Mittelstand 4.0
Kompetenzzentrum
Magdeburg

Basiswissen und Vokabular

Ihre ersten Schritte auf dem Weg zu einem Datenschutzkonzept für Ihr Unternehmen

Das können Sie selbst tun!

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Bild: opolja / fotolia.de

IMPRESSUM

Herausgeber: Mittelstand 4.0-Kompetenzzentrum Magdeburg c/o ZPVP GmbH
Redaktion: Mittelstand 4.0-Kompetenzzentrum Magdeburg c/o Otto-von-Guericke-Universität Magdeburg
Gestaltung: dripstyle designstudio
Bildnachweise: Mittelstand 4.0-Kompetenzzentrum Magdeburg, iStockphoto.com, fotolia.de
Druck: unitedprint.com Deutschland GmbH
Auflage: 250

AUTOREN

Autoren: Sebastian Nielebock, Mykkahilo Nykolaichuk, Frank Ortmeier
Lehrstuhl Software Engineering, Institut für Intelligente Kooperierende Systeme,
Fakultät für Informatik, Otto-von-Guericke Universität Magdeburg

Alle in diesem Leitfaden dargestellten Informationen entsprechen keiner Rechtsberatung bzw. **ersetzen keine rechtliche Beratung**. Sie stellen lediglich die persönliche Wahrnehmung der Autoren wider. Die Autoren übernehmen keine Haftung für eventuelle Folgeschäden, insbesondere rechtlicher Natur, die aus fehlerhaften Handlungen, die aus diesem Leitfaden herrühren, entstehen.

VORWORT

Sie informieren sich auf einer Firmen-Website im Internet. Sie möchten in einem Onlineshop bestellen oder sind Mitglied in einem Verband? Selbst wenn Sie auf den ersten Blick gar keine persönlichen Daten preisgeben, so hinterlassen Sie doch, bei allem, was Sie tun, Ihre Datenspur. Diese Datenspur gilt es zu schützen und im Umkehrschluss natürlich auch die Ihrer Kunden.

Am 25. Mai 2018 trat die so genannte Datenschutzgrundverordnung (DSGVO) in Kraft. Damit sind die Richtlinien noch strenger geworden. Wir alle wissen, dass uns der Schutz unserer Daten wichtig ist. Aber was genau bedeutet das? Welche Daten fallen zum Beispiel in meinem Unternehmen an? Welche Daten muss ich schützen und wie mache ich das? Wenn ich schon Schutzmaßnahmen ergriffen habe, sind diese ausreichend? Vor diesen Fragen stehen nicht nur Sie, sondern viele Unternehmer und Unternehmerinnen. Während Großbetriebe über eigene IT- und Rechtsabteilungen verfügen, stehen Firmenchefs kleinerer und mittlerer Unternehmen diesen Fragen häufig allein gegenüber. Oftmals fehlt schon das Basiswissen, von Zeit und Muße ganz zu schweigen.

Dazu vorab eine gute und eine weniger gute Nachricht. Beginnen wir mit der weiniger guten: Datenschutz ist komplex und entwickelt sich ständig weiter. Um wirklich auf Nummer sicher zu gehen, brauchen Sie sehr wahrscheinlich Rat und Hilfe eines Datenschutz-Experten. Dabei kann dieser Leitfaden Sie unterstützen, auf Augenhöhe mit einem Datenschutz-Profi zu reden, denn dafür statten wir Sie mit dem notwendigen Vokabular aus und vermitteln Ihnen die wichtigsten datenschutzrechtlichen Grundlagen. Am Ende eines Prozesses steht ein für Ihr Unternehmen maßgeschneidertes Datenschutzkonzept. Das ist nichts anderes als ein Maßnahmenkonzept, um den Datenschutz in Ihrer Firma einzuhalten. Wir zeigen Ihnen auch, wer genau Ihnen beim Datenschutzkonzept für Ihr Unternehmens unter die Arme greifen kann.

So kommen wir nun zur guten Nachricht: Guter Datenschutz ist wichtig, muss aber nicht teuer sein. Wichtig ist, dass Sie für Ihr Unternehmen systematisch vorgehen und im Thema stecken. So wird es Ihnen leichtfallen, die größten Risiken herauszufinden und zielgerichtet zu minimieren. Ist Ihr Blick einmal für eventuelle Sicherheitslücken geschult, sind Sie auch zukünftig für noch kommende Datenschutzmaßnahmen sensibilisiert. Datenschutz ist komplex und kompliziert. Aber Datenschutz ist auch keine „Raketenwissenschaft“. Wer es geschafft hat, ein Unternehmen aufzubauen und zu leiten, der kann auch die ersten Schritte hin zu einem Datenschutzkonzept selbständig gehen. Lassen Sie sich dazu von uns an die Hand nehmen. Datenschutz und Datensicherheit entwickeln sich stetig weiter.

Am besten ist, Sie entwickeln sich einfach mit ...

INHALT

3 Vorwort
4 Einleitung
6 Rechtliches Basiswissen
10 Bestandsaufnahme
10 Unternehmensdaten
14 IT-Strukturdaten
18 Geschäftsprozessdaten
22 Risikoeinschätzung
28 Handlungsempfehlung
31 Wer hilft mir weiter?

EINLEITUNG

In der heutigen hochgradig digitalisierten und vernetzten Welt ist ein Datenschutzkonzept ein „Muss“. Gemeint ist damit der genaue Plan, wie ein Unternehmen die gesetzlichen Regelungen zum Datenschutz einhält. Es handelt sich folglich um ein Maßnahmenkonzept, das unter anderem verhindert, dass personenbezogene Daten unbefugten Dritten zugänglich werden. Darüberhinaus beinhaltet ein Datenschutzkonzept, welche Daten im Unternehmen erfasst werden und wie sie im Hinblick auf ihr Risiko bewertet werden müssen.

Wir möchten Sie und Ihr Unternehmen daher befähigen und ermutigen, die ersten Schritte in Richtung eines eigenen Datenschutzkonzeptes selbstständig zu gehen. Somit richtet sich dieser Leitfaden in erster Linie an die Inhaber und Führungskräfte kleinerer und mittelständischer Unternehmen (KMUs) und ist sozusagen eine notwendige Vorstufe zum eigentlichen Konzept. Weitere Schritte müssen folgen, bei denen Sie sehr wahrscheinlich um juristischen und IT-technischen Expertenrat nicht herumkommen.

Dennoch sind wir überzeugt, dass Ihnen dieser Leitfaden dabei hilft zu verstehen, welche sensiblen Daten in Ihrem Unternehmen überhaupt anfallen und wie Sie mit diesen Daten umgehen sollten. So werden Sie befähigt, insbesondere eigene Datenflüsse in den Geschäftsprozessen selbstkritisch zu erfassen und in einem weiteren Schritt damit verbundene Risiken für Ihre Firma herauszufiltern. Daraus lässt sich wiederum ableiten, ob überhaupt, wo und wie dringend Handlungsbedarf besteht. Zumindest werden Sie beim Thema Datenschutzkonzept mitreden können. Zum einen mit Ihren Kunden, Mitarbeitern und Geschäftspartnern, zum anderen mit Rechtsberatern und IT-Dienstleistern – und zwar auf Augenhöhe.

Einige Sicherheitsvorkehrungen können Sie in Ihrem Unternehmen wahrscheinlich sogar ohne externe Hilfe umsetzen. Bei komplexeren IT- oder rechtsintensiven Fragestellungen werden Sie unter Umständen auf externe Expertenkompetenz zurückgreifen müssen. Wichtig für Sie ist es zu erfassen, welche Maßnahmen wichtig und welche weniger wichtig sind auf dem Weg zu einem eigenen Datenschutzkonzept. Nehmen Sie sich nun etwas Zeit für den Leitfaden. Wenn nötig, sprechen Sie Ihren IT-Dienstleister und Rechtsberater an. Auch wir beraten Sie gern,

Ihr Mittelstand 4.0-Kompetenzzentrum Magdeburg

WAS IST EIN DATENSCHUTZKONZEPT?

Unter anderem sollten folgende Punkte in Ihrem Datenschutzkonzept abgedeckt werden:

Verfahrensverzeichnis

Bestandteil eines jeden Datenschutzkonzeptes sollte das gesetzlich vorgeschriebene Verfahrensverzeichnis sein.

Auftragsdatenverarbeitung

Finden Teile der Datenverarbeitung außerhalb der Firma statt, muss dies dokumentiert und vertraglich verankert werden.

Löschung von Daten

Wann werden welche Daten gelöscht und welche gesetzlichen Aufbewahrungspflichten bilden dafür die Grundlage?

Rechtsgrundlage

Auf welcher Grundlage werden die entsprechenden Daten erhoben und verarbeitet?

Datenschutzbeauftragter

Gibt es einen Datenschutzbeauftragten im Unternehmen?

Zugriffe

Wer hat Zugriff auf die Daten?

Auskunftserteilung

Welche Daten von Betroffenen werden verarbeitet und wer hat Zugriff auf diese Daten?

INHALT UND STRUKTUR DER KAPITEL

Der Leitfaden ist in die vier Kapitel „Rechtliches Basiswissen", „Bestandsaufnahme", „Risikoeinschätzung" und „Handlungsempfehlungen" eingeteilt.

Jedes Kapitel ist wie folgt aufgebaut:

1. **Was soll erreicht werden?**
2. **Welche Fragen müssen beatwortet werden?**
3. **Praxisbeispiel**
4. **Checkliste**

Das Praxisbeispiel beschreiben wir anhand der fiktiven Meier Elektrik GmbH, einem Handwerksbetrieb, in dem neben Geschäftsführer Heinz Meier fünf Elektroinstallateure, eine Sekretärin und ein Azubi mitarbeiten. Zum Kerngeschäft der Meier Elektrik GmbH gehören Elektroinstallationen. Die Firma berät zu, prüft, installiert und wartet Elektro-, Telekommunikations- sowie EDV-Installationen und erwirtschaftet so einen Jahresumsatz von rund 1.200.000 Euro.

Begreifen Sie ein Datenschutzkonzept nicht als irgendwann abgeschlossenen Vorgang, sondern vielmehr als einen sich stetig weiter entwickelnden und wiederkehrenden Zyklus. Indem ständig neue Sicherheitslücken auftauchen, werden Sie und Ihr Unternehmen immerfort neue technische und organisatorische Maßnahmen ergreifen müssen, um Ihren Kunden den bestmöglichen Schutz Ihrer Daten garantieren zu können.

WAS SOLL ERREICHT WERDEN?

Unabhängig von der jeweiligen Branche und unabhängig davon, ob sich Ihre Firma eher an Privatpersonen oder andere Unternehmen richtet, fallen die so genannten personenbezogenen Daten an. Personenbezogene Daten sind Daten, mit denen Menschen erkannt werden können. Dabei spielt es keine Rolle, ob die Daten zum Beispiel aus dem Personalausweis stammen und damit direkt auf die Person verweisen oder ob indirekt ein besonderes Merkmal auf eine bestimmte Person schließen lässt. Letzteres ist zum Beispiel der Fall, wenn eine Person mit Hilfe von Initialen auf einer Anwesenheitsliste und Bildern auf einer Veranstaltung identifiziert werden kann. Alle diese Daten sind personenbezogen und persönlich. Somit unterliegen sie besonderem Schutz. Beispiele für personenbezogene Daten können neben Ausweis- und Bankdaten, das Geschlecht, Standorte oder dynamische IP-Adressen, die sogenannten Online-Kennungen, sein. Diese sind ähnlich der Postanschrift auf einem Briefumschlag, denn mittels einer IP-Adresse werden Datenpakete eindeutig einem Empfänger zugeordnet.

