Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Datenschutz und IT-Sicherheit in der IT-Branche

- Kompaktleitfaden -

www.itwirtschaft.de

Mittelstand-Digital

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

Inhalt

Einführung

Kein Unternehmen kommt in unserer digitalisierten Welt umhin, sich mit den Themengebieten IT- und Informationssicherheit auseinanderzusetzen. Dies betrifft insbesondere die Sicherung der digitalen Daten und der technischen Systeme sowie den Schutz von personenbezogenen und unternehmensbezogenen Daten. Es gilt ALLE in einem Unternehmen anfallenden Daten (Informationen) durch interne Vorsorgemaßnahmen, technische Lösungen und vertragliche Instrumente zu schützen.

Der vorliegende Kompaktleitfaden zum Datenschutz und zur IT-Sicherheit soll Ihnen einen kompakten und übersichtlichen Einstieg in die Thematik ermöglichen und bietet Ihnen weiterführende Verweise zu den für Sie relevanten Themenfeldern. Vertiefende Ausführungen finden Sie unter „Materialien“ in unserem Kompendium „Datenschutz und IT-Sicherheit“ unter der Rubrik „IT-Sicherheit & Datenschutz“.

1 Sicherer Schutz geheimer Daten

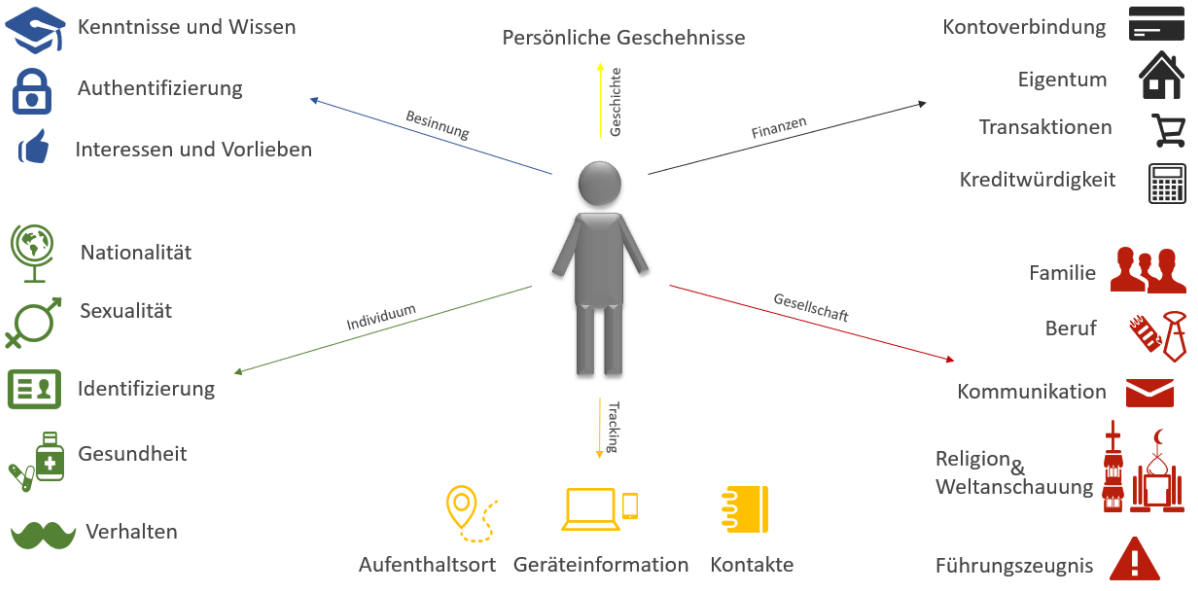
1.1 Personenbezogene Daten oder Geschäftsgeheimnisse?

In jedem Unternehmen fallen viele Daten an, die besonders geschützt werden müssen. Darunter sind sowohl personen- als auch unternehmensbezogene Daten. Personenbezogene Daten von Mitarbeiter:innen, Kund:innen und Lieferant:innen sind dabei primär aufgrund **gesetzlicher** Bestimmungen einem besonderen Schutz unterworfen, während sensible unternehmensbezogene Informationen wie etwa Geschäfts- oder Betriebsgeheimnisse von großer Bedeutung im Wettbewerb sind, sodass deren Schutz unmittelbar **im Interesse des Unternehmens** liegt. Was unterscheidet sie voneinander, was haben sie gemeinsam?

1.1.1 Personenbezogene Daten

Die DSGVO versteht unter personenbezogenen Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Identifiziert ist eine natürliche Person dann, wenn keine zusätzlichen Informationen mehr notwendig sind, um die Person zu erkennen. Identifizierbar wird eine Person, wenn ihre Identität durch die Kombination von Daten feststellbar wird. Das bedeutet, dass zwischen einer Information und einer Person eine unmittelbare oder mittelbare Verbindung herstellbar sein muss. Eine unmittelbare Verbindung ist beispielsweise mit dem Namen, dem Geburtsdatum oder der Anschrift gegeben. Eine mittelbare Verbindung erfolgt etwa mittels Zusatzwissen wie beispielsweise bei der IP-Adressen und Cookie-Kennung oder einer Kennnummer.

