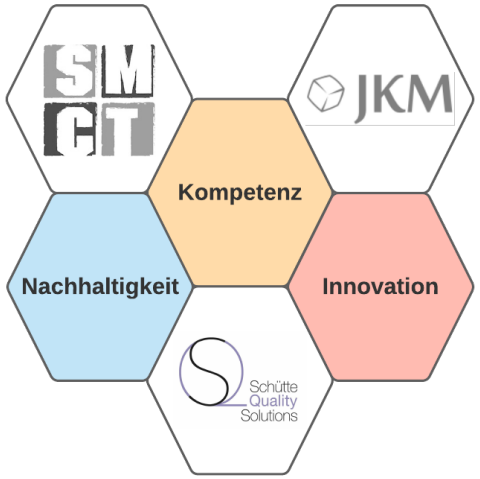
Datenschutz Schulung



Gesetzliche Grundlagen

- DSGVO (Datenschutzgrundverordnung) ist seit dem 25.5.2016 in Kraft getreten und seit dem 25.5.2018 rechtsverbindlich anzuwenden

- BDSG neu ist seit dem 25.5.2018 in Kraft und ergänzt die DSGVO

Gesetzliche Grundlagen

Für wem gelten die Gesetze der DSGVO und BDSG neu?

- In erster Linie betreffen die DSGVO und die Bundesgesetze **nicht-öffentliche** Stellen wie Unternehmen und Großkonzerne
- Aber auch **öffentliche Stellen** wie Ämter und Behörden
- Ausgenommen sind Bereiche die unter (**Artikel 2, Abs.2 DSGVO**) fallen

Einführung

- Die DSGVO ist für alle Unternehmen verbindlich, die **1)** ihren Sitz in der EU haben, **2)** in der EU Daten verarbeiten, **3)** Waren in die EU verkaufen

- Außereuropäische Unternehmen die in einer Niederlassung innerhalb der EU Daten verarbeiten sind ebenso an die DSGVO gebunden, allerdings erstreckt sich die Zuständigkeit nur auf die im EU-Inland ansässige Niederlassung.

- Die EU kann also nicht direkt über Niederlassungen außerhalb der Europäischen Union bestimmen (**Artikel 3, DSGVO**).

Einführung

Ab 25. Mai 2018 gelten in allen Mitgliedstaaten der Europäischen Union neue Datenschutzregeln. Mit der Reform soll sichergestellt werden, dass in allen Mitgliedstaaten derselbe Datenschutzstandard besteht. Da in Deutschland bereits hohe Anforderungen an den Datenschutz gelten, führen die neuen Vorschriften zwar zu zahlreichen formellen Änderungen. Eine inhaltliche Verschärfung der Anforderungen geht mit der Reform jedoch insgesamt nicht einher.

Betriebe müssen sicherstellen, dass sie bis zum 25. Mai 2018 die erforderlichen Anpassungen vornehmen. Die vorliegende Präsentation thematisiert die für die betriebliche Praxis wichtigsten Aspekte und Fragen. Er bietet neben rechtlichen Erklärungen zahlreiche Beispielfälle, Checklisten und Muster, die in der betrieblichen Praxis genutzt werden können.

Zulässige Datenverarbeitung ohne Einwilligung

Wann ist die Nutzung von Daten erlaubt?

Eine Datennutzung ist nur zulässig, wenn

- Eine gesetzliche Vorschrift diese erlaubt oder
- Derjenige, dessen Daten verarbeitet werden sollen, in die Nutzung von Daten einwilligt

Gesetzliche Erlaubnis zur Datennutzung

Vorschriften, die eine Datennutzung erlauben, finden sich hauptsächlich in **Artikel 6** der Europäischen Datenschutz-Grundverordnung (DSGVO). Diese Regelungen werden durch die §§ 22, 24, 26 des Bundesdatenschutzgesetzes (BDSG) ergänzt.

Gemäß **Art. 6 DSGVO** ist eine Datenverarbeitung ohne Einwilligung zulässig, wenn die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist (z.B. Adresse des Kunden, um den Auftrag vor Ort beim Kunden ausführen zu können).