Es wird oft sowohl von Datenschutz als auch Datensicherheit gesprochen. Datensicherheit bezieht sich zunächst einmal auf alle Daten, seien sie nun personenbezogen oder nicht. Erstens müssen Sie garantieren können, dass kein Unbefugter auf diese Daten zugreifen kann (Vertraulichkeit). Zweitens sind Sie verpflichtet, dafür zu sorgen, dass die Daten nicht manipuliert werden können (Integrität). Drittens haben Sie dafür Sorge zu tragen, dass Sie diese Daten jederzeit griffbereit haben (Verfügbarkeit).

Datenschutz hingegen bezieht sich nur auf die personenbezogenen Daten. Schließlich hat jeder Bürger das Recht auf ‚informationelle Selbstbestimmung'. Das meint, dass jeder Einzelne grundsätzlich selbst bestimmen darf, ob er seine personenbezogenen Daten überhaupt preisgibt und wie sie verwendet werden dürfen. Das wiederum hat zur Folge, dass diese empfindlichen Daten nur gespeichert oder verwendet werden dürfen, wenn die betroffene Person vorher eingewilligt hat. Wenn Sie beispielweise eine Website zum ersten Mal besuchen, poppt in der Regel ein Banner auf. Dieses fordert den Besucher der Website oder Web-App dazu auf, seine datenschutzrechtliche Einwilligung zu erklären. Tut er dies, können seine personenbezogenen Daten, wie zum Beispiel seine IP-Adresse, gespeichert und verarbeitet werden. Es versteht sich von selbst, dass personenbezogene Daten generell nur legal genutzt werden dürfen.

Um mit Kundendaten arbeiten zu können, müssen die betroffenen Personen in die Verarbeitung ihrer Daten freiwillig einwilligen. Doch Ausnahmen bestätigen die Regel. Wenn Ihr Kunde Ihnen seine Kontaktdaten übergibt, damit Sie sich bei ihm melden, um den Auftrag abzuwickeln, ist das legitim und bedarf keiner besonderen Einwilligung. Ähnliches gilt, wenn Sie bestimmte Daten nutzen, um eine Aufgabe zu erfüllen, die einem rechtlichen, lebenswichtigen oder öffentlichen Interesse unterliegt. Der Gesetzgeber spricht dabei von „berechtigtem Interesse". So muss zum Beispiel ein Verein zur Betreuung seiner Mitglieder deren personenbezogene Daten verarbeiten können. Das bedeutet zum Beispiel, dass derjenige, der die Kommunikationsfunktion für einen Verein übernommen hat, die Vereinsmitglieder anschreiben darf, ohne dass die Mitglieder dazu vorher explizit eingewilligt haben.

Dennoch besitzen Ihre Kunden eine Reihe von Rechten, wie zum Beispiel das sehr wichtige Auskunftsrecht. So müssen Sie zum Beispiel in Form einer Datenschutzerklärung auf Ihrer Firmenwebsite darlegen, welche Rechte überhaupt bestehen, welche Daten beim Besuch Ihrer Homepage gespeichert und wie diese verwendet werden. Weitere wichtige Rechte Ihrer Kunden sind das Recht auf Berichtigung, das Recht auf Einschränkung der Verarbeitung und das Widerspruchsrecht. Von diesen Rechten können Ihre Kunden, trotz ihrer Einwilligung, zu jeder Zeit Gebrauch machen. Deswegen ist es so wichtig, über ein Datenschutzkonzept zu verfügen. Dieses befähigt Sie und Ihr Unternehmen, Anfragen, Auskünfte und Forderungen Ihrer Kunden schnell und vollständig bearbeiten zu können.

Dieser Leitfaden stattet Sie mit dem notwendigen Basiswissen und Vokabular aus, um sich damit an einen Experten zu wenden. Um ein funktionierendes Datenschutzkonzept zu entwickeln, raten wir Ihnen, sich professionelle Hilfe zu holen. Das heißt, dass Sie sich für rechtliche Fragen an einen Juristen oder bei technischen Fragen an Ihren IT-Dienstleister wenden. Um die wichtigen rechtlichen oder technischen Fragen zu klären, müssen Sie auch nicht immer sofort tief in die Tasche greifen. Oft sind ähnliche Fragestellungen bereits bei Partnerunternehmen, im vertrauten Umfeld eines Vereins oder durch Ihren eigenen IT-Dienstleister gut gelöst worden. Sich informieren und einfach nachfragen hilft oft schon, die ersten Wissenslücken zu schließen. Sie suchen nach einer kostenfreien Alternative? Dann fragen Sie in Ihrem Mittelstand 4.0-Kompetenzzentrum nach. Wir agieren bundesweit, unterstützen bei der Erarbeitung Ihres Datenschutzkonzept und vermitteln zudem auch Vorträge, Workshops, Umsetzungsprojekte oder Check-Ups zum Thema.

BEISPIELE FÜR PERSONENBEZOGENE DATEN

Bild: tomertu / fotolia.de

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

Welche personenbezogenen Daten sind für mein Tagesgeschäft essentiel wichtig?

Personenbezogene Daten können erhoben, gespeichert, verwendet und schließlich wieder endgültig gelöscht werden. Alle diese Aktivitäten fallen unter den Begriff der Datenverarbeitung. Sie setzt allerdings voraus, dass die betroffenen Personen entweder vorher zur Datenverarbeitung ausdrücklich eingewilligt haben oder ein berechtigtes Interesse besteht oder die Daten zur Auftragsabwicklung essentiell sind. Das wiederum birgt für Unternehmen einige Tücken. Muss eine Einwilligung eingeholt werden, und was heißt “freiwillig geschehen” und “eindeutig sein”? Eine Kopplung an Verträge oder an sonstige Leistungen, die erbracht werden sollen, ist laut Datenschutzgrundverordnung untersagt. Jeder Verbraucher soll und darf wissen, welche Firmen persönliche Daten über ihn gesammelt haben. Unternehmen müssen transparent darlegen, wann und zu welchem Zweck persönliche Kundendaten gespeichert wurden. Auch über die Speicherdauer muss Rechenschaft abgelegt werden. Generell gilt, dass Sie nur Daten sammeln sollten, die Sie wirklich benötigen und auch nur solange zu verwahren, wie unbedingt notwendig.

Benötigt mein Unternehmen einen Datenschutzbeauftragten?

Für die Datenverarbeitung verantwortlich ist Ihr Unternehmen, vertreten durch die Geschäftsführung. Arbeiten zehn oder mehr Mitarbeiter in Ihrem Unternehmen mit diesen Daten oder geht es um sehr sensible Daten, wie zum Beispiel Gesundheitsinformationen, muss ein Datenschutzbeauftragter bestellt beziehungsweise benannt werden. Bedenken Sie, dass zum Beispiel die Schulung eines internen Datenschutzbeauftragten Kosten auslösen können. Schließlich ist es auch möglich, einen externen Datenschutzbeauftragten einzusetzen, dessen Kosten Sie sich im besten Fall mit anderen KMUs teilen können. Des Weiteren darf die Geschäftsführung selbst nicht als Datenschutzbeauftragte/r agieren. Auch wenn es einen internen oder externen Datenschutzbeauftragten für Ihr Unternehmen gibt, bleibt letztlich die Geschäftsführung verantwortlich für den Datenschutz.

Wenn mein Unternehmen mit einem externen IT-Dienstleister zusammenarbeitet, ist eine Vereinbarung abgeschlossen?

Werden Aufträge extern bearbeitet, muss ein Vertrag mit dem externen Dienstleister abgeschlossen werden. Dabei handelt es sich um einen Datenverarbeitungsvertrag. Er kommt folglich zum Einsatz, wenn ein Auftragsverarbeiter, zum Beispiel ein Hoster einer unternehmerischen Webseite, die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Der Datenverarbeitungsvertrag sorgt dafür, dass alle Grundsätze aus Artikel 5 der Datenschutzgrundverordnung in diesem Bereich eingehalten werden. Diese Grundsätze kümmern sich zum Beispiel um die Bereiche Transparenz, Zweckbindung oder Speicherbegrenzung. Ein kostenloses Datenverarbeitungsvertrags-Muster finden Sie zum Beispiel unter www.datenschutz.sachsen-anhalt.de.

Wo kann eine kompetente Hilfe zur IT-rechtlichen Fragen eingeholt werden?

Ein geeigneter Jurist sollte sich mit den Bereichen IT-Recht, Informatik und Betriebsorganisation auskennen. Da es sich beim Datenschutzrecht um ein sehr dynamisches Rechtsgebiet handelt, sollte Ihr juristischer Berater auf dem aktuellen Stand sein. Das bedeutet, einen entsprechenden Erfahrungshorizont und aktuelle Referenzen vorweisen können. Ein guter IT-Dienstleister hat die Lösungen im Portfolio, welche das Tagesgeschäft Ihres Unternehmens sichern und die notwendigen Anpassungen bereits vorgedacht hat.

“Viele Personen denken, dass die Datenschutzgrundverordnung (DSGVO) viele Geschäftsmodelle und -prozesse verbietet. Das Gegenteil ist der Fall. Durch die DSGVO werden neue Ansätze überhaupt rechtssicher möglich.”

Prof. Dr. Frank Ortmeier, Projektleiter Themenschwerpunkt Safety & Security im Mittelstand 4.0-Kompetenzzentrum Magdeburg

PRAXISBEISPIEL

Im hier beschriebenen Beispiel handelt es sich um die fiktive Meier Elektrik GmbH, einen Handwerksbetrieb. Heinz Meier leitet das Unternehmen seit 30 Jahren. Fünf Elektroinstallateure, eine Sekretärin und ein Auszubildener gehören zu seinen Angestellten. Die Meier Elektrik GmbH berät, prüft, installiert und wartet Elektro-, Telekommunikations- und EDV-Installationen. Das heißt, Elektroinstallationen zählen zum Kerngeschäft der kleinen Firma.

Geschäftsführer Heinz Meier hat erkannt, dass in seinem Unternehmen personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Nur so lassen sich Kundenaufträge überhaupt erfüllen. Die Firma betreibt eine Webseite, über die sich Kunden über die Meier Elektrik GmbH informieren können. Die Webseite wird durch einen externen IT-Dienstleister gepflegt. Deswegen muss Heinz Meier mit seinem IT-Dienstleister einen Vertrag zur Auftragsverarbeitung schließen. In diesem Vertrag werden die Arten der Datenverarbeitung festgehalten.

Wer die Webseite der Meier Elektrik GmbH besucht, für den poppt eine Datenschutzerklärung in Form eines Banners auf. Dieses Banner benennt klar 1. den Namen und die Anschrift des Verantwortlichen, also Heinz Meier und seiner Firmenadresse. Es gibt Auskunft über 2. Umfang und Rechtsgrundlage, mit der die erhobenen personenbezogenen Daten verarbeitet werden. Der Websitebesucher erfährt, dass 3. Cookies und soziale Netzwerke verwendet und 4. Kontaktformular und E-Mail-Kommunikation genutzt werden. Auch über 5. die Rechte der Websitebenutzer klärt das Banner auf.

