

THEMENHEFT:

IT-Abteilung:

Fördern Sie das

Datenschutzverständnis

SENSIBILITÄT OHNE WENN UND ABER: SCHLAUEN SIE DIE IT-ABTEILUNG AUF

GUT ARGUMENTIEREN

Datenschutz ist von Vorteil: So überzeugen Sie die IT-Kollegen

3

HILFE ZUR SELBSTHILFE

Datenschutz bei Vorhaben berücksichtigen: Empfehlen Sie dieses Vorgehen

4-5



Onlinebereich:
www.privacyxperts.de/login



Expertensprechstunde:
www.privacyxperts.de/kontaktformular/



PRIVACYXPERTS



Setzen Sie auf Ihren Freund und Helfer

Liebe Leserin, lieber Leser,

nein, mit „Freund und Helfer“ ist nicht die Polizei gemeint. Denn die wird Sie in der Regel nicht bei Ihrem Thema Datenschutz unterstützen. Ihr „Freund und Helfer“ ist jemand ganz anderes im Unternehmen: die IT-Abteilung.

Wenn Sie nun denken, dass gerade das nicht der Fall ist, sollten Sie damit beginnen, es zu ändern. Schließlich ist die IT-Abteilung nicht nur der Bereich, der das Technische rund um die Verarbeitung personenbezogener Daten verantwortet und erbringt. Dort kann man auch viel dazu beitragen, dass der Datenschutz funktioniert. Stärken Sie also Ihre Beziehung zu den Kollegen.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz

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

Inhalt

Wissen vermitteln

Sensibilität ohne Wenn und Aber:
Schlagen Sie die IT-Abteilung auf
Seiten 1–2

Gut argumentieren

Datenschutz ist von Vorteil:
So überzeugen Sie die
IT-Kollegen
Seite 3

Hilfe zur Selbsthilfe

Datenschutz bei Vorhaben
berücksichtigen: Empfehlen
Sie dieses Vorgehen
Seiten 4–5

Problemfelder

Stiefmütterlich behandelte Themen:
Diese können Sie ansprechen
Seiten 6–7

Geschickt umsetzen

7 Tipps mit Wirkung:
Stärken Sie die gute Beziehung
zur IT-Abteilung
Seite 8



Premiumbereich:
www.privacyxperts.de/login



Expertensprechstunde:
redaktion@datenschutz-aktuell.de

Bildnachweise:

Titel: Adobe Stock | Onetrack

Seite 1: Adobe Stock | Andrey Popov

Impressum



ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda
(Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung,
Bonn

Satz: Deinzer Grafik, Gartow

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

Erscheinungsweise: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Dieses monothematische Supplement „IT-Abteilung: Fördern Sie das Datenschutzverständnis“ liegt der Ausgabe April 2025 von „Datenschutz aktuell“ bei. 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



In der IT arbeiten Spezialisten. Ergänzen Sie das Wissen dort um den Datenschutz.

Sensibilität ohne Wenn und Aber: Schlaun Sie die IT-Abteilung auf

Werden im Unternehmen personenbezogene Daten verarbeitet, ist das auch für Sie als Datenschutzbeauftragten von Bedeutung. Dabei ist klar, dass es manchmal schwierig sein kann, alles im Blick zu behalten. Um dennoch Ihrem Anspruch gerecht zu werden, ist es wichtig, dass Sie Hilfe zur Selbsthilfe anbieten. Daneben sollten Sie für die nötige Sensibilität, also Awareness, sorgen. Das ist gerade in der IT-Abteilung besonders wichtig.

Orientieren Sie sich an der Zielgruppe

Bei allen Awareness-Aktivitäten sollten Sie einen schlaun Spruch beherzigen: Der Köder muss dem Fisch schmecken, nicht dem Angler. So ist es auch, wenn Sie Datenschutzwissen an den Mann oder die Frau in der IT-Abteilung bringen wollen. Überlegen Sie zunächst für sich selbst, welchen Bedarf es bei den Kollegen gibt und wie Sie beim Vermitteln am besten vorgehen können.

Sind Sie sich hier unsicher, gibt es eine ganz einfache Möglichkeit, Licht ins Dunkel zu bringen: Fragen Sie neben den zuständigen Führungskräften auch die „normalen“ Mitarbeiter. Das kann nicht nur Themen hervorbringen, die Sie bislang nicht auf Ihrer Liste hatten; eventuell fallen die Sichtweisen von Führungskräften und Mitarbeitern auseinander. Das kommt gar nicht so selten vor.

Bitte bedenken Sie auch: In der IT-Abteilung arbeiten häufig Profis und Spezialisten, die sich mit ganzem Herzen dafür einsetzen, die besten Lösungen für meist technische Herausforderungen zu finden. Manchmal empfinden sie den Datenschutz vielleicht als etwas Störendes, das Kosten verursacht und eine effektive Lösung zu erschweren scheint. Hier ist es wichtig, dass Sie nicht mit Unverständnis reagieren. Besser beraten sind Sie, wenn Sie die Interessenlage der Kollegen nachvollziehen. Zeigen Sie aber dennoch auf, dass es sich für das Unternehmen und alle Beteiligten lohnt, im Datenschutz an einem Strang zu ziehen.



Sie sind kein Spielverderber

Für die Kollegen ist vielleicht nicht klar, welche Rolle Sie spielen. Machen Sie klar: Sie sind Berater, Wissensvermittler und Kontrolleur im Datenschutz. Dabei berücksichtigen Sie einerseits die Interessen der Betroffenen und lassen andererseits dennoch nicht die wirtschaftlichen Aspekte des Unternehmens außer Acht. Müssen Sie zu etwas Nein sagen, ist das keine Gängelei. Vielmehr tragen Sie dazu bei, dass sich Ihr Unternehmen regelkonform und gesetzes-treu verhält. Nimmt man es mit Recht und Gesetz nicht so genau, rächt sich das meist – mal früher, mal später. Gewonnen ist am Ende jedoch nichts. Im Gegenteil: Verstöße bedeuten in der Regel viel Arbeit, Ärger und Kosten.

