Spezialausgabe März 2026

PRIVACY@WORK

FÜR DATENSCHUTZBEAUFTRAGTE

IT-Abteilung: Fördern Sie das Datenschutz-Verständnis

PRIVACY PERTS

ANDREAS WÜRTZ – IHR EXPERTE FÜR DATENSCHUTZ
ANDREAS WÜRTZ VERFÜGT ÜBER MEHR ALS 17 JAHRE BERUFSERFAHRUNG ALS VOLLZEIT-DATENSCHÜTZER IM UNTERNEHMEN. ER ZEIGT IHNEN, WIE SICH DATENSCHUTZ PRAGMATISCH UMSETZEN LÄSST.

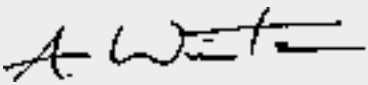
Setzen Sie auf Ihren Freund und Helfer

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. Das ist die IT-Abteilung.

Wenn Sie nun denken, dass das gerade nicht der Fall ist, sollten Sie damit beginnen, das 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, damit Datenschutz funktioniert. Stärken Sie also Ihre Beziehung zu den Kollegen.

Viele Grüße



Andreas Würtz, Rechtsanwalt und Chefredakteur des Ratgebers „Datenschutz aktuell"

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

Werden in Ihrem Unternehmen personenbezogene Daten verarbeitet, ist das auch für Sie als Datenschutzbeauftragter 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 schlauen Spruch beherzigen: Der Köder muss dem Fisch schmecken und 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, welchen Bedarf es gibt und wie Sie beim Vermitteln am besten vorgehen können.

Sind Sie sich hier unsicher, gibt es eine ganz einfache Möglichkeit, um 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.

Sensibilisieren Sie die IT-Abteilung für Ihr Thema

In der IT-Abteilung arbeiten häufig Profis und Spezialisten, die sich mit ganzem Herzen dafür einsetzen, die beste Lösung für eine meist technische Herausforderung 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 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 gesetzestreu 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 nutzen, 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 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.

Musterschreiben: 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 Arbeits-

alltag 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 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 alle 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 gerne 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 beispielsweise 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, der 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

es sich lohnen kann, ein Auge auf den Datenschutz zu haben, kann das viel zu einem gut funktionierenden Datenschutz im Unternehmen beitragen.

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 bei Weitem nicht ausgeschöpft wird. Im Übrigen ist es in Deutschland ohnehin etwas weniger wahrscheinlich, dass ein hohes Bußgeld verhängt wird. Deutsche Aufsichtsbehörden verfolgen meist einen eher kooperativen Ansatz, sodass es bei Verwarnungen und deutlichen Ansagen bleibt, zumindest bei Erstverstößen. Argumentieren Sie also nicht zu sehr mit drohenden hohen Bußgeldern.

Checkliste: 5 gute Gründe für Datenschutz

Grund	Das können Sie dazu erläutern	Besprochen?	
		ja	nein
Wir verhalten uns gesetzes- 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 „Datenschutzbürokratrie“ 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.	○	○

Die Konkurrenz schläft nicht.	Sparen wir uns den Datenschutz, muss nicht heißen, dass wir einen Vorteil gegenüber Wettbewerbern haben. Im Gegenteil: Diese sind im Vorteil, wenn sie sich an Recht und Gesetz halten. So empfehlen sich auch Kunden 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.	●	●
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 wegen guter Schutzmaßnahmen Kriminelle 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.	●	●
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 beschützt werden, und zwar ohne Wenn und Aber. Reichen Schutzmaßnahmen nicht aus oder sind diese nicht umgesetzt, muss unbedingt gehandelt werden. Jeder Datendiebstahl und jeder Schaden können für das Unternehmen existenzbedrohend werden.	●	●
Kunden wissen Datenschutz zu schätzen.	Niemand will, dass schlampig mit seinen personenbezogenen Daten 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 zu Imageschäden und Umsatzeinbrüchen führen.	●	●

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 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 auf das 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 abgedruckte Merkblatt.