Überblick über personenbezogenen Daten:



Kurzum - personenbezogene Daten sind *alle Informationen, die Rückschlüsse auf eine natürliche Person erlauben*. Folglich sind nahezu in allen Bereichen eines Unternehmens (Personalabteilung, Vertrieb, Marketing, Einkauf, Buchhaltung, etc.) die datenschutzrechtlichen Vorschriften (siehe hierzu Kap. 2.1) zu beachten.

Erlischt der Personenbezug unwiederbringlich aufgrund einer **Anonymisierung** von Daten, sind diese Daten dann nicht mehr personenbezogen, sodass die datenschutzrechtlichen Vorschriften keine Anwendung mehr finden. Dabei ist jedoch eine besondere Vorsicht geboten, denn eine Re-Identifizierung muss ausgeschlossen sein.

Werden personenbezogene Daten lediglich **pseudonymisiert**, sodass ein Bezug zu einer (konkreten) natürlichen Person unter Zuhilfenahme zusätzlicher Informationen möglich ist, bleibt das Datenschutzrecht anwendbar.

1.1.2 Geschäftsgeheimnisse

Unter einem Geschäftsgeheimnis versteht das Geschäftsgeheimnisgesetz (§ 2 GeschGehG) eine Information,

- die von wirtschaftlichem Wert ist,
- geheim und nicht offenkundig ist,
- an der ein berechtigtes Geheimhaltungsinteresse des Geheimnisinhabers besteht, und
- für die durch den rechtmäßigen Inhaber angemessene Geheimhaltungsmaßnahmen getroffen werden.

Beispiele für Geschäftsgeheimnisse sind Herstellungsverfahren, Konstruktionspläne, Prototypen, Kundenlisten, Businesspläne, Marktanalysen, Erfindungen und Lizenzen.

Das Geschäftsgeheimnis umfasst sowohl kaufmännisches als auch technisches Wissen. Die geheim zu haltende Information kann sowohl mündlich übermittelt werden oder auch in Papierform oder auf einem Tatenträger verkörpert sein. Dabei ist stets zu beachten:

Erst durch die Vornahme von Schutzmaßnahmen wird eine Information zu einem Geschäftsgeheimnis!

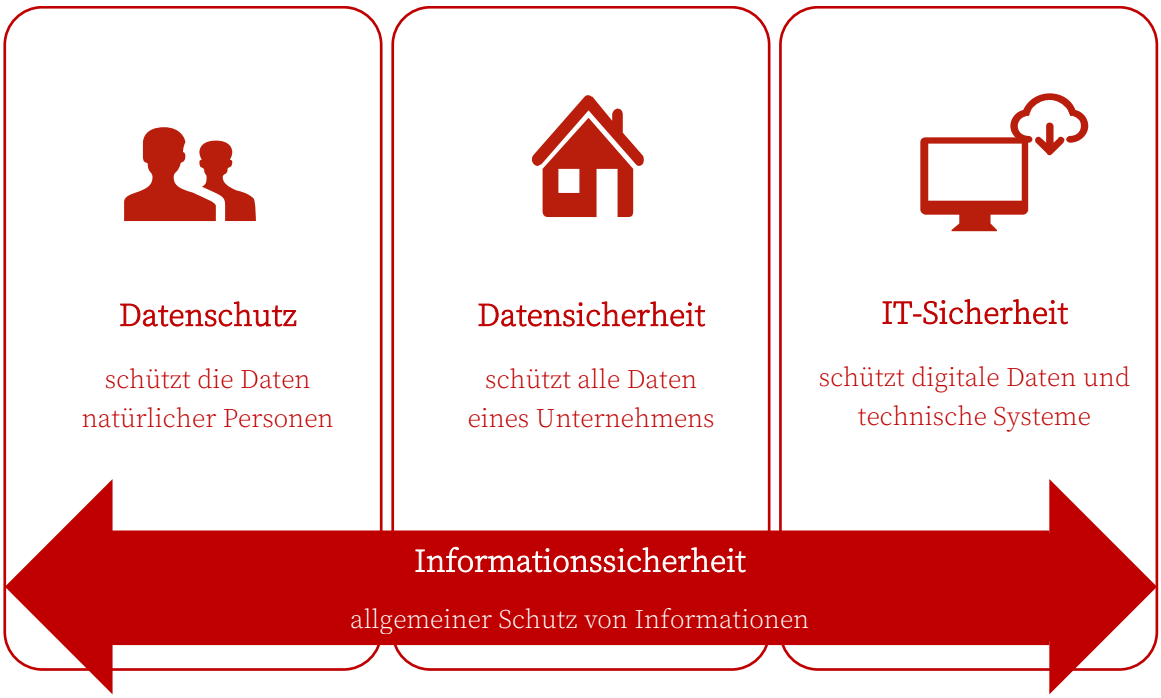
Vor dem Hintergrund der gesetzlichen Regelungen ist es daher wichtig, dass das Unternehmen taugliche und angemessene Geheimhaltungsmaßnahmen ergreift. Ausführungen zu den Schutzmaßnahmen finden Sie im Kap.3.

1.2 Datenschutz und IT-Sicherheit

Datenschutz beschreibt den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten sowie den Schutz des Rechts auf informationelle Selbstbestimmung. Die IT-Sicherheit verfolgt hingegen den Schutz digitaler Daten (Dateien wie Dokumente, Bilder, Filme, etc.) und technischer Systeme.

