Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Datenschutz und IT-Sicherheit in der IT-Branche

www.itwirtschaft.de

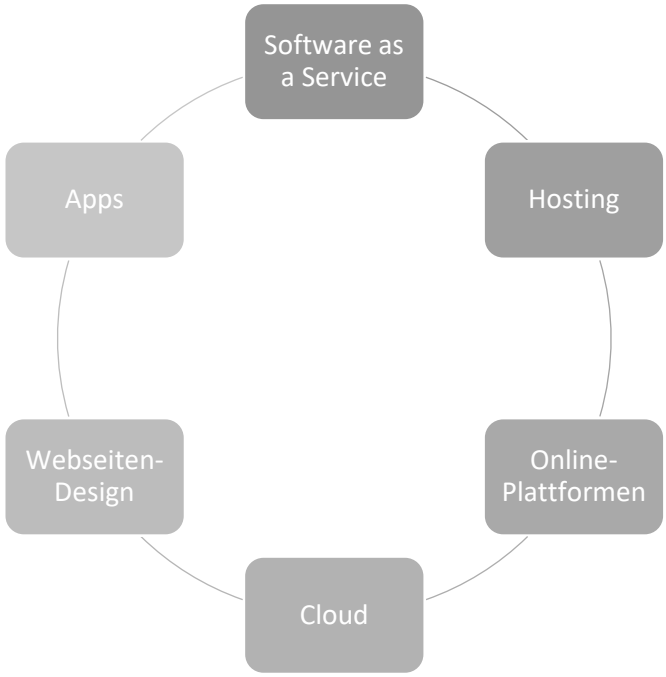
Mittelstand-Digital

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

Inhalt

Einführung

Der Leitfaden soll Ihnen beim Aufbau einer Datenschutz-Organisation in Ihrem Unternehmen helfen und die wichtigsten Prinzipien des Datenschutzrechts nahelegen. Dabei wird hier nicht lediglich der Schutz personenbezogener Daten angesprochen, sondern grundsätzlich Datensicherheit in jedem Unternehmen. Es geht darum, den Schutz von ALLEN in einem Unternehmen anfallenden Daten (Informationen) durch interne Vorsorgemaßnahmen, technische Lösungen und vertragliche Instrumente zu gewähren.



Dieser Leitfaden richtet sich an alle (IT-)Unternehmen, denn in der heutigen digitalisierten Welt ist eine Tätigkeit ohne Verarbeitung von Daten – personenbezogenen oder nicht – undenkbar.

1 Sicherer Schutz geheimer Daten

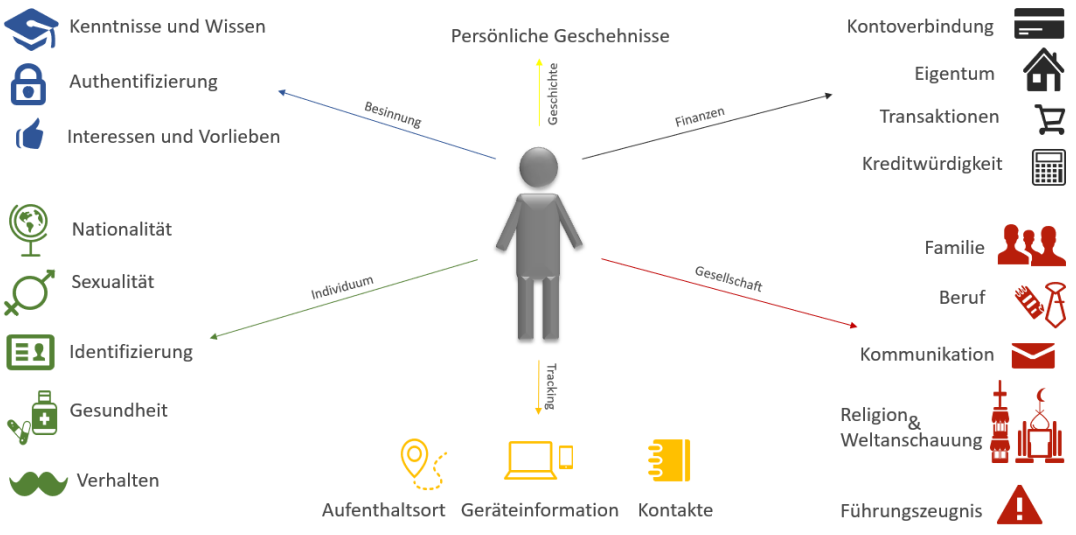
1.1 Personenbezogene Daten oder Geschäftsgeheimnisse?

In jedem Unternehmen fällt eine ganze Menge Daten an, die besonders geschützt werden müssen. Darunter sind sowohl personenbezogene Daten von Mitarbeiter:innen, Kund:innen und Lieferant:innen, die primär aufgrund gesetzlicher Bestimmungen einem besonderen Schutz unterworfen sind, als auch sensible unternehmensbezogene Informationen wie etwa Geschäfts- oder Betriebsgeheimnisse, die von großer Bedeutung im Wettbewerb sind und deren Schutz im eigentlichen Interesse des Unternehmens liegt. Was unterscheidet sie voneinander, was haben sie gemeinsam?

1.1.1 Personenbezogene Daten

Unter personenbezogenen Daten versteht die DSGVO (seit Mai 2018 in Kraft) alle Informationen, die sich auf eine konkrete (in der Terminologie der DSGVO „identifizierte oder identifizierbare“) natürliche Person beziehen. Diese Informationen gelten dann als „personenbezogen“, mithin zur Identifizierung geeignet, wenn ein konkreter Mensch mithilfe dieser Informationen direkt oder indirekt identifiziert werden kann. Es handelt sich dabei um viele verschiedene Merkmale, Kennungen, Nummer, die „Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“, sodass eine individuelle Prüfung der anfallenden Daten daraufhin, ob sie personenbezogen sind oder nicht, in aller Regel notwendig sein wird.

So ist ein in einem Übungsbuch zum Gesellschaftsrecht vorkommender (fiktiver!) Name einer natürlichen Person kein personenbezogenes Datum, da kein „echter“ Mensch dadurch identifiziert werden kann. Dahingegen ist die Bezeichnung „Bundeskanzlerin“ durchaus ein personenbezogenes Datum, auch wenn kein Name genannt wird.



1.1.2 Geschäftsgeheimnisse

Ein Geschäftsgeheimnis ist gem. § 1 GeschGehG (seit April 2019 in Kraft) eine Information,

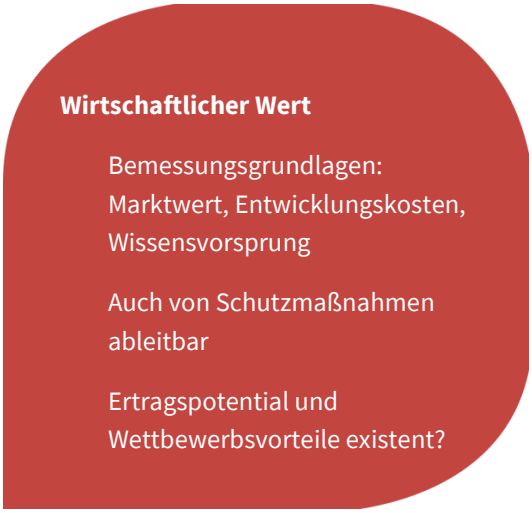
a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Die geheinzuhaltende Information muss weder auf irgendwelchen Träger noch in Papierform verkörpert werden, sie darf auch mündlich existieren. Weiterhin ist es unschädlich, wenn diese Information gegenüber bestimmten ausgewählten Personen wie etwa einer Rechtsanwältin im Rahmen eines Rechtsstreits offengelegt wird. Das Geschäftsgeheimnis umfasst sowohl kaufmännisches als auch technisches Wissen. Beispiele für Geschäftsgeheimnisse sind Herstellungsverfahren, Konstruktionspläne, Prototypen, Kundenlisten, Businesspläne, Marktanalysen, Erfindungen und Lizenzen.

Der wirtschaftliche Wert kann an den Entwicklungskosten oder dem Marktwert bemessen werden. Aber auch ohne Marktwert kann ein wirtschaftlicher Wert dann bestehen, wenn die zu schützenden Informationen beispielsweise einen Wissensvorsprung darstellen, welcher nur durch zeitliche oder monetäre Investitionen aufgeholt werden kann. Weiterhin kann der Nachweis eines wirtschaftlichen Werts für das Unternehmen auch anhand der getroffenen Schutzmaßnahmen abgeleitet werden. Entscheidend ist, dass aufgrund der geheim gehaltenen Information Ertragspotentiale und Wettbewerbsvorteile existieren.



Eine besondere Bedeutung beim Schutz von Geschäftsgeheimnissen erlangen die Schutzmaßnahmen, die vom Unternehmen ergriffen werden (müssen).

✓ Erst durch die Vornahmen von Schutzmaßnahmen wird eine Information zum Geschäftsgeheimnis!

Hier folgt das GeschGehG dem gleichen Schema wie die DSGVO: es müssen bestimmte Schutzmaßnahmen getroffen und darüber hinaus nachgewiesen werden, sodass der subjektive Wille am Schutz bestimmter geschäftlicher (geschäftswichtiger) Informationen durch objektive

Geheimhaltungsmaßnahmen flankiert wird. Es ist somit notwendig, zum Schutz von Geschäftsgeheimnissen technische, organisatorische und/oder rechtliche Maßnahmen zu treffen (ganz wie zum Datenschutz im Sinne der DSGVO!). All die getroffenen Maßnahmen müssen auch dokumentiert werden, damit der Schutz entsteht und in einem Streitfall durchgesetzt (u.a. durch Unterlassung der Beeinträchtigung und/oder Schadensersatzansprüche) werden kann.

Wie ist die Angemessenheit von Schutzmaßnahmen zu bewerten?

Eine „endgültige“ Bewertung von Schutzmaßnahmen wird von Gerichten vorgenommen. Allerdings können folgende Anhaltspunkte hinzugezogen werden:

- Wert des Geheimnisses für das Unternehmen,
- Entwicklungskosten des Geheimnisses,
- Bedeutung des Geheimnisses fürs Unternehmen,
- Art der Kennzeichnung der Information,
- Größe des Unternehmens,
- Aufwand für die Vornahme von Maßnahmen,
- Kosten der Maßnahme(n),
- Verschwiegenheitsverpflichtungen Beteiligter,
- Üblichkeit der Schutzmaßnahmen.

Welche Schutznahmen dem Schutz von Geschäftsgeheimnissen dienen könnten, erfahren Sie in Kap. 4; dort finden Sie auch eine Checkliste.

1.2 Datenschutz und IT-Sicherheit

Nicht selten werden die Begriffe Datenschutz und IT-Sicherheit beinahe synonym verwendet. Dabei sind das doch zwei unterschiedliche Bereiche, auch wenn Überschneidungen durchaus vorhanden sind. Andererseits erlaubt die wachsende Bedeutung von digitalen Daten, Prozessen und Anwendungen keine getrennte Betrachtung dieser Bereiche, denn digital anfallende personenbezogene Daten müssen von der Informationssicherheit mitumfasst werden.

Ähnlichkeit besteht auch darin, dass sowohl der Datenschutz als auch IT-Sicherheit lediglich „Mittel zum Zweck“ sind: Der Datenschutz zielt auf informationelle Selbstbestimmung von Menschen, die IT-Sicherheit – auf Zuverlässigkeit technischer Prozesse.

