater am Termin teilnimmt. Er kann ggf. manche Frage der Mitarbeiter direkt beantworten. Das erspart Ihnen vielleicht auch manche Diskussion.

Machen Sie pragmatische Vorschläge

Bestehen die Sorge der Überwachung weiterhin und damit ein psychischer Überwachungsdruck, kann man über technische Lösungen nachdenken. Beispielsweise können an den betreffenden Fenstern Spiegelfolien angebracht werden. So bleibt weiterhin ein Blick nach draussen möglich. Allerdings wird den Kameras der Blick in die Büros verwehrt. Insofern besteht auch keine theoretische Möglichkeit zur Überwachung. Eventuell ist auch das andere Unternehmen bereit, die Kosten zu tragen. Schliesslich sind es dessen Videoüberwachung und Bearbeitung von Personendaten, liegen also in dessen Interesse und Verantwortung.

Das Nachbarunternehmen ist verantwortlich

Sind die vorgenannten Ideen nicht umsetzbar, bleibt unter Umständen nur Folgendes: Ihr Unternehmen muss das Nachbarunternehmen bitten, die Videoüberwachung datenschutzkonform auszugestalten. Das bedeutet in erster Linie, die Kameras so zu installieren und auszurichten, dass eine Aufnahme der Fenster physisch ausgeschlossen ist.

Dienstleister liefert keine Infos fürs Verzeichnis: Können wir ihn zwingen?

FRAGE: Unser Unternehmen hat einen IT-Dienstleister, der im Rahmen der Bearbeitung von Personendaten unterstützt. Da ein Fall der Auftragsbearbeitung nach Art. 9 Bundesgesetz über den Datenschutz (DSG) vorliegt, wurde eine schriftliche Vereinbarung geschlossen. Enthalten ist auch eine Regelung, dass der Dienstleister bei der Erstellung und Aktualisierung des Verzeichnisses von Bearbeitungstätigkeiten nach Art. 12 Abs. 1 und 3 DSG unterstützt. Nun steht bei meinem Unternehmen als Auftraggeber eine solche Aktualisierung des Verzeichnisses an. Bei der Aktualisierung müsste nun auch der IT-Dienstleister unterstützen und Informationen liefern. Auf den Fragenkatalog und weitere Mails wurde nicht reagiert. Vielmehr stellt man sich beim Dienstleister tot. Können wir ihn irgendwie zur Unterstützung zwingen?

ANTWORT: Zunächst ist ein wichtiger strategischer Aspekt zu klären. Bevor Sie empfehlen, auf den Dienstleister massiven Druck auszuüben, sollten Sie dessen Bedeutung für Ihr Unternehmen kennen. Handelt es sich um den einzigen und nur schwer ersetzbaren Dienstleister, sollte es sich Ihr Unternehmen nicht mit ihm verscherzen. Unter Umständen muss man das Gespräch suchen, um Unterstützung bitten, gut zu reden und allenfalls sanften Druck ausüben.

Empfehlen Sie, alle Möglichkeiten zur Kontaktaufnahme zu nutzen. Vielleicht ging die bisherige Anfrage tatsächlich ohne bösen Willen unter. Scheitert die Kontaktaufnahme auf Arbeitsebene, müssen ggf. die Geschäftsführer miteinander sprechen. Ist auch das nicht von Erfolg gekrönt, bleibt meist nur eines: Ihr Unternehmen muss dann prüfen, welche Konsequenzen es zieht, etwa auch die Kündigung des Vertrags und der Wechsel zu einem anderen Dienstleister.

LG Wiesbaden: Widerspruch gegen Verarbeitung bedarf besonderer Umstände

Für das Bearbeiten von Personendaten bedarf es sowohl in EU-Ländern als auch bei uns in der Schweiz einer Rechtsgrundlage. Nicht selten setzen EU-Länder hier auf das überwiegende berechnigte Interesse nach Art. 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung (DSGVO). Einer solchen Verarbeitung können Betroffene widersprechen. Doch die Anforderungen sind hoch, wie das Urteil des Landgerichts (LG) Wiesbaden in Deutschland vom 30.7.2024 (Az. 4 O 11.24) zeigt.

Das führte zum Rechtsstreit

Der Fall: Ein Mann hatte bei einer Bank einen Kreditkartenvertrag. 2013 war er mit den Zahlungen im Rückstand. Die Bank kündigte schliesslich Mitte 2013 den Kreditkartenvertrag und stellte den offenen Betrag von rund 1.600 € fällig. Nachdem die Zahlungen weiterhin ausblieben, erwirkte die Bank im September 2013 einen Vollstreckungsbescheid. Im November 2013 meldete die Bank der Auskunft die offene Forderung als schwerwiegende Zahlungsstörung. Die Auskunft nahm einen diesbezüglichen Eintrag in ihre Datenbank auf.

2017 erkannte der Mann eine Zahlungsschuld von nunmehr über 3.000 € an und vereinbarte eine Teilzahlung mit der Bank. Im Dezember 2021 leistete der Mann die letzte Rate. Die Bank meldete der Auskunft die Erledigung. Die nahm einen Erledigungsvermerk in die Datenbank auf.