Die Informationssicherheit hat allgemein das Ziel, Informationen zu Schützen. Dabei ist es unerheblich, ob es sich um analoge oder digitale Daten handelt oder diese einen Personenbezug haben.

Auch wenn der Datenschutz und die IT-Sicherheit jeweils verschiedene Schutzbereiche umfassen, so können diese im Rahmen der Informationssicherheit nicht getrennt voneinander betrachtet werden.



Gerade in Zeiten von Cyberkriminalität ist die Informationssicherheit die Voraussetzung für eine erfolgreiche Digitalisierung.

Werden Daten nicht ausreichend gesichert, drohen dem Unternehmen Schäden durch

- den Verlust von Daten
- die Geltendmachung von Schadensersatzforderungen der betroffenen Person
- die Verhängung von Geldbußen durch Behörden (hinsichtlich personenbezogener Daten bspw. bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes)
- Reputationsverlust

2 Grundsätze des Datenschutzes

2.1 Grundlagen der Datenverarbeitung

Im Datenschutzrecht gilt das Prinzip des Verbots mit Erlaubnisvorbehalt. Das bedeutet:

jegliche Verarbeitung von personenbezogenen Daten ist verboten,

es sei denn, einer der nachstehenden Rechtfertigungsgründe (Art. 6 DSGVO) greift:

- Einwilligung (Zustimmung der/des Betroffenen in die Datenverarbeitung für einen oder mehrere bestimmte Zwecke)
- Vertragserfüllung (die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich)
- Rechtspflicht (die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich)
- Lebensrettung (die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen)
- Öffentliche Aufgabe (die Verarbeitung ist für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, erforderlich)
- Berechtigte Interessen (Grundsätzlich kann jedes von einer Rechtsordnung anerkannte, legitime Interesse eines Verantwortlichen oder Dritten darunter fallen, sofern das rechtliche Interesse der/des Betroffenen nicht überwiegt).

2.2 Verarbeitungsgrundsätze

Bei der Verarbeitung von personenbezogenen Daten sind die nachfolgenden Grundsätze der DSGVO zu beachten:

Rechtmäßigkeit	Datenverarbeitung darf lediglich dann stattfinden, wenn eine gesetzliche Grundlage dafür vorliegt.
Verarbeitung nach Treu und Glauben	Der Umgang mit personenbezogenen Daten soll redlich und ehrlich erfolgen. Die Datenverarbeitung soll dem angegebenen Zweck entsprechen und nicht darüber hinaus gehen.
Transparenz	Personenbezogene Daten sollen in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet werden.
Zweckbindung	Personenbezogene Daten sollen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
Datenminimierung	Personenbezogene Daten sollen dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Richtigkeit	Personenbezogene Daten sollen sachlich richtig sein und nötigenfalls geändert oder gelöscht werden können.
Speicherbegrenzung	Personenbezogene Daten sollen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
Integrität und Vertraulichkeit	Personenbezogene Daten sollen sicher verarbeitet werden, mithin vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt werden
Rechenschaftspflicht	Die Einhaltung der DSGVO muss stets nachgewiesen werden können.

2.3 Rechte der Betroffenen

2.3.1 Überblick

Das Datenschutzrecht zielt auf eine faire, transparente und nachvollziehbare Verarbeitung von personenbezogenen Daten ab. Daraus ergeben sich folgende Rechte für die Betroffenen, die entsprechende Pflichten für die Verantwortlichen begründen:

- Recht auf transparente Information und Kommunikation (Art. 12 DSGVO)

  Die Informationen bezüglich der Datenverarbeitung sollen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ vermittelt werden.

- Recht auf Information (Art. 13 und 14 DSGVO)

  Die Informationen über die Datenverarbeitung sollen grundsätzlich so schnell wie möglich, bestenfalls vor der Datenverarbeitung, kommuniziert werden. Im Falle der Dritterhebung besteht keine Informationspflicht, wenn die Informationserteilung sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Dies muss nachvollziehbar dokumentiert werden.

- Recht auf Auskunft (Art. 15 DSGVO)

  Zu der von der DSGVO geforderten Transparenz gehört auch, dass die/der Betroffene auf Nachfrage erfährt,

  - ✓ welche Daten zu ihrer Person verarbeitet werden,
  - ✓ zu welchem Zwecke diese Daten verarbeitet werden,
  - ✓ woher der Verantwortlicher diese Daten hat,
  - ✓ mit wem, wenn überhaupt, der Verantwortliche diese Daten teilt,
  - ✓ wie lange diese Daten voraussichtlich gespeichert werden (sofern möglich).

- Recht auf Berichtigung (Art. 16 DSGVO)

  Fehlerhafte personenbezogene Daten müssen korrigiert werden können.

- Recht auf Löschung - „Recht auf Vergessenwerden“ (Art. 17 DSGVO)

  Die/der Betroffene kann die Löschung seiner Daten verlangen, sofern diese für die Erfüllung des Zwecks, für welchen sie erhoben worden sind, nicht mehr erforderlich sind oder die Einwilligung widerrufen wurde. Darüber hinaus sind die personenbezogenen Daten zu löschen, wenn die Daten unrechtmäßig verarbeitet wurden oder die/der Betroffene einen Widerspruch gegen die Verarbeitung einlegt (s.u.).