Eine gute Grundlage für die Informationssicherheit bietet dabei der vom BSI (Bundesamt für Sicherheit in der Informationstechnik) entwickelte IT-Grundschutz, der Maßnahmen und Standards für die Ermittlung der Schutzbedarfe und für das Ergreifen von Schutzmaßnahmen umfasst. Die Grundlage für den IT-Grundschutz bietet das Risikomanagement: Risiken für die IT-Sicherheit (*safety* und *security*) müssen identifiziert, bewertet und gesteuert und die Abwehrmaßnahmen überwacht werden.

Identifikation:	Welche Bedrohungen sind für dieses bestimmte Schutzobjekt relevant?
Bewertung:	Wie hoch ist die Eintrittswahrscheinlichkeit ermittelter Risiken und wie groß könnte der dadurch verursachte Schaden ausfallen?
Steuerung:	Welche Schritte und Maßnahmen sind zum Schutz vor ermittelten Risiken bzw. zu Abwehr dieser Risiken geeignet?
Überwachung:	Werden die ermittelten Risiken tatsächlich effektiv durch die ergriffenen Gegenmaßnahmen vermieden?

Im Fokus des IT-Grundschutzes stehen die sogenannten IT-Grundschutz-Bausteine. Es handelt sich dabei um Texte, die jeweils ein Thema zu den vom BSI bestimmten relevanten Sicherheitsaspekten beleuchten, dabei werden sowohl mögliche Gefährdungen als auch Sicherheitsanforderungen erläutert. Die IT-Grundschutz-Bausteine sind in zehn unterschiedliche Schichten aufgeteilt und reichen thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS).

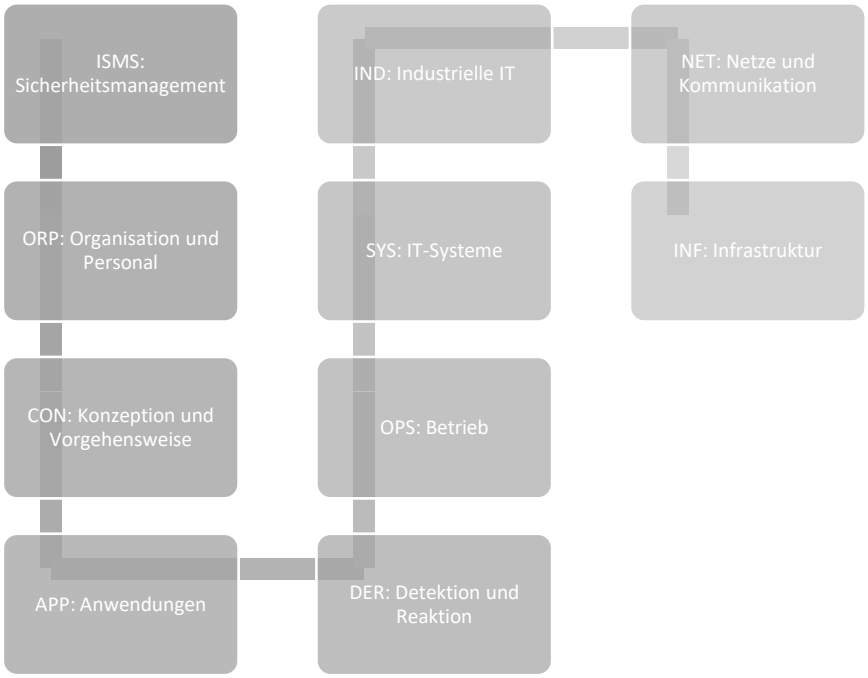


Abbildung: Überblick IT-Grundschutz (BSI)

Einzelne Bausteine des IT-Grundschutzes des BSI finden Sie nachfolgend und hier.

IT-Grundschutz des BSI

ISMS: Sicherheitsmanagement	ISMS.1 Sicherheitsmanagement	
ORP: Organisation und Personal	ORP.1 Organisation ORP.2 Personal ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	ORP.4 Identitäts- und Berechtigungsmanagement ORP.5 Compliance Management (Anforderungsmanagement)
CON: Konzeption und Vorgehensweise	CON.1 Kryptokonzept CON.2 Datenschutz CON.3 Datensicherungskonzept CON.6 Löschen und Vernichten	CON.7 Informationssicherheit auf Auslandsreisen CON.8 Software-Entwicklung CON.9 Informationsaustausch CON.10 Entwicklung von Webanwendungen
OPS: Betrieb	OPS.1.1.2 Ordnungsgemäße IT-Administration OPS.1.1.3 Patch- und Änderungsmanagement OPS.1.1.4 Schutz vor Schadprogrammen OPS.1.1.5 Protokollierung OPS.1.1.6 Software-Tests und -Freigaben	OPS.1.2.2 Archivierung OPS.1.2.4 Telearbeit OPS.1.2.5 Fernwartung OPS.2.1 Outsourcing für Kunden OPS.2.2 Cloud-Nutzung OPS.3.1 Outsourcing für Dienstleister
DER: Detektion und Reaktion	DER.1 Detektion von sicherheitsrelevanten Ereignissen DER.2.1 Behandlung von Sicherheitsvorfällen DER.2.2 Vorsorge für die IT-Forensik	DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle DER.3.1 Audits und Revisionen DER.3.2 Revision auf Basis des Leitfadens IS-Revision DER.4 Notfallmanagement
APP: Anwendungen	APP.1.1 Office-Produkte APP.1.2 Web-Browser APP.1.4 Mobile Anwendung (Apps) APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory APP.2.3 OpenLDAP APP.3.1 Webanwendungen APP.3.2 Webserver APP.3.3 Fileserver APP.3.4 Samba	APP.3.6 DNS-Server APP.4.2 SAP-ERP-System APP.4.3 Relationale Datenbanksysteme APP.4.6 SAP ABAP-Programmierung APP.5.2 Microsoft Exchange und Outlook APP.5.3 Allgemeiner E-Mail-Client und -Server APP.6 Allgemeine Software APP.7 Entwicklung von Individualsoftware
SYS: IT-Systeme	SYS.1.1 Allgemeiner Server SYS.1.2.2 Windows Server 2012 SYS.1.3 Server unter Linux und Unix SYS.1.5 Virtualisierung SYS.1.7 IBM Z-System SYS.1.8 Speicherlösungen SYS.2.1 Allgemeiner Client SYS.2.2.2 Clients unter Windows 8.1 SYS.2.2.3 Clients unter Windows 10 SYS.2.3 Clients unter Linux und Unix SYS.2.4 Clients unter macOS SYS.3.1 Laptops	SYS.3.2 Tablet und Smartphone SYS.3.2.1 Allgemeine Smartphones und Tablets SYS.3.2.2 Mobile Device Management (MDM) SYS.3.2.3 iOS (for Enterprise) SYS.3.2.4 Android SYS.3.3 Mobiltelefon SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte SYS.4.3 Eingebettete Systeme SYS.4.4 Allgemeines IoT-Gerät SYS.4.5 Wechseldatenträger
IND: Industrielle IT	IND.1 Prozessleit- und Automatisierungstechnik IND.2.1 Allgemeine ICS-Komponente IND.2.2 Speicherprogrammierbare Steuerung (SPS)	IND.2.3 Sensoren und Aktoren IND.2.4 Maschine IND.2.7 Safety Instrumented Systems
NET: Netze und Kommunikation	NET.1.1 Netzarchitektur und -design NET.1.2 Netzmanagement NET.2.1 WLAN-Betrieb NET.2.2 WLAN-Nutzung NET.3.1 Router und Switches	NET.3.2 Firewall NET.3.3 VPN NET.4.1 TK-Anlagen NET.4.2 VoIP NET.4.3 Faxgeräte und Faxserver
INF: Infrastruktur	INF.1 Allgemeines Gebäude	INF.8 Häuslicher Arbeitsplatz

	INF.2 Rechenzentrum sowie Serverraum INF.5 Raum sowie Schrank für technische Infrastruktur INF.6 Datenträgerarchiv INF.7 Büroarbeitsplatz	INF.9 Mobiler Arbeitsplatz INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum INF.11 Allgemeines Fahrzeug INF.12 Verkabelung

Die Aufteilung in einzelne Bereiche soll dabei helfen, einen Überblick zu behalten und wichtige Aspekte nicht zu übersehen, darüber hinaus können Zuständigkeiten frühzeitig festgelegt und Umsetzungstechniken klar geregelt werden.

Das IT-Grundschutz-Kompendium wird jährlich im Februar in einer neuen Edition veröffentlicht.

Die **Verbindung zwischen der IT-Sicherheit und dem Datenschutz** wird bereits beim Lesen der DSGVO klar. So folgt aus dem Gebot der Transparenz beispielsweise die Notwendigkeit, Betroffene über die Datenverarbeitung und die dafür eingesetzten Prozesse (und ggf. auch Lösungen) zu informieren sowie diese Prozesse den Aufsichtsbehörden zu zeigen. Demselben Zweck dient das EU Cybersecurity Act mit der Möglichkeit, IT-Lösungen zu zertifizieren und dadurch die Transparenz sowohl für Nutzer*innen als auch für Betroffene zu erhöhen. Auch der Verlust von Informationen und dessen Konsequenzen werden regelmäßig in Schulungen aufgegriffen, dabei drohen beim Verlust personenbezogener Daten hohe Geldbußen und Schadensersatzansprüche und beim Verlust anderer (unternehmensinterner) Informationen (durch Sicherheitslücken) eigener finanzieller Schaden des Unternehmens (und unter Umständen auch kriminelle Geldforderungen).

Unterschiedlich ist indes die gesetzgeberische Handhabung beider Bereiche. Der Datenschutz setzt mit der DSGVO und anderen Rechtsvorschriften einen engen Rahmen für die Verarbeitung personenbezogener Daten fest, formuliert Prinzipien, Gebote und Rechte der Betroffenen und stellt (überwiegend) Verbote auf, geht aber gerade nicht auf das „wie“ des Datenschutzes, mithin konkrete Umsetzungslösungen, ein. Die IT-Sicherheit im Gegenteil beruht auf überwiegend nicht-obligatorischen Standards, die aus wirtschaftlicher Sicht jedoch unabdingbar sind und dabei einzelne Lösungen, konkrete Mechanismen und passgenaue Vorgehensweisen anbietet.

Die hohe Kunst dürfte also darin bestehen, die beiden Bereiche – IT-Sicherheit und Datenschutz – zu einem funktionierenden Gesamtkonzept zu vereinen und dadurch sowohl der informationellen Selbstbestimmung als auch der Informationssicherheit im weitesten Sinne gerecht zu werden.

2 Grundsätze des Datenschutzes

2.1 Verarbeitungsgrundsätze

Art. 5 DSGVO sowie einige andere Artikel und Erwägungsgründe der DSGVO legen einige Verarbeitungsgrundsätze fest.

- **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

2.2 Rechtsgrundlagen der Datenverarbeitung

Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten, es sei denn es liegt ein Rechtfertigungsgrund vor. Diese werden im Art. 6 DSGVO explizit aufgelistet:

- **Einwilligung**: Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- **Vertragserfüllung**: die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- **Rechtspflicht**: die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- **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 erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- **Berechtigte Interessen**: die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

2.3 Rechte der Betroffenen

2.3.1 Überblick

Die DSGVO zielt explizit auf eine faire, transparente und nachvollziehbare Verarbeitung von personenbezogenen Daten. Diesem Ziel dienen auch die in der DSGVO verankerten Rechte der Betroffenen, also derjenigen Personen, deren personenbezogene Daten verarbeitet werden.