Backen Sie zunächst kleine Brötchen

Wollen Sie bei der IT-Abteilung für ein Grundverständnis für den Datenschutz sorgen, müssen Sie nicht gleich mit einer längeren Schulung für die Mitarbeiter starten. Das kann eher schaden als nützen, gerade wenn die Zielgruppe etwas schwierig ist oder mit dem Thema an sich fremdelt. Beginnen Sie hier lieber mit einer kurzen Information. Klären Sie per E-Mail über einige grundlegende Aspekte auf, die jeder beachten sollte, der mit personenbezogenen Daten zu tun hat. Doch auch eine kurze Schulung haben Sie mit dem folgenden Muster schnell erstellt. Verwenden Sie für jeden Tipp eine Folie und fassen Sie den Text in Aufzählungspunkten zusammen. Im Handumdrehen können Sie loslegen und bei den Kollegen Awareness schaffen.





MUSTER: 7 Tipps zum Datenschutz



Liebe Kolleginnen und Kollegen,

bei der Mustermann GmbH legen wir großen Wert auf den Schutz aller Daten, beispielsweise die unserer Kunden und Beschäftigten. Aber auch unsere Unternehmensinformationen und Geschäftsgeheimnisse sind schützenswert. Als Mitarbeiter der IT-Abteilung kommt Ihnen hier besondere Verantwortung zu. Schließlich unterstützen Sie alle im Unternehmen bei der Verarbeitung von Daten, indem Sie Systeme, Datenbanken, Hard- und Software entwickeln und/oder bereitstellen. Auch Sie können viel dazu beitragen, dass alles in bester Ordnung ist. Damit Ihnen das auch im Arbeitsalltag leicht von der Hand geht, möchte ich Ihnen einige Tipps vorstellen. Orientieren Sie sich an den Tipps und das Thema Datenschutz ist gar nicht so kompliziert, wie es vielleicht auf den ersten Blick erscheint.

Tipp 1: Bedenken Sie immer: Alle tragen Verantwortung

Die Verantwortung für den Datenschutz und damit die Einhaltung der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes trifft nicht nur das Unternehmen an sich. Wir alle sind das Unternehmen. Daher müssen wir und auch Sie im Rahmen Ihrer Aufgaben darauf achten, dass das Unternehmen und Sie den gesetzlichen und betrieblichen Anforderungen gerecht werden.

Dabei ist klar: Wenn es zu Datenschutzverstößen kommt, ist das für das Unternehmen und alle Beteiligten immer ein Problem. Haben Sie den Verstoß verursacht, müssen Sie die Verantwortung dafür übernehmen. Sind die Verstöße oder Ihr Fehlverhalten besonders schwerwiegend, können arbeitsrechtliche Konsequenzen, Bußgelder oder Schadensersatzforderungen auf Sie zukommen.

Tipp 2: Ohne Rechtsgrundlage keine Verarbeitung

Besonders wichtig ist die datenschutzrechtliche Regel, dass es für jede Verarbeitung personenbezogener Daten einer Erlaubnis, sprich einer Rechtsgrundlage bedarf. Nur wenn eine Rechtsgrundlage das Verarbeiten personenbezogener Daten vorschreibt oder erlaubt, ist dies zulässig. Rechtsgrundlagen finden Sie beispielsweise in Art. 6 DSGVO.

Tipp 3: Ohne Zweck keine Verarbeitung personenbezogener Daten

Auch wenn mit künstlicher Intelligenz vieles machbar scheint: Einfach personenbezogene Daten sammeln oder verarbeiten – das ist datenschutzrechtlich nicht drin. Generell müssen schon bei der Datenbeschaffung die Zwecke festgelegt sein, für die das Verarbeiten erfolgen soll. Und diese festgelegten Zwecke sind verbindlich. Von wenigen Ausnahmen abgesehen, dürfen die für einen bestimmten Zweck verarbeiteten Daten nicht für andere Zwecke verwendet werden. Hinterfragen Sie also immer: Wofür werden die Daten gebraucht? Ist der Zweck (rechtlich) in Ordnung?

Tipp 4: Weniger ist mehr

Es gibt Grundprinzipien, die bei jeder Verarbeitung personenbezogener Daten zu beachten und einzuhalten sind. Diese ergeben sich aus Art. 5 DSGVO. Besonders wichtig für Ihre Arbeit ist der Grundsatz der Datenminimierung. Der ist schnell erklärt: Je weniger personenbezogene Daten verarbeitet werden, desto besser. Gestalten Sie beispielsweise ein Registrierungsformular für die Webseite, überlegen Sie bitte kritisch, welche Informationen für den verfolgten Zweck wirklich nötig sind. Mindestens genauso wichtig ist: Auch im Hinblick auf Berechtigungen fahren Sie gut mit dem Minimalprinzip. Nur wer wirklich Kenntnis von bestimmten Informationen benötigt, sollte auch einen entsprechenden Zugriff erhalten (Need-to-know-Prinzip).

Tipp 5: Datenschutzfreundlichkeit ist das A und O

Wie gut Datenschutz funktioniert, haben auch Sie in der Hand. Geht es um die Entwicklung und die Gestaltung von Datenverarbeitungsverfahren, sollten Sie ein Auge auf Art. 25 DSGVO haben. Dieser macht „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ zur Pflicht. Das heißt: Datenverarbeitungsverfahren, etwa Apps, Webseiten oder Datenbanken, müssen so gestaltet werden, dass es problemlos möglich ist, den Betroffenenrechten gemäß Art. 12 ff. DSGVO zu entsprechen. Diese Betroffenenrechte (z. B. auf Auskunft und Löschung) sind unabdingbar und dürfen nicht ignoriert oder ausgeschlossen werden. Außerdem sollten Sie Wahlmöglichkeiten und Voreinstellungen so gestalten, dass sie dem Datenschutz am besten entsprechen – auch hier gilt das Minimalprinzip.

Tipp 6: Sicherheit ist wichtig, wichtig, wichtig!

