Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO (Datenschutz-Grundverordnung) ist eine europäische Datenschutzverordnung, die im Mai 2018 in Kraft getreten ist. Sie legt einheitliche Regeln für den Schutz personenbezogener Daten in der Europäischen Union fest. Als Datenschutzbeauftragter ist es wichtig, die Grundsätze und Anforderungen der DSGVO zu verstehen und in der Praxis umzusetzen.

Datenschutzgrundverordnung

Grundlegende Prinzipien der DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben:
  Die Verarbeitung personenbezogener Daten muss auf einer rechtlichen Grundlage beruhen und in einer fairen und transparenten Weise erfolgen.

- Zweckbindung:
  Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Sie dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist.

- Datenminimierung:
  Es dürfen nur die personenbezogenen Daten erhoben werden, die für den jeweiligen Zweck erforderlich sind. Es sollte eine möglichst geringe Menge an Daten verarbeitet werden.

- Richtigkeit:
  Die verarbeiteten personenbezogenen Daten müssen richtig und gegebenenfalls auf dem neuesten Stand sein. Angemessene Maßnahmen sollten ergriffen werden, um sicherzustellen, dass unrichtige oder unvollständige Daten gelöscht oder berichtigt werden.

- Speicherbegrenzung:
  Personenbezogene Daten sollten nur für den Zeitraum gespeichert werden, der für den Zweck der Verarbeitung erforderlich ist. Die Daten müssen anschließend gelöscht oder anonymisiert werden.

- Integrität und Vertraulichkeit:
  Es müssen angemessene technische und organisatorische Maßnahmen ergriffen werden, um die Sicherheit der

personenbezogenen Daten zu gewährleisten und sie vor unbefugtem Zugriff, Verlust oder Offenlegung zu schützen.

- Rechenschaftspflicht: Der Verantwortliche für die Datenverarbeitung muss nachweisen können, dass die Grundsätze der DSGVO eingehalten werden. Es sollten geeignete Protokolle und Dokumentationen geführt werden, um die Einhaltung zu belegen.

Wichtige Begrifflichkeiten

Der Artikel 4 der Datenschutz-Grundverordnung (DSGVO) definiert wichtige Begriffe, die in der Verordnung verwendet werden. Diese Definitionen sind entscheidend, um ein einheitliches Verständnis der relevanten Termini sicherzustellen. Im Folgenden erläutere ich einige der zentralen Definitionen aus Artikel 4:

- "Personenbezogene Daten"
  Dieser Begriff umfasst alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören beispielsweise Namen, Identifikationsnummern, Standortdaten, Online-Identifikatoren oder bestimmte physische, genetische, wirtschaftliche, kulturelle oder soziale Merkmale.

- "Verarbeitung"
  Dieser Begriff bezieht sich auf jede Operation oder Reihe von Operationen, die an personenbezogenen Daten durchgeführt werden, sei es automatisiert oder nicht. Dazu gehört das Erheben, Erfassen, Organisieren, Strukturieren, Speichern, Anpassen, Abrufen, Konsultieren, Verwenden, Offenlegen, Übermitteln, Verbreiten, Löschen oder Vernichten von Daten.

- "Verantwortlicher"
  Dies bezeichnet die natürliche oder juristische Person, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt. Der Verantwortliche trägt die Hauptverantwortung für die

Einhaltung der Datenschutzbestimmungen.

- "Auftragsverarbeiter"
  Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter handelt gemäß den Anweisungen des Verantwortlichen und unterliegt vertraglichen Verpflichtungen zur Gewährleistung des Datenschutzes.

- "Einwilligung"
  Dieser Begriff bezieht sich auf die freiwillige, informierte und eindeutige Willensbekundung der betroffenen Person, ihre personenbezogenen Daten für einen bestimmten Zweck zu verarbeiten. Die Einwilligung muss aufklaren und verständlichen Informationen beruhen und kann jederzeit widerrufen werden.

- "Datenverletzung"
  Eine Datenverletzung tritt auf, wenn personenbezogene Daten unrechtmäßig verarbeitet, gelöscht, verloren, verändert oder offengelegt werden. Im Falle einer Datenschutzverletzung müssen geeignete Maßnahmen ergriffen werden, um die betroffenen Personen zu informieren und die Behörden zu benachrichtigen, falls erforderlich.

Das Wichtigste zur EU-Datenschutzgrundverordnung in Kürze

- Die neue europäische Datenschutzgrundverordnung trat bereits am 24. Mai 2016 in Kraft. Ab dem 25. Mai 2018 sind die hierin enthaltenen Maßgaben zum Datenschutz verbindlich in den jeweiligen Mitgliedstaaten anzuwenden – auch ohne die separate Übertragung in nationales Recht.

- Gestärkt werden sollen durch die europäische Datenschutzverordnung vor allem die Verbraucherrechte.

Datenverarbeitende Stellen müssen mit strengeren Regulierungen rechnen.

- Ein Verstoß gegen die EU-Datenschutzgrundverordnung kann das betreffende Unternehmen bis zu 20 Millionen Euro Geldbuße kosten – oder bis zu 4 % dessen weltweiter Umsätze (je nachdem, welcher Wert am Ende höher ausfällt).

Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 6

Die Rechtmäßigkeit der Datenverarbeitung gemäß der Datenschutz-Grundverordnung (DSGVO) wird in Artikel 6 geregelt. Artikel 6 enthält verschiedene Rechtsgrundlagen, auf die sich ein Verantwortlicher stützen kann, um die Verarbeitung personenbezogener Daten zu legitimieren. Die sechs Rechtsgrundlagen in Artikel 6 sind:

Einwilligung (Artikel 6 Absatz 1 Buchstabe a): Die betroffene Person hat ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für einen bestimmten Zweck erteilt.

Vertragserfüllung (Artikel 6 Absatz 1 Buchstabe b): Die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich, an dem die betroffene Person beteiligt ist, oder um auf Anfrage der betroffenen Person vorvertragliche Maßnahmen zu ergreifen.

Erfüllung einer rechtlichen Verpflichtung (Artikel 6 Absatz 1 Buchstabe c): Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

Schutz lebenswichtiger Interessen (Artikel 6 Absatz 1 Buchstabe d): Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Artikel 6 Absatz 1 Buchstabe e): 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.

Berechtigtes Interesse (Artikel 6 Absatz 1 Buchstabe f): 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 überwiegen.

Es ist wichtig zu beachten, dass jede Datenverarbeitung auf einer oder mehreren dieser Rechtsgrundlagen basieren muss, um gemäß der DSGVO rechtmäßig zu sein. Der konkrete Anwendungsfall und die Art der verarbeiteten Daten bestimmen, welche Rechtsgrundlage angemessen ist.

Datenschutzverletzungen

1. Verfahren zur Meldung von Datenschutzverletzungen (Artikel 33 und 34 DSGVO):
   Gemäß Artikel 33 DSGVO müssen Datenschutzverletzungen, bei denen ein Verstoß gegen den Schutz personenbezogener Daten vorliegt, innerhalb von 72 Stunden nach Kenntnisnahme an die zuständige Aufsichtsbehörde gemeldet werden, sofern die Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. In einigen Fällen müssen auch die betroffenen Personen selbst über die Datenschutzverletzung informiert werden (Artikel 34 DSGVO). Als Datenschutzbeauftragter ist es wichtig, die Verfahren zur Meldung von Datenschutzverletzungen zu kennen und sicherzustellen, dass diese innerhalb der vorgegebenen Fristen und unter Beachtung der Meldepflichten durchgeführt werden.

2. Rechte betroffener Personen:
   Die DSGVO gewährt den betroffenen Personen verschiedene Rechte in Bezug auf ihre personenbezogenen Daten. Dazu gehören unter anderem das Recht auf Auskunft über die Verarbeitung ihrer Daten, das Recht auf Berichtigung unrichtiger

Daten, das Recht auf Löschung der Daten unter bestimmten Umständen, das Recht auf Widerspruch gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit. Als Datenschutzbeauftragter sollten Sie über diese Rechte informiert sein und sicherstellen, dass die betroffenen Personen ihre Rechte wirksam ausüben können.