Beispiele Datennutzung

Zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (z.B. E-Mail-Adresse, um dem Kunden nach seinem Wunsch einen Kostenvoranschlag senden zu können).

Zur Wahrung berechtigter Interessen des Betriebes oder eines Dritten erforderlich ist und die Interessen der betroffenen Person nicht überwiegen (z.B. die Auswertung der Kundendatei, um bestimmte Kunden zielgerichtet mit Werbung anzusprechen).

Gesetzliche Erlaubnis

Beachte:

Die Datennutzung zur Direktwerbung ist zulässig. Allerdings dürfen Betroffene der Werbung jederzeit widersprechen (**Art. 21 Absatz 2 DSGVO**). Für Werbung per E-Mail ist weiterhin eine **Einwilligung** erforderlich.

Gesetzliche Erlaubnis

Die Verarbeitung personenbezogener Daten von Arbeitnehmern konkretisiert **§ 26 BDSG**. Hiernach ist eine Verarbeitung zulässig, wenn es:

- Zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist (z.B. Speicherung von Lohnunterlagen und Krankheitstagen).

- Zur Ausübung der Interessensvertretung der Beschäftigten erforderlich ist (z.B. Weiterleitung von Arbeitnehmerdaten an den Betriebsrat).

Verwendung von Gesundheitsdaten

Gesundheitsdaten (z.B. Dioptrienzahl, Gehörschädigung etc.) gelten als besonders schutzwürdige Daten (**Art. 9 DSGVO**). Für Betriebe der Gesundheitshandwerke folgt die Berechtigung zur Verarbeitung von Gesundheitsdaten aus § 22 Abs. 1 Nr. 1 b) BDSG. Diese Vorschrift erlaubt die Verarbeitung von Gesundheitsdaten.

- zum Zweck der Gesundheitsvorsorge
- zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich
- wenn es für einen Vertrag zwischen der betroffenen Person und einem Angehörigen eines Gesundheitsberufs erforderlich ist

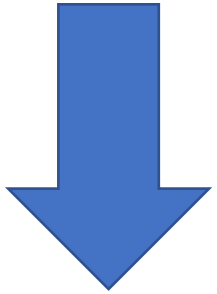
Einwilligung müssen freiwillig sein

Eine Einwilligung ist nur dann rechtmäßig, wenn derjenige, der die Einwilligung erklärt, dies freiwillig tut. Jede Form von Druck, Zwang oder Verpflichtung führt deshalb zur Unwirksamkeit der Einwilligung.

Eine Einwilligung gilt unter anderem bereits als unfreiwillig, wenn der Abschluss eines Vertrags oder die Erbringung einer Leistung von der Abgabe der Einwilligungserklärung abhängig gemacht wird und der Kunde keine Möglichkeit hat, die Leistung auf andere Weise zu erlangen.

Besonderheiten bei Minderjährigen

Die Wirksamkeit einer Einwilligung ist nicht vom Alter des Einwilligenden abhängig. Insofern spielt es an sich keine Rolle, ob es sich um einen Minderjährigen oder einen Volljährigen handelt. Für die Wirksamkeit der Einwilligung ist allein die Einsichtsfähigkeit des Einwilligenden in die Tragweite seiner Erklärung maßgeblich. Der Einwilligende muss erkennen können, welche Folgen die Einwilligung für ihn hat.



Ob Minderjährige diese Einsichtsfähigkeit besitzen, kann nicht pauschal beurteilt werden, sondern richtet sich nach den Umständen des Einzelfalls. Da die Einsichtsfähigkeit eines Minderjährigen nicht in Fall mit abschließender Sicherheit beurteilt werden kann, empfiehlt es sich in der Praxis, bei Minderjährigen stets die Einwilligungserklärung der Erziehungsberechtigten einzuholen.

Einwilligung in Textform

Einwilligungen müssen – anders als früher – nicht mehr schriftlich erklärt werden. Eine mündliche Einwilligung ist deshalb in gleicher Weise wirksam. Allerdings sollte die Einwilligungserklärung allein aus Beweis- und Dokumentationsgründen stets in Textform eingeholt werden.