Für den Datenschutz im Unternehmen ist der Geschäftsführer Herr Meier verantwortlich. Da die Firma aus 8 Personen besteht, muss nicht notwendigerweise ein Datenschutzbeauftragter bestellt werden, da dies erst ab 10 Mitarbeitern, die mit personenbezogenen Daten umgehen, vorgeschrieben ist. In seinem Bekanntenkreis hat Heinz Meier zudem guten Kontakt zu einem IT-bewanderten Tischler. Der gibt Heinz Meier immer wieder wertvolle Tipps, wie er die neuen Anforderungen der Datenschutzgrundverordnung in seiner Tischlerei umsetzt.

CHECKLISTE

- ☑ Festlegung der personenbezogenen Daten, die für mein Tagesgeschäft wichtig sind
- ☑ Einholen der Einwilligung meiner Kunden, dass ich ihre personenbezogenen Daten einholen darf
- ☑ Prüfen, ob mein Unternehmen einen Datenschutzbeauftragten benötigt
- ☑ Abschließen einer Vereinbarung zur Auftragsverarbeitung mit einem externen Dienstleister, wenn meine Firma Aufträge extern bearbeiten lässt
- ☑ Finden eines geeigneten Juristen oder IT-Dienstleisters, der mich bei der Erstellung meines Datenschutzkonzeptes professionell unterstützt

BESTANDS-
AUFNAHME

WAS SOLL ERREICHT WERDEN?

Ihre Unternehmensdaten sind ein teures Gut, dass Sie bestmöglich schützen sollten. Ziel dieser ersten Bestandsaufnahme ist es, einen klaren Blick darauf zu bekommen, welche Daten in Ihrem Unternehmen überhaupt anfallen. Diese Daten gilt es dann zu dokumentieren, um sie bei Bedarf nicht nur vorlegen zu können, sondern Sie ganz grundsätzlich erst einmal bestmöglich abzusichern. So verraten Ihnen Ihre Unternehmensdaten zum Beispiel, wie viele Personen betroffen wären, wenn Ihr Unternehmensserver gehackt würde. Sie geben damit Auskunft über drohende Sicherheitslücken.

Nur wenn Sie wissen, was Ihnen und Ihrem Unternehmen im Ernstfall droht, können Sie ausreichend vorbeugen und vorab die notwenigen Schutzmaßnahmen treffen. Deshalb sollten Sie auch genau wissen, wer in Ihrem Unternehmen auf welche Daten in bestimmten Abteilungen oder Aufgabenbereichen zugreifen kann.

Selbst wenn Sie selbst nicht verstehen, welche technischen oder organisatorischen Maßnahmen zum Schutz ausreichen, helfen diese Informationen externen Sicherheits- oder IT-Firmen, maßgeschneiderte Techniken für einen effektiveren Schutz bereitzustellen.

Für jede Unternehmensleitung ist es daher wichtig zu begreifen, welche Gefahren durch einen sicherheitstechnischen Vorfall, zum Beispiel einen Hackerangriff, drohen. Dazu sind aktuelle und vollständige Zahlen notwendig.

Die reine Datenaufnahme ist ein notwendiger aber kein hinreichender Schritt für das Datenschutzkonzept. Die Unternehmensdaten helfen Ihnen, die Stellen zu identifizieren, an denen personenbezogene Daten verarbeitet, weitergegeben oder gelöscht werden. Somit bilden sie eine Grundlage, um das Risiko für die Betroffenen, das heißt für Ihre Mitarbeiter, Geschäftspartner und Kunden, einzuschätzen.

Wesentliche Unternehmensdaten

01. Firmenname
02. Branche
03. Namen der Geschäftsführung
04. Kontaktpersonen der Firma
05. Anzahl der Mitarbeiter
06. Abteilungen und Aufgabenbereiche mit ihren jeweiligen Verantwortlichen
07. Mitgliedschaften in Organisationen wie zum Beispiel Unternehmensverbänden
08. Anzahl der Kunden
09. Anzahl und Art der Zulieferer
10. Anzahl und Art externer Dienstleister wie zum Beispiel Steuerberatung oder IT

Je nach dem, wie Ihr Unternehmen aufgestellt ist, müssen gegebenenfalls weitere Daten ergänzt werden.

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

In welcher Branche ist Ihr Unternehmen aktiv?

Das ist vor allem wichtig, wenn Sie und Ihr Unternehmen mit besonders sensiblen personenbezogenen Daten hantieren. Dazu gehören neben Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit und Sexualleben auch die Gesundheitsinformationen. Sollte Ihr Unternehmen solche besonderen Daten erfassen müssen, ist es wichtig, sensible Daten auch als solche eindeutig zu identifizieren, um einen sicheren Umgang mit ihnen gewährleisten zu können. Bei Gesundheitsdaten zum Beispiel dürfen grundsätzlich nur Daten erhoben werden, die für die Behandlung vonnöten sind. Die Erhebung darüber hinausgehender Informationen und die Weitergabe der Informationen an Dritte, das schließt auch die Angehörigen des Betroffenen mit ein, ist weitgehend nur mit ausdrücklicher Einwilligung des Betroffenen/Patienten zulässig. Die von Patienten erhaltenen Informationen unterliegen nicht nur dem Datenschutz, sondern auch der Verschwiegenheitspflicht der Behandelnden und Pfleger. Eine Zuwiderhandlung kann somit auch strafrechtlich verfolgt werden.

Wer ist der Ansprechpartner in Fragen des Datenschutzes?

In kleinen Unternehmen ist der Geschäftsführer Ansprechpartner für den Datenschutz. Falls in einem Unternehmen 10 oder mehr Mitarbeiter mit personenbezogenen Daten arbeiten, ist ein Datenschutzbeauftragter in der Pflicht. Der Datenschutzbeauftragte kann ein Mitarbeiter des Unternehmens sein, der die entsprechenden Qualifikationen erwirbt, oder extern bestellt werden. Er ist sozusagen Ihr betrieblicher Experte im Bereich Datenschutz, der Kontrolleur, nicht aber der Verantwortliche. Das bleibt der Geschäftsführer. Der Datenschutzbeauftragte ist auch nicht der Datenverarbeiter. Das kann Ihr IT-Dienstleister sein. Vielmehr ist der Datenschutzbeauftragte unter anderem für die Schulung der anderen Mitarbeiter zuständig. Zudem überprüft er, ob die datenschutzrechtlichen Bestimmungen im Unternehmen eingehalten werden. Auch Fragen rund um das Löschen, Ändern oder Richtigstellen der Daten fallen in seinen Aufgabenbereich. Er muss Auskunft darüber geben können, welche Daten gespeichert wurden und vieles mehr.

Wie groß ist Ihre Belegschaft? Welche Abteilungen oder unterschiedlichen Aufgabenbereiche gibt es?

Das hilft Ihnen dabei zu hinterfragen, ob Ihre Mitarbeiter bestimmte Daten für die tägliche Arbeit überhaupt benötigen. Haben Sie erkannt, dass Ihre Mitarbeiter auf Daten zurückgreifen können, die sie eigentlich gar nicht brauchen, können Sie diesen Datenzugriff sperren lassen.

Wie groß ist Ihr Kundenkreis?

Sollten zum Beispiel Ihre Kundendaten manipuliert worden sein, müssen Sie Auskunft darüber geben können, wie viele potenzielle Personen durch den Vorfall betroffen sind.

Wer sind Ihre Zulieferer beziehungsweise externen Dienstleister oder Berater?

Mit diesem Wissen können Sie feststellen, ob externe Dienstleister wie zum Beispiel Ihr Steuerberater, auf personenbezogene Kundendaten zugreifen können. Sollte dies der Fall sein, ist die Geschäftsführung verpflichtet, sogenannte Auftragsverarbeitungsverträge abzuschließen, um ihre Kundendaten bestmöglich zu schützen. Kostenlose Musterverträge und Vorlagen zur Auftragsverarbeitung bietet zum Beispiel der Datenschutzbeauftragte des Landes Sachsen-Anhalt an.

BESTANDS-
AUFNAHME

PRAXISBEISPIEL

Schauen wir uns an, wie die Bestandsaufnahme der Unternehmensdaten für die Firma Meier Elektrik aussieht.

Firmenname
Meier Elektrik GmbH

Domäne
Elektroinstallation, Wartung, Verkauf von Leuchtmitteln und Elektrogeräten, Prüfen und Abnahme von Schutzmaßnahmen, Beratung

Namen der Geschäftsführung
Heinz Meier

Kontaktperson/en der Firma
Heinz Meier

Anzahl der Mitarbeiter
8

Mitgliedschaften in Organisationen
Keine

Abteilungen/Aufgabenbereiche mit jeweiligen Verantwortlichen
Heinz Meier (Geschäftsführung),
Siglinde Schulze (Sekretariat, Auftragsverwaltung und Buchhaltung),
Friedhelm Meier (Installation und Wartung),
Heinz Meier (Kundenberatung)

Anzahl der Kunden
circa 1.200

Anzahl und Art der Zulieferer
12 unterschiedliche Zulieferer von Material bis Elektroinstallation

Anzahl und Art externer Dienstleister
ein Steuerberater, ein IT-Dienstleister

Mit diesen Informationen kann Heinz Meier das weitere Vorgehen planen, um zu einem Datenschutzkonzept zu gelangen. Beispielsweise weiß Heinz Meier nun, dass er Siglinde Schulze fragen muss, welche personenbezogenen Daten sie zur Auftragsverwaltung benötigt. Weiter kann Firmenchef Meier auch feststellen, dass bestimmte personenbezogene Daten gar nicht benötigt werden.

Des Weiteren kann die Geschäftsführung jetzt einschätzen, wie viele Kunden, Mitarbeiter, Zulieferer und Dienstleister von einem potentiellen Hackerangriff auf die Firma Meier Elektrik GmbH betroffen wären. Je nach Schwere des Angriffs können die Schutzmaßnahmen für bestimmte Kunden heraufgestuft werden.

Zusätzlich bringt diese Bestandsaufnahme ans Licht, dass externe Dienstleister, wie der Steuerberater, auf personenbezogene Kundendaten, wie die Bankdaten, zurückgreifen können. Die Geschäftsführung kann nun entsprechende vertragliche Vereinbarungen mit dem Steuerberater umsetzen, die den Schutz der Daten für die Kunden gewährleisten. Außerdem kann die Geschäftsführung den Kunden informieren, in welchem Rahmen der Steuerberater Zugriff auf ihre persönlichen Daten hat.

“Ein DSGVO-konformes Datenschutzkonzept vorzubereiten, ist kein Hexenwerk. Wir vom Kompetenzzentrum unterstützen Sie bei Fragestellungen hierzu gern.”

Sebastian Nielebock, Mitarbeiter Themenschwerpunkt Safety & Security
im Mittelstand 4.0-Kompetenzzentrum Magdeburg

CHECKLISTE

- [x] Klärung, in welcher Branche sich das Unternehmen bewegt
- [x] Festlegung des Datenschutz-Ansprechpartners im Unternehmen
- [x] Identifizierung der unterschiedlichen Abteilungen mit ihren jeweiligen Aufgabenbereichen und Ansprechpartnern
- [x] Überprüfung der Belegschaftsgröße
- [x] Feststellung der Kundenkreisgröße
- [x] Identifizierung der Zulieferer beziehungsweise externen Dienstleister oder Berater des Unternehmens

Bild: NicoElNino / istockphoto.com

BESTANDS-
AUFNAHME

WAS SOLL ERREICHT WERDEN?

Neben dem Wissen, wer Daten von wem hat, benötigt ein gutes Datenschutzkonzept auch Informationen darüber, wo die Daten gespeichert sind. Gemeint sind alle Netzwerke (Kommunikationsdienste), die Hardware und die gesamte Software, die Sie in Ihrem Unternehmen verwenden. Deswegen ist es in diesem Schritt notwendig, alle an der IT-Infrastruktur teilnehmenden und datenverarbeitenden Systeme zu erfassen.