3. Datenschutz-Folgenabschätzungen:
   Gemäß Artikel 35 DSGVO müssen in bestimmten Fällen Datenschutz-Folgenabschätzungen durchgeführt werden. Diese werden benötigt, wenn eine geplante Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere bei Verarbeitungen, die umfangreiche Datenverarbeitungen, systematische Überwachung oder Verarbeitung sensibler Daten umfassen. Als Datenschutzbeauftragter sollten Sie wissen, wann eine Datenschutz-Folgenabschätzung erforderlich ist und wie diese durchgeführt werden sollte.

Das BDSG (Bundesdatenschutzgesetz)

Das Bundesdatenschutzgesetz ist ein deutsches Gesetz, das den Schutz personenbezogener Daten regelt. Ein Verstoß gegen das BDSG kann verschiedene rechtliche Konsequenzen haben. Hier sind einige mögliche Folgen:

1. Bußgelder: Bei Verstößen gegen das BDSG kann die zuständige Datenschutzbehörde Bußgelder verhängen. Die Höhe der Bußgelder hängt von der Art des Verstoßes ab. Mit der Einführung der Datenschutz-Grundverordnung (DSGVO) wurden die Bußgelder erheblich erhöht. Für schwerwiegende Verstöße können Bußgelder von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes des Unternehmens verhängt werden, je nachdem, welcher Betrag höher ist.
2. Schadensersatzansprüche: Personen, deren Datenschutzrechte verletzt wurden, können Schadensersatzansprüche gegen den Verantwortlichen geltend machen. Der Verantwortliche kann

dazu verpflichtet sein, den erlittenen Schaden zu ersetzen, der beispielsweise aus finanziellen Verlusten oder dem Verlust des Ansehens resultieren kann.

3. Strafrechtliche Konsequenzen: In einigen Fällen kann ein Verstoß gegen das BDSG auch strafrechtliche Konsequenzen nach sich ziehen. Das Strafgesetzbuch sieht in bestimmten Fällen Geldstrafen oder Freiheitsstrafen vor, zum Beispiel bei der unbefugten Erhebung oder Verarbeitung personenbezogener Daten.
4. Anordnung zur Datenlöschung oder -sperrung: Die Datenschutzbehörde kann anordnen, dass personenbezogene Daten gelöscht oder gesperrt werden, wenn ein Verstoß gegen das BDSG festgestellt wird. Dies kann erhebliche Auswirkungen auf die betroffene Organisation haben, insbesondere wenn sensible Daten betroffen sind.
5. Es ist wichtig anzumerken, dass die konkreten Folgen eines Verstoßes gegen das BDSG von verschiedenen Faktoren abhängen, wie der Art und Schwere des Verstoßes, der Sensibilität der betroffenen Daten und der Compliance-Historie des Verantwortlichen. Die Datenschutzbehörden haben die Befugnis, im Einzelfall zu entscheiden und angemessene Maßnahmen zu ergreifen.

Die Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (auch Datenschutz-Folgenabschätzung, englisch: Data Protection Impact Assessment, kurz DPIA) ist ein Prozess, der gemäß Artikel 35 der Datenschutz-Grundverordnung (DSGVO) durchgeführt werden muss, wenn eine geplante Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt.

Der Zweck einer Datenschutz-Folgenabschätzung besteht darin, vorab die möglichen Auswirkungen einer Datenverarbeitung auf den Schutz personenbezogener Daten zu analysieren und geeignete Maßnahmen zu ergreifen, um Risiken zu minimieren. Durch die Durchführung einer DPIA können potenzielle Datenschutzprobleme identifiziert und

behandelt werden, bevor eine Datenverarbeitung beginnt oder geändert wird.

Der Prozess der Datenschutz-Folgenabschätzung umfasst in der Regel folgende Schritte:

1. Bewertung der Notwendigkeit:
   Es wird geprüft, ob eine geplante Datenverarbeitung einer Datenschutz-Folgenabschätzung unterliegt. Dies ist der Fall, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. Einige Kriterien, die auf ein hohes Risiko hinweisen können, sind beispielsweise die umfangreiche Verarbeitung sensibler Daten, die systematische Überwachung von Personen oder die Verarbeitung in großem Maßstab.

2. Beschreibung der Datenverarbeitung:
   Es werden alle relevanten Informationen zur geplanten Datenverarbeitung gesammelt, einschließlich des Zwecks, der Art der Daten, der betroffenen Personen, der Datenquellen und der geplanten Datenübermittlungen.
3. Bewertung der Risiken:
   Es werden die potenziellen Risiken und Auswirkungen der Datenverarbeitung auf die Rechte und Freiheiten der betroffenen Personen bewertet. Dies umfasst die Identifizierung möglicher Datenschutzverletzungen, die Wahrscheinlichkeit ihres Eintretens und die Schwere der Auswirkungen.

1. Maßnahmen zur Risikominimierung:
   Basierend auf der Bewertung werden geeignete Maßnahmen zur Minimierung der identifizierten Risiken entwickelt. Dazu gehören technische und organisatorische Maßnahmen wie Pseudonymisierung, Verschlüsselung, Zugangskontrollen oder die Durchführung von Datenschutzschulungen.

2. Konsultation der Aufsichtsbehörde:
   In bestimmten Fällen, insbesondere wenn das Risiko nicht ausreichend gemindert werden kann, muss die zuständige

Datenschutzaufsichtsbehörde konsultiert werden.

3. Dokumentation:
   Der gesamte Prozess der Datenschutz-Folgenabschätzung sowie die getroffenen Maßnahmen werden dokumentiert. Diese Dokumentation dient als Nachweis dafür, dass die Datenschutzanforderungen berücksichtigt und umgesetzt wurden.

Die Durchführung einer Datenschutz-Folgenabschätzung ermöglicht es Unternehmen, Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten frühzeitig zu erkennen und geeignete Schutzmaßnahmen zu ergreifen. Dadurch wird der Datenschutz gestärkt und die Einhaltung der DSGVO gefördert.

Rechenschaftspflicht

Die Rechenschaftspflicht ist ein wichtiger Grundsatz der Datenschutz-Grundverordnung (DSGVO) und bedeutet, dass Verantwortliche und Auftragsverarbeiter nachweisen müssen, dass sie die Datenschutzbestimmungen einhalten und geeignete Maßnahmen zum Schutz personenbezogener Daten ergriffen haben. Im Rahmen der Rechenschaftspflicht müssen sie dokumentieren, wie sie die Grundsätze und Anforderungen der DSGVO umgesetzt haben. Hier sind einige Aspekte, die zur Rechenschaftspflicht gehören:

1. Datenschutzrichtlinien und -verfahren:
   Unternehmen sollten klare Datenschutzrichtlinien und -verfahren haben, die den Grundsätzen der DSGVO entsprechen. Diese Richtlinien und Verfahren sollten dokumentiert, regelmäßig überprüft und aktualisiert werden.

2. Datenschutz-Folgenabschätzungen (DSFA):
   Bei geplanten Datenverarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen, ist die Durchführung einer Datenschutz-Folgenabschätzung erforderlich. Der Prozess und das Ergebnis der DSFA sollten

dokumentiert werden.

3. Verarbeitungsverzeichnis:
   Verantwortliche müssen ein Verzeichnis aller Verarbeitungstätigkeiten erstellen, die in ihrem Unternehmen stattfinden. Das Verarbeitungsverzeichnis enthält Informationen über die Zwecke der Verarbeitung, die Kategorien von personenbezogenen Daten, die betroffenen Personen und die geplanten Datenübermittlungen. Es muss regelmäßig aktualisiert werden.

4. Technische und organisatorische Maßnahmen (TOM):
   Unternehmen müssen angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergreifen. Diese Maßnahmen sollten dokumentiert werden und den aktuellen technischen Standards entsprechen.