Diese Rechte wandeln sich entsprechend in die Pflichten der Verantwortlichen, mithin derjenigen, die die personenbezogenen Daten der Betroffenen verarbeiten, um.

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

Die DSGVO verlangt, dass der Verantwortliche „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ die Informationen bezüglich der Datenverarbeitung übermittelt. Dies bedeutet, dass auch Menschen, die keine besonderen Kenntnisse im Datenschutz haben, anhand übermittelter Informationen verstehen können, welche Daten wie und zu welchem Zweck verarbeitet werden, wie lange dies dauert und wann diese Daten gelöscht werden.

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

Die von der DSGVO geforderte Transparenz führt zur Notwendigkeit, die Informationen über die Datenverarbeitung so frühzeitig zu kommunizieren wie möglich, in aller Regel also ***vor*** der Datenverarbeitung. Sollte dies unmöglich sein, etwa weil jegliche Kontaktdaten der betroffenen Person fehlen oder die Mitteilung einen unverhältnismäßigen Aufwand darstellt, muss dies nachvollziehbar dokumentiert werden.

- **(Reaktives) 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 (sowohl vom Verantwortlichen selbst als auch von denjenigen, wer diese Daten vom Verantwortlichen bekommen hat), gerade wenn die betroffene Person danach verlangt.

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

Die betroffene Person kann verlangen, dass sowohl der Verantwortliche selbst als auch all diejenigen, wer diese Daten vom Verantwortlichen bekommen hat, ihre personenbezogenen Daten löschen. Dieses Recht ist nicht uneingeschränkt: personenbezogene Daten können nur dann gelöscht werden, wenn sie für die Erfüllung des Zwecks, für welchen sie erhoben worden sind, nicht mehr erforderlich sind bzw. wenn die/der Betroffene ihre/seine Einwilligung widerruft. 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)**

Die/der Betroffene kann vom Verantwortlichen verlangen, dass ihre/seine Daten nicht gelöscht, sondern deren Verarbeitung eingeschränkt wird, wenn etwa diese Daten 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 Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer öffentlichen Aufgabe) oder auf Art. 6 Abs. 1 lit. e DSGVO (Wahrung der berechtigten Interessen des Verantwortlichen) stützt. Dies gilt insb. für Direktwerbung und Marketing-Profiling (Art. 21 Abs. 2 DSGVO).

- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO)**

Die/der Betroffene darf vom Verantwortlichen verlangen, dass ihr/ihm ihre/seine personenbezogenen Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ zur Verfügung gestellt und/oder an einen anderen Verantwortlichen übermittelt werden, sofern (i) die/der Betroffene diese Daten dem Verantwortlichen selbst bereitgestellt hat, (ii) diese Daten aufgrund einer Einwilligung oder zur Erfüllung eines Vertrags verarbeitet werden und (iii) die Verarbeitung mithilfe automatisierter Verfahren erfolgt

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

Die/der Betroffene dürfen bestimmen, inwiefern sie/er eine automatisierte, mithin eine ohne menschliche Einflussnahme getroffene, Entscheidung, die rechtliche Auswirkungen entfaltet, zulassen. Es handelt sich dabei sowohl um automatisierte Entscheidungen im Einzelfall, wie etwa eine Bewertung der Bewerbung lediglich durch einen Algorithmus, als auch um Profiling, wie etwa Arbeitsleistung oder Gesundheitszustand.

- **Recht auf Beratung durch den Datenschutzbeauftragten des Verantwortlichen (Art. 38 DSGVO)**

Betroffene Personen dürfen den Datenschutzbeauftragten 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

Die Datenschutzerklärung muss mindestens folgende Angaben enthalten:

- ✓ die verantwortliche Stelle (Name und Kontaktdaten),
- ✓ falls vorhanden, den Datenschutzbeauftragten (Kontaktdaten),
- ✓ 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 erforderlich, mit den entsprechenden Angaben zum Schutzniveau im Drittland,
- ✓ weitere Informationen.

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

2.4 Dokumentation

Art. 5 Abs. 2 DSGVO führt die sog. „Rechenschaftspflicht“ ein: Der Verantwortliche muss nicht nur für die Einhaltung der Verarbeitungsgrundsätze der DSGVO sorgen, sondern dies auch jederzeit nachweisen können. Der Erfüllung dieser Rechenschaftspflicht dient in jedem Unternehmen die Dokumentation datenschutzrechtlich relevanter Vorgänge.

Zu den datenschutzrechtlichen Dokumentationspflichten gehören somit:

- die Pflicht, ein Verarbeitungsverzeichnis anzufertigen, Art. 30 DSGVO,
- die Pflicht, Datenschutzverletzungen zu dokumentieren und zu melden, Art. 34 DSGVO,
- die Pflicht, Datenschutz-Folgeabschätzung durchzuführen,
- die Pflicht, Interessenabwägung zu dokumentieren,
- die Pflicht, eine Datenschutzrichtlinie aufzusetzen,
- die Pflicht, Auftragsverarbeitungsverträge zu dokumentieren,
- die Pflicht, ein Löschkonzept anzufertigen.

2.4.1 Verzeichnis der Verarbeitungstätigkeiten

2.4.1.1 Überblick

Jeder Verantwortliche muss gem. Art. 30 Abs. 1 DSGVO ein Verzeichnis der Verarbeitungstätigkeiten führen, die seiner Zuständigkeit unterliegen.

Befreit von dieser Pflicht sind Verantwortliche unter folgenden Voraussetzungen, die allesamt erfüllt werden müssen:

- ✓ das Unternehmen beschäftigt weniger als 250 Mitarbeitende,
- ✓ die vorgenommene Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- ✓ die vorgenommene Verarbeitung erfolgt nur gelegentlich (nicht regelmäßig),
- ✓ die vorgenommene Verarbeitung umfasst keine besonderen Datenkategorien gem. Art. 9 Abs. 1 DSGVO (dies sind rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung),
- ✓ die vorgenommene Verarbeitung umfasst keine personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.v. Art. 10 DSGVO.

Sofern in einem Unternehmen personenbezogene Daten von Beschäftigten verarbeitet, eine Kundendatenbank geführt oder auch ein Newsletter versandt wird, erfolgt die Verarbeitung personenbezogener Daten eben nicht nur gelegentlich, sodass das Erstellen und Führen vom Verarbeitungsverzeichnis unabdingbar wird.

Dieses Verzeichnis der Verarbeitungstätigkeiten muss folgenden Angaben enthalten:

- ✓ den Namen und die Kontaktdaten des Verantwortlichen und seines Vertreters sowie der/des Datenschutzbeauftragten, falls bestellt,
- ✓ die Zwecke der Datenverarbeitung,
- ✓ eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- ✓ die Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt werden (inkl. Empfänger in Drittländern und internationale Organisationen),
- ✓ ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation mitsamt Eingabe des Drittlandes/der internationalen Organisation sowie Dokumentierung geeigneter Garantien i.S.v. Art. 49 DSGVO,
- ✓ Fristen für die Löschung der verschiedenen Datenkategorien (wenn möglich),
- ✓ eine allgemeine Beschreibung der TOMs i.S.v. Art. 32 Abs. 1 DSGVO (wenn möglich).

Nachfolgend finden Sie auch ein Muster für das Verzeichnis der Verarbeitungstätigkeiten. Die DSK hat hier **Hinweise zum Verzeichnis von Verarbeitungstätigkeiten** (Stand Feb. 2018) und ein **Muster** (Stand Feb. 2018) veröffentlicht.

2.4.1.2 Muster für das Verzeichnis der Verarbeitungstätigkeiten

Verzeichnis der Verarbeitungstätigkeiten gem. Artikel 30 Abs. 1 DSGVO

Verzeichnis der Verarbeitungstätigkeiten der Mustermann GmbH		
Verantwortlicher[1] *Mustermann GmbH* *Musterstraße 1 10000 Musterstadt Deutschland* *Tel.: 030-1000-1000* *E-Mail: info@mustermann-gmbh.de* *www.mustermann.de*		**Datenschutzbeauftragte** *Marie Mustermann* *Musterstraße 1 10000 Musterstadt Deutschland* *Tel.: 030-1000-1002* *E-Mail: marie.mustermann@mustermann-gmbh.de* *www.mustermann.de*
Vertreter des Verantwortlichen[2] *Max Mustermann* *Chief Information Officer* *Musterstraße 1 10000 Musterstadt Deutschland* *Tel.: 030-1000-1001* *E-Mail: max.mustermann@mustermann-gmbh.de* *www.mustermann.de*		

[1] Ggf. aufzunehmen ist auch der gemeinsamer Verantwortlicher.
[2] Hier ist nicht unbedingt Geschäftsführung anzugeben, sondern diejenige Person im Unternehmen, die operativ für den Datenschutz zuständig ist.

<table>
<tr><td colspan="2">Verarbeitungstätigkeit:
_____</td><td>Seite
_____</td></tr>
<tr><td colspan="2">Datum der Ersteinführung: _____</td><td>Datum der letzten Änderung:
_____</td></tr>
<tr><td>Verantwortliche Stelle/Abteilung</td><td colspan="2"></td></tr>
<tr><td>Ansprechpartner
Telefon
E-Mail-Adresse</td><td colspan="2"></td></tr>
<tr><td>Zweck der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b DSGVO)</td><td colspan="2"></td></tr>
<tr><td>Verwendetes Verfahren, falls relevant</td><td colspan="2"></td></tr>
<tr><td>Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c DSGVO)</td><td colspan="2">Beschäftigte / Kund:innen / Lieferant:innen / Interessenten / …</td></tr>
<tr><td>Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c DSGVO)</td><td colspan="2">Name / E-Mail-Adresse / Wohnadresse / Steuer-ID / …

Besondere Kategorien personenbezogener Daten (Art. 9):
Gesundheitsdaten / Herkunft / politische Meinung / …</td></tr>
<tr><td rowspan="2">Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt werden (Art. 30 Abs. 1 S. 2 lit. d, Art. 30 Abs. 1 S. 2 lit. e, Art. 49 Abs. 1 DSGVO)</td><td colspan="2">Intern:
Zugriff durch[3]:</td></tr>
<tr><td colspan="2">Extern
Empfängerkategorie:[4]</td></tr>
</table>

[3] Namen und ggf. auch Funktionen/Positionen im Unternehmen.

[4] z.B. Newsletterversand-Dienstleister, Steuerberater, etc.

	Drittland: Datenübermittlung findet nicht statt. ODER Datenübermittlung findet wie folgt statt[5]: _____ Empfänger:[6] Garantien:[7]
	Internationale Organisation: Datenübermittlung findet nicht statt. ODER Datenübermittlung findet wie folgt statt[8]: _____ Empfänger:[9] Garantien:[10]
Löschungsfristen (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 Abs.1 DSGVO[11] (Art. 30 Abs. 1 S. 2 lit. g)	Für **Pseudonymisierung** etwa die Bestimmung der Daten, die pseudonymisiert werden, der anwendbaren Pseudonymisierungsregel, der autorisierten Personen, der getrennten Speicherung etc. Verschlüsselung personenbezogener Daten Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Weitere Informationen zu TOMs finden Sie unter 2.5 sowie hier ab Seite 8.

[5] Beschreibung.
[6] Konkrete Namen/Bezeichnungen der Empfänger.
[7] Garantien für den Schutz personenbezogener Daten.
[8] Beschreibung.
[9] Konkrete Namen/Bezeichnungen der Empfänger.
[10] Garantien für den Schutz personenbezogener Daten.
[11] Die Beschreibung einer jeden Maßnahme soll dabei unmittelbar auf die Kategorie betroffener Personen bzw. personenbezogener Daten bezogen werden.

