VdS-Richtlinien zur Umsetzung der DSGVO

Anforderungen

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

VdS-Richtlinie zur Umsetzung der DSGVO

VdS 10010

Anforderungen

Inhalt

1 Allgemeines

Für den Erfolg eines Unternehmens sind neben wettbewerbsfähigen Produkten und Dienstleistungen auch eine gesetzeskonforme Planung und das Beachten von aktuellen Verordnungen grundlegend. Gesetze und Verordnungen müssen ein fester Bestandteil bei der Planung und Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sein. Die Einhaltung der verschiedenen Anforderungen muss in jedem Prozess des Unternehmens sichergestellt werden. Änderungen an Verordnungen oder Gesetzen können gravierende Auswirkungen auf bestehende Geschäftsprozesse haben und neue Herausforderungen für das Risikomanagement bedeuten. Ein gut organisierter Datenschutz vermindert die Anzahl an Schwachstellen, verringert das verbleibende Risiko, schützt dadurch die Rechte der Betroffenen und begrenzt potentielle Schäden für das Unternehmen.

Für die Abwehr „klassischer“ Gefahren stehen etablierte Schutz-Standards, insbesondere die Richtlinien der VdS Schadenverhütung GmbH, zur Verfügung. Nun hat VdS Schadenverhütung mit den vorliegenden Richtlinien ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Verfahren für die Etablierung und Aufrechterhaltung eines Datenschutzmanagementsystems entwickelt.

1.1 Geltungsbereich

Diese Richtlinien legen Mindestanforderungen an den Datenschutz fest und können für kleine und mittlere Unternehmen (KMU), den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen angewendet werden.

1.2 Anwendungshinweise

Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch VdS Schadenverhütung.

Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf dem Gebiet des Datenschutzes. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Dienstleister gemäß VdS. Soweit bei der Umsetzung rechtliche Anforderungen des Datenschutzes im Einzelfall zu klären oder überprüfen sind, empfiehlt sich die Inanspruchnahme Rechtskundiger nach Rechtsdienstleistungsgesetz (RDG). Die Qualifizierung als Berater zum Datenschutzmanagement berechtigt nur zur Rechtsberatung, wenn die Voraussetzungen des RDG gleichzeitig erfüllt sind.

Aus Gründen der leichteren Lesbarkeit wird in diesen Richtlinien auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form verwendet. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten.

1.3 Gültigkeit

Diese Richtlinien gelten ab dem 15.12.2017.

2 Normative Verweise

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.

BSI-Standard 200-1	Managementsysteme für Informationssicherheit
BSI-Standard 200-3	Risikoanalyse auf der Basis von IT-Grundschutz
DIN 66398:2016-05	Leitlinie Löschkonzept
DIN EN ISO 9001	Qualitätsmanagementsysteme – Anforderungen
ISO 31000	Risk Management – Principles and guidelines
ISO/IEC 27001	Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27005	Information technology — Security techniques — Information security risk management
ISO/IEC 29134	Risk Management – Principles and guidelines
VdS 3473	Cyber-Security für kleine und mittlere Unternehmen (KMU), Anforderungen

3 Glossar

Administrator: Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems oder Netzwerks.

Aufgabe: Dauerhaft wirksame Aufforderung an Handlungsträger, festgelegte Handlungen wahrzunehmen.

Auftragsverarbeiter: Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Bedrohung: Möglichkeit, dass ein Schaden entsteht.

Betroffene Person: Identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen.

Datenschutzbeauftragter (DSB): Person, die die Aufgaben gem. Abschnitt 4.4 wahrnimmt.

Datenschutzmanagementsystem (DSMS): Systematischer, standardisierter und dokumentierter Ansatz zur Umsetzung der Anforderungen an den betrieblichen Datenschutz.

Datenschutzmanager (DSM): Person, die die Aufgaben gem. Abschnitt 4.3 wahrnimmt.

Datenschutzprozess: Organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung des Datenschutzes.

Datenschutzteam (DST): Gremium, das die Aufgaben gem. Abschnitt 4.5 wahrnimmt.

Datenschutzvorfall: Unerwünschtes Ereignis, bei dem mit einer hohen Wahrscheinlichkeit ein unbefugter oder rechtswidriger Zugriff auf personenbezogene Daten erfolgt ist.

Funktion: Bündel von Aufgaben, durch die ein Teil des Unternehmungsziels erreicht werden soll.

Gefahr: Mögliche Schadwirkung auf ein zu schützendes Objekt.

Gefährdung: Bedrohung plus Schwachstelle.

Informationssicherheit: Schutz von Informationen hinsichtlich gegebener Sicherheitsanforderungen (bspw. Vertraulichkeit, Verfügbarkeit oder Integrität).

Informationssicherheitsbeauftragter (ISB): Mitarbeiter, der umfassend verantwortlich für den Informationssicherheitsprozess ist, insbesondere für dessen Initiierung, Planung, Umsetzung und Steuerung.

Informationssicherheitsprozess: Organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit.

Integrität: Korrektheit (Unversehrtheit) von Informationen bzw. die korrekte Funktionsweise der Datenverarbeitung.

IT-Infrastruktur: Alle langlebigen Einrichtungen materieller und institutioneller Art für den Betrieb von Anwendungssoftware.

IT-System: Technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit bildet. Typische IT-Systeme sind z. B. Server, Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten.

IT-Verantwortlicher: Leiter der IT-Abteilung, bzw. das für die Informationstechnik zuständige Management.

Leitlinie: Dokument des Topmanagements, das ein Ziel des Unternehmens und seine Priorität definiert sowie Verantwortlichkeiten zu seiner Erreichung festlegt.

Mitarbeiter: Natürliche Person, die in einem Vertragsverhältnis mit dem Unternehmen steht und Natürliche Person, die in einem Vertragsverhältnis mit dem Unternehmen oder in einem öffentlich-rechtlichen Dienst- und Treueverhältnis mit der Verwaltung steht und eine oder mehrere Positionen im Unternehmen bzw. der Verwaltung einnimmt.

Mobiler Datenträger: Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z. B. Speichersticks und -karten sowie externe Festplatten, aber auch Speichermedien wie CD-ROMs, DVDs und Disketten.

Organisationseinheit: Einheit, in der artverwandte (Teil-)Aufgaben oder Tätigkeiten zusammengefasst sind.

Position: Platz, den ein Mitarbeiter in der Hierarchie eines Unternehmens einnimmt.

Projektverantwortlicher: Person, die für die ordnungsgemäße Durchführung eines Projekts des Unternehmens verantwortlich ist.

Prozess: System von Tätigkeiten, das Eingaben mit Hilfe von Mitteln in Ergebnisse umwandelt.

Prozessverantwortlicher: Person, die inhaltlich für einen oder mehrere Geschäftsprozesse verantwortlich ist. Sie besitzt den Überblick über die für diese Geschäftsprozesse benötigten Ressourcen und über die an sie gestellten Anforderungen.

Ressource: Betriebsmittel, das dem Unternehmen gehört oder ihm zur Verfügung steht.