- Recht auf Einschränkung (Art. 18 DSGVO)

  Statt der Löschung der Daten, kann die/der Betroffene die eingeschränkte Verarbeitung seiner Daten verlangen, sofern diese zur Ausübung von Rechtsansprüchen benötigt oder (noch) auf die Richtigkeit überprüft werden.

- Recht auf Widerspruch (Art. 21 DSGVO)

  Die betroffene Person kann der Verarbeitung von ihren personenbezogenen Daten widersprechen, falls die Datenverarbeitung sich auf die Wahrnehmung einer öffentlichen Aufgabe oder auf die der berechtigten Interessen des Verantwortlichen) stützt. Dies gilt insbesondere für Direktwerbung und Marketing-Profiling (Art. 21 Abs. 2 DSGVO).

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

  Die/der Betroffene kann die Zurverfügungstellung und Übertragung seiner/ihrer Daten, im Rahmen der technischen Möglichkeiten und in einem gängigen Format, an sich oder einen Dritten verlangen.

- Recht auf nicht ausschließlich automatisierte Entscheidungen (Art. 22 DSGVO)

  Die/der Betroffene darf bestimmen, inwiefern sie/er eine ausschließlich automatisierte Entscheidung, die rechtliche Auswirkungen entfaltet, zulassen (z.B. Profiling, Bewertung durch Algorithmen) möchte.

- Recht auf Beratung durch die/den Datenschutzbeauftragte:n des Verantwortlichen (Art. 38 DSGVO)

  Betroffene Personen dürfen die/den Datenschutzbeauftragte:n des Verantwortlichen zu allen Fragen, die sie in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und die Wahrnehmung ihrer Rechte haben, zu Rate ziehen.

- Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO)

  Jede betroffene Person hat – unabhängig davon, welche zusätzlichen Rechte ihr ggf. zustehen (wie etwa Schadensersatz) – stets das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie eine Verletzung der Vorschriften der DSGVO bei der Verarbeitung ihrer personenbezogenen Daten vermutet.

2.3.2 Datenschutzerklärung

Zuvor genannte Rechte sind in die Datenschutzerklärung aufzunehmen. Diese muss folgende Angaben enthalten:

- ✓ die verantwortliche Stelle (Name und Kontaktdaten),
- ✓ falls vorhanden, Kontaktdaten der/des Datenschutzbeauftragten,
- ✓ Zwecke und Rechtsgrundlagen der Datenverarbeitung, aufgeteilt nach den Kategorien der personenbezogenen Daten, die verarbeitet werden,
- ✓ Explizite Bezeichnung von „berechtigten Interessen“, falls die Datenverarbeitung sich auf Art. 6 Abs. 1 lit. f DSGVO (Wahrung der berechtigten Interessen) stützt,
- ✓ Empfänger von personenbezogenen Daten, falls diese an Dritte übermittelt werden,
- ✓ Datenübermittlungen in Drittländer (falls diese stattfinden), mit den entsprechenden Angaben zum Schutzniveau im Drittland,
- ✓ und weitere Informationen.

Eine Muster-Datenschutzerklärung vom Kompetenzzentrum IT-Wirtschaft finden Sie hier.

2.4 Pflichten der Verantwortlichen

Die Notwendigkeit, personenbezogene Daten natürlicher Personen zu schützen, begründet für einen Verantwortlichen (also denjenigen, wer diese Daten verarbeitet) in erster Linie eine Dokumentationspflicht sowie die Pflicht, technisch-organisatorische Maßnahmen zum Schutz der Daten zu treffen.

2.4.1 Dokumentationspflicht

Der Grundsatz der Rechenschaftspflicht wird in Art. 5 Abs. 2 DSGVO definiert. Der Verantwortliche hat für die Einhaltung der Verarbeitungsgrundsätze Sorge zu tragen und diese zu dokumentieren.

Zu den datenschutzrechtlichen Dokumentationspflichten gehören die Pflichten:

- Verarbeitungsverzeichnis anzufertigen (Art. 30 DSGVO)

  Jede:r Verantwortliche muss ein Verzeichnis der Verarbeitungstätigkeiten führen, die sie/er vornimmt. Es dient der Transparenz über die Verarbeitung personenbezogener Daten sowie der rechtlichen Absicherung des Unternehmens. Ein Muster finden Sie im Leitfaden „Datenschutz und IT-Sicherheit, Punkt 2.4.1.2“ unter „Materialien“ in der Rubrik „IT-Sicherheit & Datenschutz“.

- Datenschutzverletzungen zu dokumentieren und zu melden (Art. 34 DSGVO)

  Gem. Art. 33, 34 DSGVO muss die/der Verantwortliche eine Datenschutzverletzung sowohl binnen 72 Stunden der zuständigen Behörde melden als auch den Betroffenen mitteilen. Der Verantwortliche dokumentiert Datenschutzverletzung einschließlich aller im Zusammenhang damit stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.

- Datenschutz-Folgeabschätzung durchzuführen (Art. 35 DSGVO)

  Eine Datenschutz-Folgenabschätzung (DSFA) ist ein datenschutzrechtliches Risikomanagement-Instrument. Bei der DSFA sollte das Unternehmen (die/der Verantwortliche) die Eintrittswahrscheinlichkeit und die Schwere eines konkreten Datenschutzrisikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewerten. Ein Muster der DSFA finden Sie im Leitfaden „Datenschutz und IT-Sicherheit, Punkt 2.4.3“ unter „Materialien“ in der Rubrik „IT-Sicherheit & Datenschutz“.