Dass Daten angemessen geschützt werden müssen, kann nicht genug betont werden. Dabei müssen die technischen und organisatorischen Schutzmaßnahmen Hand und Fuß haben. Sie müssen einerseits risikoangemessen sein. Andererseits müssen sie dem Stand der Technik entsprechen, um etwa Cyberkriminellen das Leben möglichst schwer zu machen. Daher gilt: Je schutzwürdiger oder sensibler die Informationen sind, desto mehr müssen wir alles zu deren Schutz unternehmen. Die Sicherheit darf nie auf die leichte Schulter genommen werden oder aus Praktikabilitäts- oder Kostengründen auf der Strecke bleiben.

Tipp 7: Ihr Beitrag ist besonders wichtig

Daten zu schützen ist keine einmalige Sache, sondern ein fortlaufender Prozess. Das gilt für uns alle. Hinterfragen Sie regelmäßig, ob Daten noch angemessen geschützt sind, ob beispielsweise Zugriffsrechte noch den Erfordernissen entsprechen. Überlegen Sie auch, was wir besser machen können. Haben Sie Ideen zur Verbesserung des Datenschutzes, greifen Sie zum Telefonhörer. Ich bin auf Ihre Vorschläge gespannt.

Übrigens: Bei Fragen zum Datenschutz stehe ich Ihnen gern mit Rat und Tat zur Verfügung!

Ihr Datenschutzbeauftragter
Dennis Platz

Datenschutz ist von Vorteil: So überzeugen Sie die IT-Kollegen

Ob es in Ihrem Unternehmen ein gutes Datenschutzniveau gibt, hängt mitunter auch davon ab, ob die Führungskräfte und die Mitarbeiter mitziehen. Damit dies der Fall ist, müssen Sie als Datenschutzbeauftragter aktiv werden und etwa erklären, warum Datenschutz eine sinnvolle Sache ist. Die Werbetrommel für den Datenschutz sollten Sie gerade in der IT-Abteilung rühren.

Heben Sie die positiven Dinge besonders hervor

Jeder, der mit Datenschutz zu tun hat, weiß, dass Datenschutz nichts für Faule ist. Vielmehr kann das Umsetzen der Anforderungen mit einiger Arbeit und manchmal auch hohen Kosten verbunden sein. Außerdem ist das Thema komplex und nicht leicht zu verstehen. Kein Wunder also, dass mancher mit dem Thema eher auf Kriegsfuß steht. Dass sich das ändert, haben auch Sie in der Hand. Nutzen Sie beispielsweise die unten stehende Checkliste, um in einem Gespräch mit den Kollegen der IT-Abteilung die Vorteile des Datenschutzes zu thematisieren. Wird den Kollegen klar, dass sich Datenschutz lohnt, sind sie eher mit Spaß bei der Sache.



Vorsicht mit der Bußgeldkeule

Als Profi im Datenschutz wissen Sie: So gut wie alles in der Datenschutz-Grundverordnung (DSGVO) ist bußgeldbewehrt. Und der Bußgeldrahmen ist ganz schön happig. So können je nach Verstoß bis zu 20 Mio. € oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Allerdings müssen bei der Bußgeldbemessung viele Aspekte berücksichtigt werden (Art. 83 Abs. 2 DSGVO), sodass der Bußgeldrahmen eigentlich immer bei Weitem nicht ausgeschöpft wird.



CHECKLISTE: 5 gute Gründe für Datenschutz

Grund	Das können Sie dazu erläutern	Besprochen?
1. Wir verhalten uns gesetztes- und regelkonform.	- Über die Sinnhaftigkeit von Gesetzen lässt sich streiten. Sind sie jedoch da, muss man sich daran halten. Da macht der Datenschutz mit der DSGVO keine Ausnahme. - Datenschutz und die DSGVO sind kein Selbstzweck und keine Gängelei. Sie dienen der Gewährleistung der Grundrechte auf Achtung der Persönlichkeit und auf Schutz persönlicher Informationen. - Jammern, dass es anderswo weniger „Datenschutzbürokratie“ gibt, kann man sich sparen. Die DSGVO gilt in der EU und im EWR. Außerdem müssen sich auch anderswo ansässige Unternehmen daran halten, wenn sie etwa Waren in der EU anbieten. - Sich an Regeln zu halten ist auch eine Maßnahme, um Risiken zu vermeiden oder zu verringern. Typisch ist etwa das Bußgeldrisiko.	☐ Ja ☐ Nein
2. Die Konkurrenz schläft nicht.	- Sparen wir uns den Datenschutz, muss nicht heißen, dass wir einen Vorteil gegenüber Wettbewerbern haben. Im Gegenteil: Diese haben nicht nur einen Vorteil uns gegenüber, wenn sie sich an Recht und Gesetz halten. Sie empfehlen sich Kunden auch als vertrauenswürdige Geschäftspartner. - Bekommen Konkurrenten mit, dass wir im Datenschutz unsauber arbeiten, kann auch das zu Ärger führen. So können auch diese die Datenschutzaufsicht informieren.	☐ Ja ☐ Nein
3. Datenschutz spart Kosten.	- Sind personenbezogene Daten im Spiel, muss der Datenschutz von Anfang bis Ende mitgedacht werden. Weil er ohnehin eingehalten werden muss, kann späteres „Herumdoktern“ an Systemen oder Verarbeitungen besonders teuer und aufwendig werden. - Manche Anforderungen tragen auch zu Kosteneinsparungen bei. Können nicht mehr benötigte Daten gelöscht werden, ist das nicht nur im Sinne des Datenschutzes. Es kann sich auch in der Unternehmenskasse bemerkbar machen. - Beißen sich Kriminelle wegen guter Schutzmaßnahmen an unseren Systemen und Datenbanken die Zähne aus, ist das nicht nur gut für den Schutz der Daten von Kunden und Beschäftigten. Es entstehen auch keine Folgekosten, um nach einem Angriff z. B. Systeme wieder zum Laufen zu bringen.	☐ Ja ☐ Nein
4. Guter Datenschutz zahlt sich für alle Daten aus.	- Zwar zielt die DSGVO mit den verpflichtenden Schutzmaßnahmen eigentlich nur auf personenbezogene Daten ab. Allerdings gibt es bei uns auch viele andere schützenswerte Daten, etwa Geschäftsgeheimnisse. Auch hier ist risikoangemessener Schutz oberste Pflicht. - Daten sind der Schatz unseres Unternehmens. Dieser muss geschützt werden, und zwar ohne Wenn und Aber. Reichen Schutzmaßnahmen nicht aus oder werden diese nicht umgesetzt, muss unbedingt gehandelt werden. Jeder Datendiebstahl und jeder Schaden können für das Unternehmen existenzbedrohend werden.	☐ Ja ☐ Nein
5. Kunden wissen Datenschutz zu schätzen.	- Niemand will, dass mit seinen personenbezogenen Daten schlampig umgegangen wird. Auch hat jeder etwas zu verbergen, gerade in Zeiten von Hackern & Co. - Nimmt man es mit dem Datenschutz nicht so genau und kommen Daten abhanden oder werden sie gestohlen, landet das ziemlich schnell in den Medien. Und das kann leicht zu Imageschäden und Umsatzeinbrüchen führen.	☐ Ja ☐ Nein