Richtlinien: Dokumente, die im Sinne von Verfahrensanweisungen Vorgaben des Managements zum Datenschutz beinhalten, welche die DS-Leitlinie unterstützen und konkretisieren.

Rolle: Bündel von Verhaltenserwartungen und Verantwortlichkeiten, die an eine Position gerichtet wird.

Risiko: Eine nach Eintrittswahrscheinlichkeit und Schadenshöhe bewertete Gefährdung.

Schwachstelle: Umstand der es ermöglicht, dass eine Bedrohung mit einem zu schützenden Objekt räumlich und/oder zeitlich zusammentreffen kann.

Störung: Situation, in der Prozesse oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorgenommen werden.

Topmanagement: Oberste Führungsebene, wie z. B. Vorstände, Geschäftsführer oder Behördenleiter.

Verantwortlicher: Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verarbeitung: Summe aus Verarbeitungstätigkeiten, die zusammen mit den dafür benötigten personenbezogenen Daten einem definierten Zweck dienen und eine abgeschlossene Einheit bilden.

Verarbeitungstätigkeit: Handlung, die auf personenbezogene Daten einwirkt oder diese nutzt, bzw. benötigt, wie z. B. das Erheben, Erfassen, Organisieren, Speichern, Aufbewahren, Offenlegen, Auslesen, Abgleichen, Abfragen, Weitergeben, Verknüpfen, Löschen, Vernichten oder Sperren von personenbezogenen Daten.

Verbindung: Kanal, über den Daten ausgetauscht werden können.

Verfahren: Festgelegte Art und Weise, wie ein Prozess (oder auch eine einzelne Tätigkeit innerhalb eines Prozesses) auszuführen ist.

Verfügbarkeit: Wahrscheinlichkeit, dass ein System bestimmte Anforderungen zu, bzw. innerhalb, eines vereinbarten Zeitrahmens erfüllt. Die Verfügbarkeit von Informationen ist vorhanden, wenn diese stets wie vorgesehen genutzt werden können.

Vertraulichkeit: Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Die Vertraulichkeit von Informationen ist gegeben, wenn nur der dafür bestimmte Empfängerkreis diese lesen bzw. interpretieren kann.

Zugang: Einrichtung, die es erlaubt, mit der nichtöffentlichen IT des Unternehmens zu kommunizieren.

Zugriff: Nutzung einer Ressource.

4 Organisation des Datenschutzes

Datenschutz ist dynamisch und für jedes Unternehmen individuell. Um mit möglichst geringem Aufwand das vom Unternehmen angestrebte Sicherheitsniveau zu definieren, umzusetzen und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage anzupassen, ist es notwendig, einen entsprechenden Prozess (Datenschutzprozess) zu etablieren.

4.1 Verantwortlichkeiten

Verantwortlichkeiten für den Datenschutzprozess MÜSSEN eindeutig und widerspruchsfrei zugewiesen werden.

4.1.1 Zuweisung und Dokumentation

Es MUSS für jede Verantwortlichkeit im Datenschutzprozess dokumentiert werden:

1. welche Ziele erreicht werden sollen
2. für welche Ressourcen die Verantwortlichkeit besteht
3. welche Aufgaben erfüllt werden müssen, damit die Ziele erreicht werden
4. welche Berechtigungen an die Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können
5. welche Ressourcen für die Wahrnehmung der Verantwortlichkeit zur Verfügung stehen
6. wie und durch welche Position(en) die Erfüllung der Verantwortlichkeit überprüft wird
7. welche Positionen die Verantwortlichkeit wahrnehmen

4.1.2 Funktionstrennungen

Bei der Verteilung der Verantwortlichkeiten im Datenschutzprozess MUSS das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten DÜRFEN NICHT von ein und derselben Person oder Organisationseinheit wahrgenommen werden

Wenn eine Funktionstrennung nicht oder nur mit einem unverhältnismäßig hohen Aufwand durchführbar ist, KÖNNEN widersprüchliche Verantwortlichkeiten von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

In diesem Fall MÜSSEN folgende Anforderungen erfüllt werden:

1. Die rechtliche Zulässigkeit wurde geprüft.
2. Es werden andere Maßnahmen wie Überwachung von Tätigkeiten, Kontrollen oder Leitungsaufsicht umgesetzt.
3. Die nicht durchgeführte Funktionstrennung wird in der Dokumentation der Funktionsverteilung besonders hervorgehoben und begründet.

Um Zuständigkeitslücken oder Überschneidungen von Verantwortlichkeiten im Datenschutzprozess zu vermeiden, MÜSSEN die entsprechenden Regelungen jährlich vom Datenschutzmanager (DSM) bzw. falls bestellt vom Datenschutzbeauftragten (DSB) überprüft werden.

4.1.3 Ressourcen

Um Verantwortlichkeiten im Datenschutzprozess wahrzunehmen, MÜSSEN die entsprechenden Mitarbeiter im erforderlichen Umfang (siehe Abschnitt 4.1.1) von anderen Tätigkeiten freigestellt werden.

4.1.4 Delegieren von Aufgaben

Verantwortliche für den Datenschutz DÜRFEN Aufgaben an andere Personen delegieren.

Die Verantwortung für delegierte Aufgaben verbleibt jedoch bei ihnen, sodass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen MÜSSEN.

Wenn Verantwortlichkeiten des DSB oder Verantwortlichkeiten an den DSB delegiert werden sollen, MUSS zuvor die rechtliche Zulässigkeit geprüft werden.

4.2 Topmanagement

Das Topmanagement MUSS sich zur Wahrnehmung folgender Verantwortlichkeiten verpflichten:

1. übernehmen der Gesamtverantwortung für den Datenschutz
2. übernehmen der Verantwortlichkeit für den Datenschutzprozess
3. in Kraft setzen von Richtlinien für den Datenschutz (DS-Richtlinien)
4. bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für den Datenschutz
5. einbetten des Datenschutzes in die Strukturen, Hierarchien und Arbeitsabläufe des Unternehmens

4.3 Datenschutzmanager (DSM)

Das Topmanagement MUSS die Verantwortlichkeiten eines Datenschutzmanagers (DSM) einem Mitarbeiter zuweisen.

Dieser MUSS folgende Verantwortlichkeiten wahrnehmen:

1. initiieren, planen, umsetzen und steuern des Datenschutzmanagementsystems
2. erarbeiten konkreter Verbesserungsvorschläge
3. unterstützen des Topmanagements bei der Erarbeitung und jährlichen Überprüfung sowie bei der Anpassung der DS-Leitlinie (siehe Kapitel 5)
4. unterstützen des Topmanagements in zentralen Fragen des Datenschutzes
5. erarbeiten und jährliches überprüfen sowie anpassen aller DS-Richtlinien
6. untersuchen von datenschutzrelevanten Ereignissen
7. einleiten und steuern von Sensibilisierungs- und Schulungsmaßnahmen
8. Ansprechpartner bei Projekten mit Auswirkungen auf den Datenschutz, sowie bei der Einführung neuer Software und IT-Systeme sein, um sicherzustellen, dass datenschutzrelevante Aspekte ausreichend beachtet werden
9. jährliches berichten an den Datenschutzbeauftragten (falls bestellt), andernfalls an das Topmanagement über den aktuellen Stand des Datenschutzes im Unternehmen, insbesondere über Risiken und datenschutzrelevante Vorfälle
10. wahrnehmen der Rolle des zentralen Ansprechpartners für Belange des Datenschutzes, sofern kein Datenschutzbeauftragter bestellt

4.4 Datenschutzbeauftragter (DSB)

Wenn das Unternehmen gesetzlich dazu verpflichtet ist, MUSS das Topmanagement die Verantwortlichkeiten eines Datenschutzbeauftragten (DSB) einem Mitarbeiter zuweisen.