- Interessenabwägung zu dokumentieren (Art. 6 Abs. 1 lit. f DSGVO)

  Werden personenbezogene Daten „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten“ verarbeitet, ist eine dokumentierte Abwägung dieser berechtigten Interessen gegen Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person erforderlich. Denn personenbezogene Daten sollten nur dann verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

- Datenschutzrichtlinie aufzusetzen

  Die interne Datenschutzrichtlinie bzw. das interne Datenschutzkonzept sollte einerseits die Mitarbeitenden darüber informieren, wie der Datenschutz im Unternehmen gelebt und umgesetzt wird, und andererseits den Grundstein für weitere Konzepte/Dokumente bilden.

- Auftragsverarbeitungsverträge zu dokumentieren

  Viele Datenverarbeitungsvorgänge erfolgen nicht durch die/den Verantwortlichen selbst, sondern durch eine:n von dieser/diesem beauftragten Auftragsverarbeiter:in. Diese:r soll hinreichende Garantien für die DSGVO-konforme technische und organisatorische Maßnahmen bieten (über ausreichende Ressourcen und Fachwissen verfügen und zuverlässig sein). Denn bei der Prüfung der DSGVO-Compliance des Verantwortlichen wird u.a. auch berücksichtigt, ob seine Auftragsverarbeiter den Anforderungen der DSGVO genügen.

- Löschkonzept anzufertigen

  Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss ein Löschkonzept anfertigen, in dem Löschfristen für alle Arten von personenbezogenen Daten sowie das Verfahren für die Datenlöschung bestimmt werden.

Eine Checkliste hinsichtlich der Pflichten eines Verantwortlichen finden Sie im Leitfaden „Datenschutz und IT-Sicherheit, Punkt 2.4.8“ unter „Materialien“ in der Rubrik „IT-Sicherheit & Datenschutz“.

2.4.2 Technisch-organisatorische Maßnahmen (TOMs)

Um dem Datenschutz im Unternehmen zu entsprechen und die DSGVO-Compliance nachzuweisen, sind technisch-organisatorische Maßnahmen (TOMs) in die Unternehmensstruktur zu implementieren.

Eine große Hilfe für technisch-organisatorische Maßnahmen (gerade bezüglich der IT-Sicherheit) bietet das Tool Sec-O-Mat der Transferstelle IT-Sicherheit im Mittelstand.

TOMs sind notwendig, um Informationen – ob personenbezogene Daten oder sensible Unternehmensdaten – zu schützen.

2.4.2.1 Organisatorische Maßnahmen

Zu den organisatorischen Maßnahmen zählen beispielsweise Mitarbeitersensibilisierung, Notfallmanagement sowie regelmäßige Notfallübungen, die Erstellung einer IT-Sicherheitsstrategie sowie das Erheben der Datensicherheit zur Priorität.

Folgende Maßnahmen sollten Sie umsetzen:

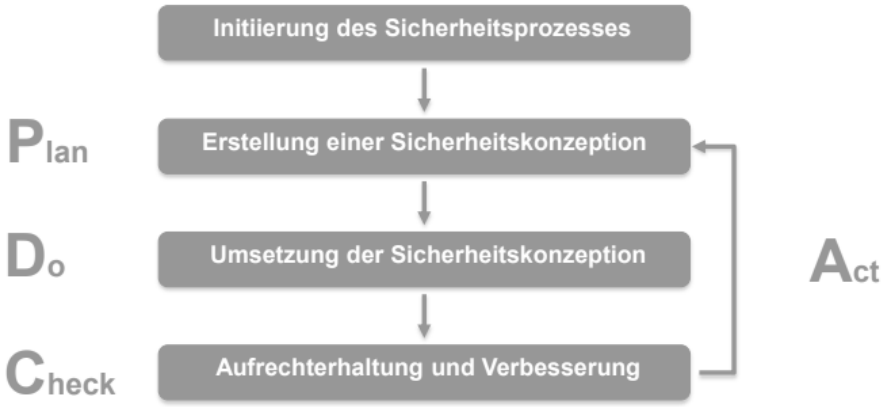
- ✓ Compliance-Organisation aufbauen
- ✓ Leitlinien für den Umgang mit Datenschutz, IT-Sicherheit und unternehmensspezifischen Risiken erstellen
- ✓ Beschäftigte im Datenschutz und in der IT-Sicherheit schulen
- ✓ Risikomanagement einrichten
- ✓ Auf IT-Notfälle vorbereiten (Notfallplan mit Reaktionsmaßnahmen und Aufklärung der Beschäftigten)
- ✓ Kriterien für Dienstleister zusammenstellen
- ✓ Verbindung mit externen Netzwerken regeln
- ✓ Passwortregeln festlegen
- ✓ Meldepflichten bei IT-Sicherheitsvorfall oder zu einer Datenpanne beachten
- ✓ Funktionierendes Informations-Management-System aufbauen (Informationsaustausch)
- ✓ Mobile Endgeräte sicher einsetzen (*Bring Your Own Device)*
- ✓ Privatnutzung der Unternehmenssoft- und -hardware klären (Orientierungshilfen finden Sie z.B. hier)

2.4.2.2 Technische Maßnahmen

Zu den technischen Maßnahmen zählen bspw. Passwortschutz, Hardware-Firewalls, regelmäßige manuelle Updates, VPN (Virtual Private Network), redundante Systeme zur Absicherung bei IT-Ausfällen, Mehr-Faktor-Authentifizierungen und vieles mehr.