Die gewählte Form der Einwilligung ist zugleich Maßstab für den Fall, dass die Einwilligung widerrufen wird. Wurde die Einwilligung mündlich erteilt, muss ein mündlich erklärter Widerruf akzeptiert werden.

Die Dokumentation mündlicher Erklärungen ist allerdings aufwändig, fehleranfällig und für effiziente Betriebsabläufe nicht zu empfehlen.

Inhalt Einwilligungserklärung

Die gesetzlichen Vorschriften geben klare Mindestanforderungen an Einwilligungen vor.

- Der Daten Verarbeiter muss seine Identität offenlegen (Angabe des Namens bzw. der Firma)
- Es muss dargelegt werden, welche Daten erhoben werden (z.B. Adressdaten, Kontodaten)
- Es muss der Zweck genannt werden, für den die Daten verarbeitet werden (z.B. Werbung, Weitergabe an Dritte)
- Hinweis auf das Widerrufsrecht: Der Einwilligende hat die Einwilligung freiwillig erklärt und kann sie jederzeit mit Wirkung für die Zukunft widerrufen. Es ist anzugeben, in welcher Form (Textform) und an welche Adresse (Postanschrift, E-Mail- Adresse) der Widerruf zu richten ist

Inhalt Einwilligungserklärung

Die Angaben müssen verständlich und in klarer, einfacher Sprache formuliert werden. Sie müssen so konkret und so umfassend sein, dass sich der Einwilligende darüber ein Bild machen kann, was mit seinen Daten passiert.

Formelle Pflichten in Betrieben

Informationspflichten (Art. 13 und 14 DSGVO)

Art. 13 regelt, welche Informationen der Verantwortliche dem Betroffenen zu erteilen hat, wenn er beim Betroffenen Daten erhebt. Art. 14 bestimmt die Informationspflichten, wenn die Daten nicht bei der betroffenen Person selbst, sondern bei einem Dritten erhoben werden.

Formelle Pflichten in Betrieben

Auskunftsrecht (Art. 15 DSGVO)

Betroffene haben das Recht, vom datenverarbeitenden Betrieb eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind und verarbeitet werden.

Ist das der Fall, hat der Betrieb Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Kunden auf Betriebe zukommen

Formelle Pflichten in Betrieben

Recht auf Berichtigung (Art. 16 DSGVO)

Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, haben die betroffenen Personen gemäß Art. 16 ein Recht auf Berichtigung. Der verantwortliche Daten Verarbeiter muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.

Formelle Pflichten in Betrieben

Recht auf Löschung (Art. 17 DSGVO)

Nach Art. 17 haben Betroffene das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich geregelten Löschungsgründe vorliegt. Ein solcher Grund liegt vor, wenn:

- die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist,
- die Daten unrechtmäßig verarbeitet wurden,
- der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat.

Formelle Pflichten in Betrieben

Recht auf Löschung (Art. 17 DSGVO)

Selbst wenn einer der vorgenannten Gründe vorliegt, dürfen Daten aber nicht gelöscht werden, wenn gesetzliche Aufbewahrungsfristen bestehen und der Verantwortliche damit zur Aufbewahrung verpflichtet ist (z.B. bei rentenrelevanten Unterlagen von Mitarbeitern).

Anstelle einer Löschung tritt die sog. Einschränkung der Verarbeitung gemäß § 35 BDSG, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse des Betroffenen an der Löschung als gering anzusehen ist (siehe hierzu unten).

Formelle Pflichten in Betrieben

Recht auf Vergessenwerden (Art. 17 DSGVO)

Eine besondere Form des Löschungsanspruchs ist das „Recht auf Vergessenwerden“. Dieses Recht bezieht sich auf Daten, die veröffentlicht wurden und zielt insbesondere auf Veröffentlichungen im Internet ab. Für Betriebe dürfte dies in der Praxis jedoch keine große Rolle spielen.