Dieser MUSS folgende Verantwortlichkeiten wahrnehmen:

1. beraten bei der Durchführung der Datenschutz-Folgeabschätzungen (DSFA)
2. Ansprechpartner bei Projekten mit Auswirkungen auf den Datenschutz, sowie bei der Einführung neuer Software und IT-Systeme sein, um sicherzustellen, dass datenschutzrechtliche Aspekte ausreichend beachtet werden
3. jährliches berichten an das Topmanagement über den aktuellen Stand des Datenschutzes im Unternehmen, insbesondere über Risiken und datenschutzrelevante Vorfälle
4. wahrnehmen der Rolle des zentralen Ansprechpartners für Belange des Datenschutzes für betroffene Personen, das Unternehmen und dessen Beschäftigte sowie für die Aufsichtsbehörde.
5. unterrichten und beraten des Topmanagements und der Mitarbeiter hinsichtlich der geltenden Datenschutzvorschriften
6. überwachen der Einhaltung der geltenden Datenschutzvorschriften

Dabei MUSS das Topmanagement sicherstellen, dass der DSB

1. bei der Erfüllung seiner Aufgaben unabhängig ist
2. wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden kann
3. frühzeitig in alle Fragen des Datenschutzes eingebunden wird
4. die für seine Aufgaben notwendigen Zugangsberechtigungen erhält
5. mit seinen Kontaktdaten veröffentlicht und der zuständigen Aufsichtsbehörde mitgeteilt wird

4.5 Datenschutzteam (DST)

Das Topmanagement MUSS ein Datenschutzteam (DST) bestellen.

In diesem MÜSSEN folgende Unternehmenseinheiten bzw. Positionen persönlich oder durch einen Repräsentanten vertreten sein:

1. DSM
2. DSB (falls bestellt)
3. Topmanagement
4. ISB (siehe Abschnitt 11)
5. Mitarbeiter (z. B. über den Betriebsrat)

Das Team MUSS den DSM bei folgenden Tätigkeiten unterstützen:

1. erstellen der DS-Leitlinie und aller DS-Richtlinien
2. jährliches überprüfen der DS-Leitlinie und aller DS-Richtlinien
3. unternehmensweites koordinieren und lenken der Datenschutzmaßnahmen
4. erkennen neuer Gefährdungen

4.6 Eigentümer einer Verarbeitung

Für jede Verarbeitung MÜSSEN die Verantwortlichkeiten eines Eigentümers einem Mitarbeiter zugewiesen werden.

Der Eigentümer einer Verarbeitung MUSS folgende Verantwortlichkeiten wahrnehmen:

1. Unterstützung bieten bei allen Fragen zur Verarbeitung, insbesondere bei der Ermittlung der im Unternehmen verarbeiteten personenbezogenen Daten und vorhandenen Verarbeitungen (siehe Kapitel 9), der Überprüfung der Verarbeitung (siehe Abschnitt 10.13) sowie der Untersuchung von Datenschutzvorfällen (siehe Kapitel 13)
2. melden des Bedarfs an Sensibilisierungs- und Schulungsmaßnahmen an den DSM

4.7 Vorgesetzte

Vorgesetzte, die Verantwortung für Mitarbeiter tragen, MÜSSEN sicherstellen, dass die getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz in Bezug auf die ihnen unterstellten Mitarbeiter umgesetzt werden.

4.8 Mitarbeiter

Mitarbeiter MÜSSEN die folgenden Aufgaben wahrnehmen:

1. einhalten und umsetzen aller sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zum Datenschutz
2. melden von Datenschutzvorfällen (siehe Abschnitt 13.1).

4.9 Projektverantwortliche

Projektverantwortliche MÜSSEN den DSB (falls bestellt), anderenfalls den DSM bei allen Projekten mit Auswirkung auf die Verarbeitung personenbezogener Daten konsultieren, um sicherzustellen, dass datenschutzrelevante Aspekte ausreichend beachtet werden.

4.10 Auftragsverarbeiter

Das Unternehmen MUSS Auftragsverarbeiter verpflichten, die sie betreffenden Maßnahmen und Regelungen zum Datenschutz einzuhalten bzw. umzusetzen (siehe Abschnitt 12.1.4).

5 Leitlinie zum Datenschutz (DS-Leitlinie)

Die Leitlinie zum Datenschutz (DS-Leitlinie) ist das zentrale Dokument für den gesamten Datenschutzprozess. In ihr werden die zu erreichenden Ziele durch das Topmanagement vorgegeben und Verantwortlichkeiten sowie Befugnisse definiert.

5.1 Allgemeine Anforderungen

Die Leitlinie MUSS vom Topmanagement beschlossen und bekannt gegeben werden.

Das Topmanagement MUSS die Leitlinie jährlich auf Aktualität prüfen und ggf. eine Aktualisierung veranlassen.

Die Leitlinie MUSS nach jeder Aktualisierung zeitnah bekannt gegeben werden und in der jeweils aktuellen Form den Mitarbeitern zur Verfügung stehen.

5.2 Inhalte

Die Leitlinie MUSS folgende Anforderungen erfüllen:

1. Sie definiert die Ziele und den Stellenwert des Datenschutzes im Unternehmen.
2. Sie verpflichtet das Unternehmen, die rechtlichen Anforderungen des Datenschutzes umzusetzen.
3. Sie definiert sämtliche Positionen für den Datenschutzprozess und weist auf deren Aufgaben hin.
4. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

6 Richtlinien zum Datenschutz (DS-Richtlinien)

Zur Unterstützung und Konkretisierung der DS-Leitlinie ist es notwendig, weitere Vorgaben für den Datenschutz zu verabschieden und in einzelnen Dokumenten, den DS-Richtlinien, zu sammeln.

6.1 Allgemeine Anforderungen

Jede DS-Richtlinie MUSS vom DSM unter Mitarbeit des DST erstellt und vom Topmanagement in Kraft gesetzt werden.

Der DSM MUSS jede DS-Richtlinie jährlich auf Aktualität prüfen und ggf. eine Aktualisierung veranlassen.

Bei der Erstellung und Anpassung von DS-Richtlinien SOLLTEN alle gesetzlichen, behördlichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.