5. Datenschutzbeauftragter:
   Wenn ein Unternehmen einen Datenschutzbeauftragten ernennen muss, sollte dies dokumentiert sein. Der Datenschutzbeauftragte spielt eine wichtige Rolle bei der Überwachung der Einhaltung der Datenschutzbestimmungen.

6. Datenschutzverletzungen:
   Unternehmen müssen Datenschutzverletzungen melden und dokumentieren, einschließlich der Art der Verletzung, der betroffenen Personen und der ergriffenen Maßnahmen zur Minderung der Auswirkungen.

4. Mitarbeiter-Sensibilisierung:
   Unternehmen sollten Schulungsprogramme und Richtlinien entwickeln, um ihre Mitarbeiter für den Datenschutz zu sensibilisieren. Diese Schulungsmaßnahmen sollten dokumentiert werden.

5. Zusammenarbeit mit Aufsichtsbehörden:
   Unternehmen sollten nachweisen können, dass sie mit

Datenschutzaufsichtsbehörden kooperieren und auf Anfragen oder Untersuchungen reagieren.

Die Rechenschaftspflicht ist entscheidend, um die Einhaltung der Datenschutzbestimmungen sicherzustellen und das Vertrauen der betroffenen Personen in die Verarbeitung ihrer Daten zu stärken. Die genannten Aspekte sind einige Beispiele dafür, was zur Rechenschaftspflicht gehört, und können je nach Unternehmen und Kontext variieren.

Datenschutzbeauftragter

Benennung des Datenschutzbeauftragten

Die Benennung des Datenschutzbeauftragten ist in Artikel 37 der Datenschutz-Grundverordnung (DSGVO) geregelt. In diesem Artikel werden die Bedingungen und Kriterien festgelegt, unter denen die Benennung eines Datenschutzbeauftragten erforderlich ist. Die genauen Bestimmungen können je nach nationalen Datenschutzgesetzen und -vorschriften in den einzelnen EU-Mitgliedstaaten variieren.

Gemäß Artikel 37 DSGVO müssen Verantwortliche und Auftragsverarbeiter einen Datenschutzbeauftragten benennen, wenn sie einer der folgenden Kriterien erfüllen:

1. Öffentliche Stellen und Behörden:
   Wenn die Datenverarbeitung von einer öffentlichen Stelle oder Behörde durchgeführt wird, ist die Benennung eines Datenschutzbeauftragten in der Regel verpflichtend.

2. Regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang:
   Wenn ein Unternehmen Personen in großem Umfang regelmäßig und systematisch überwacht, ist die Benennung eines Datenschutzbeauftragten erforderlich. Dies kann beispielsweise auf Unternehmen zutreffen, die Videoüberwachung,

Kundenprofilierung oder ähnliche Aktivitäten durchführen.

3. Großangelegte Verarbeitung besonderer Kategorien von Daten: Wenn ein Unternehmen in großem Umfang besondere Kategorien von personenbezogenen Daten gemäß Artikel 9 DSGVO verarbeitet, ist die Benennung eines Datenschutzbeauftragten erforderlich. Besondere Kategorien von Daten umfassen sensible Daten wie Gesundheitsdaten, ethnische Herkunft, religiöse Überzeugungen, politische Meinungen usw.

Es liegt in der Verantwortung des Verantwortlichen oder Auftragsverarbeiters, sicherzustellen, dass ein Datenschutzbeauftragter benannt wird, wenn dies erforderlich ist. Der Datenschutzbeauftragte sollte über Fachkenntnisse im Bereich Datenschutz und Datenschutzrecht verfügen und unabhängig seine Aufgaben wahrnehmen können. Die genauen Anforderungen an den Datenschutzbeauftragten können ebenfalls durch nationale Datenschutzgesetze ergänzt werden.

Ergänzende Regelungen gemäß Bundesdatenschutzgesetz zur Bestellung eines Datenschutzbeauftragten

Wann Unternehmen einen Datenschutzbeauftragten benennen müssen, regelt die DSGVO in Art. 37. Die dort genannten Bedingungen sind so gefasst, dass nur wenige Formen der Datenverarbeitung der Pflicht zur Benennung unterliegen.

Der Artikel 38 BDSG wurde 2018 neu gefasst mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU – vom 30.06.2017, BGBl. I, vom 05.07.2017, S. 2097 und trat am 25.05.2018 in Kraft.

Das neue Bundesdatenschutzgesetz und die Datenschutzgrundverordnung regeln zusammen, wann ein Datenschutzbeauftragter benannt werden muss.

So müssen die hauptsächlich verarbeiteten Informationen entweder zu den besonderen Kategorien personenbezogener Daten gehören, also von hoher Schutzwürdigkeit sein, oder aber in der Art ihrer Verarbeitung eine umfangreiche Überwachung der jeweiligen Personen erforderlich machen. Es handelt sich hierbei also nur um Fälle, die sehr weit in die schutzwürdigen Bereiche der betroffenen Personen eingreifen.

Art. 37 Abs. 4 sieht jedoch explizit vor, dass weitere Fälle durch nationale Gesetzgebung vorgeschrieben werden können. Dies wird im deutschen Datenschutzgesetz in seiner neu gefassten Ausführung in § 38 getan. Die dortige Ergänzung nennt zusätzlich folgende Bedingungen:

"Mindestens zehn Personen sind ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt."

- Und weiter: "Es werden Datenverarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen." Und ferner: "Es werden geschäftsmäßig personenbezogene Daten verarbeitet zum Zweck der (anonymisierten) Übermittlung oder der Markt- oder Meinungsforschung."

Im Vergleich zum alten BDSG ergibt sich hieraus die Änderung, dass eine Regelung bezüglich nicht-automatisierter Datenverarbeitung (Pflicht zur Bestellung eines Datenschutzbeauftragten ab 20 beschäftigten Personen) nun entfallen ist. Da alles, was mit Computern durchgeführt wird, bereits als automatisierte Verarbeitung gilt, ist davon auszugehen, dass dies heutzutage der Regelfall ist.

Im Bundesdatenschutzgesetz (BDSG) finden sich ergänzende Regelungen zur Bestellung eines Datenschutzbeauftragten in Deutschland. Gemäß § 38 BDSG ist die Bestellung eines Datenschutzbeauftragten erforderlich, wenn:

Die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung von personenbezogenen Daten besteht. Dabei ist insbesondere auf die Menge der verarbeiteten Daten, den Umfang der Datenkategorien sowie die Dauer der Verarbeitung abzustellen.

Die Verarbeitung personenbezogener Daten einer öffentlichen Stelle erfolgt, sofern diese mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Es gibt jedoch Ausnahmen von der Bestellpflicht. Gemäß § 38 Absatz 2 BDSG müssen Unternehmen keinen Datenschutzbeauftragten benennen, wenn:

Das Unternehmen weniger als 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Die Verarbeitung der Daten nur gelegentlich erfolgt und keinen umfangreichen Umfang hat.

Es ist wichtig zu beachten, dass dies eine allgemeine Zusammenfassung der Regelungen im BDSG ist. Je nach spezifischer Situation und Branche können weitere Anforderungen gelten. Es wird empfohlen, die genauen Bestimmungen im BDSG zu überprüfen oder rechtlichen Rat einzuholen, um sicherzustellen, dass die Anforderungen ordnungsgemäß erfüllt werden.

Rolle des Datenschutzbeauftragten

Als Datenschutzbeauftragter tragen Sie eine wichtige Rolle bei der Sicherstellung des Datenschutzes in einem Unternehmen. Hier sind einige Aufgaben und Verantwortlichkeiten, mit denen Sie vertraut sein sollten:

1. Beratung des Unternehmens:
   Als Datenschutzbeauftragter sind Sie Ansprechpartner für das Unternehmen in allen Fragen des Datenschutzes. Sie beraten das Unternehmen bei der Entwicklung und Umsetzung datenschutzkonformer Prozesse, Richtlinien und Verfahren. Dabei unterstützen Sie bei der Bewertung und Umsetzung der Datenschutzanforderungen der DSGVO und anderer relevanten Datenschutzgesetze.