Formelle Pflichten in Betrieben

Recht auf Beschwerde Artikel 77 DSGVO

Der Betroffene hat das Recht auf Beschwerde bei derAufsichtsbehörde

Die Beschwerde ist dann begründet, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

Formelle Pflichten in Betrieben

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Mit dem Recht auf Einschränkung der Verarbeitung können Betroffene in bestimmten Fällen erwirken, dass der Daten Verarbeiter ihre Daten sperrt und somit nicht weiter verarbeiten darf. Dies gilt u.a. für den Fall, dass

- die Richtigkeit gespeicherter Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll,
- die Datenverarbeitung unrechtmäßig ist und der Betroffene anstatt der Löschung die Nutzungseinschränkung bevorzugt.

Formelle Pflichten in Betrieben

Pflicht zur Datenübertragung (Art. 20 DSGVO)

Das Recht auf Datenübertragung gibt Betroffenen unter bestimmten Voraus-setzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten. Der Betroffene hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“.

Die Regelung soll den Wechsel zu einem anderen Anbieter insbesondere bei sozialen Netzwerken oder Verträgen mit Energieversorgern, Banken und Versicherungen erleichtern. Für Betriebe wird dieses Recht jedoch keine Praxisrelevanz haben.

Formelle Pflichten in Betrieben

Widerspruchsrecht (Art. 21 DSGVO)

Betroffenen steht ein Widerspruchsrecht gegen eine Verarbeitung ihrer Daten zum Zweck der Direktwerbung zu. Obwohl die Nutzung von Daten zur Direktwerbung zulässig ist, können betroffene Personen hiergegen jederzeit und ohne Angabe von Gründen widersprechen.

Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zur Direktwerbung genutzt werden.

Formelle Pflichten in Betrieben

Dokumentationspflicht (Art. 30 DSGVO)

Betriebe sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „**Verzeichnis von Verarbeitungstätigkeiten**“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden.

Erweist sich eine beabsichtigte Datennutzung als risikoreich, ist zusätzlich eine **„Datenschutz-Folgenabschätzung**“ nach Art. 35 DSGVO vorzunehmen.

Formelle Pflichten in Betrieben

Bewerberdaten

- Bewerberdaten nur für Auswahlentscheidung der Stelle verwenden, auf die sich Bewerbung bezieht
- Bewerberdaten nur Mitarbeitern zugänglich machen, die mit Auswahl-entscheidung befasst sind

Formelle Pflichten in Betrieben

Bewerberdaten

Nach Abschluss der Auswahlentscheidung und Nichteinstellung des Bewerbers:

- Bewerberdaten 3 Monate nach Eingang Bewerbung löschen
- Bewerberpool: Schriftliche Einwilligung des Bewerbers
- Löschung 6 Monaten nach Einwilligung

Informationspflicht bei Erhebung personen-bezogener Daten

Transparenz durch Informationen

Personen, deren Daten von einem anderen verarbeitet werden, sollen im Vorlauf zur Datenverarbeitung informiert werden. Insbesondere sollen sie erfahren, welche Daten über sie erhoben und zu welchem Zweck sie genutzt werden.

Um diese Transparenz herzustellen, sind Betriebe verpflichtet, den jeweils betroffenen Personen zahlreiche Informationen über die beabsichtigte Datennutzung zu erteilen.

Welche Informationen dies im Einzelnen sind, ist in den **Art. 13 und 14** der Europäischen Datenschutz-Grundverordnung (DSGVO) aufgelistet, die durch §§ 32 und 33 des Bundesdatenschutzgesetzes (BDSG) ergänzt werden.

Informationspflicht bei Erhebung personen-bezogener Daten

Bei den Informationspflichten sind drei Situationen zu unterscheiden:

- Die Daten werden bei der Person, deren Daten verarbeitet werden sollen, direkt erhoben.
- Die Daten, die verarbeitet werden sollen, werden nicht bei der betroffenen Person selbst, sondern von einem Dritten erhoben.
- Der Daten Verarbeiter hat die Daten bereits vorliegen und möchte die Daten zu einem anderen Zweck nutzen, als zu dem, zu dem sie ursprünglich bei der betroffenen Person erhoben wurden.