DS-Richtlinien MÜSSEN nach jeder Aktualisierung den Zielgruppen zeitnah bekannt gegeben werden.

Dies MUSS in einer für die Zielgruppe zugänglichen und verständlichen Form geschehen, bspw. im Zuge einer Schulung.

DS-Richtlinien MÜSSEN im Unternehmen umgesetzt oder vom Topmanagement aufgehoben werden.

6.2 Inhalte

Jede DS-Richtlinie MUSS folgende Anforderungen erfüllen:

1. Sie enthält, für wen sie verbindlich ist.
2. Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll.
3. Sie verstößt nicht gegen die DS-Leitlinie oder andere Richtlinien.
4. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

DS-Richtlinien KÖNNEN Ausnahmen ermöglichen, sofern diese begründet, genehmigt und dokumentiert werden.

DS-Richtlinien KÖNNEN auf weitere mitgeltende Unterlagen verweisen.

6.3 DS-Richtlinien für Mitarbeiter

Es MÜSSEN DS-Richtlinien für den Umgang mit personenbezogenen Daten festgelegt werden, die für alle Mitarbeiter (inkl. aller Führungsebenen) verbindlich sind:

1. Personenbezogene Daten werden nicht eigenmächtig verarbeitet. Es werden ausschließlich die vom Unternehmen bereitgestellten Verarbeitungen genutzt.
2. Der Bedarf weiterer Verarbeitungen wird der zuständigen Stelle gemeldet.
3. Mitarbeiter halten alle sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zur Sicherheit personenbezogener Daten ein, bzw. setzen diese um.
4. Mitarbeiter melden mögliche Datenschutzvorfälle an den DSM.

Das Unternehmen SOLLTE Ausnahmen von den obigen DS-Richtlinien in besonders begründeten Fällen ermöglichen.

Ausnahmen MÜSSEN vom DSM im Vorfeld genehmigt und zusammen mit ihrer Begründung dokumentiert werden.

6.4 DS-Richtlinien für Verarbeitungen

Es MÜSSEN DS-Richtlinien für die Gestaltung von Verarbeitungen festgelegt werden, die für das gesamte Unternehmen verbindlich sind:

1. Personenbezogenen Daten werden nur aufgrund einer wirksamen Einwilligung des Betroffenen oder einer anderen Rechtsgrundlage verarbeitet. (Rechtmäßigkeit)
2. Personenbezogenen Daten werden nur für festgelegte und eindeutige Zwecke verarbeitet. Wenn der Verwendungszweck von personenbezogenen Daten geändert werden soll, wird im Vorfeld die rechtliche Zulässigkeit geprüft und ggf. die Einwilligung der Betroffenen eingeholt. (Zweckbindung)
3. Die Verarbeitung personenbezogener Daten ist für die Erreichung ihres Zwecks geeignet, erforderlich und angemessen (verhältnismäßig). (Fairness, Treu und Glauben)
4. Die Betroffenen werden über die Verwendung ihrer personenbezogenen Daten umfassend und verständlich informiert. (Transparenz)
5. Es werden nur die unbedingt benötigten personenbezogenen Daten verarbeitet. (Datenminimierung)
6. Es werden Maßnahmen etabliert, um unrichtige personenbezogene Daten zu vermeiden und zu erkennen. Wenn personenbezogene Daten im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, werden diese korrigiert oder gelöscht. (Richtigkeit)
7. Nicht mehr benötigte personenbezogene Daten werden gelöscht, sofern dem keine Aufbewahrungspflichten entgegenstehen. Personenbezogenen Daten werden anonymisiert oder pseudonymisiert, wenn deren Personenbindung nicht mehr benötigt wird. (Speicherbegrenzung)
8. Die Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten werden im Zuge einer nachvollziehbaren Risikoanalyse und -behandlung ermittelt und umgesetzt. (Vertraulichkeit, Integrität und Verfügbarkeit)
9. Eingesetzte Prozesse, Produkte und Systeme werden datenschutzfreundlich ausgewählt bzw. implementiert und standardmäßig datenschutzfreundlich konfiguriert (Datenschutz durch Technikgestaltung/Privacy by Design und Datenschutz durch Voreinstellung/Privacy by Default).
10. Die Einhaltung der DS-Richtlinien wird dokumentiert.

6.5 Weitere DS-Richtlinien

Das Unternehmen MUSS die Notwendigkeit weiterer DS-Richtlinien prüfen, insbesondere

1. Zutritts-, Zugangsrichtlinien
2. Private Nutzung der IT
3. Abwesenheitsregelung, insbesondere Zugang zum Datenbestand des Abwesenden
4. Homeoffice, Mobileoffice
5. Integration privater IT-Systeme in die Informationsverarbeitung des Unternehmens (Bring Your Own Device -BYOD)

7 Mitarbeiter

Die Mitarbeiter sind ein zentraler Faktor für die Implementierung und Aufrechterhaltung des Datenschutzes. Es ist deshalb notwendig, auch in diesem Bereich die Anforderungen des Datenschutzes zu berücksichtigen.

7.1 Vor der Einstellung

Wenn eine für den Datenschutz des Unternehmens relevante Position besetzt wird, MUSS das Unternehmen sicherstellen, dass der Bewerber über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.

7.2 Einstellung und Einarbeitung

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das im Zuge der Einstellung bzw. des Einarbeitens von neuen Mitarbeitern folgende Punkte sicherstellt:

1. Mitarbeiter verpflichten sich mittels einer schriftlichen Erklärung zur Vertraulichkeit; die Erklärung definiert auch die Pflichten in Bezug auf Datenschutz, die nach Beendigung oder Veränderung des Arbeitsverhältnisses fortbestehen.
2. Neue Mitarbeiter werden in die DS-Leitlinie, in sämtliche für sie verbindliche DS-Richtlinien und sonstige verbindliche Regelungen zum Datenschutz eingewiesen.
3. Neue Mitarbeiter werden im Umgang mit den für sie relevanten Mechanismen für die Umsetzung des Datenschutzes geschult (siehe Abschnitt 8.2).

7.3 Beendigung oder Wechsel der Anstellung

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden das bei Beendigung oder Wechsel einer Anstellung folgende Punkte sicherstellt:

1. Soweit erforderlich, werden Mitarbeiter, Kunden sowie Lieferanten und sonstige Auftragnehmer über Änderungen im Personal- und betrieblichen Bereich informiert.
2. Die Zugriffsmöglichkeiten des Mitarbeiters auf personenbezogene Daten werden umgehend überprüft und bei Bedarf angepasst.

8 Wissen

Viele Gefährdungen entstehen aus Unkenntnis oder mangelndem Problembewusstsein, oder werden zumindest durch diese Faktoren verstärkt. Deshalb ist es notwendig, dass das Unternehmen über aktuelles Wissen in Bezug auf Datenschutz verfügt, die Mitarbeiter ihre Verantwortlichkeiten verstehen und sie für ihre Aufgaben geeignet und qualifiziert sind.