2. Überwachung der Einhaltung der DSGVO:
   Sie überwachen die Verarbeitung personenbezogener Daten im

Unternehmen, um sicherzustellen, dass sie gemäß den Anforderungen der DSGVO erfolgt. Dazu gehört die Prüfung von Datenverarbeitungsaktivitäten, Datenschutzfolgenabschätzungen, Einhaltung der Grundsätze der DSGVO und Umsetzung angemessener technischer und organisatorischer Maßnahmen zum Datenschutz.

3. Zusammenarbeit mit Aufsichtsbehörden:
   Sie sind die Kontaktperson für Aufsichtsbehörden in allen Datenschutzangelegenheiten. Sie kommunizieren und kooperieren mit den Behörden, insbesondere bei Datenschutzverletzungen, Beschwerden oder Anfragen. Sie unterstützen das Unternehmen bei der Zusammenarbeit mit den Aufsichtsbehörden und bei der Erfüllung ihrer Anforderungen und Anfragen.

4. Sensibilisierung von Mitarbeitern:
   Sie sind dafür verantwortlich, das Bewusstsein für Datenschutzfragen im Unternehmen zu schärfen. Sie entwickeln und führen Schulungen und Schulungsprogramme durch, um Mitarbeiter über ihre Verantwortung im Umgang mit personenbezogenen Daten zu informieren und Datenschutzbestimmungen zu vermitteln. Ziel ist es, das Datenschutzbewusstsein zu stärken und Verstöße zu vermeiden.

5. Dokumentation und Aufzeichnungen:
   Sie führen Protokolle und Aufzeichnungen über Datenschutzaktivitäten im Unternehmen. Dies umfasst die Dokumentation von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzverletzungen, Datenschutzrichtlinien und -verfahren sowie die Kommunikation mit Aufsichtsbehörden.

   In Deutschland gelten die Rechte und Pflichten des Datenschutzbeauftragten gemäß der Datenschutz-Grundverordnung (DSGVO) sowie dem Bundesdatenschutzgesetz (BDSG). Hier sind die spezifischen Rechte und Pflichten des

Datenschutzbeauftragten im Hinblick auf die Tätigkeit in Deutschland:

Rechte des Datenschutzbeauftragten

1. Zugang zu personenbezogenen Daten:
   Sie haben das Recht, Zugang zu allen personenbezogenen Daten zu erhalten, die im Rahmen der Verarbeitungstätigkeiten des Unternehmens erhoben und verarbeitet werden.

2. Unabhängigkeit:
   Als Datenschutzbeauftragter haben Sie das Recht auf Unabhängigkeit bei der Erfüllung Ihrer Aufgaben. Sie dürfen keine Weisungen von der Geschäftsführung oder anderen internen Stellen erhalten, die Ihre Aufgaben beeinflussen könnten.

3. Zugang zu Informationen und Ressourcen:
   Sie haben das Recht, alle erforderlichen Informationen und Ressourcen zu erhalten, um Ihre Aufgaben angemessen erfüllen zu können. Dazu gehören beispielsweise Schulungen, Unterstützung bei der Umsetzung von Datenschutzmaßnahmen und die Bereitstellung von technischen Hilfsmitteln.

Pflichten des Datenschutzbeauftragten

1. Überwachung der Einhaltung:
   Sie sind verpflichtet, die Einhaltung der Datenschutzbestimmungen im Unternehmen zu überwachen. Dazu gehört die Überprüfung von Datenverarbeitungstätigkeiten, die Sicherstellung der Umsetzung angemessener technischer und organisatorischer Maßnahmen sowie die regelmäßige Überprüfung der Datenschutzrichtlinien und -verfahren.

2. Beratung und Schulung:
   Sie beraten das Unternehmen in allen Fragen des Datenschutzes und geben Empfehlungen zur Verbesserung der Datenschutzpraktiken. Sie unterstützen bei der Entwicklung von

Datenschutzrichtlinien und -verfahren und bieten Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter an.

3. Zusammenarbeit mit Aufsichtsbehörden:
   Sie sind die Kontaktperson für die Datenschutzaufsichtsbehörden und arbeiten eng mit ihnen zusammen. Sie unterstützen das Unternehmen bei der Zusammenarbeit mit den Aufsichtsbehörden, insbesondere bei Datenschutzverletzungen, Untersuchungen oder Anfragen.

4. Dokumentation:
   Sie führen Protokolle und Aufzeichnungen über Datenschutzaktivitäten im Unternehmen. Dazu gehören beispielsweise die Dokumentation von Datenverarbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzverletzungen und die Kommunikation mit Aufsichtsbehörden.

5. Sensibilisierung der Mitarbeiter:
   Sie sind verpflichtet, das Bewusstsein für Datenschutzfragen bei den Mitarbeitern zu schärfen. Sie entwickeln Schulungsprogramme, um Mitarbeiter über ihre Verantwortung im Umgang mit personenbezogenen Daten zu informieren und die Einhaltung der Datenschutzbestimmungen zu fördern.

Diese Rechte und Pflichten sind grundlegende Aspekte, die in Deutschland für Datenschutzbeauftragte gelten. Es ist wichtig zu beachten, dass es zusätzliche Anforderungen und spezifische Bestimmungen geben kann, die je nach Unternehmensgröße, Branche und Art der Datenverarbeitung variieren. Daher sollten Sie immer die geltenden Datenschutzgesetze und -vorschriften, einschließlich der DSGVO und des BDSG, berücksichtigen.

Datenschutzmanagement

Datenschutzmanagement bezieht sich auf die Gesamtheit der Maßnahmen, Strukturen und Prozesse, die ein Unternehmen implementiert, um den Schutz personenbezogener Daten sicherzustellen und die Anforderungen der Datenschutzgesetze zu erfüllen. Es umfasst die systematische Planung, Umsetzung, Überwachung und kontinuierliche Verbesserung von Datenschutzpraktiken in einer Organisation. Hier sind einige wichtige Aspekte des Datenschutzmanagements:

1. Datenschutzrichtlinien und -verfahren:
   Ein Unternehmen sollte klare Datenschutzrichtlinien und -verfahren entwickeln, die den gesetzlichen Anforderungen entsprechen. Diese Richtlinien legen die Grundsätze, Verantwortlichkeiten und Verfahren fest, um den Schutz personenbezogener Daten sicherzustellen.

2. Datenschutzbeauftragter:
   Die Benennung eines Datenschutzbeauftragten kann eine wichtige Komponente des Datenschutzmanagements sein. Der Datenschutzbeauftragte überwacht die Einhaltung der Datenschutzbestimmungen, berät das Unternehmen in Datenschutzfragen und unterstützt bei der Umsetzung von Datenschutzmaßnahmen.

3. Datenschutz-Folgenabschätzung: Bei geplanten Datenverarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen, sollte eine Datenschutz-Folgenabschätzung durchgeführt werden. Dieser Prozess bewertet die Auswirkungen der Datenverarbeitung auf den Datenschutz und hilft bei der Identifizierung und Umsetzung geeigneter Schutzmaßnahmen.

4. Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSVGO:
   Ein Verzeichnis von Verarbeitungstätigkeiten enthält Informationen über die Datenverarbeitung im Unternehmen, einschließlich der

Zwecke, Kategorien von personenbezogenen Daten, betroffene Personen und geplante Datenübermittlungen. Es dient der Transparenz und Dokumentation der Verarbeitungstätigkeiten.

5. Technische und organisatorische Maßnahmen (TOM):
   Unternehmen sollten angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergreifen. Dazu gehören Maßnahmen wie Zugangskontrollen, Datensicherung, Verschlüsselung, Datenschutzschulungen für Mitarbeiter und regelmäßige Sicherheitsüberprüfungen.

6. Datenschutzverletzungen:
   Ein Unternehmen sollte ein Verfahren zur Meldung und Behandlung von Datenschutzverletzungen haben. Dies beinhaltet die Erfassung, Untersuchung und Meldung von Datenschutzverletzungen an die zuständigen Behörden und betroffenen Personen gemäß den gesetzlichen Anforderungen.