2.4.2 Datenpannen

Gem. Artt. 33, 34 DSGVO muss der Verantwortliche eine Datenschutzverletzung sowohl binnen 72 Stunden der zuständigen Behörde melden als auch den Betroffenen mitzuteilen. Der Verantwortliche dokumentiert Datenschutzverletzung einschließlich aller im Zusammenhang damit stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen. Dabei muss der Verantwortliche auch wissen, welches Risiko eine solche Datenschutzverletzung für die Rechte und Freiheiten natürlicher Personen darstellt, sowie eine Beschreibung der von ihm ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen beifügen.

Dieser Pflicht kann man nur nachkommen, wenn eine solche Dokumentierung im Unternehmen etabliert ist, mithin wenn die Geschäftsführung und die Mitarbeitenden wissen, wer wofür zuständig ist, was eine Datenpanne darstellt, welche Maßnahmen von wem wie vorgenommen werden müssen und wer genau die Datenpanne meldet.

Eine Datenpanne (eine „Verletzung des Schutzes personenbezogener Daten“ in der Terminologie der DSGVO) könnte dabei in folgenden Vorgängen vorliegen:

- zufällige/unbeabsichtigte Datenlöschung, wenn die Daten unwiederbringlich vernichtet werden, ohne dass hierfür ein rechtlicher Grund (wie etwa das Verlangen nach der Löschung oder Ablauf der Frist) vorliegen würde,
- Verlust von personenbezogenen Daten, auch wenn dieser lediglich temporär ist,
- Veränderung der personenbezogenen Daten ohne einen Grund,
- unbefugte Offenlegung bzw. Weitergabe von personenbezogenen Daten (ohne einen rechtlichen Grund),
- unbefugter Zugang zu personenbezogenen Daten (korrekt sind hierfür sogar fehlerhafte Berechtigungskonzepte ausreichend durch die unberechtigte Personen Zugang bekommen könnten),
- u.v.m.

Datenschutzverletzungen sollten fortlaufend dokumentiert werden, damit sowohl das Unternehmen selbst als auch die Aufsichtsbehörden einen Überblick behalten können, zu welchen Verletzungen es bereits gekommen ist, wie diese beseitigt worden sind und welche Risikominimierungsmaßnahmen getroffen worden sind. Notwendig ist die Vornahme technisch-organisatorischer Maßnahmen sowie Schulungen von Mitarbeitenden.

2.4.3 Datenschutz-Folgeabschätzung

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein datenschutzrechtliches Risikomanagement-instrument. Was versteht die DSGVO unter einem Datenschutzrisiko?

Datenschutzrisiko ist ein Risiko bei der Verarbeitung personenbezogener Daten, wenn

- diese zu einem physischen, materiellen oder immateriellen Schaden führen könnte,
- diese zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,
- diese die betroffenen Personen um ihre Rechte und Freiheiten bringt oder sie daran hindert, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden,
- persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden,
- wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Bei der DSFA sollte das Unternehmen (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.

Risikobewertung könnte dabei dem folgenden Muster (aus *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248, Stand 2017)) folgen:

Punkt aus Guidelines	***Vorhanden***
Profiling	
Automatisierte Einzelentscheidung (mit Rechtswirkung)	
Systematische Überwachung	
Besondere Kategorien von persbez. Daten	
Umfangreiche Datenverarbeitung	
Verkettung von Daten	
Besonders schutzwürdige Betroffene	
Neue Technologien/Verarbeitungen	
Hürde für den Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen zu können	

Hinzu kommt noch – spätestens nach der Schrems II Entscheidung des EuGH – die Datenverarbeitung außerhalb der Europäischen Union. Sind wenigstens 5 dieser Punkte vorhanden, muss eine DSFA durchgeführt werden.

Dabei sollte sich diese DSFA mit den Maßnahmen, Garantien und Verfahren befassen, durch die das konkrete Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen. Ein besonderer Augenmerk ist dabei auf umfangreiche Verarbeitungsvorgänge zu richten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und – beispielsweise aufgrund ihrer Sensibilität – wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird. Darüber hinaus sind auch andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren, zu bewerten.

Eine DSFA muss durchgeführt werden, wenn:

- ✓ personenbezogene Daten für Profiling (mit Rechtswirkung) verwendet werden
- ✓ besondere Kategorien von personenbezogenen Daten (wie etwa biometrische Daten oder Daten über strafrechtliche Verurteilungen) verarbeitet werden
- ✓ die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt (bspw. die Betroffenen an der Ausübung ihrer Rechte hindert)
- ✓ die Verarbeitung systematisch in großem Umfang vorgenommen wird
- ✓ öffentlich zugängliche Bereiche systematisch umfangreiche überwacht werden

Insbesondere bei Verwendung neuer Technologien ist regelmäßig eine DSFA geboten.

Die DSFA enthält mindestens folgende Angaben:

- eine Beschreibung der geplanten Verarbeitungsvorgänge
- eine Beschreibung der Zwecke der Verarbeitung
- eine Beschreibung der von dem Verantwortlichen verfolgten berechtigten Interessen, falls zutreffend
- eine Bewertung der Notwendigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- eine Beschreibung der geplanten Abhilfemaßnahmen
- eine Beschreibung der Verfahren, mithilfe derer der Nachweis der Einhaltung der DSGVO erfolgen kann

Der Verantwortliche sollte dabei regelmäßig die Verarbeitungsvorgänge darauf überprüfen, ob diese im Einklang mit der durchgeführten DSFA vorgenommen werden.

Stellt der Verantwortliche bei der Durchführung der DSFA fest, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das nicht durch geeignete Maßnahmen hinsichtlich verfügbarer Technik und Implementierungskosten eingedämmt werden kann, so sollte die Aufsichtsbehörde konsultiert werden, **bevor** ein solcher Verarbeitungsvorgang vorgenommen wird.

Der Prozess einer DSFA könnte den folgenden Schritten folgen:

(1) DSFA-Verantwortung bestimmen (Datenschutzbeauftragte*r, Datenschutz Task Force, operativ tätige Mitarbeitende, etc.)
(2) Den zu bewertenden Verarbeitungsvorgang festlegen und beschreiben
(3) Zwecke der Verarbeitung beschreiben
(4) Betroffene identifizieren
(5) Mitwirkende identifizieren (zB Betriebsrat)
(6) Rechtsgrundlagen der Verarbeitung prüfen und dokumentieren
(7) Notwendigkeit der Datenverarbeitung prüfen und dokumentieren
(8) Verhältnismäßigkeit der Datenverarbeitung prüfen und dokumentieren
(9) Risiken der Datenverarbeitung identifizieren und bewerten
(10) Geeignete Abhilfemaßnahmen (auch die TOMs) bestimmen
(11) DSFA-Bericht erstellen
(12) Verarbeitungsvorgänge implementieren
(13) Abhilfemaßnahmen umsetzen
(14) Wirksamkeit der Verarbeitungsvorgänge und Abhilfemaßnahmen regelmäßig überprüfen und ggf. (bei Änderungen) anpassen

✓ **All diese Vorgänge, Maßnahmen und Bewertung sind dabei sauber zu dokumentieren!**

2.4.4 Interessenabwägung

Werden personenbezogene Daten „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten“ im Sinne des Art. 6 Abs. 1 lit. f DSGVO 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.

Um die Abwägung durchzuführen, sind zunächst die konkreten Interessen des Verantwortlichen an der Verarbeitung konkreter personenbezogener Daten zu identifizieren. Es kann sich dabei beispielsweise um rechtliche (wie etwa Geltendmachung rechtlicher Ansprüche) oder wirtschaftliche (wie etwa Beschleunigung von Betriebsabläufen) Interessen handeln. Ist das konkrete Interesse identifiziert, muss es gewichtet werden und daraufhin geprüft, ob dieses Interesse anderweitig, also ohne Verarbeitung personenbezogener Daten, befriedigt werden kann. Sodann sind die Interessen der Betroffenen zu ermitteln und zu gewichten. Es kann sich dabei beispielsweise um den Schutz der Privatsphäre der Betroffenen oder den Schutz der Kommunikation oder die Selbstbestimmung handeln. Daraufhin sind die Interessen gegeneinander fair abzuwiegen. Bei der Abwägung sollte der Verantwortliche stets versuchen, eigene Interessen nicht zu überschätzen und die Interessen der Betroffenen nicht zu vernachlässigen. Teilweise könnte die Stellungnahme der Betroffenen die ggf. entstehenden Zweifel an der Verarbeitung ausräumen.

Wird bei der Abwägung festgestellt, dass Interessen der Betroffenen ein höheres Gewicht haben und der geplanten Verarbeitung entgegenstehen, müssen anderweitige Möglichkeiten der Datenverarbeitung ermittelt werden (wie etwa eine anonymisierte Datenerhebung) oder von der Verarbeitung abgesehen werden.

Der gesamte Prozess der Abwägung ist dabei sauber zu dokumentieren und bei Bedarf der Aufsichtsbehörde vorzulegen bzw. den Betroffenen nachweisen zu können, dass eine Abwägung tatsächlich stattfand und die Interessen der Betroffenen gebührend berücksichtigt worden sind.

2.4.5 Datenschutzrichtlinie

Die Interne Datenschutzrichtlinie bzw. 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.

Was ist bei der Erstellung der Datenschutzrichtlinie zu beachten?

- **Umfang**: So kurz wie für das jeweilige Unternehmen machbar. Sollte die interne Organisation des Datenschutzes im Unternehmen darstellen, aber sich nicht in Einzelheiten und Beispielen verlieren.
- **Struktur**: Am Anfang bietet sich eine Erklärung an, welchen Wert der Datenschutz im Unternehmen hat. Je nach der Art und Branche des Unternehmens und anderen Aspekten des Einzelfalls können Definitionen sinnvoll sein. Klare Aufteilung in Bereiche bzw. Abteilungen kann vorteilhaft sein, muss aber sinnvoll umgesetzt werden.
- **Sprache**: Klar, präzise, verständlich, transparent.

Inhalt der Datenschutzrichtlinie bzw. des Datenschutzkonzepts:

- ✓ Präambel (mit dem Stellenwert des Datenschutzes und Privacy im Unternehmen)
- ✓ Verantwortung und Kompetenzen bzgl. des Datenschutzes
- ✓ Sensibilisierung und Training
- ✓ Datenschutzorganisation
  - Risikoanalyse
  - Technisch-organisatorische Maßnahmen
  - Auftragsverarbeitung
  - weitere Dokumentation, wie etwa zu Bestellung eine*r Datenschutzbeauftragten
  - Prozesse und Verfahren
- ✓ Kooperation mit der Aufsichtsbehörde
- ✓ Sanktionen
- ✓ Meldung von Datenpannen
- ✓ Kontrolle und Audit
- ✓ Anpassung der Datenschutzrichtlinie

Eine Datenschutzrichtlinie sollte im Wesentlichen den Mitarbeitenden des Unternehmens (sowie allen anderen Personen in einer vergleichbaren Position wie etwa Freelancer, freie Mitarbeiter:innen, in Geschäftsprozesse integrierte Personen aus anderen Unternehmen, Leiharbeiter:innen etc.) Klarheit darüber verschaffen, wie interne Prozesse datenschutzrechtlich konform gestaltet werden und welche Maßnahmen jede/r einzelne/r unternehmen muss, um die Compliance mit der DSGVO zu gewährleisten.