8.1 Aktualität des Wissens

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, mit dem alle relevanten Stellen des Unternehmens sowie ggf. relevante externe Stellen in geeigneter Weise über geänderte rechtliche und technische Bedingungen im Bereich des Datenschutzes informiert werden.

Das Verfahren MUSS folgende Punkte sicherstellen:

1. Es werden regelmäßig aus verlässlichen Quellen Informationen über die aktuellen technischen und rechtlichen Entwicklungen im Bereich des Datenschutzes, insbesondere über neue Gefährdungen und mögliche Gegenmaßnahmen, bezogen.
2. Die Informationen werden im Hinblick auf die Bedeutung für die Maßnahmen zur Gewährleistung des Datenschutzes zeitnah ausgewertet, um geänderte Gefahrenlagen zu erkennen.
3. Die jeweils Verantwortlichen werden über die relevanten Entwicklungen zeitnah informiert.

Es SOLLTEN Kontakte und Verbindungen zu Interessengruppen und Sicherheitsforen gepflegt werden, damit die Verantwortlichen auf dem aktuellen Wissensstand sind und auf Fachinformationen und -beratung zugreifen können.

8.2 Sensibilisierung, Aus- und Weiterbildung

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das folgende Punkte sicherstellt:

1. Betroffene Mitarbeiter werden regelmäßig zielgruppenorientiert über Gefährdungen sowie ihre gesetzlichen und betrieblichen Pflichten aufgeklärt und im Umgang mit den vorhandenen Datenschutzmaßnahmen geschult.
2. Die Inhalte der Leitlinie und sämtlicher relevanter DS-Richtlinien werden vermittelt.
3. Es informiert über Konsequenzen bei Zuwiderhandlung gegen verbindliche Vorgaben.

Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einem Wissenstest oder einer Analyse abschließen, um das Verständnis der Mitarbeiter zu ermitteln.

9 Analyse

Der DSM MUSS in regelmäßigen Abständen die im Unternehmen verarbeiteten personenbezogenen Daten ermitteln und prüfen, ob die dafür benötigten Verarbeitungen definiert sind.

Das Unternehmen MUSS sicherstellen, dass entdeckte Mängel zeitnah behoben werden.

Hierfür MUSS ein Verfahren (siehe Anhang A 1) definiert werden, das die Anforderungen folgender Abschnitte erfüllt.

9.1 Prozesse

Das Unternehmen MUSS die Geschäftsprozesse identifizieren, in denen eine Verarbeitung personenbezogener Daten stattfindet.

Das Unternehmen SOLLTE dokumentieren, wer für den jeweiligen Geschäftsprozess verantwortlich ist (Prozessverantwortlicher).

Für die Identifizierung der Geschäftsprozesse SOLLTEN bereits vorhandene Dokumentationen wie z. B. Organigramme, Prozesshandbücher oder ein bereits bestehendes Verarbeitungsverzeichnis (siehe Abschnitt 10.1) hinzugezogen werden.

9.2 Verarbeitungen

Das Unternehmen MUSS seine Verarbeitungen ermitteln.

Dabei MÜSSEN folgende Anforderungen erfüllt werden:

1. Es werden die Geschäftsprozesse untersucht, in denen eine Verarbeitung personenbezogener Daten stattfindet (siehe Abschnitt 9.1).
2. Der Eigentümer der Verarbeitung wird (siehe Abschnitt 4.6) ermittelt.
3. Es wird geprüft, ob die Ergebnisse mit dem Verarbeitungsverzeichnis (siehe Abschnitt 10.1) übereinstimmen.

Für die Ermittlung der Verarbeitungen SOLLTEN die jeweiligen Prozessverantwortlichen (siehe Abschnitt 9.1) involviert und bereits vorhandene Dokumentationen wie z. B. Organigramme oder Prozesshandbücher sowie die Ergebnisse aus Abschnitt 9.1 hinzugezogen werden.

9.3 Personenbezogene Daten

Das Unternehmen MUSS für jede Verarbeitung (siehe Abschnitt 9.2) ermitteln, welche Kategorien personenbezogener Daten sie verarbeitet.

Es MUSS geprüft werden, ob die Ergebnisse mit dem Verarbeitungsverzeichnis (siehe Abschnitt 10.1) übereinstimmen.

Für die Ermittlung der Datenkategorien SOLLTEN die jeweiligen Prozessverantwortlichen (siehe Abschnitt 9.1) sowie die Eigentümer der Verarbeitung (siehe Abschnitt 4.6 und Abschnitt 9.2) involviert und bereits vorhandene Dokumentationen wie z. B. Organigramme, Prozesshandbücher oder ein bereits bestehendes Verarbeitungsverzeichnis (siehe Abschnitt 10.1) sowie die Ergebnisse aus Abschnitt 9.1 und Abschnitt 9.2 hinzugezogen werden.

10 Verarbeitungen

Für jede Verarbeitung MÜSSEN die Maßnahmen der folgenden Abschnitte implementiert werden.

10.1 Verarbeitungsverzeichnis

Das Unternehmen MUSS ein Verzeichnis seiner Verarbeitungen führen (Verarbeitungsverzeichnis).

Das Verzeichnis MUSS alle internen und alle ausgelagerten Verarbeitungen (siehe Kapitel 12) beinhalten.

Das Verarbeitungsverzeichnis MUSS den Namen und die Kontaktdaten des Unternehmens, des Topmanagements, des DSB (falls benannt) und ggf. auch die der gemeinsam Verantwortlichen (siehe Abschnitt 10.5) enthalten.

Es MUSS für jede Verarbeitung die Abschnitte 10.3 bis 10.11 dokumentieren.

Das Verarbeitungsverzeichnis SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 gelenkt werden.

10.2 Lebenszyklus

10.2.1 Etablierung und Änderung

Es MUSS ein Verfahren (siehe Anhang A 1) für die Etablierung und Änderung einer Verarbeitung implementiert werden, das folgende Punkte sicherstellt:

1. Die Anforderungen der Abschnitte 10.3 bis 10.11 werden umgesetzt.
2. Das Datenmanagement (siehe Kapitel 14) wird bei Bedarf angepasst.
3. Das Verarbeitungsverzeichnis (siehe Abschnitt 10.1) wird aktualisiert und vom DSM freigegeben.

10.2.2 Einstellung (Beendigung)

Es MUSS ein Verfahren (siehe Anhang A 1) für die Einstellung einer Verarbeitung implementiert werden, das folgende Punkte sicherstellt:

1. Bei Einstellung der Verarbeitung werden die nicht mehr benötigten personenbezogenen Daten gelöscht (siehe Abschnitt 14.1).
2. Die Verarbeitung wird nur aus dem Verarbeitungsverzeichnis gelöscht, wenn alle ihre personenbezogenen Daten gelöscht wurden.
3. Das Verarbeitungsverzeichnis (siehe Abschnitt 10.1) wird aktualisiert und vom DSM freigegeben.

10.3 Zweck

Der Zweck der Verarbeitung MUSS definiert werden.

10.4 Beschreibung

Die Verarbeitung MUSS beschrieben werden.