7. Schulungen und Sensibilisierung:
   Mitarbeiter sollten über ihre Verantwortung im Umgang mit personenbezogenen Daten geschult und sensibilisiert werden. Schulungen und Schulungsmaterialien sollten regelmäßig bereitgestellt werden, um ein Bewusstsein für Datenschutzthemen zu schaffen
   .
8. Überwachung und Überprüfung:
   Das Datenschutzmanagement umfasst auch die regelmäßige Überwachung und Überprüfung der Datenschutzpraktiken im Unternehmen. Dies kann interne Audits, Überprüfung der Datenschutzdokumentation, Überwachung der Einhaltung von Richtlinien und Verfahren sowie die Bewertung von Datenschutzrisiken umfassen.

Das Datenschutzmanagement ist ein kontinuierlicher Prozess (PDCA), der eine ganzheitliche Herangehensweise an den Datenschutz erfordert. Es ist wichtig, dass Unternehmen ihre Datenschutzmaßnahmen regelmäßig überprüfen, aktualisieren und an

neue rechtliche Anforderungen anpassen, um den Schutz personenbezogener Daten zu gewährleisten.

Rechte der Betroffenen

Die Datenschutz-Grundverordnung (DSGVO) gewährt betroffenen Personen eine Reihe von Rechten im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Hier sind die wichtigsten Rechte der betroffenen Personen gemäß der DSGVO:

1. Recht auf Information (Artikel 13 und 14 DSGVO):
   Betroffene Personen haben das Recht, transparente Informationen darüber zu erhalten, wie ihre personenbezogenen Daten verarbeitet werden. Dies umfasst Informationen wie den Verarbeitungszweck, die Kategorien der verarbeiteten Daten, die Empfänger der Daten und die Dauer der Datenspeicherung.

2. Recht auf Auskunft (Artikel 15 DSGVO):
   Betroffene Personen haben das Recht, Auskunft darüber zu erhalten, ob und welche ihrer personenbezogenen Daten von einem Unternehmen verarbeitet werden. Sie können auch Informationen über den Verarbeitungszweck, die Kategorien der verarbeiteten Daten, die Empfänger der Daten und die geplante Speicherdauer verlangen.

3. Recht auf Berichtigung (Artikel 16 DSGVO):
   Wenn betroffene Personen feststellen, dass ihre personenbezogenen Daten unrichtig oder unvollständig sind, haben sie das Recht, eine Berichtigung oder Vervollständigung dieser Daten zu verlangen.

4. Recht auf Löschung (Artikel 17 DSGVO):
   Betroffene Personen haben unter bestimmten Bedingungen das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen. Dies gilt beispielsweise, wenn die Daten nicht mehr für den ursprünglichen Verarbeitungszweck benötigt werden, die Einwilligung widerrufen wurde oder die Daten unrechtmäßig

verarbeitet wurden.

5. Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO): Betroffene Personen können unter bestimmten Umständen verlangen, dass die Verarbeitung ihrer personenbezogenen Daten eingeschränkt wird. Dies bedeutet, dass die Daten zwar gespeichert, aber nicht weiterverarbeitet werden dürfen.

6. Recht auf Datenübertragbarkeit (Artikel 20 DSGVO): Betroffene Personen haben das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln, wenn dies technisch möglich ist.

7. Recht auf Widerspruch (Artikel 21 DSGVO): Betroffene Personen haben das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen. Das Unternehmen muss die Verarbeitung einstellen, es sei denn, es kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

8. Recht auf Beschwerde bei einer Aufsichtsbehörde (Artikel 77 DSGVO): Betroffene Personen haben das Recht, eine Beschwerde bei einer Datenschutzaufsichtsbehörde einzureichen, wenn sie der Meinung sind, dass ihre Datenschutzrechte verletzt wurden.

Es ist wichtig zu beachten, dass diese Rechte bestimmten Voraussetzungen und Ausnahmen unterliegen. Unternehmen müssen sicherstellen, dass sie die Rechte der betroffenen Personen respektieren und angemessene Mechanismen implementieren, um diesen Rechten nachzukommen.

Verantwortlichkeiten

Die DSGVO regelt in Artikel 38, wer zum Datenschutzbeauftragten

ernannt werden kann. Gemäß Artikel 38 Absatz 6 DSGVO dürfen Mitarbeiter des Unternehmens, insbesondere der Arbeitgeber oder derjenige, der über die Verarbeitung personenbezogener Daten entscheidet, nicht gleichzeitig Datenschutzbeauftragte sein, wenn es ein Interessenkonflikt gibt.

Die Trennung zwischen der Rolle des Datenschutzbeauftragten und anderen Positionen im Unternehmen, wie dem Chef oder der Personalabteilung, dient dazu, einen Interessenkonflikt zu vermeiden. Der Datenschutzbeauftragte sollte unabhängig und frei von Weisungen sein, um seine Aufgaben im Sinne des Datenschutzes objektiv und effektiv wahrnehmen zu können.

Die DSGVO fordert, dass der Datenschutzbeauftragte seine Aufgaben in einer Weise ausübt, die von anderen Aufgaben oder Verpflichtungen getrennt ist, um Interessenkonflikte zu vermeiden. Dadurch wird sichergestellt, dass der Datenschutzbeauftragte unabhängig agieren kann und keine Interessenkonflikte zwischen dem Schutz personenbezogener Daten und anderen betrieblichen oder wirtschaftlichen Interessen des Unternehmens entstehen.

Daher ist es empfehlenswert, eine unabhängige Person als Datenschutzbeauftragten zu benennen, die nicht in einer anderen Schlüsselposition im Unternehmen, wie dem Chef oder der Personalabteilung, tätig ist, um die Unabhängigkeit und Objektivität in der Datenschutzrolle zu gewährleisten.

Technische und Organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOMs) sind Maßnahmen, die Unternehmen und Organisationen ergreifen, um den Schutz personenbezogener Daten zu gewährleisten. Diese Maßnahmen sollen sicherstellen, dass die Datenschutzprinzipien eingehalten werden und die Risiken für die Rechte und Freiheiten der betroffenen Personen minimiert werden. Im Folgenden werden einige konkrete Beispiele für technische und organisatorische Maßnahmen genannt:

Technische Maßnahmen

- Zugangskontrolle:
  Implementierung von Passwörtern, Zugriffsberechtigungen und Benutzerkonten, um sicherzustellen, dass nur autorisierte Personen auf die Daten zugreifen können.

- Verschlüsselung:
  Verwendung von Verschlüsselungstechniken, um personenbezogene Daten während der Übertragung und Speicherung zu schützen.

- Anonymisierung und Pseudonymisierung:
  Entfernung oder Ersetzung von Informationen, die Rückschlüsse auf bestimmte Personen ermöglichen, um die Identifizierbarkeit zu verringern.

- Firewall und Intrusion Detection/Prevention Systeme:
  Einsatz von Sicherheitsmechanismen wie Firewalls und Systemen zur Erkennung und Verhinderung von Eindringversuchen, um unbefugten Zugriff auf Systeme und Daten zu verhindern.

- Sicherung von Daten:
  Regelmäßige Datensicherungen, um Datenverluste zu vermeiden, sowie physische und logische Sicherheitsmaßnahmen, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.

Organisatorische Maßnahmen

- Datenschutzrichtlinien und -verfahren:
  Entwicklung und Implementierung von internen Richtlinien und Verfahren, die den Umgang mit personenbezogenen Daten regeln und sicherstellen, dass die Datenschutzprinzipien eingehalten werden.

- Datenschutz-Folgenabschätzung:
  Durchführung einer Bewertung der potenziellen Auswirkungen auf

den Datenschutz vor der Verarbeitung besonders riskanter Daten oder bei der Durchführung von umfangreichen Verarbeitungstätigkeiten.

- Schulung und Sensibilisierung:
  Schulung der Mitarbeiter in Bezug auf den Datenschutz, um ihr Bewusstsein für Datenschutzfragen zu schärfen und sicherzustellen, dass sie die erforderlichen Verfahren einhalten.