Datenschutz bei Vorhaben berücksichtigen: Empfehlen Sie dieses Vorgehen

Werden im Unternehmen viele Daten verarbeitet, kommt der IT-Abteilung eine besondere Bedeutung zu. Meist gestaltet, organisiert und betreibt diese Abteilung alles, was für das Verarbeiten der Daten erforderlich ist. Kein Wunder, dass man bei neuen Vorhaben zunächst mit der IT-Abteilung spricht. Sorgen Sie als Datenschutzverantwortlicher dafür, dass auch bei deren Beratung Datenschutz ein Thema ist.

Befähigen Sie die Kollegen

Merken die Kollegen der IT-Abteilung, dass das neue Vorhaben auch etwas mit personenbezogenen Daten zu tun hat, sollten diese direkt wissen: Hier gilt es, einiges zu beachten, beispielsweise um den Anforderungen der Datenschutz-Grundverordnung (DSGVO) gerecht zu werden. Also müssen Sie dafür sorgen, dass diese zumindest grob Bescheid wissen.

Dabei ist klar: Dass Sie den Kollegen erklären, worauf es ankommt und wie man vorgehen kann, ist nicht nur gut für den Datenschutz. Sie erleichtern sich damit auch die Arbeit als Datenschutzbeauftragter. So können die Kollegen nicht nur bei deren Beratung einige wichtige Punkte mit Datenschutzrelevanz ansprechen. Sie können auch viele wichtige Informationen sammeln, die für Sie als Datenschutzbeauftragter für Ihre Beratung von Bedeutung sind. Außerdem stellen Sie sicher, dass man frühzeitig ein Auge auf den Datenschutz hat.



Erstellen Sie ein kurzes Merkblatt

Sie können Kollegen noch so gut erklären, wie sie am besten vorgehen sollen. Doch es liegt nahe, dass man im Fall der Fälle den einen oder anderen Punkt vergessen hat. Um der Erinnerung auf die Sprünge zu helfen, können Sie aus den hier beschriebenen Schritten ein Merkblatt erstellen. Und darauf können die Kollegen schnell zurückgreifen.

Packen Sie beispielsweise auf die Vorderseite einer DIN-A4-Seite die Schritt-für-Schritt-Anleitung und auf die Rückseite einen groben Überblick zum technisch-organisatorischen Datenschutz, etwa das auf Seite 5 gezeigte Merkblatt.

Empfehlen Sie den IT-Kollegen die folgenden Schritte für deren datenschutzfreundliche Beratung:

Schritt 1: Umfassenden Überblick verschaffen

Kommt man auf ein neues Vorhaben zu sprechen, sollten Sie direkt in Erfahrung bringen, inwieweit Daten eine Rolle spielen, die sich auf Menschen beziehen lassen. Ist das der Fall, besteht auch Datenschutzrelevanz. Denn die DSGVO dient dem Schutz personenbezogener Daten bei deren Verarbeitung, etwa durch das Unternehmen. Ist die DSGVO anzuwenden, müssen viele Aspekte berücksichtigt werden.

Wichtig ist auch, dass Sie konkret in Erfahrung bringen, was man warum und wie vorhat. Die Motivation für eine bestimmte Verarbeitung von Daten deutet meist auch auf den verfolgten Zweck hin. Der kann entscheidend sein, wenn es um die

Beurteilung einer Rechtsgrundlage geht. Das ist die Erlaubnis, personenbezogene Daten zu verarbeiten. Findet sich keine solche Erlaubnis, muss die Verarbeitung der personenbezogenen Daten unterbleiben.

Idealerweise wird das Vorhaben konkret beschrieben, etwa in einer Präsentation. Doch auch Übersichten und Datenflussdiagramme können viele Informationen für die spätere Bewertung durch den Datenschutzbeauftragten liefern.

Schritt 2: Gefahren ausmachen und Risiken bewerten

Auch diese Aspekte sind entscheidend, um die richtigen Schlüsse zu ziehen und beispielsweise für angemessenen Schutz der betreffenden Daten zu sorgen. Dabei ist das prinzipielle Vorgehen schnell erklärt.

Zunächst werden die denkbaren Gefahren zusammengestellt. Das sind Aspekte, die bei ungehindertem Fortgang der Dinge zu einem Schaden führen. Eine typische Gefahr ist beispielsweise ein erfolgreicher Hackerangriff aufgrund einer veralteten Software für den Onlineshop. Diesbezüglich wird überlegt, welcher Schaden entstehen kann, wenn dieser Fall tatsächlich eintritt.

Außerdem wird eingeschätzt, wie wahrscheinlich es ist, dass sich eine Gefahr realisiert und der betreffende Schaden eintritt. Die Bewertung kann beispielsweise mit 1 (niedrig), 2 (mittel) und 3 (hoch) erfolgen. Werden die Bewertungen multipliziert, erhält man die bewerteten Risiken. So wird schnell klar, wo man die größten Anstrengungen unternehmen muss, um die Risiken auf ein niedrigeres oder akzeptables Niveau zu bringen.

Schritt 3: Legen Sie passende Schutzmaßnahmen fest

Jede Verarbeitung personenbezogener Daten muss sicher sein. Das ergibt sich aus Art. 32 DSGVO. Auf Basis der Risikobewertung müssen Schutzmaßnahmen ergriffen werden, um die Risiken auf null oder zumindest auf ein vertretbares Level zu bringen. Die Schutzmaßnahmen können technischer oder organisatorischer Natur sein, Beispiel gefälltig? Die Einstellungen in einer Software können technisch für Zugriffsbeschränkungen sorgen. Organisatorisch sind hingegen die Regelungen zu den betreffenden Berechtigungen, sprich wer Zugriff erhalten soll.