Die Beschreibung SOLLTE so gestaltet sein, dass sie für die Kommunikation mit den Betroffenen (siehe Abschnitt 10.7 und Abschnitt 10.12.2) und den Aufsichtsbehörden verwendet werden kann.

10.5 Gemeinsam Verantwortliche

Wenn personenbezogene Daten gemeinsam von verschiedenen Parteien verarbeitet werden, MUSS eine Vereinbarung geschlossen werden, die folgende Anforderungen erfüllt:

1. sie beschreibt, welche Partei für welche Datenschutzaufgaben verantwortlich ist, insbesondere, wer welchen Informationspflichten nachkommt und gegenüber wem die Betroffenen ihre Rechte wahrnehmen können
2. sie wird auf Nachfrage den Betroffenen zugänglich gemacht

10.6 Eigentümer

Der Eigentümer der Verarbeitung (siehe Abschnitt 4.6) MUSS ermittelt werden.

10.7 Rechtsgrundlage

Die Rechtsgrundlage der Verarbeitung MUSS ermittelt werden.

Wenn die Rechtsgrundlage auf einer Einwilligung beruht MUSS eine Vorgehensweise etabliert werden, die sicherstellt, dass die gesetzlichen Vorgaben eingehalten werden.

Insbesondere SOLLTE die Vorgehensweise die Erfüllung der folgenden Anforderungen gewährleisten:

1. *Der Betroffene wird vor seiner Einwilligung über den Zweck der Verarbeitung informiert (siehe Abschnitt 10.3).*
2. *Der Betroffene erhält vor seiner Einwilligung eine Beschreibung, anhand derer er die Datenverarbeitung nachvollziehen kann (siehe Abschnitt 10.4).*
3. *Der Betroffene wird vor seiner Einwilligung auf seine Rechte (siehe Abschnitt 10.12) hingewiesen.*
4. *Alle Informationen sind für die Betroffenen verständlich formuliert und übersichtlich strukturiert.*
5. *Alle Informationen werden nachweislich erbracht.*
6. *Die Identität des Betroffenen wird geprüft.*
7. *Der Einwilligungstext, der Zeitpunkt der Einwilligung und die erhobenen personenbezogenen Daten werden protokolliert.*
8. *Wenn sich der angebotene Dienst direkt an Kinder richtet, werden Anstrengungen unternommen, das Einverständnis der Erziehungsberechtigten einzuholen.*

10.8 Personenbezogene Daten

10.8.1 Datenkategorien

Die personenbezogenen Daten der Verarbeitung MÜSSEN ermittelt und in Kategorien eingeteilt werden.

Für jede Kategorie MUSS festlegt werden:

1. für welche Zwecke sie verwendet wird
2. ob sie zwingend für die Verarbeitung erforderlich ist
3. welche Kategorien von Personen darin betroffen sind
4. ab wann ihre Daten nicht mehr benötigt werden
5. ab wann die Personenbindung ihrer Daten nicht mehr benötigt wird
6. welche Aufbewahrungsfristen bestehen
7. welche Löschfristen bestehen
8. welchen Kategorien von Empfängern die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, sowohl innerhalb als auch außerhalb des Unternehmens

10.8.2 Datenübermittlung

Wenn personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt werden sollen, MUSS eine Vorgehensweise etabliert werden, die sicherstellt, dass dabei die gesetzlichen Vorgaben eingehalten werden.

Insbesondere SOLLTE die Vorgehensweise die Erfüllung der folgenden Anforderungen gewährleisten:

1. *Die Rechtsgrundlage wird festgestellt.*
2. *Es werden Garantien erbracht, dass ein angemessenes Datenschutzniveau bei dem Empfänger existiert.*

10.9 IT-Systeme, mobile Datenträger und Verbindungen

Für die Verarbeitung MUSS ermittelt werden, welche IT-Systeme, mobilen Datenträger und Verbindungen für das Verarbeiten, Speichern oder Übertragen von personenbezogenen Daten verwendet werden (siehe Kapitel 11).

10.10 Risikoanalyse und -behandlung

Für die Verarbeitung MUSS eine Risikoanalyse und -behandlung (siehe Anhang A2) durchgeführt werden, in der die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen untersucht werden.

Das Unternehmen MUSS sicherstellen, dass die Risikoanalyse den gesetzlichen Vorgaben entspricht.

Insbesondere SOLLTE die Risikoanalyse folgende Risiken untersuchen:

1. *unberechtigter Zugang zu Verarbeitungsanlagen (Zugangskontrolle)*
2. *unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern (Datenträgerkontrolle)*
3. *unbefugte Eingabe von personenbezogenen Daten sowie unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)*
4. *unbefugte Nutzung von IT-Systemen über Verbindungen (Netzwerke) hinweg (Benutzerkontrolle)*
5. *unbefugter Zugang der zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten auf personenbezogene Daten (Zugriffskontrolle)*
6. *es kann nicht überprüft und festgestellt werden, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)*
7. *es kann nicht nachträglich überprüft und festgestellt werden, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)*
8. *Verlust der Vertraulichkeit und Integrität bei der Übermittlung personenbezogener Daten sowie beim Transport von entsprechenden Datenträgern (Transportkontrolle)*
9. *IT-Systeme lassen sich im Störungsfall nicht wiederherstellen (Wiederherstellbarkeit)*
10. *Funktionen stehen nicht zur Verfügung oder auftretende Fehlfunktionen werden nicht gemeldet (Zuverlässigkeit)*

11. *gespeicherte personenbezogene Daten werden durch Fehlfunktionen des Systems beschädigt (Datenintegrität)*
12. *personenbezogene Daten, die im Auftrag verarbeitet werden, werden nicht entsprechend den Weisungen des Auftraggebers verarbeitet (Auftragskontrolle)*
13. *personenbezogene Daten sind nicht gegen Zerstörung oder Verlust geschützt (Verfügbarkeitskontrolle)*
14. *personenbezogene Daten die zu unterschiedlichen Zwecken erhoben wurden, werden nicht getrennt verarbeitet (Trennbarkeit)*

Risikoanalysen für vergleichbare Verarbeitungen können zusammen erstellt werden.

10.11 Datenschutz-Folgenabschätzung (DSFA)

Es MUSS geprüft werden, ob für die Verarbeitung eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden muss.

Das Unternehmen MUSS sicherstellen, dass die Prüfung den gesetzlichen Vorgaben entspricht.

I*nsbesondere SOLLTEN folgende Kriterien geprüft werden:*

1. *Vorliegen eines gesetzlichen Regelbeispiels*
2. *Positiv- und Negativlisten entsprechender Aufsichtsbehörden*
3. *Vorhandensein eines hohen Risikos für die Rechte und Freiheiten der Betroffenen (siehe Abschnitt 10.10)*
4. *Gesetzliche Befreiung von der Pflicht zur Durchführung einer DSFA*

Das Unternehmen MUSS die notwendigen DSFA durchführen.