Folgende Maßnahmen sollten Sie umsetzen:

- ✓ Verschlüsselung bei vertraulichen Informationen einsetzen
- ✓ Sichere Einstellungen für IT-Systemen und Software-Anwendungen wählen
- ✓ Schadsoftware verhindern
- ✓ Schwachstellen finden und schließen
- ✓ Eigenes Netzwerk (WLAN-Netz, VPN, etc.) absichern
- ✓ Software und IT-Systeme aktuell halten (regelmäßige Updates)
- ✓ Datensicherung durchführen und testen
- ✓ Aufgabenbezogene Zugriffsrecht bestimmen
- ✓ IT-Administration dokumentieren und überprüfen



2.4.2.3 Informationssicherheit

Jede verantwortliche und jede auftragsverarbeitende Person müssen also geeignete technische und organisatorische Maßnahmen (TOMs) treffen, um einen Schutz etwa vor unbefugter oder unrechtmäßiger Verarbeitung oder dem unbeabsichtigten Verlust der personenbezogenen Daten zu gewährleisten. Zu berücksichtigen sind dabei der Stand der Technik, die Implementierungskosten sowie die Art, die Umstände und der Zweck der Datenverarbeitung, aber auch die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen. Das Sicherheitsniveau muss dabei dem Risiko angemessen sein.

Unterstützung erfahren Unternehmen dabei von zwei Seiten: vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutz und von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit dem Standard-Datenschutzmodell (SDM).

Der IT-Grundschutz dient als Hilfestellung bei der Bestimmung und Umsetzung von notwendigen Sicherheitsmaßnahmen. Anhand von bewährten Vorgehensweisen aus den BSI-Standards liefert das IT-Grundschutz-Kompendium konkrete Anforderungen an die Informationssicherheit. Bei der Auswahl von Maßnahmen orientiert sich der Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen **Verfügbarkeit**, **Integrität** und **Vertraulichkeit**.

Beim SDM trifft man dagegen auf einen anderen Blickwinkel – die Sicherheit von Daten wird vor dem Hintergrund des Datenschutzes betrachtet. Dies führt dazu, dass zusätzlich noch solche Risiken für Rechte und Freiheiten natürlicher Personen Berücksichtigung finden, die sich aus der Tätigkeit des Unternehmens ergeben. Dementsprechend erhöht sich die Anzahl der Risiken, die bewertet werden müssen. Es entsteht ein globales Verständnis der **Datensicherheit als Sicherheit von allen im Unternehmen anfallenden Daten, ob mit Personenbezug oder ohne**.

Hinzu kommt noch der Schutz wettbewerbsrelevanter Informationen: Geschäftsgeheimnisse dürfen nicht durch einen unbefugten Zugang oder durch Verletzung der Geheimhaltungsverpflichtung oder durch jedes sonstige (widerrechtliche) Verhalten erlangt werden. Im Idealfall sollte in jedem Einzelfall geprüft werden, welches Geschäftsgeheimnis mit welchen Maßnahmen wirksam geschützt werden kann. Dabei ist auf die Bedeutung des Geheimnisses und die Angemessenheit der Schutzmaßnahmen besonders zu achten.

Mehr dazu finden Sie in unserem Leitfaden „Datenschutz und IT-Sicherheit“ unter „Materialien“ in der Rubrik „IT-Sicherheit & Datenschutz“.

2.5 Datentransfer

Werden personenbezogene Daten an Dritte übertragen, bedarf dies sowohl einer Rechtsgrundlage als auch geeigneter Garantien zur Einhaltung der Datenschutzniveaus.

Hierzu hat der Europäische Datenschutzausschuss Empfehlungen bezüglich des Datentransfers außerhalb der Europäischen Union herausgegeben. Diese Empfehlungen richten sich an alle Verantwortlichen und stellen eine Roadmap für Datentransfer außerhalb der EU zur Verfügung. Diese Roadmap stellt sechs Schritte dar, die notwendig sind, um ein Datentransfer in Drittländer rechtskonform zu gestalten:

- ✓ Schritt 1. "Know your transfers"
- ✓ Schritt 2. Transfer-Tools identifizieren
- ✓ Schritt 3. Bewertung der Effizienz der gewählten Transfer-Tools
- ✓ Schritt 4. Vornahme zusätzlicher Schutzmaßnahmen
- ✓ Schritt 5. Umsetzung
- ✓ Schritt 6. Monitoring

Die weiterführenden Erörterungen zu den jeweiligen Schritten entnehmen Sie bitte den hier für Sie verlinkten Empfehlungen.

Darüber hinaus hat die Europäische Kommission im Sommer 2021 Standardvertragsklauseln, die bei EU-weiten sowie internationalen Datentransfers angewandt werden können, verabschiedet. Diese Standardvertragsklauseln bieten Unternehmen ein nützliches Instrument für einen Datenaustausch außerhalb der EU, da sie die Vertragspartner besonderen Pflichten in Bezug auf die übermittelten personenbezogenen Daten unterwerfen. Eine individuelle Bewertung der Rechtslage im Drittland (insb. im Hinblick auf die Zugriffsrechte der Sicherheitsbehörden) bleibt dennoch nach wie vor notwendig.