Schritt 4: Datenschutzbeauftragten einbinden

Weil beim Verarbeiten von personenbezogenen Daten bzw. bei der Gestaltung von Verfahren und Prozessen vieles zu beden-

ken ist, sollte unbedingt der Datenschutzbeauftragte einbezogen werden. Er kann auf Basis seiner Expertise und seiner Erfahrung Hinweise geben, wie das Vorhaben datenschutzfreundlich realisiert werden kann. Auch kann eine frühzeitige Einbindung vor Fehlentscheidungen oder Fehlentwicklungen schützen.

Schritt 5: Rahmenbedingungen regeln

Auch das Drumherum spielt häufig eine wichtigere Rolle, als es auf den ersten Blick erscheint. Werden etwa Dienstleister oder Softwareanbieter in die Verarbeitung von Daten eingebunden, ist eine Vereinbarung zum Datenschutz meist unumgänglich. Doch es sind noch weitere Aspekte zu bedenken. Möglicherweise muss der Betriebsrat eingebunden werden. Dieser kann ein Mitbestimmungsrecht haben. Auch müssen ggf. Regelwerke, Arbeitsanweisungen oder Trainings für die Anwender erstellt werden.

Schritt 6: Vorhaben umsetzen

Wurden etwa Schutzmaßnahmen festgelegt, dürfen diese nicht nur auf dem Papier stehen. Sie müssen tatsächlich umgesetzt sein, damit der mit ihnen verfolgte Zweck eintritt. Hier kann es auch sinnvoll sein, den Datenschutzbeauftragten ein-

zubinden. Dieser kann einen unabhängigen Soll-Ist-Abgleich machen und auf Defizite hinweisen, bevor diese zum Problem werden.

Schritt 7: Beobachten Sie die Sache fortlaufend

Ist etwa ein Projekt abgeschlossen und wird eine Verarbeitung, ein System oder eine Software eingesetzt, heißt das nicht, dass man die Hände in den Schoß legen kann. Im Gegenteil: Nicht nur die Technik entwickelt sich immer weiter. Auch neue Gefahren können auftreten. Selbst ohne das Zutun des Unternehmens können sich Gefahren und Risiken verändern. Insofern ist es unerlässlich, immer wieder ein Auge auf gemachte Bewertungen und umgesetzte Maßnahmen zu haben. Diese müssen immer passen, umgesetzt sein und funktionieren.



Fördern Sie den Schutz

Dass etwa Schutzmaßnahmen immer auf der Höhe der Zeit sind, können auch Sie als Datenschutzbeauftragter aktiv unterstützen. Bekommen Sie etwa aus den Medien mit, dass es beim Produkt eines Wettbewerbers oder bei einer eingesetzten Technologie zu Problemen kommt, sprechen Sie das offen an. Laden Sie die Kollegen zu einem kurzen Austausch ein und klären Sie die Relevanz.



MUSTER: Merkblatt zu technisch-organisatorischen Schutzmaßnahmen



Merkblatt 2

Schneller Überblick: Sicherheit der Verarbeitung – technisch-organisatorische Schutzmaßnahmen

Art. 32 Datenschutz-Grundverordnung (DSGVO) macht zur Vorgabe, dass für jede Verarbeitung personenbezogener Daten risikoangemessene Maßnahmen ergriffen werden müssen, damit die Daten geschützt sind. Dabei können technische oder organisatorische Maßnahmen ergriffen werden. Meist zeigt die Kombination von Maßnahmen aus beiden Bereichen die beste Wirkung, um Risiken einzudämmen. Dabei dürfen die Maßnahmen nicht willkürlich ausgewählt werden. Sie müssen zu den identifizierten Risiken passen, damit sie entsprechend Wirkung entfalten.

In Art. 32 DSGVO finden Sie folgende Schutzziele, für die Schutzmaßnahmen festzulegen und umzusetzen sind. Viele der genannten Beispiele können auch bei anderen Bereichen passen. Eine Maßnahme kann also auch mehrfach wirken.

Schutzziele	Beispiele
Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)	Gerade in größeren Unternehmen und Konzernen ist die Bezeichnung eine Art „Nummernschild“, aus dem man viel ablesen kann. So z. B. die Bedeutung, die Zuordnung zu einem Geschäftsbereich, die hierarchische Ebene oder die Aufgabe.
Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)	Diese Person trägt meist die Verantwortung für die Erfüllung der Aufgabe, das Personal und das Budget. Klar ist auch: Diese Person ist auf dieser Ebene auch für den Umgang mit personenbezogenen Daten verantwortlich.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)	Das ist eine wichtige Information, etwa wenn Sie im Fall der Fälle ein Thema ganz oben adressieren wollen oder müssen. Dann brauchen Sie sich nicht lange durchzufragen.
Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. c DSGVO)	Lassen Sie sich einen Überblick über die Strukturen geben. Idealerweise kann man Ihnen ein Organigramm zur Verfügung stellen. Achten Sie bei Organigrammen darauf, dass es nicht nur um die Funktion geht. Am besten gehen daraus Über- und Unterordnungen hervor bzw. wer wem was zu sagen hat.
Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 Buchst. d DSGVO)	Ist Ihr Unternehmen oder ist ein spezielles Projekt international aufgestellt, kann das auch von großer Tragweite für den Datenschutz sein. Meist müssen auch personenbezogene Daten zwischen Rechtseinheiten, also Verantwortlichen, übertragen werden.

Übrigens: Haben Sie Fragen zur Festlegung und Auswahl von Maßnahmen zum Schutz personenbezogener Daten? Dann zögern Sie nicht lange! Kontaktieren Sie den Datenschutzbeauftragten. Er unterstützt Sie gern mit Rat und Tat.