2.4.6 Auftragsverarbeitung

Viele Datenverarbeitungsvorgänge erfolgen nicht durch den Verantwortlichen selbst, sondern durch einen von diesem beauftragten Auftragsverarbeiter. Dies befreit den Verantwortlichen allerdings nicht von der Pflicht, die Datenverarbeitung DSGVO-konform zu gestalten.

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der grundlegende Unterschied zum Verantwortlichen im Sinne der DSGVO liegt dabei darin, dass der Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, wohingegen der Auftragsverarbeiter auf Weisung des Verantwortlichen handelt (Art. 28 Abs. 3 lit. a DSGVO).

Typische Fälle sind:

- Anbieter webbasierter Softwarelösungen (“Software as a Service“), in denen Kunden personenbezogene Daten speichern, wie etwa Software für das „Customer Relationship Management“ (CRM-Systeme), Online Shops, Newsletter und Online-Marketing Software, Bewerbermanagement-Tools, HR-Software, Web-Tracking Anbieter, Online Software für das Projektmanagement oder die Zeiterfassung, Anwendungen im Bereich Fakturierung und Finanzbuchhaltung oder web-basierte ERP-Systeme
- Unternehmen, die für ihre Kunden Backend-Dienste für mobile Apps betreiben und darin Nutzerdaten erfassen, wie etwa Speicherung der E-Mail-Adresse und Einstellungen von App-Nutzern in einem Backend
- Online-Agenturen, die auch das Hosting oder den Betrieb von Webseiten übernehmen, wenn diese personenbezogene Daten verarbeiten, wie etwa Betrieb einer Webseite mit Kontaktformular oder Newsletter-Bestellfunktion
- Sonstige IT-Dienstleister, zu deren Leistungen der Umgang mit personenbezogenen Kundendaten gehört, wie etwa Datenkonvertierungen, Import von Kundendaten in ein ERP-System, Analyse und Auswertung von Kundendaten
- Shared Service Center für IT-Dienste im Konzern, wie etwa IT-Dienstleistungen für alle Konzernunternehmen von einer Tochtergesellschaft (mit Verarbeitung personenbezogener Daten von Mitarbeitenden).

Der Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, sollte dabei nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf **Fachwissen**, **Zuverlässigkeit** und **Ressourcen** – hinreichende Garantien dafür bieten, dass ausreichende DSGVO-konforme technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden.

Denn bei der Prüfung der DSGVO-Compliance des Verantwortlichen wird u.a. auch berücksichtigt, ob der (jeder) Auftragsverarbeiter genehmigte Verhaltensregeln einhält und den Anforderungen der DSGVO genügt.

Die Verarbeitung durch einen Auftragsverarbeiter wird regelmäßig auf Grundlage eines Vertrags erfolgen, der folgende Inhalte unbedingt haben muss:

- ✓ Gegenstand und Dauer der Verarbeitung
- ✓ Art und Zwecke der Verarbeitung
- ✓ Art der personenbezogenen Daten
- ✓ Kategorien von betroffenen Personen
- ✓ Risiken für die Rechte und Freiheiten der betroffenen Personen
- ✓ Aufgaben und Pflichten des Auftragsverarbeiters
- ✓ Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
- ✓ Umgang mit personenbezogenen Daten nach Beendigung der Verarbeitung
- ✓ Vertraulichkeitsverpflichtung (auch für die zur Verarbeitung befugten Personen)
- ✓ Unterstützungsverpflichtung bzgl. Anträge, TOMs etc.
- ✓ Nachweispflicht des Auftragsverarbeiters

Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden.

Ein Muster für die Auftragsverarbeitung finden Sie hier.

2.4.7 Löschkonzept

Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss ein Löschkonzept anzufertigen. Dort sind Löschfristen für alle Arten von personenbezogenen Daten zu bestimmen sowie das Verfahren, wie die Daten insb. in Sondersituationen wie etwa unberechtigte Verarbeitung personenbezogener Daten oder Aufforderung zur Löschung der Daten von Betroffenen gelöscht werden müssen, beschreiben.

Es geht dabei primär darum, dass Löschroutinen etabliert werden, damit personenbezogene Daten, die nichtmehr notwendig sind, entsprechend gelöscht werden können.

Ein Löschkonzept beantwortet mindestens folgende Fragen:

- ? Welche Arten von personenbezogenen Daten werden im Unternehmen erhoben?
- ? Zu welchem Zweck werden welche Daten verarbeitet?
- ? Welchen Löschfristen gelten für welche Art der Daten?
- ? Welche Systeme und/oder Tools werden für die Speicherung und Verarbeitung von Daten verwendet?
- ? Welche Daten und wie werden in Back-Ups gespeichert?
- ? Werden die Daten weitergegeben?
- ? Wer ist für die Löschung der Daten (ggf. in Abteilungen) verantwortlich?
- ? Wer ist für die Dokumentation zuständig?

Bei der Erstellung des Löschkonzepts müssen auch alle „alten“ Daten überprüft und ggf. gelöscht werden.

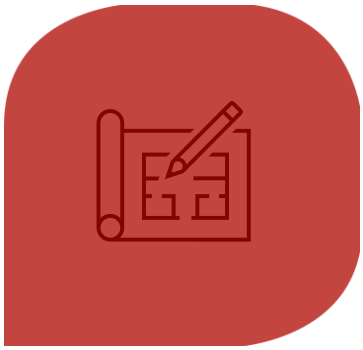
2.4.8 Checkliste: Rechenschaftspflicht

Anhand des Prüfkatalogs „Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO bei (Groß-)Konzernen und Datengetriebenen Unternehmen“ des Bayerischen Landesamtes für Datenschutzaufsicht haben wir eine Checkliste für die Rechenschaftspflicht in Ihrem Unternehmen erstellt:

Maßnahmen und Vorkehrungen	✓
Organisatorische Maßnahmen:	☐
Wir haben eine Datenschutz-Richtlinie bzw. ein Datenschutz-Konzept	☐
Wir haben eine*n Datenschutzbeauftragte*n bestellt	☐
Wir haben der/dem Datenschutzbeauftragten folgende Aufgaben übertragen:	☐
▪ Beratung der Geschäftsführung	☐
▪ Beratung der Fachabteilungen	☐
▪ Sensibilisierung der Mitarbeitenden	☐
▪ Durchführung interner Audits/Kontrollen	☐
▪ Beantwortung/Klärung von Datenschutzbeschwerden	☐
▪ Durchführung von Anfragen zu Betroffenenrechten	☐
▪ Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO)	☐
Uns ist klar, wer im Bereich des Datenschutzes wofür wie zuständig ist, etwa für die Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen oder Erstellung des Verfahrensverzeichnisses	☐
Wir haben Schulungen und andere Weiterbildungsmaßnahmen bzgl. des Datenschutzes eingeführt	
Wir haben interne Kontrollen zur Einhaltung datenschutzrechtlicher Vorschriften eingeführt	☐
Wir wissen, wie wir auf die Berichte der/des Datenschutzbeauftragten reagieren müssen	☐
Wir haben eine Zusammenarbeit der verschiedenen Abteilungen in Datenschutzfragen gut organisiert	☐
Basics:	☐
Wir haben ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) angelegt	☐
Wir wissen, wer von uns das Verzeichnis der Verarbeitungstätigkeiten pflegt	☐
Wir haben datenschutzrechtliche Risiken in das unternehmensinterne Risiko-Managements integriert	☐
Uns ist der Unterschied zwischen unternehmensbezogenen und datenschutzrechtlichen Risiken bewusst	☐
Wir erheben und verarbeiten nur die Daten, die für die Erfüllung des Verarbeitungszwecks notwendig sind	☐
Wir verarbeiten personenbezogene Daten zweckgebunden	☐
DSGVO-Maßnahmen:	☐
Wir haben für jede Verarbeitungstätigkeit eine Rechtsgrundlage i.S.v. Art. 6 Abs. 1 DSGVO und können dies jederzeit nachweisen	☐

Wir dokumentieren Begründungen für die Nutzung der Rechtsgrundlage „berechtigtes Interesse“ i.S.v. Art. 6 Abs. 1 lit. f DSGVO für jede Art von personenbezogenen Daten und jede Verarbeitungstätigkeit	☐
Wir haben ein Einwilligungs-Management (Nachweis und Widerruf der Einwilligung) implementiert	☐
Wir wissen, wer in welcher Situation wie eine Datenschutzfolgenabschätzung durchführen muss	☐
Wir haben ein Löschkonzept, bei dem auch Archive und Backups bedacht worden sind	☐
Wir haben geeignete IT-Sicherheitsmaßnahmen getroffen, um die Verfügbarkeit, Vertraulichkeit und Integrität von personenbezogenen Daten sicherzustellen	☐
Wir überprüfen diese Maßnahmen regelmäßig und passen sie wenn nötig an	☐
Bei der Wahl der Auftragsverarbeiter achten wir darauf, dass diese wirksame und effiziente TOMs umsetzen	☐
Wir schließen mit allen Auftragsverarbeitern Auftragsverarbeitungsvereinbarung ab	☐
Wir anonymisieren personenbezogene Daten, sofern es uns möglich ist	☐
Wir pseudonymisieren personenbezogene Daten	☐
Wir nutzen eine Verschlüsselung für personenbezogene Daten	☐
Betroffenenrechte:	☐
Wir wissen, wie wir auf eine Auskunftsanfrage reagieren	☐
Wir wissen, wie wir die/den Auskunftsersuchenden identifizieren	☐
Wir wissen, wo die personenbezogenen Daten der/des Auskunftsersuchenden zu finden sind	☐
Wir haben unsere Datenschutzerklärung angepasst und passen sie, wenn nötig, auch weiterhin an	☐
Wir wissen, wie wir auf eine Anfrage einer Aufsichtsbehörde reagieren Wir haben die Fristen der DSGVO im Blick	☐
Wir wissen, welche Daten wir (etwa auf einen anderen Dienstleister) übertragen können und welche nicht	☐
Verstöße gegen die DSGVO:	☐
Wir haben keine Verstöße gegen die DSGVO	☐
Wir haben ein Konzept entwickelt, wie etwaige Datenschutzverletzungen in unserem Unternehmen entdeckt werden	☐
Wir haben ein Konzept entwickelt, wie das Risiko unserer Datenschutzverletzung einzustufen ist und ob (und dann auch wie) die Betroffenen informiert werden	☐
Wir haben einen Prozess etabliert, um etwaige Datenschutzverletzungen der Aufsichtsbehörde innerhalb von 72 Stunden zu melden	☐

2.5 TOMs



Technisch-organisatorische Maßnahmen sind notwendig, um einerseits den Datenschutz im Unternehmen überhaupt erst möglich zu machen, und andererseits die DSGVO-Compliance nachzuweisen. Da sie bereits für das Verzeichnis der Verarbeitungstätigkeiten vorgesehen sind, können Sie hier eine (natürlich nicht abschließende) Liste organisatorischer und technischer Maßnahmen sehen, die von Ihrem Unternehmen vorgenommen werden können, um den Datenschutz in Ihrem Unternehmen aufzubauen.

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

Der Sec-O-Mat startet mit einer Befragung zu IT-Sicherheit relevanten Bereichen Ihres Unternehmens. Im Anschluss erhalten Sie Ihren TISiM-Aktionsplan mit konkreten Handlungsempfehlungen und passenden Umsetzungsvorschlägen für Ihre IT-Sicherheit. So haben Sie Ihre IT-Sicherheit immer gut im Blick.