Empfehlen Sie den IT-Kollegen folgende 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 gefällig? 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 bedenken 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 Daten-

schutzbeauftragten einzubinden. 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.

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)	• Beschränkung des Zutritts zum Firmengelände, zu Gebäuden, Bereichen oder Büros • Begrenzung des Zugangs und Zugriffs auf Systeme und Daten • Trennung von Daten, das heißt keine Vermischung von personenbezogenen Daten • Verwendung von Pseudonymisierungsmethoden, um den direkten Personenbezug aufzuheben • Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren • Regelungen und Prozesse zur Sicherstellung des Datenschutzes • Löschung nicht mehr erforderlicher Daten • Schulung und Sensibilisierung von Beschäftigten • Durchführung von regelmäßigen Checks und Audits • Bewertung und Kontrolle der Vertraulichkeit durch den Datenschutzbeauftragten
Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)	• Gewährleistung der Unveränderbarkeit von Daten z. B. durch Signaturen und Veränderungssperren • Überwachung bzw. Erkennung der Veränderung von Daten • Einschränkung der Weitergabe von Daten • Umsetzung eines restriktiven Rollen- und Berechtigungskonzepts
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)	• Durchführung von System-, Software- und Datensicherungen • Vorbereitung auf Not- und Katastrophenfälle • Bereithalten von Redundanzsystemen, um bei Ausfällen weiterarbeiten zu können • Auswertung von Logdateien und Fehlerberichten
Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. c DSGVO)	• Sicherung von Daten auf verschiedene Weisen • sichere Aufbewahrung von Back-ups an verschiedenen Orten • Prüfung der Vollständigkeit und Funktionsfähigkeit von Sicherungen und Daten • festgelegte Prozesse zur Wiederherstellung von Systemen und Daten • Tests und Übungen zur Umsetzung nötiger Maßnahmen im Ereignisfall

Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 Buchst. d DSGVO)	• Festlegung und Umsetzung eines Datenschutzmanagementsystems • Gewährleistung der Aktualität und Sicherheit von Systemen und Software durch Regelungen, Prozesse und Kontrollen • Durchführung von eigenen Kontrollen • Überprüfung der Einhaltung durch den Datenschutzbeauftragten • fortlaufende Beobachtung der Risikosituation und der technischen Entwicklungen • Kontrolle der Arbeit von eingebundenen Dienstleistern • Anpassung von Schutzmaßnahmen bei veränderten Rahmenbedingungen oder veränderter Risikosituation

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, für die Ihre Beratung als Datenschutzbeauftragter gefragt ist.

Sie sind Teil des Risikomanagements

Verdeutlichen Sie im Bedarfsfall zudem auch, dass Sie das Ganze nicht deshalb machen, um die Kollegen zu gängeln oder zu quälen. Vielmehr geht es darum, die Einhaltung gesetzlicher Anforderungen unter die Lupe zu nehmen. Auch das ist Teil des Risikomanagements des Unternehmens. Und Risikomanagement muss jedes Unternehmen betreiben. Denn klar ist: Gesetzeswidriges Verhalten kann gerade im Datenschutz so manchen Ärger nach sich ziehen. Da wären die Aufsichtsbehörde mit einem möglichen Bußgeld und Betroffene mit Schadensersatzforderungen oder Umsatzeinbrüche, weil schludriger Umgang mit persönlichen Informationen garantiert manchen Kunden verprellt.

Prüfen Sie häppchenweise

Wollen Sie etwa eine Prüfung oder ein Audit in der IT-Abteilung durchführen, können Sie in den meisten Fällen problemlos Prüfthemen für mehrere Tage oder gar Wochen finden. Doch wenn Sie eine Prüfung auf mehrere Tage oder gar Wochen ausdehnen, werden Sie eines ganz schnell merken: Die Akzeptanz für Ihr Vorhaben wird schnell gegen null sinken.

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 –– 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autor: Andreas Würtz, Freiberg am Neckar, Produktmanagement: Lisa Greiling, Bonn,

Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen,
Bildrechte S. 1: Angelina – Adobe.Stock.com,

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

Erscheinungsweise: 16 mal im Jahr; im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work 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.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.