Stiefmütterlich behandelte Themen: Diese können Sie ansprechen

Gerade wenn in Ihrem Unternehmen die IT-Abteilung klein ist oder manche Aufgaben von Kollegen mit thematisch ganz anderer Qualifikation übernommen werden, kann das zum Problem werden. Denn Hacker und Cyberkriminelle nehmen keine Rücksicht darauf, dass sich Ihr Unternehmen und die Mitarbeiter bemühen, alles bestmöglich zu managen. Schauen Sie daher genauer hin.

Ihr Job: beraten und kontrollieren

Führen Sie sich und ggf. auch den Kollegen stets vor Augen: Ihre Kernaufgaben bestehen einerseits im Beraten in allen Fragen mit Datenschutzrelevanz. Das umfasst auch das Erkennen von Gefahren und das Ausmachen von Risiken, insbesondere beim Umgang mit personenbezogenen Daten. Andererseits ist es Ihr Job, dass Sie die Einhaltung der Anforderungen zum Datenschutz, und zwar gerade aus der Datenschutz-Grundverordnung und aus dem Bundesdatenschutzgesetz, kontrollieren. Hier prüfen Sie, ob das Ist zum Soll passt. Ist das nicht der Fall, ergeben sich auch hieraus Gefahren und Risiken, bezüglich derer Ihre Beratung als Datenschutzbeauftragter gefragt ist. Insofern ergänzen sich Beraten und Kontrollieren und das eine führt immer wieder zum anderen.

Prüfen Sie häppchenweise

Wollen Sie etwa eine Prüfung oder ein Audit in der IT-Abteilung durchführen, können Sie in den meisten Fällen problemlos Prüft Themen für mehrere Tage oder gar Wochen finden. Doch wenn Sie eine Prüfung auf mehrere Tage oder gar Wochen ausdehnen, werden Sie schnell merken: Die Akzeptanz für Ihr Vorhaben wird schnell gegen null sinken. Denn bei allem Verständnis für den Datenschutz und Ihren Kontrollauftrag als Datenschutzbeauftragter hat jede Prüfung meist erhebliche Auswirkungen auf das Tagesgeschäft der IT-Abteilung. So muss man sich auf Ihre Prüfung vorbereiten, Unterlagen und Nachweise zusammenstellen und auch Mitarbeiter als Gesprächspartner oder für die Begleitung Ihrer Prüfung abstellen.

Dem Frust und Akzeptanzverlust können Sie insbesondere damit entgegenwirken, dass Sie Ihre Prüfung aufteilen und die für Sie besonders relevanten Aspekte in kurzen Prüfungen kontrollieren. Nehmen Sie sich ein Thema vor, kündigen Sie die Prüfung frühzeitig an und ziehen Sie das Ganze beispielsweise an einem Nachmittag in einigen Stunden durch.

Anstatt einer Prüfung: Reden!

Doch es muss nicht unbedingt eine Prüfung sein, damit sich etwas zum Positiven verändert. Manchmal reicht schon ein ausführliches Gespräch, um die zuständigen Personen nachdenklich zu machen und zum Handeln zu motivieren. Im Übrigen ist es einen Versuch wert, es zunächst mit einem Gespräch zu probieren. Fruchtet das nicht, können Sie immer noch zur Prüfung übergehen.

Setzen Sie auf stiefmütterlich behandelte Themen

Nicht alles wird immer mit der gebotenen Aufmerksamkeit und dem eigentlich nötigen Engagement angegangen. Das ist wohl in jedem Unternehmen so. Und dennoch ist es keine Rechtfertigung, die Dinge einfach laufen zu lassen. Denn geht etwas schief, helfen auch hier die bestklingenden Ausreden wenig. Daher: Überlegen Sie zunächst, welche Themen in Ihrer IT-Abteilung vielleicht etwas auf der Strecke bleiben oder eher stiefmütterlich betreut werden. Vertrauen Sie hier auch auf Ihre Intuition als Mitarbeiter Ihres Unternehmens und als Datenschutzbeauftragter. Sollte Ihnen auf Anhieb nichts Relevantes für eine Prüfung oder ein Gespräch einfallen, können Sie Ihren Ideen mit folgender Checkliste auf die Sprünge helfen.

 CHECKLISTE: „Problemzonen“ in der IT-Abteilung		
Aspekt	Hintergrund	Besprochen bzw. geklärt?
Risikomanagement	› Lassen Sie sich erläutern, wie man beim Identifizieren und Behandeln von Risiken vorgeht. Hierzu sollte es klare Regeln geben. Sprechen Sie auch an, wie das Ganze dokumentiert wird. › Haben Sie auch ein Auge auf Risiken, die meist in der Verantwortung der IT-Abteilung liegen und die auch Auswirkungen auf den Datenschutz haben können. Dazu können beispielsweise risikoangemessene Schutzmaßnahmen zählen. Auch das Entsorgen von Datenträgern (z. B. Festplatten und Computer) birgt großes Risikopotenzial, wenn etwa Daten in falsche Hände geraten können.	☐ Ja ☐ Nein
Vorbereitung auf und Umgang mit Ausnahme-situationen	› Um richtig reagieren zu können, braucht es durchdachte Pläne und Prozesse. Hinterfragen Sie, wie man auf Zwischen-, Not-, Krisen- oder Katastrophenfälle vorbereitet ist. Auch hier besteht oft großer Datenschutzbezug, etwa wenn es um die Verfügbarkeit von Systemen und Daten geht oder um den Schutz vor unbefugtem Zugriff. › Damit im Fall der Fälle schnell und geordnet gehandelt wird, sind Schriftdokumente meist unerlässlich. Schauen Sie nach der Aktualität der Dokumente und prüfen Sie deren Plausibilität und Praxistauglichkeit.	☐ Ja ☐ Nein