- Auftragsverarbeitungsverträge:
  Abschluss von Verträgen mit Auftragsverarbeitern, um sicherzustellen, dass diese angemessene Datenschutzmaßnahmen ergreifen und die Rechte der betroffenen Personen schützen.

- Zugriffskontrolle und Berechtigungsmanagement:
  Verwaltung und Überwachung der Zugriffsrechte auf personenbezogene Daten, um sicherzustellen, dass nur autorisierte Mitarbeiter Zugriff haben und dass die Zugriffe protokolliert werden.

Diese Beispiele sollen veranschaulichen, welche Maßnahmen ergriffen werden können, um den Datenschutz zu gewährleisten. Die konkreten Maßnahmen, die ein Unternehmen ergreifen sollte, hängen von verschiedenen Faktoren ab, wie der Art der verarbeiteten Daten, dem Umfang der Datenverarbeitung und den Risiken für die betroffenen Personen.

7 Schritte zur Umsetzung der DSVGO

Die Umsetzung der Datenschutz-Grundverordnung (DSGVO) erfordert eine sorgfältige Planung und Implementierung geeigneter Maßnahmen. Hier sind sieben Schritte, die Unternehmen bei der Umsetzung der DSGVO beachten sollten:

1. Datenschutz-Folgenabschätzung durchführen:
   Eine Datenschutz-Folgenabschätzung (DSFA) hilft dabei, potenzielle Risiken für den Datenschutz zu identifizieren und geeignete Maßnahmen zu ergreifen, um diese Risiken zu mindern.

Unternehmen sollten DSFA durchführen, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

2. Datenschutzrichtlinien und Verfahren entwickeln: Unternehmen sollten klare Datenschutzrichtlinien und -verfahren entwickeln, die den Anforderungen der DSGVO entsprechen. Diese Richtlinien sollten den Umgang mit personenbezogenen Daten, die Rechte der betroffenen Personen, die Datensicherheit und andere relevante Aspekte des Datenschutzes abdecken.

3. Einwilligung einholen:
   Unternehmen müssen sicherstellen, dass sie eine gültige Einwilligung von den betroffenen Personen einholen, wenn sie deren personenbezogene Daten verarbeiten wollen. Die Einwilligung sollte freiwillig, informiert, eindeutig und für den spezifischen Verarbeitungszweck gegeben werden.

4. Datenschutzrechte der betroffenen Personen gewährleisten:
   Unternehmen müssen sicherstellen, dass sie die Datenschutzrechte der betroffenen Personen, wie das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit, respektieren und angemessene Mechanismen zur Erfüllung dieser Rechte bereitstellen.

5. Datensicherheit gewährleisten:
   Unternehmen sollten geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit personenbezogener Daten zu gewährleisten. Dazu gehören die Verschlüsselung von Daten, die Zugriffskontrolle, regelmäßige Sicherheitsüberprüfungen und die Sensibilisierung der Mitarbeiter für Datensicherheitspraktiken.

6. Auftragsverarbeitungsverträge abschließen:
   Wenn ein Unternehmen personenbezogene Daten an Auftragsverarbeiter übermittelt, muss es mit diesen Auftragsverarbeitungsverträge abschließen, die die Verpflichtungen und Verantwortlichkeiten der Auftragsverarbeiter

in Bezug auf den Datenschutz festlegen.

7. Datenschutzdokumentation führen:
   Unternehmen müssen eine angemessene Datenschutzdokumentation führen, in der sie ihre Verarbeitungstätigkeiten dokumentieren. Dies umfasst beispielsweise das Verzeichnis von Verarbeitungstätigkeiten, Datenschutzrichtlinien, Einwilligungen und Datenschutz-Folgenabschätzungen.

Es ist wichtig zu beachten, dass diese Schritte nur einen allgemeinen Überblick über die Umsetzung der DSGVO bieten und dass die spezifischen Anforderungen je nach Unternehmen und Verarbeitungstätigkeiten variieren können. Es wird empfohlen, dass Unternehmen spezifische Richtlinien und Unterstützung von Datenschutzexperten in Anspruch nehmen, um sicherzustellen, dass sie die DSGVO ordnungsgemäß umsetzen.

Verzeichnis von Verarbeitungstätigkeiten

Gemäß Artikel 30 der Datenschutz-Grundverordnung (DSGVO) müssen Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten führen. Das Verzeichnis für Verarbeitungstätigkeiten ist eine Dokumentation, die Informationen über die Verarbeitung personenbezogener Daten im Unternehmen enthält.

Das Verzeichnis für Verarbeitungstätigkeiten sollte zumindest folgende Informationen enthalten:

1. Name und Kontaktdaten des Verantwortlichen (Unternehmens) und gegebenenfalls des Datenschutzbeauftragten.

2. Zwecke der Verarbeitung:
   Eine Beschreibung der beabsichtigten Zwecke, für die personenbezogene Daten verarbeitet werden.

3. Kategorien betroffener Personen:
   Eine Aufstellung der betroffenen Personengruppen, deren Daten verarbeitet werden.

4. Kategorien personenbezogener Daten:
   Eine Auflistung der Arten von personenbezogenen Daten, die verarbeitet werden.

5. Kategorien von Empfängern:
   Eine Aufstellung der Empfänger, denen personenbezogene Daten offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen.

6. Übermittlung personenbezogener Daten in Drittländer: Angabe, ob personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt werden, sowie gegebenenfalls die Angabe des geeigneten Schutzniveaus.

7. Fristen für die Löschung der Daten:
   Angabe der geplanten Fristen für die Löschung der verschiedenen Datenkategorien.

8. Technische und organisatorische Maßnahmen:
   Eine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

9. Datenübermittlung an Auftragsverarbeiter:
   Angabe, ob personenbezogene Daten an Auftragsverarbeiter übermittelt werden, und gegebenenfalls die Angabe der Rechtsgrundlage und des Umfangs der Übermittlung.

Das Verzeichnis für Verarbeitungstätigkeiten dient der Transparenz und Dokumentation der Datenverarbeitungstätigkeiten des Unternehmens und ist auch für die Zusammenarbeit mit den Aufsichtsbehörden relevant. Es sollte regelmäßig aktualisiert und auf dem aktuellen Stand gehalten werden.

Es ist wichtig zu beachten, dass die genauen Anforderungen an das Verzeichnis für Verarbeitungstätigkeiten von Unternehmen zu Unternehmen unterschiedlich sein können. Es wird empfohlen, bei der Erstellung des Verzeichnisses die spezifischen Anforderungen der DSGVO und ggf. nationale Datenschutzgesetze zu berücksichtigen.

Verpflichtung zur Vertraulichkeit

Die Verpflichtung zur Vertraulichkeit ist eine wichtige Aufgabe des Datenschutzbeauftragten, um sicherzustellen, dass personenbezogene Daten angemessen geschützt werden. Es gibt jedoch kein spezifisches Formular, das vom Datenschutzbeauftragten bereitgestellt wird, um diese Verpflichtung festzuhalten.

In der Regel wird die Verpflichtung zur Vertraulichkeit in einer schriftlichen Vereinbarung oder einem Vertrag zwischen dem Unternehmen und dem Datenschutzbeauftragten festgehalten. Diese Vereinbarung kann die Vertraulichkeit der personenbezogenen Daten

sowie die Verpflichtung des Datenschutzbeauftragten zum Schutz und zur Einhaltung der geltenden Datenschutzgesetze regeln.

Die genauen Inhalte und Details der Vertraulichkeitsvereinbarung können je nach Unternehmen und individuellen Umständen variieren. Es ist wichtig, dass die Vereinbarung klar und präzise formuliert ist und die Verpflichtungen des Datenschutzbeauftragten im Hinblick auf den Schutz personenbezogener Daten angemessen abdeckt.

Es wird empfohlen, sich bei der Erstellung einer Vertraulichkeitsvereinbarung für den Datenschutzbeauftragten von rechtlichen Experten oder Datenschutzbeauftragten beraten zu lassen, um sicherzustellen, dass alle relevanten Aspekte berücksichtigt werden und die Vereinbarung den gesetzlichen Anforderungen entspricht.