2.5.1 Organisatorische Maßnahmen

Zu den organisatorischen Maßnahmen zählen bspw. Mitarbeitersensibilisierung, Notfallmanagement sowie regelmäßige Notfallübungen, Erstellung einer IT-Sicherheitsstrategie sowie das Erheben der Datensicherheit zur Chefsache. Folgende Maßnahmen wollen wir für Sie hier kurz skizzieren:

- ✓ **Compliance-Organisation aufbauen**

Überprüfen Sie, welche gesetzliche Vorschriften auf Ihr Unternehmen anwendbar sind, und bauen Sie in Ihrem Unternehmen eine solche Organisation auf, die die Erfüllung gesetzlicher Vorschriften durch Unternehmensangehörige sicherstellen kann. Heben Sie klare Kompetenzzuweisung und Aufgabenverteilung hervor und machen die Verantwortung eine*r jeden Mitarbeiter*in für den Erfolg des Unternehmens deutlich. Achten Sie dabei besonders auf den Datenschutz und IT-Sicherheit.

- ✓ **Leitlinien erstellen**

Erstellen Sie klare Leitlinie für den Umgang Ihres Unternehmens mit dem Datenschutz, der IT-Sicherheit und anderen Risiken. Geben Sie klare Handlungsanweisungen und Verfahrenswegen vor.

- ✓ **Schulungen**

Schulen Sie Ihre Beschäftigte im Datenschutz und in der IT-Sicherheit. Achten Sie besonders auf kollektive Annahmen, vermeiden Sie „leere“ und offenkundige Inhalte, konzentrieren Sie sich auf den Schutz unternehmens- und personenbezogener Daten, der für den Erfolg des Unternehmens unabdingbar ist.

✓ Risikomanagement

Ermitteln und bewerten Sie die für Ihr Unternehmen vorhandenen Risiken. Bestimmen Sie Risikovermeidungsmaßnahmen, legen Sie fest, was beim Eintritt eines Risikos passieren soll. Überprüfen Sie Ihr Risikomanagement regelmäßig.

✓ Auf IT-Notfälle vorbereiten

Vom Stromausfall bis zum Angriff auf Ihre IT-Systeme – IT-Notfälle können verheerende Folgen haben. Bereiten Sie sich entsprechend vor: erstellen Sie einen Notfallplan mit Reaktionsmaßnahmen, Abschaltmechanismen und Sperrungen. Klären Sie Ihre Beschäftigten auf, wer und wie im Notfall zu kontaktieren ist.

✓ Kriterien für Dienstleister zusammenstellen

Stellen Sie Mindestanforderungen (wie etwa Mindestverfügbarkeit der IT-Systeme oder Umgang mit IT-Angriffen) für Ihre Dienstleister auf.

✓ Verbindung mit externen Netzwerken regeln

Formulieren Sie klare und verständliche Regeln zur sicheren Verbindung mit offenen WLAN-Netzen oder auch anderen Netzwerken außerhalb Ihres Unternehmens.

✓ Passwortregeln festlegen

Formulieren Sie präzise Regeln zum sicheren Umgang mit Passwörtern in Ihrem Unternehmen.

✓ Meldepflichten beachten

Kommt es zu einem IT-Sicherheitsvorfall oder zu einer Datenpanne, müssen diese ggf. (je nach Branche und Art des Vorfalls) bei einer entsprechenden Aufsichtsbehörde gemeldet werden. Stellen Sie klar, wer die Meldung machen muss, welche Informationen mitgeteilt werden, welche zusätzlichen Schritte vorzunehmen sind. Dokumentieren Sie das und überprüfen Sie regelmäßig, ob diese Verfahren den Verantwortlichen in Ihrem Unternehmen auch geläufig sind.

✓ Informationsaustausch

Bauen Sie ein funktionierendes Informations-Management-System in Ihrem Unternehmen auf. Dort sollen sowohl allgemein Informationen über unternehmensrelevante Sachverhalte reinfließen als auch News zu (neuen) Bedrohungen und Risiken. Wenn nötig, erweitern Sie Ihre Systeme, damit diese Bedrohungen und Risiken so weit wie möglich reduziert werden können.

✓ Mobile Endgeräte sicher einsetzen

Bestimmen Sie, inwiefern in Ihrem Unternehmen *Bring Your Own Device* und anderweitige Nutzung mobiler Endgeräte Ihrer Beschäftigten zulässig sind. Wie werden personenbezogene und unternehmensbezogene daten getrennt? Wie werden Verbindungen hergestellt? Wie ist damit umzugehen?

✓ Privatnutzung klären

Fall in Ihrem Unternehmen die Nutzung der Unternehmenssoft- und -hardware für private Zwecke zumindest geduldet wird, achten Sie darauf, dass Ihre Mitarbeitende die Risiken einschätzen können

und selbst kein zusätzlichen Risiko für die IT-Sicherheit oder für den Datenschutz darstellen. Klären Sie den Umfang dieser Privatnutzung und kontrollieren Sie diese. Hier kann Ihnen eine Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz weiterhelfen.

2.5.2 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 wollen wir für Sie hier kurz skizzieren:

- ✓ **Verschlüsselung einsetzen**

Vertrauliche Informationen müssen besonders geschützt werden. Verschlüsseln Sie Ihre geschäftskritischen Dokumente sowohl bei der Speicherung als auch beim Versand (etwa per E-Mail).

- ✓ **Sichere Einstellungen wählen**

Sorgen Sie für sichere Einstellungen in von Ihnen verwendeten IT-Systemen und Software-Anwendungen. Hierzu gehören z. B. das Entfernen von nicht benötigten Anwendungen, das Vermeiden von Tracking-Cookies, das Sperren vom Bildschirm oder die Nutzung integrierter Sicherheitsmechanismen wie Malware-Erkennung und Code-Signatur-Prüfung.

- ✓ **Schadsoftware verhindern**

Schützen Sie Ihre IT-Systeme so weit wie möglich (etwa mithilfe von Antivirus-Software und anderen Abwehrmechanismen) vor Schadprogrammen.

- ✓ **Schwachstellen finden und schließen**

IT-Systeme werden mit der Zeit immer angreifbarer, da Hacker bisher noch nicht bekannte Schwachstellen finden und diese publik machen. Durch regelmäßige Überprüfungen Ihrer IT-Systeme und Software-Anwendungen können Sie bekannte Schwachstellen aufspüren. Automatisierte Verfahren unterstützen Sie dabei. Schließen Sie die gefundenen Schwachstellen dann schnellstmöglich.

- ✓ **Eigenes Netzwerk absichern**

Sichern Sie daher Ihr Netzwerk ab, damit unbefugte Dritte nicht auf Ihr Netzwerk zugreifen können, etwa indem Sie fremde Geräte in Ihrem WLAN-Netz abweisen oder VPN-Lösungen nutzen.

- ✓ **Software und IT-Systeme aktuell halten**

Eine der größten Bedrohungen ist eine veraltete Software und IT-Systeme. Stellen Sie sicher, dass alle IT-Systeme und Software-Anwendungen stets auf aktuellem Stand sind (überprüfen Sie Updates, ersetzen Sie veraltete Systeme).

- ✓ **Datensicherung durchführen und testen**

Stellen Sie sicher, dass Ihre (unternehmens- und personenbezogene) Daten durch Ausfälle oder Angriffe nicht endgültig verloren gehen. Führen Sie regelmäßig eine Datensicherung durch, überprüfen Sie, ob die gesicherten Daten eine Wiederherstellung Ihrer Systeme ermöglichen.

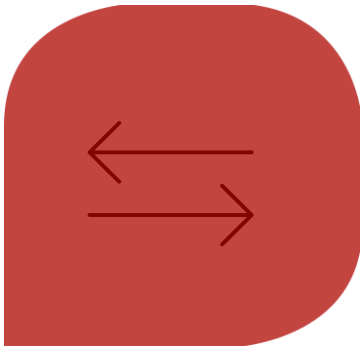
- ✓ **Zugriffsrecht bestimmen**

Um feindliche Angriffe zu vermeiden, erteilen Sie in Ihrem Unternehmen die Berechtigungen aufgrund von Rollen und Positionen, achten Sie auf die Umsetzung des Need-To-Know-Prinzips und stellen Sie sicher, dass bspw. ausgeschiedene Mitarbeitende keine Zugriffsrechte behalten. Dokumentieren Sie Ihre Berechtigungen und stellen Sie sicher, dass Zugriffsrechte schnell erteilt und schnell entzogen werden können.

- ✓ **IT-Administration dokumentieren**

Dokumentieren Sie Befugnisse und Zugriffsrechte Ihrer IT-Administratoren und überprüfen Sie diese regelmäßig.

2.6 Datentransfer



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

Der Europäische Datenschutzausschuss hat bereits zum zweiten Mal 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"**

Jedes Unternehmen muss die eigenen Datentransfers außerhalb der EU kennen. Es geht dabei sowohl um die Datenverarbeitung anhand eines Verarbeitungsauftrags als auch um den Transfer von Daten in eine Cloud außerhalb der EU, Facebook- oder Google-Tracking etc.

Es soll bei diesem Schritt auch gleichzeitig überprüft werden, ob die personenbezogenen Daten, die übertragen werden, tatsächlich für die Erfüllung des Verarbeitungszwecks notwendig sind.

✓ Schritt 2. Transfer-Tools identifizieren

Jedes Unternehmen muss die Grundlage für den Datentransfer (im Sinne von Kap. 5 DSGVO) ermitteln.

Liegt ein Angemessenheitsbeschluss (Art. 45 DSGVO) vor?

Gibt es geeignete Garantien wie etwa Standarddatenschutzklauseln oder Zertifizierung (Art. 46 DSGVO)?

Existieren verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO)?

Liegen für bestimmte Fälle (wie etwa eine explizite informierte Einwilligung der Betroffenen) Ausnahmen vor (Art. 49 DSGVO)?

✓ Schritt 3. Bewertung der Effizienz der gewählten Transfer-Tools

Jedes Unternehmen muss bewerten, inwiefern das Datenschutzniveau der DSGVO im Transfer-Land eingehalten werden kann. Dies ist beispielsweise dann definitiv nicht der Fall, wenn aufgrund nationaler Gesetze des Transfer-Landes die Erfüllung der DSGVO-Vorschriften unmöglich ist (wie etwa dann, wenn nationale Behörden gesetzlich das Recht haben, Zugriff auf personenbezogene Daten zu erhalten). Demensprechend sollte die Prüfung der nationalen Rechtslage im Transfer-Land als erstes erfolgen. Diese Prüfung sollte dabei bezüglich einer jeden konkreten Datenverarbeitung bzw. bezüglich eines jeden Datentransfers erfolgen und auch die Anwendungspraxis im Transfer-Land mitberücksichtigen. Diese Prüfung kann dabei – abhängig von den Zwecken der Datenverarbeitung (zB Marketing oder Durchführung klinischer Studien), der Art von personenbezogenen Daten (Kunden-IP oder Kindergesundheitsdaten), dem Format der Daten (plain text oder verschlüsselt) – sehr unterschiedlich ausfallen. Auch die Möglichkeiten der Auftragsverarbeiter, ihre Pflichten DSGVO-konform zu erfüllen, sollte in die Bewertung einfließen. Am Ende der Bewertung wird entweder feststehen, dass das Transfer-Land personenbezogene Daten DSGVO-konform verarbeiten kann, oder nicht.

Die Bewertung muss (wie auch der gesamte Prozess) sauber dokumentiert werden.