In der heutigen, stark vernetzten Zeit läuft ohne funktionierende IT-Systeme in Unternehmen gar nichts mehr. War früher ein Desktoprechner die einzige datenverarbeitende Maschine, finden sich IT-Systeme heute in unterschiedlicher Form wieder. So zum Beispiel in Firmen-Smartphones, Firmen-Fahrzeugen oder auf dem Webserver, von dem Ihre Firmenwebseite betrieben wird.

In diesem Arbeitsschritt ist es wichtig zu erfahren, welche dieser Systeme personenbezogene Daten speichern und/ oder verarbeiten. Wenn Sie nämlich herausfiltern, dass auf bestimmten Systemen sehr sensible Daten benutzt werden, können Sie die Sicherheitsmaßnahmen für diese Systeme höher ansetzen als bei Systemen, deren Daten kein so hohes Schutzbedürfnis benötigen.

Ebenso sollten Sie aufnehmen, ob die Daten intern oder extern gespeichert werden. Intern meint dabei zum Beispiel nur auf dem firmeneigenen Laptop. Externe Speicherung finden Sie zum Beispiel in Cloud-Systemen. Sicherlich verfügt Ihr Unternehmen bereits über IT-Infrastruktur-Schutzvorkehrungen, wie eine Firewall oder Zugangspins. Auch diese bestehenden Abwehrmechanismen sollten Sie auflisten. Dies wird Ihnen dabei helfen, effektiv nachzurüsten, sollten die bestehenden Maßnahmen noch nicht ausreichen.

IT-Infrastruktursicherheit ist ein kompliziertes Terrain. Insbesondere bei den Details sollten Sie sich von einem Experten beraten lassen. Das kann zum Beispiel ein externer IT-Dienstleister sein. Sie haben zudem natürlich die Möglichkeit bei Software-Herstellern nachzufragen, ob und in welcher Form personenbezogene Daten extern gespeichert werden.

IT-SYSTEME IN UNTERNEHMEN

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

Welche Hardware erfasst in meinem Unternehmen personenbezogene Daten?

Die IT-Infrastruktur eines Unternehmens umfasst zum einen die Hardware. Gemeint sind physische Geräte wie zum Beispiel Laptops oder Smartphones. Auch Navigationsgeräte in Firmenwagen gehören dazu, da darin zum Beispiel Kundenadressen gespeichert werden.

Welche Software erfasst personenbezogene Daten?

Zu IT-Infrastruktur gehört natürlich auch die Software, also zum Beispiel welche Programme oder Web-Services zur Finanzbuchhaltung oder Materialbestellung verwendet werden. Die Unternehmens-Software umfasst somit alle Programme, Web-Services und die zugehörigen Daten, mit denen Ihr Unternehmen hantiert. Sogar die bestehende Netzwerkstruktur im Unternehmen rechnet man dazu, wenn Sie beispielsweise an ein firmeneigenes Netzwerk denken.

Speichert die Hardware/Software Daten intern, extern oder beides?

In Ihrer Auflistung darf nicht fehlen, wo und wie Sie Ihre Daten ablegen. Das heißt, ob Sie intern oder extern speichern oder sogar beide Arten verwenden. Die richtige Datensicherung ist ein wichtiger Punkt bei der Erstellung eines Datenschutzkonzeptes.

Wer verwendet und hat damit Zugriff auf die Hardware und Software?

In einem nächsten Punkt gilt es zu erfassen, wer in Ihrem Unternehmen auf die einzelnen Komponenten Ihrer IT-Infrastruktur zugreifen kann. Das macht es Ihnen möglich, weitere Sicherheitslücken und Schwachstellen zu erkennen und zu beheben.

Welche Schutzmaßnahmen bestehen aktuell?

Finden Sie heraus, wie Sie Ihre Netzwerke, Maschinen und Programme, mit denen Ihr Unternehmen arbeitet, derzeit schützen und ob dieser Schutz ausreichend ist. Dazu müssen Sie erst einmal alle IT-Infrastruktur-Schutzvorkehrungen erfassen und auflisten. Das ermöglicht Ihnen ein zielgerichtetes und kostensparendes Nachrüsten, wenn es überhaupt notwendig ist.

Bild: vege / fotolia.de

BESTANDS-
AUFNAHME

PRAXISBEISPIEL

Die Firma Meier Elektrik GmbH wird nun exemplarisch ihre bestehende IT-Infrastruktur aufnehmen. Heinz Meier macht das gemeinsam mit seinem IT-Dienstleister.

Dazu betrachten wir zunächst das Büro. Dort finden wir einen stationären Rechner, eine Internetverbindung inklusive WLAN Router, zwei Laptops und drei Smartphones für den mobilen Einsatz beim Kunden vor Ort. All diese Geräte gelangen über den Router ins Internet und kommunizieren so mit dem Rest der Welt. Für Geschäftsführer Heinz Meier sind das vor allem seine Kunden, seine Angestellten, sein Steuerberater, die Aufsichtsbehörde oder der IT-Dienstleister. Unterwegs nutzen die Smartphones das mobile Internet. Des Weiteren verfügen die zwei Firmenfahrzeuge jeweils über einen Board-Computer mit Navigationsgerät. In diesem werden Kundenadressen für den jeweiligen Tag hinterlegt.

Zusammengefasst ergibt dies die folgende Übersicht der vorhandenen Hardware:

Was	Daten intern/extern gespeichert?	Bestehende Schutzmaßnahmen
WLAN Router	intern	Interne Firewall, WPA2-Verschlüsselung des Internetzugangs
2 Laptops	intern / teilweise extern	Passwort, Lagerung im abgeschlossenen Büro
3 Smartphones	intern / teilweise extern	PIN, Lagerung im Safe
2 Firmenfahrzeuge mit Board-Computer	intern	Fahrzeug abgeschlossen und in Garage eingeschlossen

Diese Endgeräte haben vieles gemeinsam: Sie werden genutzt, um Aufträge einzusehen, zu bearbeiten und intern zu speichern. Fakt ist, die Nutzer dieser Geräte kommen in direkten Kontakt mit den personenbezogenen Daten. Zudem sind die Auftragsdaten auch für Aktivitäten außerhalb des Büros wichtig, wenn Kunden angefahren, Aufträge extern buchhalterisch abgerechnet werden oder per E-Mail mit einem Kunden kommuniziert wird.

Neben der Hardware verwendet die Firma Meier Elektrik GmbH zahlreiche Computer-Programme, die den Geschäftsbetrieb unterstützen. Dabei handelt es sich zum Beispiel um Software, die auf den Firmen-Laptops und -Handys gespeichert ist. Auch bei der Kundenkommunikation per E-Mail, oder in der Lohn- und Finanzbuchhaltung werden Computer-Programme verwendet. Darüber hinaus wird die Steuererklärung online erledigt.

Für die Unternehmens-Webseite hat der externe IT-Dienstleister ein sogenanntes Content Management System (CMS) eingerichtet, mit dem Inhalte auf der Firmen-Webseite bearbeitet und angezeigt werden können. In den Firmenfahrzeugen wird lediglich das Navigationssystem benutzt, ohne dabei das Internet zu gebrauchen.

Heinz Meier und sein IT-Dienstleister fassen nun alle Software-Komponenten, die für das Datenschutzkonzept relevant sind, in einer Tabelle (siehe Seite 17) zusammen.

Mit der Übersicht über die verwendete IT-Infrastruktur kann die Firma Meier Elektrik GmbH nun gezielt feststellen, welche Daten in der verwendeten Hard- und Software überhaupt verarbeitet und gespeichert werden. Im nun folgenden Schritt werden diese Daten genauer zugeordnet und gewichtet. Durch das Gespräch mit seinem IT-Dienstleister konnte Heinz Meier auch herausfiltern, welche Schutzmaßnahmen bereits bestehen.

Was	Daten intern/extern gespeichert?	Bestehende Schutzmaßnahmen
Windows 10	intern / teilweise extern	Windows-Benutzerverwaltung mit Passwortschutz
Android 8.0	intern / teilweise extern	Android-Benutzerverwaltung mit PIN
E-Mail-Dienst	extern	TSL-Verschlüsselung, Passwortschutz
Outlook	intern	Passwortschutz
DATEV	extern	SSL-verschlüsselter Zugang und SmartCard über Webseite
ERP-System	extern	SSL-verschlüsselter Zugang und SmartCard über Webseite
Elster	extern	SSL-verschlüsselter und zertifikatsbasierter Zugang über Webseite
Wordpress – CMS	extern	SSL-verschlüsselter Zugang, Sicherungs-maßnahmen durch IT-Dienstleister
Navigationssystem in Firmenfahrzeug	intern	PIN

“Datenschutz und -sicherheit dürfen nicht vernachlässigt werden. Ein gutes Datenschutzkonzept hilft aber häufig auch dabei, die eigenen Prozesse und die IT-Landschaft zu verbessern”

Prof. Dr. Thomas Leich, Leiter des Mittelstand 4.0-Kompetenzzentrum Magdeburg

CHECKLISTE

- ☑ Auflistung der im Unternehmen verwendeten Hard- und Software
- ☑ Erfassung der Hard- und Software-Komponenten, die mit personenbezogenen Daten hantieren
- ☑ Lokalisierung der internen und externen Speichersicherung
- ☑ Feststellung der Verwender der Hard- und Software
- ☑ Identifizierung bereits bestehender Schutzmaßnahmen

WAS SOLL ERREICHT WERDEN?

In diesem Abschnitt wird es darum gehen, in welchen Geschäftsprozessen nun konkret die unterschiedliche Hard- und Software verwendet wird und welche personenbezogenen Daten verarbeitet werden. So können Sie herausfinden, ob Ihre bestehenden Schutzmaßnahmen bereits ausreichen oder ob Sie weitere Maßnahmen ergreifen müssen.

Geschäftsprozesse verfolgen das Ziel, ein bestimmtes Ergebnis, zum Beispiel die Abwicklung eines Auftrages, zu erreichen. Heutzutage verfügt ein Großteil der KMUs über eine eigene Webadresse, die das Unternehmen vorstellt und seine Leistungen bewirbt. So ist zu erwarten, dass die potenziellen Kunden auf diesen Webauftritt stoßen und Kontakt zum Unternehmen aufnehmen. Schon dabei fallen personenbezogene Daten an. Erheben Sie allerdings darüberhinaus weitere Daten, die eigentlich unerheblich sind, um den Auftrag zu bearbeiten, müssen Sie die betroffene Person vorher einwilligen lassen, dass Sie ihre Daten auch für weitere Zwecke verwenden dürfen. Um folglich eine möglichst vollständige Einwilligung vorzubereiten, ist es notwendig, alle internen und externen Datenverarbeitungsprozesse Ihres Unternehmens, während Sie einen Auftrag bearbeiten, genauer zu betrachten. Geben Sie erfasste Daten sogar weiter, müssen Sie dies in Verträgen zur Auftragsverarbeitung mit Ihren Partnern fixieren.