Unternehmensweite Passwortrichtlinie

Eine unternehmensweite Passwortrichtlinien ist eine wichtige Maßnahme, um die Sicherheit von Benutzerkonten und den Schutz sensibler Informationen zu gewährleisten. Hier sind einige Empfehlungen für die Gestaltung solcher Richtlinien:

1. Passwortkomplexität:
   Fördern Sie die Verwendung von starken Passwörtern, die aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie einfache und vorhersehbare Passwörter.

2. Passwortlänge:
   Legen Sie eine Mindestlänge für Passwörter fest, beispielsweise acht oder mehr Zeichen. Je länger das Passwort, desto schwieriger ist es zu knacken.

3. Passwortänderungen:
   Legen Sie fest, wie häufig Benutzer ihre Passwörter ändern sollten. Eine gängige Empfehlung ist eine Änderung alle drei bis sechs Monate. Es ist jedoch wichtig, eine angemessene Balance zu

finden, um unnötige Belastungen für Benutzer zu vermeiden.

4. Passworthistorie:
   Verbieten Sie die Verwendung früher verwendeter Passwörter, um die Wiederverwendung von alten und möglicherweise kompromittierten Passwörtern zu verhindern.

5. Mehrstufige Authentifizierung:
   Ermutigen Sie zur Verwendung von zusätzlichen Sicherheitsmaßnahmen wie der Zwei-Faktor-Authentifizierung (2FA) oder der Multi-Faktor-Authentifizierung (MFA), um die Sicherheit von Benutzerkonten zu erhöhen.

6. Passwort-Speicherung:
   Betonen Sie die Wichtigkeit, dass Passwörter sicher und verschlüsselt gespeichert werden. Vermeiden Sie unsichere Praktiken wie das Speichern von Passwörtern in Klartext.

7. Sensibilisierung der Mitarbeiter:
   Schulen Sie die Mitarbeiter über bewährte Sicherheitspraktiken im Umgang mit Passwörtern. Dies kann Schulungen, regelmäßige Erinnerungen oder Schulungsmaterialien umfassen.

8. Zugriffskontrolle:
   Stellen Sie sicher, dass Mitarbeiter nur Zugriff auf die Ressourcen haben, die sie benötigen. Begrenzen Sie den Zugriff auf sensible Informationen und Systeme.

9. Richtlinien durchsetzen:
   Es ist wichtig, dass die Passwortrichtlinien aktiv durchgesetzt werden. Überwachen Sie die Einhaltung der Richtlinien und ergreifen Sie geeignete Maßnahmen bei Verstößen.

10. Regelmäßige Überprüfung und Aktualisierung: Überprüfen Sie die Passwortrichtlinien regelmäßig und passen Sie sie bei Bedarf an. Technologische Entwicklungen und neue Bedrohungen erfordern möglicherweise eine Aktualisierung der Richtlinien.

Die genauen Passwortrichtlinien können je nach Unternehmen und Sicherheitsanforderungen variieren. Es ist wichtig, dass die Richtlinien angemessen sind und sowohl Sicherheitsaspekte als auch die Benutzerfreundlichkeit berücksichtigen. Es wird empfohlen, sich bei der Erstellung von Passwortrichtlinien von Sicherheitsexperten oder Fachleuten für Datenschutz beraten zu lassen.

Beispiel einer Rechtsgrundlage

Ein konkretes Beispiel für eine Rechtsgrundlage gemäß Artikel 6 der Datenschutz-Grundverordnung (DSGVO) ist die "Vertragserfüllung" (Artikel 6 Absatz 1 Buchstabe b).

Angenommen, ein Online-Shop hat einen Kunden, der eine Bestellung aufgegeben hat. Um die Bestellung abwickeln zu können, müssen personenbezogene Daten des Kunden wie Name, Lieferadresse und Zahlungsinformationen verarbeitet werden. In diesem Fall dient die Verarbeitung dieser Daten der Erfüllung des Vertrags zwischen dem Kunden und dem Online-Shop.

Die Verarbeitung der personenbezogenen Daten ist daher rechtmäßig, da sie zur Durchführung vorvertraglicher Maßnahmen (z. B. Aufnahme der Bestellung) und zur Erfüllung des Vertrags erforderlich ist. Der Kunde hat dem Online-Shop seine Einwilligung zur Verarbeitung seiner Daten für diesen bestimmten Zweck gegeben, indem er die Bestellung aufgegeben hat.

Es ist wichtig zu beachten, dass die Rechtmäßigkeit der Datenverarbeitung nicht ausschließlich auf dieser einen Rechtsgrundlage beruhen muss. In bestimmten Fällen können auch weitere Rechtsgrundlagen, wie beispielsweise die Erfüllung einer rechtlichen Verpflichtung oder das berechtigte Interesse des Verantwortlichen, anwendbar sein. Die konkrete Rechtsgrundlage hängt von den spezifischen Umständen und der Art der Datenverarbeitung ab.

Zusammenarbeit mit Dienstleistern oder externen Lieferanten

Datenschutzbeauftragte sollten bei der Zusammenarbeit mit Dienstleistern oder externen Mitarbeitern darauf achten, dass angemessene Datenschutzmaßnahmen getroffen werden. Dazu gehören:

- Sicherstellung, dass die Dienstleister, externen Mitarbeiter, Lieferanten oder Auftragsnehmer angemessene Sicherheitsmaßnahmen (Technische und Organisatorische Maßnahmen) zum Schutz personenbezogener Daten implementiert haben.
- Abschluss von schriftlichen Vereinbarungen (Auftragsverarbeitungsverträgen) mit Dienstleistern, um sicherzustellen, dass diese die Datenschutzvorschriften einhalten und die Daten nur gemäß den Anweisungen des Verantwortlichen verarbeiten.
- Überprüfung der Datenschutzrichtlinien und -praktiken der Dienstleister oder externen Mitarbeiter, um sicherzustellen, dass sie den geltenden Datenschutzgesetzen entsprechen.
- Überwachung der Aktivitäten der Dienstleister oder externen Mitarbeiter, um sicherzustellen, dass die Daten in Übereinstimmung mit den Datenschutzvorschriften verarbeitet werden.
- Durchführung regelmäßiger Datenschutzprüfungen oder Audits bei Dienstleistern, um sicherzustellen, dass sie weiterhin den Datenschutzanforderungen gerecht werden. Jede Datenverarbeitung muss den Betreffenden entsprechend bekannt gemacht werden.

Dokumentation der Auftragsverarbeiter und das dazugehörige Auftragswesen ist zu regeln. Speziell für den Auftragnehmer, also wenn Aufgaben für Kunden verarbeitet werden, müssen zusätzliche Pflichten erfüllt werden. Dazu gehört, dass das Verzeichnis von Verarbeitungstätigkeiten fortwährend gepflegt werden muss.

Erfüllung der Informationspflicht

Um der Informationspflicht gegenüber den Betreffenden nachzukommen, sollten die Datenschutzhinweise sorgfältig erstellt

werden. Dafür sollte nach einer praktikablen Lösung gesucht werden.
Bei einer Direkterhebung (also bei der sofortigen Verwendung der Daten) müssen Betroffene sofort während der Datenverarbeitung informiert werden.
Bei der indirekten Datenerhebung (hier liegen die Daten bereits vor) handelt es sich um die Erhebung personenbezogener Daten, die nicht direkt von den betroffenen Personen selbst stammen, sondern auf andere Weise beschafft werden. Dies kann beispielsweise durch die Nutzung von öffentlich zugänglichen Quellen, den Kauf von Daten von Drittanbietern, die Verwendung von Cookies oder Tracking-Technologien auf Websites oder die Zusammenarbeit mit Partnern oder Dienstleistern erfolgen.
In diesem Fall muss der Betroffene innerhalb von 4 Wochen über die Datenverarbeitung informiert werden.