Eintrag wird zum Problem

Im Sommer 2023 machte der Mann über einen Anwalt einen Anspruch auf Löschung des betreffenden Eintrags bei der Auskunft geltend. Aus seiner Sicht würde der Eintrag ihn in seiner persönlichen Lebensgestaltung erheblich behindern. Er verdiene inzwischen gut und wolle aus der Wohnung seiner Mutter ausziehen. Allerdings hätte er wegen der Bonitätsinformation bei der Auskunft keine Chance, eine Wohnung anzumieten. Er hätte stets gegenüber anderen Mitbewerbern für Wohnungen das Nachsehen, weil Vermieter regelmässig eine Bonitätsauskunft forderten. Weil auch die Mieten steigen würden, drohe ihm ein erheblicher finanzieller Schaden. Insofern würde ihm nicht nur ein Lösungsanspruch, sondern auch ein Anspruch auf immateriellen Schadensersatz nach Art. 82 DSGVO zustehen, welcher mindestens 5.000 € betragen müsste. Die Auskunft lehnte die Forderungen ab. Der Mann klagte also vor dem LG Wiesbaden. Doch das Gericht erteilte den Forderungen des Mannes eine Absage.

So entschied das LG Wiesbaden

Die Klage ist unbegründet und die geltend gemachten Ansprüche auf Löschung und auf Schadensersatz bestehen nicht. Die Speicherung der Informationen bei der Auskunft ist rechtmässig, und zwar auf Basis von Art. 5 und 6 DSGVO.

Der Mann war 2013 gegenüber der Bank in Zahlungsrückstand. Die Forderung wurde mehrfach angemahnt. Danach erst wurde der Kreditvertrag fristlos gekündigt. Den erwirkten Vollstreckungsbescheid hat der Kläger nicht angegriffen. Erst 2017 schloss der Kläger eine Zahlungsvereinbarung mit der Bank und beglich die offene Forderung ratenweise bis 2021.

Berechnigtes Interesse gegeben

Die Verarbeitung der Informationen ist zur Wahrung der berechtigten Interessen von Vertragspartnern des Klägers erforderlich. Die Auskunft verarbeitet die Informationen zur Wahrung ihrer Interessen als Schutzorganisation der Wirtschaft sowie im Interesse der Vertragspartner der Auskunft. Sie erfolgt insofern im Interesse der Allgemeinheit, aber auch von Vertragspartnern der Auskunft.

Zugleich ermöglicht sie die Einschätzung von Chancen und Risiken vor Geschäftsabschlüssen. Ausserdem schützt sie vor Verlusten und Risiken im Kreditgeschäft. Ferner werden Wirtschaftsteilnehmer vor zahlungsunfähigen oder zahlungsunwilligen Schuldern geschützt.

Kein Lösungsanspruch gegeben

Weil die Daten rechtmässig verarbeitet werden, besteht kein Lösungsanspruch nach Art. 17 Abs. 1 Buchst. d DSGVO. Auch wenn eine Forderung beglichen wird, besteht kein Anspruch auf Löschung des Negativeintrags. Dieser wird um die entsprechende Information ergänzt. Es besteht nämlich weiterhin ein Informationsinteresse über das Zahlungsverhalten des Klägers.

Auch besteht kein Lösungsanspruch nach Art. 17 Abs. 1 Buchst. c DSGVO im Zusammenhang mit einem Widerspruch des Klägers gegen die Verarbeitung nach Art. 21 Abs. 1 DSGVO. Es liegt nämlich keine besondere Situation vor, die einen solchen Widerspruch begründen könnte. Die Situation ist nicht atypisch und entspricht vielmehr derjenigen anderer Schuldner vergleichbarer Forderungen. Nachteilige Folgen bei der Wohnungssuche begründen keine atypische Situation. Insbesondere hat der Kläger keine konkreten Umstände vorgetragen, aufgrund derer man eine solche besondere Situation annehmen könnte.

§

Das können Sie für Ihre Arbeit folgern

Nur weil jemand einer Verarbeitung auf Basis eines überwiegenden berechtigten Interesses widerspricht (Art. 21 Abs. 1 DSGVO), muss die Verarbeitung nicht gestoppt werden. Vielmehr muss der Betroffene Gründe geltend machen, die sich aus seiner besonderen Situation ergeben.

In der Schweiz könnten sich Rechtsansprüche aus Art. 32 Bundesgesetz über den Datenschutz ergeben. Danach kann die betroffene Person verlangen, dass unrichtige Daten berichtigt werden. Die Daten in diesem Fall waren jedoch nicht unrichtig.

„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 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

**IT- & INFORMATIONSSICHERHEIT** **UPDATE**

Ihr digitaler Praxisratgeber für mehr Schutz Ihrer betrieblichen Informationen

Schnelles Filtern der News, die Sie brauchen

Aus Fehlern anderer lernen

Praxisnahe (Video-)Anleitungen

Audit-Prüflisten

Schulungsmaterial

Interpretation der Gesetze und Richtlinien

Darum sollten Sie nicht auf das IT- & Informationssicherheit Update verzichten:

- Erhalten Sie alle 2 Wochen News, Praxistipps und Rechtsempfehlungen
- Sicherheitsmaßnahmen messbar machen, dank interaktiver Checklisten
- Arbeitshilfen im Onlinebereich sparen Zeit bei Schulungen, Richtlinien & Co.

Testen Sie das E-Magazin für mehr IT- und Informationssicherheit 1 Monat GRATIS



 <http://bit.ly/IT-Info-Update>

Vorschau:

Herausforderung KI: Setzen Sie auf die Grundprinzipien
Einfachheit: Machen Sie das zu Ihrem Arbeitsmotto Nummer 1



www.privacyxperts.de/login



www.privacyxperts.de/kontaktformular/



Telefon: +49 2 28 95 50 150

Fax: +49 2 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
Deutschland