Informationspflicht bei Erhebung personen-bezogener Daten

Erhebung personenbezogener Daten beim Betroffenen selbst (Art. 13 DSGVO)

Werden personenbezogene Daten bei Betroffenen direkt erhoben (z.B. von Kunden oder Besuchern von Webseiten), müssen diesen folgende Informationen mitgeteilt werden:

Identität des Verantwortlichen: Name und Kontaktdaten des Daten Verarbeiters (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers).

Kontaktdaten des Datenschutzbeauftragten (DSB): Dies gilt nur, sofern ein DSB bestellt ist. Der Name des DSB ist hierbei nicht zwingend zu nennen.

Informationspflicht bei Erhebung personen-bezogener Daten

Zweckänderung

Für den Fall, dass der Verantwortliche die Daten bereits vorliegen hat und für einen anderen Zweck weiterverarbeiten möchte, muss er die betroffenen Personen vor der Weiterverarbeitung über folgende Aspekte informieren:

- den neuen Zweck der Verarbeitung, die Dauer der Verarbeitung
- die Rechte des Betroffenen,
- Beschwerderecht

Informationspflicht bei Erhebung personen-bezogener Daten

Wann ist zu informieren?

Im Fall der Datenerhebung beim Betroffenen müssen die Informationen zum Zeitpunkt der Datenerhebung mitgeteilt werden.

Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilen.

Bei einer Zweckänderung ist der Betroffene vor der Verwendung der Daten zum neuen Zweck zu unterrichten.

Informationspflicht bei Erhebung personen-bezogener Daten

Drohen bei Verstößen Sanktionen?

Verstöße gegen die datenschutzrechtlichen Informationspflichten können gemäß Art. 83 Abs. 5 DSGVO Strafen in Höhe von bis zu 20 Mio. EUR oder vier Prozent des Weltjahresumsatzes ausgesprochen werden.

Erteilung von Auskünften

Das Auskunftsrecht

Das Datenschutzrecht gewährt Personen, deren Daten verarbeitet werden, umfassende Rechte. Eines dieser Rechte ist das Auskunftsrecht. Das Auskunftsrecht ist in Art. 15 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt und wird durch § 34 Bundesdatenschutzgesetz (BDSG) ergänzt.

Hiernach haben Betroffene das Recht, vom datenverarbeitenden Betrieb eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind oder verarbeitet werden. Ist das der Fall, hat der Betrieb Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Kunden auf Betriebe zukommen.

Erteilung von Auskünften

Inhalt der Auskunft

Verlangt der Antragsteller eine pauschale Auskunft über seine Daten, sind sämtliche vom Gesetz vorgesehene Informationen zu erteilen. Dies sind im Einzelnen:

- Alle über den Betroffenen gespeicherten Daten (z.B. Name, Anschrift, E-Mail-Adresse, Bankverbindung).
- Die Kategorien der Daten, die verarbeitet werden (z.B. Vertragsdaten, Adress- und Kontaktdaten).
- Die Bezeichnung der Datei (z.B. Kundendatei, Neukunden)

Erteilung von Auskünften

Angaben über die Herkunft der Daten (z.B. Daten wurden beim Betroffenen selbst erhoben, Daten wurden von einem Dritten gekauft).

- Die Empfänger, an die die Daten weitergeleitet wurden
- Die geplante Dauer, für die die Daten gespeichert werden (i.d.R. sind Daten so lange zu speichern, bis sie nicht mehr benötigt werden)
- Der Zweck der Speicherung, d.h. aus welchem Grund werden die Daten gespeichert? (z.B. Nutzung zur Direktwerbung)

Erteilung von Auskünften

Zusätzlich zu den vorgenannten Angaben über die gespeicherten Daten, sind u.a. weitere Informationen zu den Rechten des Betroffenen zu erteilen:

- Hinweis auf das Bestehen eines Rechts auf Berichtigung oder Löschung (Art. 16 DSGVO) oder auf eine Einschränkung der Verarbeitung (Art. 18 DSGVO)

- Das Bestehen eines Beschwerderechts des Betroffenen bei der Daten-schutzaufsichtsbehörde.