Dies SOLLTE auf Basis eines anerkannten Standards wie ISO/IEC 29134 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS das Unternehmen sicherstellen, dass die DSFA den gesetzlichen Vorgaben entspricht.

Insbesondere SOLLTE die DSFA folgende Anforderungen erfüllen:

1. *Der DSB begleitet die DSFA beratend.*
2. *Es wird überprüft, ob ein im Rahmen der Risikoanalyse zuvor bejahtes voraussichtlich hohes Risiko tatsächlich auch hoch ist.*
3. *Es wird eine Dokumentation der DSFA erstellt, die folgende Informationen beinhaltet:*
    a. *eine systematische Beschreibung der beabsichtigten Verarbeitungen*
    b. *deren Zwecke*
    c. *die legitimen Interessen des Verantwortlichen an den Verarbeitungen*
    d. *eine Bewertung, inwieweit die Verarbeitung zur Erreichung des jeweiligen Zwecks notwendig und verhältnismäßig sind*
    e. *eine Bewertung der Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen, die mit den Verarbeitungen verbunden sind*
    f. *die beabsichtigten Abhilfemaßnahmen zur Bewältigung der dargestellten Risiken*
    g. *falls erfolgt das Einbinden der Betroffenen*

Wenn die DFSA trotz der beabsichtigten Abhilfemaßnahmen mit hohen Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen verbunden ist, MUSS die entsprechende Aufsichtsbehörde konsultiert werden.

10.12 Betroffenenrechte

10.12.1 Anfrage und Reaktion

Es MUSS ein Verfahren (siehe Anhang A 1) für die Entgegennahme und Behandlung von Anfragen implementiert werden.

Das Unternehmen MUSS sicherstellen, dass mit dem Verfahren die entsprechenden gesetzlichen Anforderungen erfüllt werden.

Insbesondere SOLLTEN folgende Anforderungen geprüft werden:

1. *Anfragen können von den Betroffenen leicht gestellt werden.*
2. *Die Anfrage wird dokumentiert.*
3. *Die Identität des Betroffenen wird geprüft.*
4. *Es wird geprüft, ob ein Versagungsgrund besteht.*
5. *Jede Auskunftserteilung erfolgt nachweislich und innerhalb der gesetzlichen Fristen.*
6. *Wenn die Auskunft über ein unsicheres Medium wie z. B. E-Mail erfolgt, wird zuvor das Einverständnis des Betroffenen eingeholt.*

Die Erfüllung der Anforderungen KANN durch standardisierte Texte, Tabellen oder Checklisten vereinfacht werden.

Wenn im Zuge der Abarbeitung einer Anfrage Mängel erkannt werden, SOLLTE eine Nachbereitung stattfinden, bei der konkrete Verbesserungen erarbeitet werden mit dem Ziel, zukünftige Anfragen zu vermeiden bzw. die Betroffenenrechte mit möglichst geringem Aufwand zu erfüllen.

10.12.2 Erfüllung

Für die Verarbeitung MUSS eine Vorgehensweise zur Erfüllung sämtlicher Betroffenenrechte implementiert und dokumentiert werden.

Das Unternehmen MUSS sicherstellen, dass die Vorgehensweise den gesetzlichen Vorgaben entspricht.

Insbesondere SOLLTEN folgende Anforderungen geprüft werden:

1. *Recht auf Auskunft*
   a. *Es werden sämtliche personenbezogenen Daten des Betroffenen erfasst und in Kopie zur Verfügung gestellt.*
   b. *Die personenbezogenen Daten können in einem gängigen elektronischen Format exportiert werden.*
   c. *Der Betroffene erhält Auskunft über Datenkategorien, Verarbeitungszwecke, Herkunft, Empfänger oder Empfängerkategorien, Speicherdauer oder falls nicht möglich Kriterien für die Festlegung der Dauer.*
   d. *Der Betroffene wird darüber informiert, ob seine personenbezogenen Daten miteinander verknüpft und ausgewertet werden (Profiling) und wenn ja, nach welcher Logik dies geschieht.*

2. *Recht auf Löschung*
    a. *Sämtliche personenbezogenen Daten werden aus dem aktiven Datenbestand gelöscht.*
3. *Recht auf Berichtigung*
    a. *Korrekturen werden vor ihrer Umsetzung geprüft.*
    b. *Unrichtige personenbezogene Daten werden im aktiven Datenbestand berichtigt.*
4. *Recht auf Widerruf und Widerspruch*
    a. *Die Verarbeitung der betroffenen personenbezogenen Daten wird auf Antrag beendet.*
5. *Recht auf Einschränkung*
    a. *Die Verarbeitung der betroffenen personenbezogenen Daten wird auf Antrag ausgesetzt.*
    b. *Vor einer Fortsetzung der Verarbeitung wird der Betroffene hierüber informiert.*
6. *Recht auf Datenmitnahme*
    a. *Sämtliche personenbezogenen Daten des Betroffenen werden erfasst und in Kopie zur Verfügung gestellt.*
    b. *Die Daten werden in einem strukturierten, gängigen und maschinenlesbaren Format exportiert.*
    c. *Die exportierten Daten werden einem vom Betroffenen benannten Empfänger übermittelt.*
7. *Protokollierung*
    a. *Jede Durchführung wird nachvollziehbar protokolliert.*

10.13 Überprüfung

Das Unternehmen MUSS die Umsetzung und Dokumentation seiner Verarbeitungen überprüfen und erkannte Mängel beheben.

Dies SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 geschehen.

Wenn eine andere Vorgehensweise gewählt wird, so MÜSSEN folgende Anforderungen erfüllt werden:

1. Umsetzung und Dokumentation werden jährlich bei einem Drittel der Verarbeitungen überprüft.
2. Die zu überprüfenden Verarbeitungen werden nach dem Zufallsprinzip ausgewählt.
3. Wenn die jährliche Überprüfung ergibt, dass bei mehr als der Hälfte der überprüften Verarbeitungen Mängel bestehen, werden alle Verarbeitungen überprüft.
4. Erkannte Mängel werden zeitnah behoben.

11 Informationssicherheit

Das Unternehmen MUSS die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen auf Dauer sicherstellen (Informationssicherheitsprozess).

Der Informationssicherheitsprozess MUSS so gestaltet werden, dass die Anforderungen des Datenschutzes berücksichtigt werden und er sämtliche IT-Systeme, mobilen Datenträger und Verbindungen abdeckt, mit denen personenbezogene Daten verarbeitet, übertragen oder gespeichert werden (siehe Abschnitt 10.9).

Dies SOLLTE auf Basis eines anerkannten Standards wie z. B. VdS 3473, IS0 27001 oder BSI 200-1 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS der Informationssicherheitsprozess folgende Anforderungen erfüllen:

1. Die Anforderungen an die Informationssicherheit werden ermittelt.
2. Die durch den Informationssicherheitsprozess zu erreichenden Ziele werden durch das Topmanagement vorgegeben.
3. Die Verantwortlichkeiten und Befugnisse für den Informationssicherheitsprozess werden vom Topmanagement eindeutig und widerspruchsfrei zugewiesen, insbesondere wird ein Informationssicherheitsbeauftragter (ISB) benannt.
4. Es werden Vorgaben für die Informationssicherheit durch das Topmanagement beschlossen (Richtlinien), die den sicheren Umgang mit der IT-Infrastruktur definieren.
5. Das angestrebte Niveau der Informationssicherheit wird definiert, durch technische und organisatorische Maßnahmen umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst.
6. Risiken werden identifiziert, bewertet und behandelt. Risiken werden nur aufgrund einer Entscheidung oder Vorgabe des Topmanagements akzeptiert.