CHECKLISTE: „Problemzonen“ in der IT-Abteilung

Aufbau von Know-how	- Die Welt bleibt nicht stehen. Daher müssen gerade Beschäftigte der IT-Abteilung das für ihre Aufgabe relevante Wissen „up to date“ halten. - Hinterfragen Sie den Wissensstand rund um den Datenschutz. Sieht es hier mau aus, besteht schon allein zur Risikominimierung Schulungsbedarf. Hier können Sie unterstützen. - Früher oder später wird in Ihrem Unternehmen künstliche Intelligenz (KI) ein Thema sein. Zum Thema Know-how macht die KI-Verordnung (KI-VO) Vorgaben, die bereits seit 2.2.2025 verbindlich sind. Auch wenn Ihr Unternehmen KI nur nutzt, gilt es als Betreiber. Nach Art. 4 KI-VO muss es nach besten Kräften sicherstellen, dass das mit dem Betrieb oder der Nutzung betraute Personal über ein ausreichendes Maß an KI-Kompetenz verfügt.	☐ Ja ☐ Nein
Administration und Rechtemanagement	- Administratoren haben meist weitreichende Rechte, um etwa Systeme und Daten verwalten oder Mitarbeitern Berechtigungen einräumen zu können. Sind die Berechtigungen zu weitreichend und nicht für die Arbeitsaufgabe erforderlich, kann das als Zugriff Unbefugter auf schutzwürdige Informationen zu werten sein. Das wäre ein großes Datenschutzproblem. - Hinterfragen Sie die Vorgehensweise zur Vergabe und zum Entzug von Berechtigungen. Hier sollte es klare Regelungen und Prozesse geben, an denen niemand vorbeikommt. Insbesondere darf es auch keinen „kleinen Dienstweg“ geben, mit dem die Regelungen umgangen werden können. - Schauen Sie sich für Systeme bzw. Datenablagen an, wer darauf Zugriff hat. Prüfen Sie, inwieweit hier Personen Zugriff haben, bei denen keine Berechtigung vorliegt.	☐ Ja ☐ Nein
Entsorgung	- Manche IT-Abteilung vermittelt den Eindruck einer „Elektroschrotthalde“. Schauen Sie, was Sie vor Ort finden, und klären Sie, inwieweit die Gerätschaften noch über schutzwürdige Informationen verfügen bzw. inwieweit ein Zugriff Unbefugter möglich ist. Das darf es nicht geben. - Nehmen Sie die relevanten Prozesse unter die Lupe, etwa im Zusammenhang mit der Ausgabe oder Rückgabe von Computern, bei Garantiefällen, der Löschung oder der tatsächlichen Entsorgung der datenspeichernden Geräte - Auch die Dokumentation ist wichtig. So z. B., wenn geleaste Geräte zurückgegeben werden, sollte etwa die Löschung durch die IT-Abteilung dokumentiert sein.	☐ Ja ☐ Nein
Server- und Technikräume	- Der Serverraum beherbergt das Gehirn Ihres Unternehmens. Also sollte dieser im Topzustand sein. Haben Sie hier zudem ein Auge darauf, wer Zutrittsrechte hat bzw. wie man mit externen Technikern und Servicemitarbeitern umgeht. - Das hohe Niveau des Serverraums suchen Sie in Technikräumen vielleicht vergebens. Nicht selten sind diese unverschlossen und werden dennoch als Lager für Technik und ausgemusterte Geräte genutzt. Das sollte so nicht sein.	☐ Ja ☐ Nein
Datensicherungen	- Lassen Sie sich erklären, welche Systeme bzw. Daten wie gesichert werden. Die Vorgehensweise sollte klar festgelegt sein. Auch sollten die durchgeführten Sicherungen nachvollziehbar dokumentiert sein. - Klären Sie, inwieweit Datensicherungen vor unbefugtem Zugriff und vor Beschädigung bzw. Zerstörung geschützt sind. Schließlich müssen die Sicherungen im Fall der Fälle lesbar sein. - Scheuen Sie sich nicht, danach zu fragen, wann das letzte Mal eine Wiederherstellung erfolgt ist bzw. wann man diese geprobt hat. Eine Datensicherung ist nur die halbe Miete. Klappt die Wiederherstellung von Systemen oder Daten nicht, kann das die Existenz Ihres Unternehmens bedrohen.	☐ Ja ☐ Nein
Austritt oder Wechsel von Mitarbeitern	- Verlassen Mitarbeiter das Unternehmen, gibt es für die IT-Abteilung viel zu tun. Und vieles hat Datenschutzrelevanz, weil der ehemalige Mitarbeiter mit dem Austritt zum Unbefugten wird. - Lassen Sie sich die Prozesse erläutern und klären Sie, welche Rolle die IT-Abteilung spielt. Achten Sie insbesondere auf die Dokumentation der Umsetzung wichtiger datenschutzrelevanter Aspekte, wie etwa des Entzugs von Berechtigungen zum Zugriff auf Daten oder der Deaktivierung von E-Mail-Postfächern. Auch sollte die Möglichkeit zur Einwahl in das Firmennetzwerk unverzüglich beendet werden. - Machen Sie den Check bezüglich erst kürzlich ausgetretener oder gewechselter Mitarbeiter. Lassen Sie sich in den Systemen die Umsetzung der erforderlichen Maßnahmen zeigen.	☐ Ja ☐ Nein
Datenlöschung	- Schauen Sie zunächst auf die Löschung personenbezogener Daten. Gibt es für deren Verarbeitung keine Berechtigung mehr, müssen sie gelöscht werden. - Auch andere schutzwürdige Daten sollten nicht gehortet werden, wenn sie nicht mehr gebraucht werden. Das spart nicht nur Speicherkosten. Auch Langfinger oder Cyberkriminelle gehen leer aus, wenn nichts da ist.	☐ Ja ☐ Nein



7 Tipps mit Wirkung: Stärken Sie die gute Beziehung zur IT-Abteilung

Damit das Arbeiten Spaß macht, brauchen Sie gute Beziehungen, auch im Unternehmen. Wenn es mit der IT-Abteilung bislang nicht so rundläuft, sollten Sie das ändern. Bereiten Sie mit den folgenden sieben Tipps die Basis für eine gute Beziehung zur IT-Abteilung:

Tipp 1: Machen Sie sich bekannt

Wie steht es um Ihre Bekanntheit bei der Leitung der IT-Abteilung, bei Themenverantwortlichen oder einzelnen Mitarbeitern? Wenn Sie sich nicht sicher sind, dass beim Begriff Datenschutzbeauftragter jeder sofort an Sie, Ihr Gesicht und Ihren Namen denkt, dann sollten Sie aktiv werden. Entscheidend für eine gute Zusammenarbeit ist nämlich, dass man Sie kennt und weiß, was Sie machen.