Ein weiterer, wichtiger Aspekt ist die Speicherung der sensiblen Daten. Wie das vergangene Kapitel gezeigt hat, können die Speicherorte für diese Daten zum Beispiel Firmenrechner mit Netzwerkverzeichnissen, Firmen-Smartphones, Webseitenserver, Finanzbuchhaltung, Logistiksoftware und E-Mail-Programme sein. Für Sie und Ihr Unternehmen ist es zum einen wichtig zu wissen, wo Sie Daten speichern. Denken Sie auch an eine wirksame Löschstrategie. Seit Einführung der neuen Datenschutzgrundverordnung genießen Verbraucher neue Auskunftsrechte. Jeder Nutzer soll erfahren können, welche personenbezogenen Daten gespeichert werden und zu welchem Zweck. Die neue Rechtsprechung wirkt sich auch auf die Art der Speicherung aus, sprich in welchem Datenformat die Daten gespeichert werden. Es wird erwartet, dass Sie Ihre Daten in üblichen Formaten speichern. Beispielsweise sind Kundendatensätze, wenn Sie in Ihre firmeneigene Datenbank eingetragen werden, typischerweise in der sogenannten SQL-Sprache beschreibbar. Sollten Sie also feststellen, dass Sie Daten in einem unüblichen Format speichern, sollten Sie dies korrigieren.

Einen hohen Stellenwert hat die Fragestellung, wer überhaupt berechtigt ist, personenbezogene Daten in Ihrer Firma zu verarbeiten. Üblicherweise haben die Geschäftsführer und deren Assistenzen uneingeschränkten Zugriff auf die sensiblen Daten. Mitarbeiter verfügen in der Regel nur über die aktuellen Auftragsdaten, um den Geschäftsprozess abwickeln zu können.

Wenn Sie oder Ihr Unternehmen personenbezogene Daten erheben, die Daten verarbeiten oder auch speichern, müssen Sie die Person bereits zum Zeitpunkt der Erhebung davon in Kenntnis setzen. Zum Beispiel in Form einer Datenschutzerklärung auf Ihrer Firmenwebsite, mit der Sie Ihrer Informationspflicht nachkommen. Der Inhalt ist verbindlich und muss präzise, transparent leicht verständlich und in leicht zugänglicher Form zur Verfügung stehen. Jede Webseite nutzt dynamische IP-Adressen. Diese gehören laut DSGVO zu den personenbezogenen Daten. Es können noch weitere Informationen in die Datenschutzerklärung aufgenommen werden, je nachdem, wie sie beschaffen ist.

Auch und besonders bei Kontaktformularen und Newslettern sollten Sie genau hinschauen, denn dabei werden sensible Daten nicht nur erhoben, sondern auch verarbeitet, weitergegeben und verwendet. Nach Bedarf sollte Ihr Unternehmen jederzeit bereit sein, Ihren Kunden Auskünfte zu geben über die: 1. Verantwortlichen, 2. erhobenen Daten, 3. Legitimation, 4. Zwecke der Verarbeitung, 5. Speicherorte und Speicherdauer, 6. Personenzugriffe und Weitergabe, 7. Rechte Betroffener. Deshalb sollte Ihr Unternehmen ein durchdachtes und an die jeweiligen Geschäftsprozesse angelehntes Datenschutzkonzept besitzen.

Zusammengefasst sollte Ihr Unternehmen bei jedem Geschäftsprozess, in dem personenbezogene Daten anfallen, daher mindestens folgende Punkte betrachten und dokumentieren.

Dokumentation bei Geschäftsprozessen

01. Benötigte personenbezogene Daten
02. Legitimierung der Datenverarbeitung
03. Berechtigte Personen
04. Verwendungszwecke
05. Speicherung der Daten
06. Löschstrategie
07. Datenweitergabe
08. Dokumentation
09. Informationsrecht des Kunden

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

Welche personenbezogenen Daten sind für mein Tagesgeschäft essentiell wichtig?

Um einen Geschäftsprozess abzuwickeln, sind wahrscheinlich einige personenbezogene Daten essentiell notwendig. Das sind der Kundenname, die Kundenadresse, die Telefonnummer sowie E-Mail-Adresse des Kunden und sein Anliegen beziehungsweise der Auftragsinhalt. Stichwort Datensparsamkeit: Speichern und sammeln Sie aber nur die Daten, die Ihr Unternehmen wirklich benötigt, um den Auftrag zu erfüllen. Der Gesetzgeber spricht dabei von Datensparsamkeit als einem wichtigen Grundsatz der Datenverarbeitung. Erheben Sie nämlich mehr Daten, als die, die zur Auftragsabwicklung nötig sind, muss die betroffene Person vorher einwilligen, dass ihre Daten auch für weitere Zwecke verwendet werden dürfen. Sie benötigen demzufolge auch die Einwilligung Ihres Kunden, wenn Sie dessen Daten an ein Logistikunternehmen weitergeben, damit seine Lieferung auch bei ihm ankommt. Auch wenn Sie Kundendaten an Ihr Steuerbüro weitergeben, muss Ihr Kunde dies vorab genehmigen.

Wie lange werden die sensiblen Daten gespeichert?

Habe ich eine Löschstrategie ausgearbeitet? Haben Sie die Mindestaufbewahrungszeiten der personenbezogenen Daten und eine wirksame Löschstrategie im Blick. Beispielsweise sollten Sie Namen und Telefonnummern nach Auftragsende von den mobilen Firmen-Smartphones löschen. Grundsätzlich gilt: Daten sind zu löschen, wenn Sie diese nicht mehr für den Zweck benötigen, zu dem sie ursprünglich gesammelt wurden. Ihr Datenschutzkonzept sollte eine Löschstrategie enthalten.

Habe ich die Verträge zur Auftragsverarbeitung mit den Partnern abgeschlossen?

Geben Sie personenbezogene Daten weiter, müssen Sie dies nicht nur Ihren Kunden kommunizieren. Sie sind darüber hinaus verpflichtet, die Grundlage dieser Weitergabe in den Verträgen zur Auftragsverarbeitung mit Ihren Partnern zu fixieren. So können das Verträge darüber sein, dass Zulieferfirmen oder Subunternehmen für die Auftragszeit bestimmte Auftragsdaten erhalten. Auch Ihre Finanzbuchhaltung im DATEV benötigt wahrscheinlich sämtliche Auftragsdaten. Ihr IT-Dienstleister muss über die Auftragsdaten, die über das Webformular reinkommen, verfügen können. Logistikunternehmen benötigen Namen und Adressen Ihrer Kunden, um Lieferungen zustellen zu können.

Sind meine Kommunikationskanäle sicher?

Indem Sie analysieren, welche Hard- und Software Sie in Ihren unterschiedlichen Geschäftsprozessen verwenden und welche konkreten personenbezogenen Daten Sie benutzen, können Sie eruieren, ob Ihre bestehenden Schutzmaßnahmen bereits ausreichen oder ob Sie weitere Maßnahmen ergreifen müssen.

Wie schnell kann mein Unternehmen dem Kunden eine Auskunft geben?

Nach Bedarf sollte Ihr Unternehmen jederzeit bereit sein, Ihren Kunden bezogen auf deren personenbezogene Daten Auskünfte zu geben über: den Verantwortlichen, die erhobenen Daten, die Legitimation, die Zwecke der Verarbeitung, Speicherorte und Speicherdauer, Personenzugriffe und Weitergaben sowie die Rechte der Betroffenen. Deshalb sollte Ihr Unternehmen ein durchdachtes und an die jeweiligen Geschäftsprozesse angelehntes Datenschutzkonzept besitzen.

Welche technischen und organisatorischen Maßnahmen nutzt mein Unternehmen?

Kein Unternehmen beginnt mit dem Thema Datenschutz auf der grünen Wiese. Nehmen Sie bestehende Schutzmaßnahmen vorab auf, bevor Sie weitere Schritte durchführen. Gegebenenfalls sind die bestehenden Vorkehrungen schon ausreichend. Wenn Sie beispielweise eine aktuelle Virensoftware installiert haben, dokumentieren Sie diese als eine technische Maßnahme. Gehört zu Ihrer Belehrung der Belegschaft zum Beispiel eine Verschwiegenheitserklärung zu personenbezogenen Daten, erfassen Sie diese als eine organisatorische Maßnahme.

Wie oft ändern sich in meinem Unternehmen die Geschäftsprozesse?

Ist eine Anpassung des Datenschutzkonzeptes notwendig? Geschäftsprozesse ändern sich bereits, wenn Sie zum Beispiel auf Ihrer Firmen-Homepage einen neuen Service anbieten oder sich neue Geschäftsfelder auftun. Auch wenn Sie auf neue Soft- und Hardware oder einen neuen Dienstleister zurückgreifen, hat das sehr wahrscheinlich Auswirkungen auf die Datenverarbeitung in Ihrem Unternehmen. Seien Sie sich daher Ihrer Verantwortung bewusst und überprüfen Sie die notwendigen Neuerungen auch immer wieder hinsichtlich datenschutzrechtlicher Aspekte.

BESTANDS-
AUFNAHME

PRAXISBEISPIEL

Gönnen wir uns einen Blick auf unsere Beispielfirma Meier Elektrik GmbH. Welche digitalisierten Prozesse fallen bei einer Auftragsbearbeitung an?

Die personenbezogenen Daten zu einem Auftrag werden in einem zentralen Verwaltungsrechner (Server) gespeichert. Geschäftsführer Heinz Meier, seine Sekretärin Siglinde Schulze sowie ein durchführender Mitarbeiter (Geselle) und sein Steuerberater kommen in Berührung mit diesen Daten. Der Zugriff ist durch Authentifizierung geschützt, wobei neben Meister Meier selbst auch seine Sekretärin Schreibrechte, das heißt Änderungsrechte, besitzt. Die Auftragsdetails werden unter anderem per E-Mail ausgehandelt. Eine Schwachstelle könnte die Sicherheit der E-Mail-Kommunikation sein. Kunden-Adressdaten werden verwendet, wenn zum Beispiel beim Kunden vor Ort etwas repariert und er daher angefahren werden muss, wenn eine Rechnung erstellt, kommuniziert oder ein steuerlicher Nachweis erbracht wird.

Die Daten werden neben dem Server auch auf den mobilen Geräten wie Firmen-Smartphones, Tablets, PCs oder Laptops genutzt. Nach Auftragsende werden die sensiblen Daten auf den mobilen Geräten gelöscht und nur auf dem zentralen Rechner für eine längere, gesetzlich geregelte Nachweispflicht gespeichert. Ferner werden die Daten an das Finanzamt als auch an den Steuerberater und den IT-Dienstleister weitergegeben. Auf der Webseite sind Webservices aktiv, die personenbezogene Daten sammeln. Der Kunde wird mittels der dortigen Datenschutzerklärung darauf aufmerksam gemacht, dass die Daten an bestimmte Institutionen weitergegeben, oder automatisch, wenn Drittanbieter die Webseite besuchen, gesammelt.