Erteilung von Auskünften

Verfahren der Auskunftserteilung

Der Betrieb hat sich vor Erteilung der Auskunft über die Identität des Antragstellers zu vergewissern. Der Antragsteller und die betroffene Person, deren Daten gespeichert sind, müssen identisch sein. Wie die Identitäts-prüfung erfolgt, bestimmt der Betrieb.

Erteilung von Auskünften

Kann die Auskunft insgesamt verweigert werden?

Neben einer Verweigerung wegen überwiegender Geschäftsgeheimnisse kommt eine vollständige Verweigerung der Auskunft nur in Betracht, wenn die Auskunft unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Wird die Auskunft verweigert, ist dies zu begründen.

Dokumentationspflicht

Weshalb ist eine Dokumentation nötig?

Betriebe, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „**Verzeichnis von Verarbeitungstätigkeiten**“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden.

Auf Grundlage dieser Übersicht sollen sich Betriebsinhaber über das Ausmaß und die Intensität der betrieblichen Datenverarbeitung bewusst werden.

Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind in **Artikel 30** der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt.

Dokumentationspflicht

Was ist zu dokumentieren?

Nach **Art. 30 DSGVO** sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten betrieblichen Situationen vorkommen

(z.B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera im Betrieb).

Ablauf der Dokumentationspflicht

Schritt 1: Risikobewertung

Im ersten Schritt ist zu bewerten, ob die Datenverarbeitung ein hohes oder geringes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind (z.B. betriebliche Videoüberwachung mit Blick auf eine öffentliche Straße).

Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten, ethnische Herkunft, religiöse Zugehörigkeit) umfangreich verarbeitet werden. Dies ist bei Betrieben gewöhnlich nicht der Fall. Ausnahmen sind in der Regel jedoch Betriebe der Gesundheitshandwerke oder große Betriebe mit vielen Mitarbeitern, die in der Personalabteilung solche Daten umfangreich verarbeiten.

Ablauf der Dokumentationspflicht

Sollte ausnahmsweise ein hohes Risiko bestehen, ist eine „Datenschutz-Folgenabschätzung“ vorzunehmen. Die Anforderungen dieser Folgenabschätzung richten sich nach **Art. 35 DSGVO** und umfassen folgende Prüfungspunkte:

- eine Beschreibung der geplanten Verarbeitungsvorgänge,
- eine Beschreibung der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit der Verarbeitungsvorgänge,
- eine Bewertung der Risiken für die Personen, deren Daten verarbeitet werden sollen,
- eine Beschreibung der Maßnahmen, die zur Bewältigung der Risiken vorgesehen werden.

Ablauf der Dokumentationspflicht

Schritt 2: Erstellen des Verarbeitungsverzeichnisses

Art. 30 DSGV zählt die Punkte auf, die in einem Verarbeitungsverzeichnis enthalten sein müssen. Dies sind im Einzelnen:

- **Name und die Kontaktdaten des Betriebs** (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers)
- **Name und Kontaktdaten des Datenschutzbeauftragten** (DSB): Nur erforderlich, wenn ein DSB bestellt wurde,
- **Zwecke der Verarbeitung**: Z.B. für Werbemaßnahmen oder zur Abwicklung eines Vertrags,
- Beschreibung der **Kategorien betroffener Personen**: Z.B. Kunden, Mitarbeiter, Zulieferer etc.

Ablauf der Dokumentationspflicht

- Beschreibung der Kategorien personenbezogener Daten: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?

- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden: Gilt nur, wenn die Daten an Dritte weitergeleitet werden (z.B. Weitergabe von Daten an die Creditreform).

- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien: In der Regel gilt, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden.

- Wenn möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen

Dokumentationspflicht

Technische und organisatorische Maßnahmen

- Betriebe sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken zu begegnen, die mit der Datenverarbeitung einhergehen. § 64 Bundesdatenschutzgesetz zählt zahlreiche Maßnahmen auf, die zu berücksichtigen sind. Diese lassen sich thematisch auf folgende Kernmaßnahmen zusammenfassen:

Vertraulichkeit der Datenverarbeitung (u.a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle)

- Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden (z.B. Abschließen des Serverraums).