✓ Schritt 4. Vornahme zusätzlicher Schutzmaßnahmen

Ergibt die Bewertung aus dem Schritt 3, dass das Datenschutzniveau der DSGVO nicht eingehalten werden kann, müssen ggf. weitere Möglichkeiten für den Transfer überprüft werden. Es geht dabei explizit um zusätzliche Maßnahmen, also solche, die nicht in Art. 46 DSGVO bereits genannt worden sind. Zusätzliche Maßnahmen sollen verarbeitungsbezogen und konkret sein; können technischer, organisatorischer oder vertraglicher Natur sein. Zu berücksichtigen ist jedoch, dass vertragliche und organisatorische Maßnahmen allein nicht in der Lage sind, gesetzliche Vorschriften des Transfer-Landes außer Kraft zu setzen, sodass in aller Regel zusätzliche technische Maßnahmen (Verschlüsselung, Übertragungstechnik etc.) notwendig sein werden (Beispiele solcher Maßnahmen liefert der Europäische Datenschutzausschuss ab S. 29 der Empfehlungen).

✓ **Schritt 5. Umsetzung**

Nun müssen die im Schritt 4 identifizierten zusätzlichen Maßnahmen tatsächlich umgesetzt werden. So müssen beispielsweise Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften oder Vertragsklauseln implementiert werden.

✓ **Schritt 6. Monitoring**

Die Transfers außerhalb der EU müssen regelmäßig (neu) überprüft werden, insbesondere auch die Effizienz der vorgenommenen Maßnahmen sowie die Rechtsgrundlagen des Transfer-Landes. 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 Urteil) oder aufgrund eigener internen Überprüfung notwendig wird.

2.7 Fachperson für Datenschutz

Eine Fachperson für Datenschutz 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 eine Fachperson für Datenschutz bestellt worden, müssen ihre Kontaktdaten veröffentlicht der Aufsichtsbehörde mitgeteilt werden. Wird eine Fachperson für Datenschutz 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 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 Fachperson für Datenschutz 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 Fachperson für Datenschutz 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 IT-Sicherheit im Kontext des Datenschutzes

3.1 Verhältnis zwischen IT-Sicherheit und Datenschutz

Der Datenschutz zielt auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als Grundrecht ab. Diesem Ziel untergeordnet ist die Gewährleistung der Datensicherheit bei der Verarbeitung personenbezogener Daten, wie Art. 5 Abs. 1 lit. f DSGVO zum Ausdruck bringt: personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. So ist die Datensicherheit unmittelbar von der DSGVO vorgeschrieben und muss deswegen in die internen Prozesse eines jeden Unternehmens integriert werden.

Jede verantwortliche und auftragsverarbeitende Person muss also geeignete technische und organisatorische Maßnahmen treffen, um einen Schutz etwa vor unbefugter oderunrechtmäßiger 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. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch Vernichtung, Verlust, Veränderung oder (unbefugte) Offenlegung/Zugang zu personenbezogenen Daten entstehen.

Unterstützung erfahren die 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 bietet systematisches Vorgehen an und hilft so 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**.

Dieses Verständnis findet sich auch IT-Grundschutz wieder. Im Baustein „CON.2 Datenschutz“ geht das BSI auf das Verhältnis zwischen dem Datenschutz und der Informationssicherheit ein und definiert Abgrenzungsmerkmale zwischen den beiden: „Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes. Dieser legt den Schwerpunkt vorrangig auf die Informationssicherheit und soll die datenverarbeitenden Institutionen schützen. Für die Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss.“ Trotz unterschiedlicher Blickwinkel ist die Umsetzung von IT-Sicherheitsmaßnahmen für den Datenschutz essenziell und unabdingbar, sodass der BSI-Grundschutz und das SDM sich ergänzen. Zusammen helfen sie beim Aufbau von Prozessen, Verfahren und Routinen, die notwendig sind, um die Datenschutz-Compliance zu erreichen und Datensicherheit zu gewähren.

3.2 Checkliste: Konzept für ein Datensicherheitsmanagement

Diese Checkliste soll Ihnen bei der Erstellung (oder auch bei der Anpassung) eines Konzepts des Datensicherheitsmanagements helfen.

I. Verfügbarkeit	
1. Welches Konzept existiert zur Anfertigung von Sicherheitskopien von Daten, Verfahren, Konfigurationen, Datenstrukturen etc.?	
2. Welche Maßnahmen werden zum Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) angewendet?	
3. Sind Server-Räume einbruchs- und brandsicher gebaut?	
4. Gibt es ein Notfallvorsorgekonzept bzgl. IT-Sicherheit? Wurde dies bereits getestet? Ist das (noch) geplant?	
5. Ist es klar, was nach einem Ausfall von IT-Systemen bzw. deren einzelnen Komponenten passiert, wie lange die Wiederherstellung dauern darf, wer hierfür zuständig ist? Wurde dies bereits erprobt?	
6. Sind/werden die Daten strukturiert abgelegt? Wird das regelmäßig überprüft?	
7. Gibt es Maßnahmen bzgl. des redundanten Betriebs von Hard- und Software? Wie sieht die räumliche Situation aus?	
8. Sind Reparaturstrategien und Ausweichprozesse ausgearbeitet worden?	
9. Wie werden fehlende (zB aufgrund eines Urlaubs o. einer Erkrankung) Beschäftigte „ersetzt“ bzw. vertreten? Ist es allen Beschäftigten auch klar?	
II. Integrität	
1. Gibt es ein Datensicherungskonzept, also Bestimmungen über Wiederaufbau der IT im Falle eines (großen) Datenverlustes (etwa wg. technischer Fehler, unbefugter Löschung etc.)? Wird das regelmäßig getestet?	
2. Werden Datensicherungen räumlich getrennt vom Server aufbewahrt? Wie wird dieser Raum abgesichert (Zugang, Zutritt)?	
3. Werden Virenscanner regelmäßig eingesetzt und aktualisiert?	
4. Werden kritischen und Sicherheitsupdates regelmäßig vorgenommen? Wie genau wird das im Unternehmen gewährleistet?	
5. Wie ist es sichergestellt, dass jeder Nutzer*in eigene geheime Passwörter vergibt und verwendet?	
6. Gibt es Verfahren, bei denen ein Authentizitätsnachweis gesetzlich vorgeschrieben ist? Wie wird die Compliance gewährleistet?	
7. Werden Gruppen- oder Funktionskennungen verwendet (nicht empfohlen)?	
III. Vertraulichkeit	
Zutrittsberechtigung	
1. Sind Zutrittsbefugnisse für Gebäude und Räume definiert? Wie wird das gewährleistet? Wie wird das überprüft?	
Zugangsberechtigung	
2. Wurde ein Rollen- und Berechtigungskonzept erarbeitet? Wie wird dieses umgesetzt? Wird das regelmäßig kontrolliert?	
3. Wie ist die Zugangsberechtigung zu Informationen/Daten/Akten geregelt? Wie wird das gewährleistet? Wie wird das überprüft?	

4. Wie ist die Zugangsberechtigung zu IT-Systemen geregelt? Wie wird das gewährleistet? Wie wird das überprüft?	
5. Wie ist die Zugangsberechtigung zu personenbezogenen Daten geregelt? Wird hierbei zwischen den zu löschenden/vernichtenden Daten und den zu speichernden Daten unterschieden? Wie wird das gewährleistet und überprüft?	
6. Wie wird gewährleistet, dass Daten/Informationen/Akten (in beliebigen Formaten) für die Stellen, die ihre Aufgaben persönlich wahrnehmen (wie etwa Personalrat oder DSB), nur diesen selbst zur Kenntnis gelangen?	
7. Wie ist der Umgang mit Datenträgern geregelt?	
8. Ist die Einbindung der/des DSB bei der Einführung neuer IT-Verfahren sichergestellt?	
9. Sind alle notwendigen Auftragsverarbeitungsverträge abgeschlossen worden? Wie wird das gewährleistet?	
10. Ist die (private) Nutzung von Internet und E-Mail am Arbeitsplatz geregelt?	
11. Wie sind Aufgaben und Zugriffsrechte der Administratoren von IT-Systemen geregelt?	
12. Wie werden besondere Sicherheitsbereiche geregelt?	
13. Welche Vorgaben sind bezüglich Datenlöschung vorhanden?	
14. Nach welchen Vorgaben werden Hard- und Software ausgesondert?	
15. Welche Archivierungsregeln sind getroffen worden?	
Sensible Daten	
16. Wie wird sichergestellt, dass besondere Kategorien von personenbezogenen Daten i.S.v. Art. 9 und Art. 10 DSGVO nur unter Umsetzung zusätzlicher TOMs verarbeitet werden? Welche TOMs sind das? Wird das regelmäßig überprüft?	
17. Werden Verarbeitungsvorgänge von besonderen Kategorien von Daten	
Nichtverkettung	
18. Ist ein Rechte- und Rollenkonzept erarbeitet worden, um bestimmte Arten von Verarbeitung einzuschränken?	
19. Wie wird gewährleistet, dass Schnittstellen bei Verarbeitungsverfahren bzw. Komponenten von Software nicht für andere als die vorgesehenen Zwecke benutzt werden können? Gibt es hierfür eine technische Lösung? Wird das regelmäßig überprüft?	
20. Wie wird sichergestellt, dass sog. „Backdoors“ geschlossen werden?	
21. Wie werden verschiedene Abteilung technisch voneinander getrennt, um mögliche Datenzugriffe zu vermeiden?	
22. Werden zweckspezifische Pseudonymisierung- und Anonymisierungsdienste verwendet?	
IV. Transparenz	
1. Werden das Sicherheitskonzept und die sich daraus ergebenden bzw. darauf basierenden Anweisungen, Verfahren, Prozesse etc. regelmäßig überprüft und aktualisiert? Wer ist dafür zuständig? Wie genau und wie häufig erfolgt die Überprüfung?	
2. Existiert eine systematische, nachvollziehbare und aktuelle Dokumentation zur eingesetzten IT?	
3. Wie wird festgestellt, ob DSFA notwendig ist? Wie wird diese durchgeführt und dokumentiert? Wie wird sichergestellt, dass keine Verarbeitung von	

personenbezogenen daten vor der Durchführung der DSFA (falls diese notwendig ist) stattfindet?	
4. Wurden existierende IT-Verfahren einer Risikoanalyse unterzogen? Wie wurde das dokumentiert?	
5. Gibt es Verfahren, die aufgrund rechtlicher Vorschriften ein separates Sicherheitskonzept erfordern? Welche sind das? Ist in einem solchen Sicherheitskonzept der aktuelle Stand der Technik berücksichtigt?	
V. Datenübertragung	
1. Ist die Datenübertragung für alle IT-Verfahren nachvollziehbar dokumentiert?	
2. Sind Datentransfers in die Drittländer überprüft und nachvollziehbar dokumentiert?	
3. Werden alle Beschäftigten, die an Datenübertragungen/Datentransfers beteiligt sind oder sein können, ausreichend geschult?	
4. Werden Datenübertragungen und Datenzugriffe protokolliert? Werden diese Protokolle ausgewertet/kontrolliert?	
VI. Intervinierbarkeit	
1. Wie werden einzelne Informationspflichten aus der DSGVO umgesetzt und die Umsetzung kontrolliert?	
2. Wie werden Einwilligungen, Widerrufe und Widersprüche von betroffenen Personen gespeichert/gehandhabt?	
3. Wie wird Datenschutz-/Einwilligungsmanagement technisch organisiert?	
4. Existieren standardisierte Abfrage- und Dialogschnittstellen für betroffene Personen?	
5. Wie werden (datenschutzrechtlich relevante) Handlungen dokumentiert? Werden sie überprüft?	
6. Werden automatisierte Entscheidungen mit rechtlicher Wirkung oder in ähnlicher Weise erheblicher Beeinträchtigung getroffen? Falls ja, wie sind die Mitwirkungsmöglichkeiten der Betroffenen geregelt? Wie wird sichergestellt, dass der/dem Betroffenen ihre/seine Mitwirkungsmöglichkeiten mitgeteilt werden? Wie wird das dokumentiert?	
7. Können einzelne Funktionen von (IT-)Systemen abgeschaltet werden?	
8. Wie genau ist die operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten sichergestellt?	