Die Firma Meier Elektrik GmbH nutzt bereits die folgenden technischen Maßnahmen:

1. SSL Verschlüsselung der Webseite durch IT-Dienstleister
2. die Festplatte auf dem zentralen Rechner sowie eine Sicherungskopie sind verschlüsselt
3. es werden alle Aktivitäten bezüglich personenbezogener Daten dokumentiert

Nachfolgende Übersicht stellt dar, wie die Dokumentation des Geschäftsprozesses „Auftrag anlegen“ für die Firma Elektrik Meier GmbH aussehen könnte:

Information zu, Geschäftsprozess	**Geschäftsprozess „Auftrag anlegen“**
Benötigte personenbezogenen Daten	Name, Adresse, Telefonnummer des Kunden
Legitimierung der Datenverarbeitung	Erfüllung des Auftrages (Art. 6 Abs. 1 lit. B DSGVO)
Berechtigte Personen	Heinz Meier, Sekretärin, durchführende Mitarbeiter
Verwendungszwecke	Kommunikation mit dem Kunden, Anfahrt, Rechnung, Buchhaltung
Speicherung der Daten	Zentraler Rechner, Smartphone, Buchhaltungssoftware, Mail-Programm, Daten werden in einer Datenbank mit der Standardsprache SQL gespeichert
Löschstrategie	Nach Ablauf gesetzlicher Fristen für Speicherung der Auftragsdaten (5 Jahre), auf den mobilen Geräten nach dem Auftragsende (spätestens nach 2 Wochen)
Datenweitergabe	IT-Dienstleister, Steuerberater
Dokumentation	Dokumentation ist diese Tabelle
Informationsrecht des Kunden	Datenschutzerklärung auf der Webseite oder in Papierform während einer Vertragsunterzeichnung, Auskunft auf der Basis der geführten Dokumentation

In Kürze möchte Heinz Meier einen neuen Service auf seiner Firmen-Website anbieten. Seit Kurzen installiert Heinz Meier auch intelligente Stromzähler, die sogenannten Smart-Regler. Wie sich Meiers neues Angebot auf den Datenschutz in seinem Unternehmen auswirkt, auch das bespricht Heinz Meier mit seinem IT-Dienstleister.

“Unternehmer können durch die Berücksichtigung der Anforderungen aus der DSGVO dazu beitragen, dass ihre Mitarbeiter und Kunden die Souveränität über ihre persönlichen Daten behalten und in der Folge den digitalen Anwendungen mehr Vertrauen schenken.”

Prof. Dr. Dagmar Gesmann-Nuissl, Mittelstand 4.0-Kompetenzzentrum Chemnitz

CHECKLISTE

- ☑ Lokalisierung der Speicherarten und Speicherorte personenbezogener Daten
- ☑ Gewährleistung eines datensparsamen Umgangs mit Geschäftsprozessdaten
- ☑ Erarbeitung einer Löschstrategie
- ☑ Erstellung von Auftragsverarbeitungsverträgen mit Geschäftspartnern und Dienstleistern
- ☑ Kontrolle der Sicherheit der Kommunikationskanäle
- ☑ Überprüfung der Auskunftsfähigkeit gegenüber Kunden
- ☑ Identifizierung der technischen und organisatorischen Maßnahmen
- ☑ Anpassung des Datenschutzkonzeptes

Bild: Natali_Mis / istockphoto.com

WAS SOLL ERREICHT WERDEN?

Obwohl das Thema Risikomanagement im betrieblichen Alltag längst angekommen ist, stellt die Grundverordnung Unternehmen vor besondere Herausforderungen. Neu ist, dass die DSGVO bei der datenschutzrechtlichen Risikobeurteilung auf die betroffene Person ausgerichtet ist. Die Risikobeurteilung muss sozusagen aus Sicht Ihrer Kunden erfolgen. In diesem Abschnitt möchten wir Sie folglich dafür fit machen, das Risiko für betroffene Personen, von denen Sie und Ihr Unternehmen personenbezogene Daten speichern und verarbeiten, ausreichend einzuschätzen. Wahrscheinlich benötigen Sie dazu die Expertise eines Datenschutzexperten.

Im Fokus stehen Datenschutzrisiken wie Diskriminierung, Identitätsdiebstahl oder Identitätsbetrug, finanzieller Verlust und Rufschädigung. Ein Beispiel: Sie speichern die Kontodaten Ihrer Angestellten, damit Sie ihnen ihren Lohn auszahlen können. Doch was ist, wenn diese Daten entweder missbraucht werden oder verloren gehen? Welcher potenzielle Schaden entsteht Ihnen und Ihrem Unternehmen dadurch? Es gibt diese und andere Arten von Bedrohungen, die eine Risikoquelle darstellen.

Bedrohungen im Überblick

Bedrohung	Beispiel
Unangemessener Gebrauch	E-Mail-Adressen von Kunden werden ohne Einwilligung von anderen Händlern genutzt.
Überwachung	Lohnzahlungen werden von nicht-autorisierten Mitarbeitern ausgespäht.
Überlastung	Webseite ist nicht mehr abrufbar, da Dritte künstlich viele Zugriffe erzeugen.
Beschädigung	Brand zerstört den Firmenlaptop.
Veränderung/Manipulation	Dritte ändern die Kontodaten von Lohnempfängern.
Verlust	Sekretärin löscht ungewollt alle Mitarbeiterdaten.

(Commission Nationale de l'Informatique et des Libertés (CNiL), 2015)

Es ist aber nicht damit getan, abstrakt die Frage zu beantworten, ob aus der Verarbeitung materielle oder immaterielle Schäden für die Rechte und Freiheiten von Betroffenen entstehen können. Vielmehr müssen Sie und Ihr Unternehmen diese Frage aus Betroffenensicht zumindest auf die maßgeblichen Faktoren „Eintrittswahrscheinlichkeit" und „Schwere" (Auswirkung) herunterbrechen.

Ein Risiko ist zunächst einmal die Unsicherheit darüber, ob eine Bedrohung eintritt oder nicht. Dementsprechend gilt es als Erstes zu untersuchen, wie wahrscheinlich es ist, dass ein Ereignis mit potenziell negativen Folgen eintritt. Allerdings ist es schwierig, die Eintrittswahrscheinlichkeit von Betroffenenrisiken zu beurteilen. Auf der einen Seite scheinen Datenschutzvorfälle zwar an der Tagesordnung zu sein. Andererseits lassen sich daraus kaum Rückschlüsse auf die konkrete Eintrittswahrscheinlichkeit solcher Risiken ziehen.

Um die Eintrittswahrscheinlichkeit von Betroffenenrisiken zu beurteilen, ist es daher oftmals unvermeidlich, qualitative Faktoren heranzuziehen. Das bezieht sich nicht nur auf die Bewertung der Eintrittswahrscheinlichkeit (gering, mittel, hoch), sondern auch auf die Bewertungskriterien selbst. Deshalb sollten Sie sich für sich und Ihr Unternehmen fragen:

1. Wie hoch ist das Interesse unbefugter Dritter, die betroffenen Daten zu löschen oder zu manipulieren (Missbrauchsinteresse)?
2. Wie hoch ist der erforderliche Aufwand für unbefugte Dritte, einen Schaden zu verursachen (Aufwand für Schaden)?
3. Wie hoch ist das Risiko für unbefugte Dritte, dass der Missbrauch entdeckt wird (Entdeckungsrisiko)?
4. Wie häufig werden die betroffenen Daten verarbeitet, wobei ein Missbrauch möglich ist (Verarbeitungshäufigkeit)?

Andernfalls lässt sich eine praktisch umsetzbare, aber dennoch ausreichend konkrete Risikobeurteilung kaum gewährleisten. Vor allem, soll diese nicht ausschließlich durch den Datenschutzbeauftragten erfolgen.

Faktor Eintrittswahrscheinlichkeit

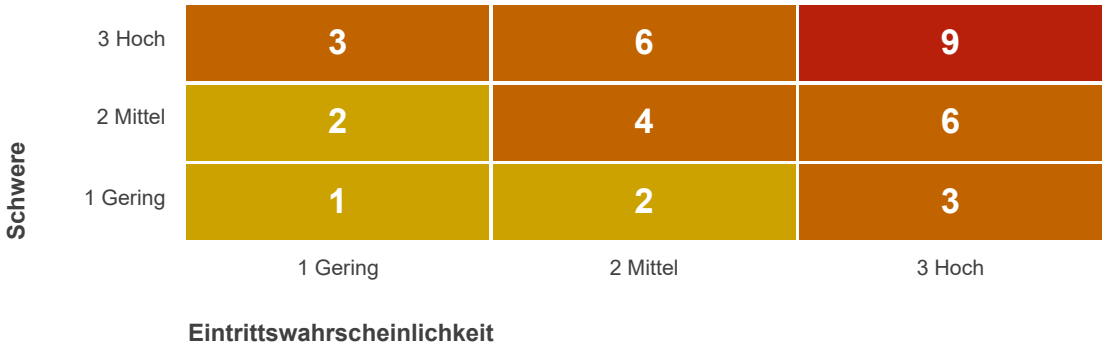
Eintrittswahrscheinlichkeit	Beispiel Dokumenten-Diebstahl...
Hoch 3	... aus einem öffentlichen Raum ohne permanente Überwachung
Mittel 2	... aus einem Raum mit Chipkarten-Zugangskontrolle, zum Beispiel durch Entwenden der Chipkarte
Gering 1	... aus einem kameraüberwachten Raum mit permanenten Wachdienst

Wie sich ein Betroffenenrisiko auswirken kann, wird als **Schwere** bezeichnet. Eintrittswahrscheinlichkeit und Schwere lassen sich nach vorher festgelegten Stufen bewerten, etwa nach „gering“, „mittel“ und „hoch“.

Faktor Schwere

Schwere	Auswirkungen Betroffenenrisiko ...
Hoch 3	Gesundheitliche: Tod einer Person Finanzielle: Verlust der Arbeitsstelle Soziale: Beziehungsprobleme
Mittel 2	Gesundheitliche: Angstzustände Finanzielle: nicht gewollte Banküberweisungen Soziale: Opfer von Online-Belästigung
Gering 1	Gesundheitliche: vorübergehende Kopfschmerzen Finanzielle: Zeitverlust durch Empfang von Spam Mails Soziale: Angst, Kontrolle über eigene Daten zu verlieren

Um nun das Risiko für ein sicherheitsrelevantes Ereignis zu berechnen, müssen Sie entsprechend den betriebsintern festgelegten Bewertungsstufen gewichten. Schwere und Eintrittswahrscheinlichkeit werden dabei aufsteigend mit den Zahlen eins bis drei dargestellt. Die Multiplikation dieser Ziffern ergibt dann das Risiko.



RISIKO-EINSCHÄTZUNG

Bei drei Bewertungsstufen („gering“, „mittel“, „hoch“) und einer Multiplikation der Faktoren, das heißt „Eintrittswahrscheinlichkeit x Schwere (Auswirkung)“ folgt daraus die Gesamtrisikomatrix, aus der Sie das Risiko exemplarisch ablesen können.

Hoch	Hohes Risiko! Hier sollten Sie die ersten technischen und organisatorischen Maßnahmen treffen und auch qualitativ sehr hoch ansetzen, um das Risiko zu minimieren.
Mittel	Mittleres Risiko! Hier sollten in mittelbarer Zeit weitere technische und organisatorische Maßnahmen getroffen werden, um so in den gelben Bereich der Risikobewertung zu gelangen.
Gering	Geringes Risiko! Hier sind nur geringe Maßnahmen notwendig. Nichtsdestotrotz sollten die Bedrohungen regelmäßig neu betrachtet werden, um potenzielle weitere Schäden zu vermeiden.

Risiko in Zahlen darzustellen ist ein sehr schematischer Prozess. Sie sollten dabei auch immer bedenken, dass Zahlen trügen können. So können Schwere und Eintrittswahrscheinlichkeit falsch eingeschätzt oder bestimmte Angriffsszenarien vergessen werden. Ein guter Tipp ist es, im Zweifel die Maßnahmen einfach etwas höher anzusetzen insofern das für Ihr Unternehmen machbar ist.

Bild: Wavebreak Media LTD / fotolia.de

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

Welche Risikoquellen bestehen für personenbezogene Daten, die in meinem Unternehmen anfallen?