Nutzen Sie am besten alle Gelegenheiten, um sich bei den Kollegen bekannt zu machen. Wird etwa im Unternehmen kommuniziert, dass jemand die Leitung der IT-Abteilung übernimmt, suchen Sie das Gespräch und stellen Sie sich vor. Ferner: An Veranstaltungen sollten Sie nicht einfach nur teilnehmen und direkt wieder verschwinden. Sprechen Sie am Ende etwa Referenten an und beglückwünschen Sie diese zu einem gelungenen Vortrag. So kommen Sie nicht nur ins Gespräch. Man wird Sie länger in guter Erinnerung behalten.

Tipp 2: Vermeiden Sie jeglichen Konfrontationskurs

Die IT-Abteilung hat manchmal ein gewisses Eigenleben. Und manchmal steht man auch mit dem Datenschutz auf Kriegsfuß. Das muss jedoch nicht heißen, dass Sie jede Gelegenheit nutzen, um klarzumachen, was man im Datenschutz alles falsch macht. Das verbietet sich gerade dann, wenn Sie mit Ihrer „Klarstellung“ jemandem in die Parade fahren und ziemlich alt aussehen lassen. Suchen Sie lieber im Nachgang das Gespräch und machen Sie Ihre Sicht der Dinge klar. Auch dann lässt sich Falsches geschickt und ohne viel Aufhebens korrigieren, etwa indem man auf eine „nochmalige Bewertung der Sachlage“ verweist.

Tipp 3: Fördern Sie den regelmäßigen Austausch mit der Leitung

Für Ihre Arbeit ist wichtig, dass Sie auf dem Laufenden sind, was das Unternehmen und entsprechend auch die IT-Abteilung in Sachen Datenverarbeitung vorhaben. Hier ist wichtig, dass es Ihnen zunächst nur darum geht, gut informiert zu sein. Beißen Sie sich auf die Zunge und vermeiden Sie negative oder abwertende Kommentare. Viel besser ist es, wenn Sie zuhören und feststellen: „Da sollten wir demnächst noch mal drüber reden. Schließlich kann das größere Datenschutzrelevanz haben.“ So vermeiden Sie nicht nur, dass man Sie als Schwarzseher oder Verhinderer wahrnimmt. Sie gewinnen auch Zeit, um sich mit den betreffenden Themen und den tatsächlichen Auswirkungen auf den Datenschutz auseinanderzusetzen. Dann können Sie beim nächsten Termin mit fundiertem Wissen aufwarten. Auch das unterstreicht Ihre Professionalität und macht Sie zum geschätzten Gesprächspartner.

Tipp 4: Informieren Sie über Wichtiges im Datenschutz

Ein gutes Verhältnis beruht auf Gegenseitigkeit. Das gilt gerade für den Wissenstransfer. Haben Sie Informationen, die auch für die IT-Abteilung von Relevanz sind, können Sie diese beispielsweise mittels E-Mail-Newsletter verteilen. Achten Sie hier darauf, dass Sie die Informationen lesenswert gestalten. Das bedeutet insbesondere, dass die Texte nicht zu kompliziert und lang werden sollten. Auch kann es eine gute Idee sein, dass Sie in den Newsletter nur kurze Texte aufnehmen und etwa auf den vollständigen Artikel auf Ihrem Intranetangebot verlinken.

Alternativ können Sie anbieten, dass Sie bei einer Abteilungsbesprechung über Neuerungen im Datenschutz berichten. Hier können schon 20 Minuten ausreichen, um wichtige Infos zu geben und Ihr Thema bzw. Ihre Arbeit zu präsentieren. Dabei sollten Sie stets versuchen, auch die Kollegen mit ihren Fragen und Erfahrungen zu Wort kommen zu lassen.

Tipp 5: Bieten Sie Ihre Unterstützung an

Natürlich sieht es die Datenschutz-Grundverordnung vor, dass man eher auf Sie zukommen muss, um Ihre Beratung in Anspruch zu nehmen. Doch warten, bis man Sie fragt, kann der Sache nicht dienlich sein und auch Ihre Arbeit unnötig schwer und aufwendig machen. Daher sind Sie mit folgender Handhabung viel besser beraten: Erfahren Sie von einem neuen Vorhaben, suchen Sie den Kontakt mit den Verantwortlichen. Vereinbaren Sie einen Termin zum Austausch und bieten Sie Ihre beratende Unterstützung an.

Tipp 6: Erleichtern Sie Kontaktaufnahme und Austausch

Das gelingt Ihnen beispielsweise dadurch, dass Sie bei Veranstaltungen immer ein Namensschild mit Ihrer Funktion tragen oder ein Schild auf dem Tisch platzieren. Wer Sie noch nicht kennt, kann sich unter Funktion und Namen nun endlich jemanden vorstellen. Geben Sie immer dem Reden den Vorzug. Fragt man Sie per E-Mail zu einem Thema, antworten Sie nicht lang und breit per E-Mail. Greifen Sie zum Hörer. Nach dem Gespräch kann Ihre E-Mail meist viel kürzer ausfallen. Auch vermeiden Sie, dass es Missverständnisse gibt oder man lange aneinander vorbeiredet.

Tipp 7: Beteiligen Sie sich an Arbeitsgruppen

Arbeitsgruppen gibt es meist zu vielen Themen. Sehen Sie zu, dass man Sie in relevante Arbeitsgruppen aufnimmt. Denn so haben Sie die Gelegenheit, Ihr Thema einzubringen und die Dinge mitzugestalten. Die Unterstützung wird man meist auch sehr positiv wahrnehmen.

„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

Automatisieren Sie Ihre Mitarbeiterschulung!

Jetzt Test-Account gratis aktivieren:



<https://t1p.de/cyberxperts-gratis-test>



DEUTSCHE
FACHPRESSE
**FACHMEDIUM
DES JAHRES 2024
GEWINNER**

Beste Workflow-Lösung



www.privacyxperts.de/login



www.privacyxperts.de/kontaktformular/



Telefon: 02 28 95 50 150

Fax: 02 28 36 96 480

E-Mail: kundendienst@privacyxperts.de

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