4 Schutz von Geschäftsgeheimnissen

4.1 Was sind Geschäftsgeheimnisse?

Wie oben (Kap. 1.1.2) bereits beschrieben, ist ein Geschäftsgeheimnis solche Information,

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Mit dem Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) wurde die Europäische Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung ins deutsche Recht umgesetzt und die früher geltenden §§ 17-19 UWG abgelöst. In diesem Gesetz wurde auch erstmals die gesetzliche Definition eines Geschäftsgeheimnisses vorgenommen.

Grundsätzlich folgt das GeschGehG dem gleichen Schema wie die DSGVO: es müssen bestimmte Schutzmaßnahmen getroffen und darüber hinaus nachgewiesen werden, sodass der subjektive Wille am Schutz bestimmter geschäftlicher (geschäftswichtiger) Informationen durch objektive Geheimhaltungsmaßnahmen flankiert wird. Es ist somit notwendig, zum Schutz von Geschäftsgeheimnissen technische, organisatorische und/oder rechtliche Maßnahmen zu treffen (ganz wie dem Datenschutz im Sinne der DSGVO!). All die getroffenen Maßnahmen müssen auch dokumentiert werden, damit der Schutz entsteht und in einem Streitfall durchgesetzt (u.a. durch Unterlassung der Beeinträchtigung und/oder Schadensersatzansprüche) werden kann.

Je nach der Bedeutung von bestimmten Informationen für das Unternehmen lassen sich unterschiedlich hohe Anforderungen an deren Schutz stellen. Hier darf man sich der Tools des Risikomanagements bedienen: zunächst sind die geheinzuhaltenden Informationen im Unternehmen zu identifizieren, sodann müssen diese in verschiedene Kategorien – je nach deren Bedeutung fürs Unternehmen – klassifiziert werden. Daraufhin sollte die Einstufung folgen und letztlich die Bestimmung konkreter Schutzmaßnahmen bzw. deren Kombinationen.

Eine Einteilung könnte beispielsweise in

- Existenzielle (existenznotwendige) Informationen („Schlüssel-Know-How")
- Strategisch notwendige Informationen, und
- Sonstige wettbewerblich relevante Informationen

vorgenommen werden.

4.2 Welche Schutzmaßnahmen könnten dem Schutz von Geschäftsgeheimnissen dienen?

Welche Schutzmaßnahmen in Betracht kommen, kann u.a. aus § 4 GeschGehG abgeleitet werden, denn dort werden Verbote aufgelistet. So dürfen Geschäftsgeheimnisse nicht durch einen unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, oder durch Verletzung der Geheimhaltungsverpflichtung, oder durch jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht, erlangt werden.

Dementsprechend könnten folgende Schutzmaßnahmen eingesetzt werden:

- Technisch-organisatorische Maßnahmen wie etwa Zugangs- und Zugriffsberechtigungen, Verschlüsselung, Firewalls, 2-Faktor-Authentifizierung, Berechtigungskonzepte, Lese-, Kopier-, Änderungsschutz, technische Einschränkung der Speicherung unternehmensinterner Informationen auf privaten Geräten (hier darf man sich der Schutzmaßnahmen der DSGVO (mehr zu diesen in weiteren Abschnitten dieses Leifadens) durchaus bedienen);
- Vertraulichkeitsvermerke auf Dokumenten/Dateien;
- Arbeitsanweisungen, interne Verhaltensrichtlinien, Schulungen von Mitarbeitenden;
- Geheimhaltungsvereinbarungen mit Vertragspartnern und Mitarbeitenden;
- Fest etablierter Kontrollrahmen mit Kontrollmaßnahmen.

Im Idealfall sollte in jedem Einzelfall geprüft werden, welches Geheimnis mit welchen Maßnahmen wirksam geschützt werden kann. Dabei ist auf die Bedeutung des Geheimnisses und die Angemessenheit der Schutzmaßnahmen besonders zu achten.

Wichtig ist dabei, dass der Gesetzgeber im § 5 GeschGehG einige Ausnahmen aus dem Schutz von Geschäftsgeheimnissen kennt, die eine Offenlegung vertraulicher Informationen durchaus rechtfertigen können. Dies sind (1) die Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, (2) die Aufdeckung einer rechtswidrigen Handlung oder eines Fehlverhaltens, wenn dadurch das öffentliche Interesse geschützt werden kann (mithin Whistleblowing), und (3) die Offenlegung gegenüber der Arbeitnehmervertretung, wenn erforderlich. Dies ist bei der Bestimmung der Schutzmaßnahmen ebenfalls zu berücksichtigen.

Auch wenn sensible unternehmensinterne Informationen in aller Regel keine personenbezogenen Daten darstellen werden, bedient man sich zu deren Schutz gleicher oder ähnlicher Schutzmaßnahmen technischer, organisatorischer und auch rechtlicher Natur. Dies sollte bei der Umsetzung dieser Maßnahmen stets berücksichtigt werden, sodass diese von Anfang an sowohl dem Datenschutz als auch dem Schutz von Geschäftsgeheimnissen dienen können.

4.3 Checkliste: Geschäftsgeheimnisschutz

Ist-Zustand	
- Ermittlung der schützenswerten Informationen	
o Beurteilung und Kategorisierung anhand folgender Indizien: Entwicklungskosten, Marktwert, Marktrelevanz, Wettbewerbsvorteil, Unternehmensgröße	
- Feststellung der bereits bestehenden Schutzmaßnahmen	
o Vertragliche Vereinbarungen mit Arbeitnehmern und Geschäftspartnern, bestehende Strukturen: Geheimhaltungsvorschriften, IT-Sicherheit	
Maßnahmen	
- organisatorisch	
o interne Richtlinien und Anweisungen hinsichtlich Passwortvergabe, Zugangsberechtigungen, Datenweitergabe	
o Ausgestaltung interner Prozesse (Schaffung von need-to-know-Strukturen)	
o Mitarbeiterschulungen (Sensibilisierung um Bewusstsein für den Umgang mit Geschäftsgeheimnissen zu schaffen)	
- technisch	
o Zugangsberechtigungen	
o Passwortschutz	
o Einsatz von Authentifizierungsverfahren, Verschlüsselungstechnik	
o Protokollierungen und Datensicherheit	
o Reglementierung der Nutzung externer Speichermedien (z.B. USB-Sticks)	
- vertraglich	
o Individualvertragliche Verschwiegenheitsverpflichtungen mit Beschäftigten	
o Wettbewerbsverbote in Arbeitsverträgen	
o Geheimhaltungsvereinbarung mit Geschäftspartnern	
o Datennutzungsverträge mit Kooperationspartnern	

5 Datenschutz in Kooperationen

5.1 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 genau Daten später im Laufe der Kooperation noch auszutauschen sind.

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

5.2 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 Umgang mit personenbezogenen Daten innerhalb der Kooperation. Auch zusätzliche technische und organisatorische Maßnahmen sind denkbar, gerade wenn nicht lediglich berufliche E-Mail-Adressen weniger Beschäftigten ausgetauscht werden, sondern beispielsweise Gesundheitsdaten oder Vermögensverhältnisse von Kund*innen.

5.3 Rechtsgrundlage

In aller 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 möglich, mithin nur solche Daten, die für die Kommunikation und die Durchführung der Zusammenarbeit unbedingt notwendig sind.

Beim Austausch personenbezogener Kundendaten ist Vorsicht geboten. Hier ist die Rechtsgrundlage für die Verarbeitung solcher Daten durch den Kooperationspartner von den Zwecken dieser Verarbeitung und der „ursprünglichen“ Rechtsgrundlage der erhebenden Kooperationspartners. Grundsätzlich ist auch hier die Verarbeitung aufgrund eines berechtigten

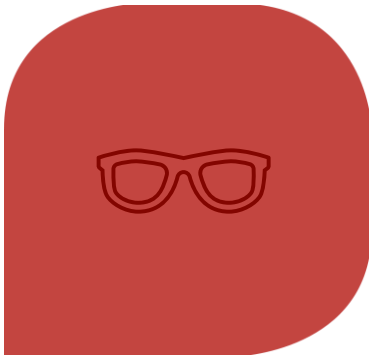
Interesses (Art. 6 Abs. 1 lit. f DSGVO) möglich. Wie auch stets bei Verwendung dieser Rechtsgrundlage, muss auch hier dann die Abwägung zwischen den Interessen des Kooperationspartners und denen der betroffenen Personen nachvollziehbar durchgeführt und dokumentiert werden.

Darüber hinaus kann der Kooperationspartner nach der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) jeder betroffenen Person suchen, beispielsweise dann, wenn die Kooperation den Kund:innen zusätzliche (für diese vorteilhafte) Funktionen anbietet, etwa eine Verschlüsselung, sichere Speicherung oder digitalen Abruf von bestimmten Daten.

5.4 Gemeinsames Konzept zur Datenverarbeitung

Es empfiehlt sich, ein gemeinsames Konzept zur Datenverarbeitung für die Kooperation zu erarbeiten. In diesem können sowohl geschäftsbezogene als auch personenbezogene Daten bedacht und deren Austausch geregelt werden. Gerade für eine auf Dauer ausgelegte Kooperation bietet so ein Konzept eine gute Grundlage: innerhalb der Kooperation kennen die Partner und ihre Beschäftigten ihre Pflichten und Vorgehen im Zusammenhang mit dem Datenaustausch, außerhalb der Kooperation bekommen die Betroffenen einen Überblick über die Verarbeitung ihrer personenbezogenen Daten.

6 Ausblick



Vernetzung und Kooperationen bringen Unternehmen der IT-Wirtschaft stets weiter. Jedoch ist eine ausgewogene Berücksichtigung der Interessen aller Partner in den Verträgen notwendig, um eine nachhaltige Zusammenarbeit zu ermöglichen und potenzielle Konflikte zu vermeiden. Dazu kommen noch allgemeine rechtliche Risiken, deren vertragliche Klärung vor späteren Geldbußen und Rechtsstreitigkeiten schützen soll.

Das Kompetenzzentrum IT-Wirtschaft unterstützt Sie durch Sensibilisierung in kooperationsrechtlichen Fragestellungen sowie durch gezielte Vermittlung von juristischen Kompetenzen und Fertigkeiten. Es entwickelt Vorlagen für die wichtigsten Erklärungen und Vereinbarungen zur Umsetzung von Kooperationsprojekten. Sie sind gesetzeskonform gestaltet, vorausschauend strukturiert und können agil angepasst werden.

7 Unsere Angebote für Ihre Kooperation

Wir, das Kompetenzzentrum IT-Wirtschaft (KIW), unterstützen Sie dabei, systemische Kooperationen in Ihrem Unternehmen umzusetzen. Dazu begleiten wir Ihre Kooperation von der Partnerfindung bis zur konkreten Umsetzung. Sie können aus über 15 Service-Bausteinen, wie Webinaren, Fachvorträgen, Musterdokumenten, Tools (z.B. Matching-Plattform IT2match) und Unternehmenssprechstunden wählen und sich so auf Ihre Kooperation ganz individuell vorbereiten.

Alle unsere Angebote sind leicht und kostenfrei zugänglich!

8 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, Shahadat Rahma – unsplash.com