Eine Vertragsklausel bezieht sich auf die Übermittlung personenbezogener Daten in Drittländer, eine zweite zur Verwendung zwischen Verantwortlichen und Auftragsverarbeitern.

Die Datentransfers außerhalb der EU müssen regelmäßig auf Effizienz der vorgenommenen Maßnahmen sowie hinsichtlich der Rechtsgrundlagen des Transfer-Landes überprüft werden. Darüber hinaus muss ein Verfahren eingeführt werden, damit die Transfers sofort abgestellt werden können, falls dies beispielsweise aufgrund einer neuen Rechtsprechung des EuGH (wie im Schrems II Fall) oder aufgrund eigener internen Überprüfung notwendig wird.

2.6 Datenschutzbeauftragte:r

Die/der Datenschutzbeauftragte:r muss jedenfalls dann bestellt werden, wenn:

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird,
- die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen,
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO bzw. von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht,
- das Unternehmen in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt,
- Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung unterliegen,
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Ist die/der Datenschutzbeauftragte:r bestellt worden, müssen ihr Kontaktdaten veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

Wird die/der Datenschutzbeauftragte:r bestellt, muss das Unternehmen sicherstellen, dass diese

- ✓ ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird,
- ✓ bei der Erfüllung ihrer Aufgaben unterstützt wird,
- ✓ mit erforderlichen Ressourcen und dem Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen ausgestattet wird,
- ✓ die zur Erhaltung ihres/seines Fachwissens erforderlichen Ressourcen zur Verfügung gestellt bekommt,
- ✓ keine Anweisungen bezüglich der Ausübung ihrer Aufgaben erhält,
- ✓ wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt wird,
- ✓ unmittelbar der höchsten Managementebene des Unternehmens berichtet,
- ✓ von Betroffenen bezüglich der Verarbeitung ihrer personenbezogenen Daten und der Wahrnehmung ihrer Rechte zu Rate gezogen werden kann,
- ✓ bei der Erfüllung ihrer Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden ist,
- ✓ frei von Interessenkonflikten agiert.

Die/der Datenschutzbeauftragte:r muss mindestens folgende Aufgaben übernehmen:

- ⇧ Unterrichtung und Beratung des Unternehmens und der mit der Verarbeitung personenbezogener Daten betrauten Beschäftigten zu ihren datenschutzrechtlichen Pflichten,
- ⇧ Kontrolle über die Einhaltung datenschutzrechtlicher Vorschriften
- ⇧ Kontrolle über die der Unternehmensstrategien zum Schutz personenbezogener Daten (inkl. Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter, datenschutzrechtliche Überprüfungen),

- ⇧ Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Kontrolle ihrer Durchführung,
- ⇧ Zusammenarbeit mit der Aufsichtsbehörde,
- ⇧ Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen (inkl. vorherige Konsultation und Beratung zu allen sonstigen Fragen).

Die/der Datenschutzbeauftragte:r muss bei ihrer Arbeit datenschutzrechtliche und andere im Zusammenhang mit der Verarbeitung personenbezogener Daten entstehenden Risiken einberechnen und dabei die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen.

3 Datenschutz in Kooperationen

3.1 Datenaustausch bei der Zusammenarbeit

Wenn zwei oder mehrere Unternehmen kooperieren, ist der Austausch personenbezogener Daten zwischen diesen Unternehmen kaum auszuschließen. Es werden sowohl Kunden- als auch Mitarbeiterdaten ausgetauscht und vom Kooperationspartner verarbeitet. Um diesen Datenaustausch rechtskonform zu gestalten, sollten beteiligte Unternehmen rechtszeitig (vor der Verarbeitung) die konkret betroffenen Personen informieren. In der Regel stellt sich dies als recht kompliziert heraus, da zum Beginn einer Zusammenarbeit häufig keine Klarheit darüber besteht, welche Daten konkret im weiteren Verlauf der Kooperation noch auszutauschen sind.

Dennoch empfiehlt sich eine rechtzeitige Berücksichtigung datenschutzrechtlicher Aspekte beim Anbahnen einer Kooperation. Dafür können folgende Instrumente verwendet werden:

3.2 Vertragliche Klärung

In der Kooperationsvereinbarung sollte der Datenaustausch bedacht werden. Da kooperierende Unternehmen regelmäßig auch Unternehmensdaten sowie Geschäftsinformationen austauschen, wäre eine zusätzliche Erwähnung personenbezogener Daten in diesem Kontext unkompliziert. Zu bedenken sind die Modalitäten der Datenübertragung (verschlüsselt, über einen (sicheren) Datenträger etc.), Löschfristen (insb. nach der Beendigung der Kooperation) und der Umgang mit personenbezogenen Daten innerhalb der Kooperation. Auch zusätzliche technische und organisatorische Maßnahmen sind denkbar, gerade wenn nicht lediglich berufliche E-Mail-Adressen einiger Beschäftigten ausgetauscht werden, sondern beispielsweise Gesundheitsdaten oder Vermögensverhältnisse von Kunden.