Zunächst einmal unterscheiden wir menschliche und nichtmenschliche Risikoquellen. Eine interne menschliche Risikoquelle sind zum Beispiel Ihre Mitarbeiter, die einen Schaden unbeabsichtigt oder vorsätzlich hervorrufen können. Ihre Mitbewerber zählen zum Beispiel zu den externen menschlichen Risikoquellen. Ein Wasserschaden oder Stromausfall gehören zu den nichtmenschlichen Risikoquellen, die sich auch noch einmal in intern und extern unterteilen lassen. Von diesen Risikoquellen gehen wiederum unterschiedliche Arten von Bedrohungen aus.

Welche Bedrohungen finden sich in den Geschäftsprozessen meines Unternehmens?

Die folgenden Beispiele sollen Ihnen vor Augen führen, welches existenzielle Ausmaß unangemessener Gebrauch, Überlastung, Überwachung, Beschädigung, Veränderung, Manipulation oder auch Verlust personenbezogener Daten für Ihr Unternehmen bedeuten können. Ein unangemessener Gebrauch liegt vor, wenn zum Beispiel E-Mail-Adressen von Kunden ohne deren Einwilligung von einem anderen Händler genutzt werden. Ist Ihre Webseite nicht mehr abrufbar, da Dritte künstlich viele Zugriffe erzeugen, spricht man von Überlastung. Werden Lohnzahlungen von nicht-autorisierten Mitarbeitern ausgespäht, fällt das unter die Kategorie Überwachung. Zu einer Beschädigung kommt es beispielweise, wenn ein Brand einen Firmenlaptop zerstört. Ändern Dritte die Kontodaten von Lohnempfängern, ist die Rede von Veränderung oder Manipulation. Löscht Ihre Sekretärin ungewollt alle Mitarbeiterdaten, zählt das zur Kategorie Verlust.

Wenn mein Unternehmen personenbezogene Daten verliert oder diese Daten missbraucht werden, wie schwerwiegend wäre das?

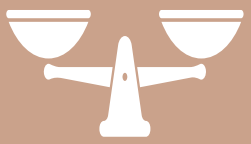
Konkret müssen physische, materielle oder immaterielle Schäden für die betroffene Person ermittelt werden. Dazu gehören gesundheitliche Auswirkungen, die das physische oder psychische Wohlbefinden des Betroffenen negativ beeinflussen. Angefangen bei Irritationen und leichtem Stress bis hin zu Schäden, wie Depressionen, wenn zum Beispiel Daten aus der Intimsphäre des Betroffenen preisgegeben werden. Eine weitere Dimension sind finanzielle Auswirkungen, die zu finanziellen Nachteilen des Betroffenen führen. Auch soziale Auswirkungen können negativen Einfluss auf die gesellschaftliche Stellung des Betroffenen haben. Das ist zum Beispiel bei Rufschädigung oder Diskriminierung der Fall. Zudem zählen Auswirkungen auf das informationelle Selbstbestimmungsrecht dazu. Dazu gilt es, die Schwere (Auswirkung) in entsprechende Risiko-Niveaus („gering“, „mittel“, „hoch“) einzustufen.

Wie wahrscheinlich sind denn Verlust und Missbrauch der, in meinem Unternehmen anfallenden, personenbezogenen Daten?

Um die Eintrittswahrscheinlichkeit einzuschätzen, sind ebenfalls keine festen Stufen vorgegeben. Auch hier ist die Anwendung der drei vorher definierten Stufen möglich. „Gering“ bedeutet, dass es für die ausgewählte Risikoquelle sehr schwierig ist, eine Schwachstelle ausnutzen. „Mittel“ heißt: Für die ausgewählte Risikoquelle ist es mit mittlerem Aufwand möglich, die Schwachstelle auszunutzen. „Hoch“ meint: Für die ausgewählte Risikoquelle ist es sehr einfach, die Schwachstelle auszunutzen.

Welche personenbezogenen Daten haben innerhalb meines Unternehmens ein höheres Risiko und benötigen daher weitere Schutzmaßnahmen?

Um das Risiko zu berechnen, müssen Sie entsprechend den betriebsintern festgelegten Bewertungsstufen gewichten. Die Niveaus von Schwere und Eintrittswahrscheinlichkeit werden dabei aufsteigend mit den Zahlen eins bis drei dargestellt. Die Multiplikation dieser Ziffern ergibt dann das Risiko. Bei einem sehr hohen Risikowert im roten Bereich sollten Sie schnellstmöglich handeln. Auch bei mittlerem Risiko sollten Sie zeitnah technische und organisatorische Maßnahmen treffen, um das Risiko zu minimieren.



RISIKO-
EINSCHÄTZUNG

PRAXISBEISPIEL

Betrachten wir nun die Risikoeinschätzung für das Beispielunternehmen Meier Elektrik GmbH. Hierbei bedienen wir uns des Geschäftsprozesses „Auftrag anlegen“ aus dem vorherigen Schritt.

Zunächst will Elektromeister Meier das Risiko für die einzelnen personenbezogenen Daten einschätzen. Dazu nutzt er eine tabellarische Übersicht, in der Heinz Meier den Werten potenzielle Risikoquellen und Bedrohungen als auch die jeweilige Einschätzung zur Schwere und Eintrittswahrscheinlichkeit zuordnet. Um übersichtlich zu sein, stellt Meiers Tabelle nur einen Ausschnitt dar. Zudem markiert sich der Elektroinstallateur die einzelnen Risikos farblich, um auf einen Blick höhere und niedrigeren Risikos zu unterscheiden. (Ergebnis der Multiplikation von Schwere und Eintrittswahrscheinlichkeit). Des Weiteren schreibt sich Heinz Meier zu den laufenden Nummern die Begründungen für seine eingeschätzte Schwere und Eintrittswahrscheinlichkeit auf.

Nr.	Personen-bezogene Daten	Risikoquelle(n)	
1	**Kundenname**	**Interner Mitarbeiter, Verlust durch interne/ externe Schäden**	Aus dem Verlust oder Missbrauch des Kundennamens (nochmaliges Nachfragen, ob der Name korrekt ist) ist nur eine minimale Belästigung zu erwarten (1). Die Wahrscheinlichkeit, dass Mitarbeiter dies tun bzw. dies durch interne/externe Schäden auftritt, ist ebenfalls durch die bestehenden Maßnahmen gering (1). **RISIKO = gering (1)**
2	**Kundenname**	**Externe Personen**	Aus dem Verlust oder Missbrauch des Kundennamens (nochmaliges Nachfragen, ob der Name korrekt ist) ist nur eine minimale Belästigung zu erwarten (1). Die Wahrscheinlichkeit durch externe Personen ist durch die bestehenden Maßnahmen ebenfalls gering (1). **RISIKO = gering (1)**
3	**Kundenadresse**	**Verlust durch interne/ externe Schäden**	Aus dem Verlust der Kundenadresse (nochmaliges Abfragen der Adresse) ist nur eine minimale Belästigung zu erwarten (1). Die Wahrscheinlichkeit durch externe Personen ist durch die bestehenden Maßnahmen ebenfalls gering (1). **RISIKO = gering (1)**
4	**Kundenadresse**	**Interner Mitarbeiter**	Wenn ein Dritter die Kundenadresse kennt, kann eine unzulässige Belästigung auftreten. Die Schwere bei unzulässiger Verwendung ist daher hoch (3). Die Wahrscheinlichkeit, dass ein interner Mitarbeiter das macht, ist aber gering (1), da er sich im Angestelltenverhältnis befindet und entsprechend von mir unterwiesen wurde. **RISIKO = mittel (3)**
5	**Kundenadresse**	**Externe Person**	Die Schwere durch unzulässige Verwendung ist mittel (2), da durch Kenntnis der Adresse durch einen Dritten eine unzulässige Belästigung auftreten kann. Die Wahrscheinlichkeit, dass dies eine externe Person begeht, ist auch mittel (2), da Adressen durch eine eventuelle unverschlüsselte E-Mail-Kommunikation leicht erhalten werden können. **RISIKO = mittel (4)**
6	**E-Mail-Adresse Kundenadresse IP-Adresse**	**Externe Person**	Mit dem IT-Dienstleister gibt es keinen Vertrag zur Datenverarbeitung. Sollte der Server des IT-Dienstleisters gehackt werden, wiegt das schwer (3). Die Wahrscheinlichkeit ist aber gering (1). **RISIKO = mittel (3)**

Für seine Risikoeinschätzung nutzt Inhaber Heinz Meier nicht nur die Informationen aus den vorherigen Schritten. Um die potenziellen Folgen abzuschätzen, holte er sich den Rat bei seinen Mitarbeitern, externen IT-Beratern, aber auch bei seinen Berufspartnern, die bereits eine Risikoanalyse durchgeführt haben. Mit ihrer strukturierten Risiko-Aufarbeitung kann die Firma Meier Elektrik nun konkret entscheiden, an welchen Stellen noch weitere Maßnahmen zur Risikominimierung umgesetzt werden müssen.

“Sicherheit und Datenschutz sind Voraussetzungen für den Erfolg von Unternehmen auf ihrem Weg in die digitale Transformation. Deshalb unterstützt das Bundesministerium für Wirtschaft und Energie mit den Initiativen „Mittelstand Digital“ und „IT-Sicherheit in der Wirtschaft“ deutschlandweit kostenlos kleinere und mittlere Unternehmen bei der Datenschutz-konformen Digitalisierung ihrer Geschäftsmodelle.”

Frank Fischer, Bundesministerium für Wirtschaft und Energie, Referatsleiter Mittelstand-Digital

CHECKLISTE

- ☑ Erfassung der Risikoquellen für personenbezogene Daten in Geschäftsprozessen
- ☑ Eruierung der Folgen für betroffene Personen (Schwere) bei Verlust und Missbrauch ihrer personenbezogenen Daten
- ☑ Begründung für die Einschätzung der Schwere
- ☑ Berechnung der Eintrittswahrscheinlichkeit bezüglich des Verlustes und Missbrauches personenbezogener Daten
- ☑ Begründung für die Einschätzung der Eintrittswahrscheinlichkeit
- ☑ Herausarbeitung der personenbezogenen Daten mit erhöhtem Risiko

Bild: Sergey Nivens / fotolia.de

HANDLUNGS-
EMPFEHLUNG

WAS SOLL ERREICHT WERDEN?

Jetzt kennen Sie die potenziellen Risiken rund um personenbezogene Daten, die den betroffenen Personen und damit schließlich auch Ihrem Unternehmen drohen. Daher ist es nun an der Zeit, sich damit zu beschäftigen, wie Sie diese Risiken minimieren können – natürlich ressourcenschonend und kosteneffizient. Doch welche Sicherheitsvorkehrungen stehen Ihnen überhaupt zur Verfügung? Damit beschäftigen wir uns in diesem Abschnitt des Leitfadens. Ganz grundsätzlich unterscheiden wir in technische und organisatorische Maßnahmen, kurz TOM.

Technische Maßnahmen realisieren einen zusätzlichen Schutz, indem entsprechende Hard- oder Software eingesetzt wird. Das ist zum Beispiel bei einem Kartenleser der Fall, wenn mit der entsprechenden Software der Zutritt zu einem Raum überwacht werden kann. Organisatorische Maßnahmen involvieren typischerweise den Menschen. So können Sie Ihre Mitarbeiter schulen, damit sie sich datenschutzkonform verhalten.