Datenschutzhinweise erstellen

Datenschutzbeauftragte müssen verschiedene Datenschutzhinweise erstellen, um die betroffenen Personen über die Verarbeitung ihrer Daten zu informieren. Diese Hinweise können Folgendes enthalten:

- Informationen über den Verantwortlichen und den Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Rechtsgrundlage für die Verarbeitung
- Empfänger oder Kategorien von Empfängern der Daten
- Speicherdauer der Daten
- Rechte der betroffenen Personen (Auskunftsrecht, Berichtigung, Löschung, etc.)
- Beschwerderecht bei einer Aufsichtsbehörde
- Hinweise zur freiwilligen oder erforderlichen Bereitstellung von Daten

Die spezifischen Inhalte der Datenschutzhinweise können je nach Art der Datenverarbeitung und dem Umfang der Verarbeitung variieren.

Datenschutzkonforme Webpräsenzen

Um herauszufinden, ob eine Webseite DSGVO-konform ist, können Datenschutzbeauftragte folgende Schritte unternehmen:

1. Überprüfung der Datenschutzerklärung:
   Stellen Sie sicher, dass die Datenschutzerklärung auf der Webseite vorhanden ist und alle erforderlichen Informationen gemäß den Anforderungen der DSGVO enthält.

2. Prüfung der Einwilligungen:
   Überprüfen Sie, ob die Webseite Einwilligungen von Nutzern einholt, wenn dies erforderlich ist, und ob diese Einwilligungen den Anforderungen der DSGVO entsprechen.

3. Überprüfung der Cookie-Richtlinie:
   Stellen Sie sicher, dass die Webseite eine Cookie-Richtlinie hat, die den Nutzern klare Informationen über die Verwendung von Cookies und ähnlichen Technologien gibt und ihnen die Möglichkeit bietet, ihre Einwilligung zu geben oder abzulehnen.

4. Prüfung der Sicherheitsmaßnahmen:
   Stellen Sie sicher, dass angemessene technische und organisatorische Maßnahmen implementiert wurden, um die Sicherheit der personenbezogenen Daten auf der Webseite zu gewährleisten. Es sollte möglichst jedwede Kommunikation (zum Beispiel in Form von Kontaktformularen) verschlüsselt erfolgen.

5. Durchführung einer Datenschutz-Folgenabschätzung:
   Bei bestimmten Verarbeitungstätigkeiten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, ist eine Datenschutz-Folgenabschätzung erforderlich. Überprüfen Sie, ob eine solche Abschätzung durchgeführt wurde, wenn dies relevant ist.

Gemäß der Datenschutz-Grundverordnung (DSGVO) müssen bei einem Impressum die folgenden Punkte beachtet werden:

- Klare und transparente Informationen:
  Das Impressum sollte klare und leicht zugängliche Informationen über den Verantwortlichen für die Webseite bereitstellen. Dazu gehören Name oder Firma, Anschrift, Kontaktmöglichkeiten (E-Mail-Adresse, Telefonnummer) und gegebenenfalls weitere relevante Angaben.

- Rechtsgrundlage für die Verarbeitung:
  Wenn personenbezogene Daten im Rahmen des Impressums verarbeitet werden, muss die Rechtsgrundlage für die Verarbeitung angegeben werden. Dies kann beispielsweise die Erfüllung eines Vertrags oder die Einwilligung der betroffenen Person sein.

- Zweck der Datenverarbeitung:
  Das Impressum sollte den Zweck der Datenverarbeitung klar angeben, insbesondere wenn personenbezogene Daten über das Kontaktformular oder andere Kommunikationskanäle erhoben werden.

- Informationspflichten:
  Das Impressum muss den Informationspflichten gemäß Art. 13 und 14 DSGVO nachkommen. Das bedeutet, dass betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten informiert werden müssen, einschließlich der Zwecke der Verarbeitung, der Empfänger der Daten und der Speicherdauer.

- Rechte der betroffenen Personen:
  Das Impressum sollte darauf hinweisen, dass betroffene Personen ihre Rechte gemäß der DSGVO ausüben können, wie z. B. das Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung.

- Datensicherheit:
  Es sollte darauf hingewiesen werden, dass angemessene technische und organisatorische Maßnahmen ergriffen wurden, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

- Beschwerderecht:
  Das Impressum sollte Informationen über das Beschwerderecht bei einer Aufsichtsbehörde enthalten, einschließlich der Kontaktdaten der zuständigen Aufsichtsbehörde.

Es ist wichtig zu beachten, dass diese Anforderungen allgemein gehalten sind und je nach den spezifischen Umständen und Anforderungen variieren können. Daher wird empfohlen, sich mit den lokalen Datenschutzbestimmungen und -richtlinien vertraut zu machen, um sicherzustellen, dass das Impressum den rechtlichen Anforderungen entspricht.

Risikomanagement in der Praxis

Risikomanagement in der Praxis bezieht sich auf den Prozess der Identifizierung, Bewertung und Steuerung von Risiken in einer Organisation. Es umfasst die systematische Analyse potenzieller Risiken, um Maßnahmen zu entwickeln, um diese Risiken zu minimieren oder zu kontrollieren. Im Datenschutzkontext bedeutet dies, dass Datenschutzbeauftragte Maßnahmen ergreifen, um die Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu erkennen und zu bewerten. Dazu gehören die Identifizierung von Sicherheitslücken, die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zum Schutz der Daten sowie die Überwachung und regelmäßige Bewertung der getroffenen Maßnahmen, um sicherzustellen, dass sie wirksam sind.

Mögliche Fragen der Aufsichtsbehörde

Datenschutzbeauftragte sollten auf Fragen der Aufsichtsbehörde vorbereitet sein, die sich auf die Einhaltung der Datenschutzvorschriften beziehen können. Einige mögliche Fragen könnten sein:

- Wie werden personenbezogene Daten auf der Webseite verarbeitet und welche Zwecke werden verfolgt?

- Welche rechtliche Grundlage wird für die Verarbeitung der Daten herangezogen?

- Welche technischen und organisatorischen Maßnahmen wurden ergriffen, um die Sicherheit der Daten zu gewährleisten?

- Wie werden die Rechte der betroffenen Personen, z.B. das Recht auf Auskunft oder Löschung, umgesetzt?

- Wie werden Datenübermittlungen an Dritte gehandhabt und welche Schutzmaßnahmen wurden ergriffen?

- Wie werden Datenpannen gemeldet und welche Vorkehrungen wurden getroffen, um solche Vorfälle zu verhindern?

Projektnacharbeit

Nach Abschluss des Projekts ist es wichtig, einige Schritte zu unternehmen

- Dokumentation:
  Halten Sie alle relevanten Informationen, Prozesse und getroffenen Maßnahmen schriftlich fest.

- Schulung und Sensibilisierung:
  Sorgen Sie dafür, dass Mitarbeiter über Datenschutzpraktiken und -richtlinien informiert sind und halten Sie regelmäßige Schulungen ab, um sicherzustellen, dass das Bewusstsein für Datenschutz erhalten bleibt.

- Überprüfung und Aktualisierung:
  Überprüfen Sie regelmäßig Ihre Datenschutzpraktiken und -richtlinien, um sicherzustellen, dass sie den aktuellen gesetzlichen Anforderungen entsprechen, und aktualisieren Sie sie bei Bedarf.

- Überwachung:
  Führen Sie regelmäßige interne Audits und Kontrollen durch, um sicherzustellen, dass die Datenschutzmaßnahmen eingehalten werden.

- Kommunikation:
  Informieren Sie betroffene Personen über die durchgeführten Datenschutzmaßnahmen und stehen Sie für Fragen oder Anliegen zur Verfügung.

- Datenlöschung:
  Stellen Sie sicher, dass personenbezogene Daten gemäß den gesetzlichen Vorgaben gelöscht werden, sobald sie nicht mehr benötigt werden.

Quellenverzeichnis

Datenschutz-Grundverordnung (DSGVO) –
Finaler Text der DSGVO inklusive Erwägungsgründe (dsgvo-gesetz.de)