3.3 Rechtsgrundlage

In der Regel wird sich der Austausch personenbezogener Daten zwischen den Kooperationspartnern auf die berechtigten Interessen des jeweiligen Partners (Art. 6 Abs. 1 lit. f DSGVO) stützen lassen, kann doch keine Kommunikation zwischen den Unternehmen ohne Namen der für die Kooperation zuständigen Beschäftigten erfolgen. Dabei ist insbesondere der Grundsatz der Datenminimierung zu beachten, denn es sollten grundsätzlich nur so wenige personenbezogenen Daten ausgetauscht werden wie nötig, mithin nur solche Daten, die für die Kommunikation und die Durchführung der Zusammenarbeit unabdingbar sind.

Bei dem Austausch personenbezogener Kundendaten ist Obacht geboten. Hier ist zu bedenken, dass sich die Rechtgrundlage des (ursprünglich) erhebenden Kooperationspartners nicht auf eine weitere Verarbeitung erstreckt. Werden beispielsweise vom Unternehmen A Kundendaten aufgrund einer Einwilligung von Betroffenen verarbeitet, dürfen sie nicht ohne Weiteres an Unternehmen B weitergeleitet werden (es sei denn die Einwilligung bezieht sich unmittelbar auch auf den Datentransfer). Lässt sich die Verarbeitung in einer konkreten Situation auf die berechtigten Interessen (Art. 6 Abs. 1 lit. f DSGVO) stützen, muss die Abwägung zwischen den Interessen des Kooperationspartners und denen der betroffenen Personen nachvollziehbar durchgeführt und dokumentiert werden.

3.4 Gemeinsames Konzept zur Datenverarbeitung

Es empfiehlt sich, ein gemeinsames Konzept zur Datenverarbeitung für die Kooperation zu erarbeiten. In diesem können sowohl unternehmensbezogene (bzw. kooperationsbezogene) als auch personenbezogene Daten bedacht und deren Austausch geregelt werden. Gerade für eine auf Dauer ausgelegte Kooperation bietet so ein Konzept eine gute Grundlage für einen Datenaustausch. Die Kooperationspartner selbst sowie ihre Beschäftigten kennen dadurch ihre Pflichten und das Vorgehen im Zusammenhang mit dem Datenaustausch, die Betroffenen (etwa Kunden und Lieferanten) bekommen einen Überblick über die Verarbeitung ihrer personenbezogenen Daten.

4 Ausblick

Die Digitalisierung von Management- und Produktionsprozessen ist Treiber zahlreicher innovativer Kooperationen, bei denen unter anderem sensible Unternehmensinformationen ausgetauscht werden. Sie hat aber auch Auswirkungen auf die Unternehmens- und Informationssicherheit eines Unternehmens. Da sich konkrete IT-Sicherheitsmaßnahmen aus der Bedrohungsanalyse und der Risikobewertung ergeben, müssen alle IT-Unternehmen ihr eigenes Risikoprofil und ihre individuelle Bedrohungslage eruieren und das Risiko, Opfer eines Angriffs zu werden, stets vor Augen haben (und ihren Kunden vor Augen führen). Darüber hinaus hat die Covid-19 Pandemie die Digitalisierungsprozesse beschleunigt, sodass auch der Wert der Informationssicherheit gestiegen ist.

Besondere Bedeutung kommt dabei der fachlichen Qualifikation von Beschäftigten und Führungskräften zu, denn viele IT-Sicherheitsvorfälle lassen sich mit entsprechenden IT-

Sicherheitsschulungen, Trainings und regelmäßigen Auffrischungskursen vermeiden. Jeder muss verstehen, dass der Schutz von (sowohl unternehmensbezogenen als auch von personenbezogenen) Daten keine einmalige Aufgabe, sondern ein dauerhafter Prozess ist.

Wir, das Kompetenzzentrum IT-Wirtschaft, unterstützen Sie mit konkreten Angeboten im Bereich Datenschutz! Wir beantworten zudem Ihre datenschutz-, IT-Sicherheits- und kooperationsrechtlichen Fragen und vermitteln gezielt Kompetenzen und Fertigkeiten, die zum Aufbau Ihrer vertrauensvollen und sicheren Kooperation notwendig sind. Bei uns finden Sie Muster und Vorlagen, die gesetzeskonform gestaltet und vorausschauend strukturiert sind, und angepasst werden können.

Schauen Sie gern bei uns vorbei unter www.itwirtschaft.de.

5 Kontakt

Haben Sie Fragen oder Anregungen, melden Sie sich gerne bei uns. Wir freuen uns auf Sie!

Ansprechpartnerin:

Olga Kunkel, LL.M.
Telefon: +49 3375 508 641
E-Mail: olga.kunkel@itwirtschaft.de

Kompetenzzentrum IT-Wirtschaft
vertreten durch:

Bundesverband IT-Mittelstand e.V. (BITMi)
Hauptstadtbüro Berlin:
Haus der Bundespressekonferenz

Schiffbauerdamm 40, 10117 Berlin
T +49 30 22605 005

www.itwirtschaft.de

Was ist Mittelstand-Digital?

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft ist Teil der Förderinitiative Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren vor Ort helfen dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen.

Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

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

Impressum

Konzeption und Text: Olga Kunkel, Kompetenzzentrum IT-Wirtschaft

Bildnachweis: Hirofumi Nobukuni

Stand: August 2021