Betrieblicher Datenschutzbeauftragter

Gesetzliche Verpflichtung

Die Anforderungen an den betrieblichen Datenschutzbeauftragten ergeben sich aus den Artikeln 37 bis 39 der Europäischen Datenschutz-Grundverordnung (DSGVO) und § 38 Bundesdatenschutzgesetz (BDSG).

Betrieblicher Datenschutzbeauftragter

Welcher Betriebe muss einen Datenschutzbeauftragten benennen?

Sind im Betrieb mindestens 20 Personen angestellt, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein DSB zu benennen. Automatisierte Verarbeitung ist z.B. die Nutzung digitaler Kundendateien oder die Verwendung von Kundendaten auf einem Tablet-PC oder Smartphone.

Als **„ständig befasst“** gelten nur solche Mitarbeiter, deren alltägliche Kerntätigkeit die Verarbeitung von Daten ist. Dies ist z.B. bei Mitarbeitern der Lohnbuchhaltung oder der Personalabteilung der Fall. Mitarbeiter, die lediglich die Daten zur Ausübung ihrer betrieblichen Tätigkeit benötigen, fallen grundsätzlich nicht unter diese Regelung.

Für mehrere Standorte bzw. Filialen kann ein einziger DSB bestellt werden. Hierbei ist zu beachten, dass die Anzahl der Filialen nur so hoch sein darf, dass der DSB seine Aufgaben in jeder Filiale realistisch erfüllen kann.

Auftragsverarbeitung

Was ist eine Auftragsverarbeitung?

Eine Auftragsverarbeitung liegt vor, wenn ein Betrieb zwar personenbezogene Daten für seine Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung dieser Daten aber nicht selbst durchführt, sondern von einem Dienstleister vornehmen lässt.

Der Dienstleister verarbeitet die Daten für und im Auftrag des Betriebs. Dies ist z.B. bei Anbietern von Cloud-Lösungen der Fall, die auf ihren Servern Daten für den Betrieb speichern. Dasselbe gilt für Lohnbuchhaltungsanbieter, die für den Betrieb die Lohnbuchhaltung erstellen und dabei z.B. Mitarbeiterdaten verarbeiten.

Auftragsverarbeitung

Ist die Auftragsverarbeitung gesetzlich geregelt?

- Die Auftragsverarbeitung ist hauptsächlich in **Art. 28** der Datenschutz-Grundverordnung (DSGVO) geregelt. Darüber hinaus enthält die DSGVO vereinzelte Vorschriften, die jedoch für Handwerksbetriebe nicht einschlägig sind.

- Das Gesetz bezeichnet den Dienstleister als „Auftragsverarbeiter“. Der beauftragende Betrieb wird „**Verantwortlicher**“ genannt, da er die Daten nutzt und damit trotz Einschaltung eines Dienstleisters auch für die Rechtmäßigkeit der Datenverarbeitung einstehen muss und verantwortlich bleibt.

- Deshalb haften bei Datenschutzverstößen Auftragsverarbeiter und Verantwortlicher gemeinsam.

Auftragsverarbeitung

Ist bei der Auftragsverarbeitung eine besondere Form zu beachten?

Art. 28 DSGVO schreibt keine besondere Form vor. In der Praxis ist es jedoch allein wegen der Dokumentation und aus Beweisgründen empfehlenswert, einen Vertrag in Textform zu schließen. So kann der Vertrag in elektronischen Formaten (z.B. PDF) oder schriftlich in Papierform geschlossen werden.

Danke für Ihre Aufmerksamkeit

Diese Datenschutzschulung wurde gewissenhaft und unter Einbeziehung von der DSGVO und BDSG neu erstellt. Sollten sich Fehler oder bereits im Gesetz Aktualisierungen zum Zeitpunkt der Erstellung ergeben haben, übernehme ich keine Gewähr für die Richtigkeit der Angaben.

Bitte überprüfen Sie die Anforderungen ggf. gegenüber der DSGVO und BDSG neu.