Übersicht über mögliche TOM-Maßnahmen

Art	Beschreibung	Beispiel
Zutrittskontrolle	Maßnahmen zur Beschränkung des räumlichen Zugangs	Türschlösser
Zugangskontrolle	Maßnahmen zur Beschränkung des Zugangs zu datenverarbeitenden Systemen	Zugriff auf den Laptop nur mit Fingerabdrucksensor oder mit persönlichen Kennwort
Zugangskontrolle	Maßnahmen zur Beschränkung des Zugangs zu datenverarbeitenden Systemen	Zugriffseinschränkung auf die Übersicht der Lohnabrechnung durch die Nutzerrollen
Weitergabekontrolle	Maßnahmen zur Gewährleistung, dass Daten beim elektronischen Transport nicht von Dritten gelesen, gelöscht, verändert oder genutzt werden.	Verwendung von verschlüsselter E-Mail-Kommunikation
Eingabekontrolle	Maßnahmen zur Überprüfung, welche Personen personenbezogene Daten bearbeitet haben	Software, die automatisch speichert, welcher Nutzer eine Datei wann verändert hat
Auftragskontrolle	Maßnahmen zur Überprüfung der Weisungen des Auftragsgebers bei Auftragnehmern	Vorortttermin mit Kontrolle der Maßnahmen
Verfügbarkeitskontrolle	Maßnahmen zum Schutz von Daten gegen zufällige Zerstörung oder Verlust	Verwendung von Backupsystemen in andere Gebäuden
Trennungsgebot	Maßnahmen zur Gewährleistung, dass unterschiedliche Daten je nach Zweck an unterschiedlichen Orten gespeichert werden	Verwendung eines ausgewählten Laptops für die Buchhaltung, während normale Mitarbeiter einen anderen Rechner verwenden.

Quelle: Anhang zum §9 Satz 1 der alten Fassung des Bundesdatenschutzgesetzes (BDSG) vom Juni 2010

In allen in der Tabelle genannten Bereichen können sowohl technische als auch organisatorische Maßnahmen wirken.

Übersicht über ausgewählte technische Maßnahmen:

- Software zum Generieren von sichereren Passwörtern
- Passwortschutz/Nutzerauthentifizierung bei Rechnern und mobilen Endgeräten
- Verschlüsselung von Festplatten
- Verschlüsselung des E-Mail-Verkehrs
- Verschlüsselter Zugang zur Firmenwebseite
- Befristung von Accounts
- Rechteeinschränkung von Accounts
- Blockieren von bestimmten Funktionalitäten in der Software
- Verwendung von Backup-Systemen
- Software zum sicheren Löschen von Daten

Übersicht über ausgewählte organisatorische Maßnahmen:

- Regelmäßige Weiterbildung und Schulung von Mitarbeitern zum Thema Datenschutz und Umgang mit personenbezogenen Daten
- Erstellung und Anwendung von Mitarbeiterhandbüchern
- Erstellung und Anwendung eines Rechte- und Rollenkonzeptes, um den Zugriff auf Daten zu planen
- Erstellung und Anwendung eines Löschkonzeptes, um nicht mehr benötigte personenbezogene Daten rechtzeitig zu löschen
- Erstellung und Erprobung eines Notfallplans bei Datenschutzpannen

Wie Sie leicht erkennen können, stehen Ihrem Unternehmen eine Vielzahl an technischen und organisatorischen Möglichkeiten zur Verfügung. Welche Maßnahmen für Ihre Firma die geeignetsten sind, ist eine höchst individuelle Entscheidung. Risikowahrscheinlichkeit, aber auch die finanziellen und organisatorischen Möglichkeiten Ihres Unternehmens spielen bei der Entscheidungsfindung eine essentielle Rolle. Es ist dabei immer ratsam, geplante Maßnahmen nach der Risikoanalyse mit den jeweiligen Fachleuten, das heißt mit IT-, Rechts- oder Sicherheitsexperten hinsichtlich Wirksamkeit und Machbarkeit genau zu besprechen. Auch der Landesbeauftragte für den Datenschutz kann im Zweifel Auskunft geben. An der Hand eines Experten wird es Ihnen leichter fallen, die richtigen Schritte auszuwählen und schließlich auch zu gehen.

WELCHE FRAGEN MÜSSEN BEANTWORTET WERDEN?

Welche Schutzmaßnahmen für personenbezogene Daten muss mein Unternehmen sicherstellen?

Die Risikoanalyse für die personenbezogenen Daten, wie im vorangegangenen Kapitel 3 dieses Leitfadens beschrieben, wird für jedes Unternehmen unterschiedlich ausfallen. Daher sind auch die Schutzvorkehrungen, die Sie und Ihr Unternehmen treffen müssen, eine für Ihr Unternehmen individuelle Entscheidung.

Welche technischen Maßnahmen können das Risiko senken?

Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die in Soft- und Hardware umgesetzt werden, wie etwa ein Benutzerkonto, Passworterzwingung, Loggins oder biometrische Benutzeridentifikation.

Welche organisatorischen Maßnahmen können das Risiko senken?

Als organisatorische Maßnahmen sind solche Schutzversuche zu verstehen, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind Besucheranmeldung, Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen, Vier-Augen-Prinzip oder Intervalle zur Stichprobenprüfungen.

Wie stark muss ich die personenbezogenen Daten in meinem Unternehmen schützen?

Für TOM gilt ein Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich stark geschützt werden, wenn die Maßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden. Schutzmaßnahmen müssen mit den drei Säulen der IT-Sicherheit, also Verfügbarkeit, Vertraulichkeit und Integrität, übereinstimmen.

HANDLUNGS-
EMPFEHLUNG

PRAXISBEISPIEL

Die Firma Meier Elektrik GmbH konnte erkennen, dass für Kundenadressen und E-Mail-Adressen ein leicht erhöhtes Risiko besteht. Daher möchte Heinz Meier durch technische und organisatorische Maßnahmen das Risiko verringern, indem er konkret die Eintrittswahrscheinlichkeit herabsenkt.
Das wesentliche Problem ist dabei, dass Kunden mit ihrer Kundenadresse oder per E-Mail Kontakt mit der Meier Elektrik GmbH aufnehmen. Die Kontaktaufnahme-Mails können unzureichend geschützt sein, sodass die Daten unverschlüsselt versendet und somit von Dritten mitgelesen werden können. Um dies zu vermeiden bespricht und vergleicht Geschäftsführer Heinz Meier zusammen mit seinem IT-Dienstleister verschiedene Vorkehrungen.

Maßnahme	Vorteile	Nachteile
Verschlüsselung von E-Mails	Sichere Ende-zu-Ende Verschlüsselung (nur Firma und Kunde können E-Mail lesen); Erlaubt auch zusätzlich die Authentifizierung von Firma und Kunde	Notwendige Kosten für ein Zertifikat zur Verschlüsselung; Kunden können Verschlüsselung vielleicht nicht verwenden
Kontaktaufnahme über ein Formular auf der Webseite, dass Inhalte verschlüsselt überträgt	Sichere Ende-zu-Ende Verschlüsselung Kein Mehraufwand für Kunde zur Verschlüsselung; Erlaubt die Authentifizierung der Firma gegenüber des Kunden (schafft Vertrauen)	Notwendige Kosten für ein Zertifikat zur Verschlüsselung; Kommunikation von der Firma zum Kunden ist dann eventuell per Mail und damit eventuell unverschlüsselt
Abschluss eines Auftragsverarbeitungsvertrages mit dem IT-Dienstleister	effektiverer Datenschutz durch geschultes Personal; Sicherstellung der Verfügbarkeit von Informationen und Diensten: 24 Stunden-Betrieb/365 Tage	Haftungs- und Schadensrisiken, wenn sich der Auftragsverarbeiter nicht an die Vorgaben hält

Alle Maßnahmen stammen aus dem Bereich der Weitergabekontrolle und sind sowohl technischer als auch organisatorischer Natur. In diesem Falle hat sich die Firma Meier Elektrik GmbH dazu entschieden, auf ihrer Webseite ein Kontaktformular anzubieten. Dieses gibt den Kunden die Möglichkeit, neben der üblichen Anfrage per Telefon oder einer persönlichen Beratung im Geschäft, Aufträge auch digital auszulösen.

Um zu vermeiden, dass Kunden ungewollt unverschlüsselte Mails mit personenbezogenen Daten senden, wird auf der Webseite darüber informiert, dass bei der Kontaktaufnahme per Mail die Kommunikation eventuell nicht gesichert ist und im Zweifelsfall lieber das Kontaktformular verwendet werden soll. Zudem schult Heinz Meier seine Mitarbeiter. So weist er sein Team an, möglichst wenige personenbezogene Daten zu verwenden, wenn sie Kunden per Mail kontaktieren. Darüber hinaus werden Meiers Kunden in den Antwortmails darüber informiert, dass eine Kommunikation gegebenenfalls unverschlüsselt stattfindet und daher im Zweifelsfall auf das Kontaktformular zurückgegriffen werden soll.

CHECKLISTE

- ☑ Besprechung technischer Maßnahmen zur Risikominimierung mit einem Experten
- ☑ Durchführung dieser technischen Maßnahmen
- ☑ Herausarbeitung organisatorischer Maßnahmen mit einem Datenprofi
- ☑ Risikosenkung durch Umsetzung organisatorischer Maßnahmen
- ☑ Wahrung des Verhältnismäßigkeitsprinzip beim Treffen geeigneter Schutzmaßnahmen

WER HILFT MIR WEITER?

Das Mittelstand 4.0-Kompetenzzentrum Magdeburg gehört zu Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Der DLR Projektträger begleitet im Auftrag des BMWi die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

MITTELSTAND 4.0-KOMPETENZZENTRUM MAGDEBURG

Geschäftsstelle
Zentrum für Produkt-, Verfahrens- und Prozessinnovation – ZPVP GmbH
Sandtorstraße 23, 39106 Magdeburg
www.vernetzt-wachsen.de

Nadine Hiller
+ 49 (0) 391 544 86 220
nadine.hiller@vernetzt-wachsen.de

Online-Angebote der Mittelstand 4.0-Kompetenzzentren der Mittelstand-Digital Initative

- **Sicherheitstool-Mittelstand (SiTOM)** Werkzeug zum Einschätzen des Status der IT-Sicherheit in Ihrem Unternehmen
  https://www.sitom.de
- **Wissensbox-Recht 4.0**
  https://betrieb-machen.de/wissensbox-recht-4-0
- Weitere Veröffentlichungen zum Thema IT-Sicherheit der Mittelstand-Digital-Initiative
  https://www.mittelstand-digital.de/MD/Redaktion/DE/Dossiers/A-Z/it-sicherheit.html

Weiterführende Literatur

- Webseite mit Informationsmaterialien des Datenschutzbeauftragten des Landes Sachsen-Anhalts
  https://datenschutz.sachsen-anhalt.de
- Webseite des Bayrischen Landesamt für Datenschutzaufsicht
  https://www.lda.bayern.de/
- Informationen des Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Thema IT-Grundschutz
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- Leitfäden des Bitkom e.V. u.a. zur Risikoeinschätzung (Susanne Dehmel, 2017) aber auch weitere siehe
  https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/index.jsp

Literaturverzeichnis

- Commission Nationale de l'Informatique et des Libertés (CNiL). (2015). Privacy Impact Assessment (PIA) Tools (templates and knowledge bases).
- Susanne Dehmel. (2017). Risk Assessment & Datenschutz-Folgenabschätzung. Berlin: Bitkom e.V.

MITTELSTAND-DIGITAL

Die Mittelstand 4.0-Kompetenzzentren finden Sie bundesweit.