Durch geeignete Verfahren (siehe Anhang A 1) wird sichergestellt, dass

1. bei Einstellung, Einarbeitung sowie Beendigung oder Wechsel der Anstellung von Mitarbeitern die Anforderungen der Informationssicherheit berücksichtigt werden.
2. das Unternehmen über aktuelles Wissen in Bezug auf Informationssicherheit verfügt.
3. die Mitarbeiter ihre jeweiligen Verantwortlichkeiten verstehen und für ihre Aufgaben geeignet und qualifiziert sind.
4. Zugänge und Zugriffsrechte strukturiert verwaltet werden.
5. eine strukturierte Datensicherung vorhanden ist.
6. Störungen und Ausfälle in der elektronischen Datenverarbeitung rechtzeitig erkannt und behandelt werden.
7. Informationssicherheitsvorfälle rechtzeitig erkannt und behandelt werden.

12 Auftragsverarbeitung

Nutzen und Anbieten von Auftragsverarbeitungen setzt bei Kunden und Anbietern ein strukturiertes Vorgehen voraus.

12.1 Als Auftraggeber

Wenn Verarbeitungen ausgelagert werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung hilft dem Unternehmen dabei, Haftungsrisiken vorzubeugen.

12.1.1 DS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS das Unternehmen in einer DS-Richtlinie festlegen, unter welchen Bedingungen eine Verarbeitung ausgelagert werden darf.

12.1.2 Vorbereitung

Für Jedes Vorhaben, das zur Auslagerung einer Verarbeitung führt, MÜSSEN folgende Punkte dokumentiert werden:

1. welche Verarbeitungen ausgelagert werden sollen
2. welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen in Bezug auf den Datenschutz der ausgelagerten Verarbeitungen erfüllt werden müssen
3. ob für die auszulagernden Verarbeitungen eine DSFA (siehe Abschnitt 10.11) durchzuführen ist

12.1.3 Eignung des Auftragsverarbeiters

Wenn eine Verarbeitung ausgelagert werden soll, MUSS das Unternehmen vor der Beauftragung sicherstellen und dokumentieren, dass der Auftragsverarbeiter über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.

Insbesondere SOLLTE das Unternehmen prüfen, ob der Auftragsverarbeiter über das notwendige Fachwissen, die Zuverlässigkeit und Ressourcen verfügt, die gesetzlichen, betrieblichen und vertraglichen Anforderungen zu erfüllen.

Auftragsverarbeiter KÖNNEN ihre Eignung durch entsprechende Zertifizierungen z. B. nach diesen Richtlinien nachweisen.

12.1.4 Vertragsgestaltung

Wenn Verarbeitungen ausgelagert werden sollen, so MUSS mit dem Auftragsverarbeiter ein Vertrag geschlossen werden, der folgende Anforderungen erfüllt:

1. Anforderungen an den Datenschutz
   a. er enthält die Anforderungen aus Abschnitt 12.1.2 und verpflichtet den Auftragsverarbeiter zu deren Erfüllung
2. Leistungen
   a. Der Gegenstand und die voraussichtliche Dauer der Verarbeitung werden festgelegt.

b. Die Zwecke der Auftragsverarbeitung, die Art der verarbeiteten personenbezogenen Daten und die Kategorien der betroffenen Personen werden festgelegt.

c. Es wird definiert, dass personenbezogene Daten nur auf Weisungen in Textform hin verarbeitet werden (Vertragsbestandteile oder Weisungen während der Dauer der Verarbeitung) und dass der AV entsprechende technische oder organisatorische Maßnahmen in seiner Organisation umsetzen muss.

d. Der AV wird verpflichtet und ermächtigt, auf potentielle Rechtsverstöße die durch eine Weisung entstehen könnten, aufmerksam zu machen.

e. Der AV wird ermächtigt, Weisungen, durch die ein potentieller Rechtsverstoß entstehen kann, bis zur Klärung des Sachverhalts nicht zu befolgen.

f. Der AV stellt sicher, dass die an der Verarbeitung beteiligten Mitarbeiter zur Vertraulichkeit verpflichtet sind.

3. Datensicherheit

   a. Die Sicherheitsmaßnahmen, die der Auftragsverarbeiter zum Schutz der personenbezogenen Daten des Unternehmens treffen muss, werden vereinbart.

   b. Eine Informationspflicht des Auftragsverarbeiters bei Sicherheitsvorfällen die die externen Verarbeitungen betreffen, wird vereinbart.

4. Unterstützung des Unternehmens

   a. Es werden technische und organisatorische Maßnahmen definiert, wie der AV das Unternehmen bei der Wahrung der Betroffenenrechte unterstützt, insbesondere bei Erteilung von Auskünften sowie der Korrektur oder der Löschung von personenbezogenen Daten.

   b. Die Mitwirkungspflichten des Auftragsverarbeiters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, insbesondere die vollständige Herausgabe oder Löschung der personenbezogenen Daten des Unternehmens sowie die aktive Unterstützung des Migrationsprozesses durch den AV.

   c. Die Mitwirkungspflichten bei Datenschutzvorfällen werden vereinbart, insbesondere die Unterstützung bei der Meldung an Aufsichtsbehörden und bei der Benachrichtigung von Betroffenen.

   d. Die Mitwirkungspflichten bei der Durchführung von Datenschutz-Folgeabschätzungen sowie bei der vorherigen Konsultation der Aufsichtsbehörden werden vereinbart.

5. Dokumentation und Kontrolle

   a. Es werden Dokumentationspflichten vereinbart, insbesondere jene, die das Unternehmen zum Nachweis der Einhaltung der oben genannten Punkte benötigt.

   b. Es wird vereinbart, dass der AV Inspektionen durch das Unternehmen oder einen beauftragten Prüfer bezgl. der Einhaltung der oben genannten Punkte ermöglicht und unterstützt.

   c. Der AV wird verpflichtet, ein Verzeichnis der für das Unternehmen erbrachten Verarbeitungen (siehe Abschnitt 10.1) zu führen und dem Unternehmen in der jeweils aktuellen Form zur Verfügung zu stellen.

6. Unterauftragnehmer

   a. Eine Genehmigung in Textform bei jeder Einschaltung oder Ersetzung von Unterauftragnehmern wird vereinbart.

   b. Der AV schließt mit jedem Unterauftragnehmer einen Vertrag, der ihn zur Erfüllung der oben genannten Punkte verpflichtet.

Darüber hinaus SOLLTE sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Auftragsverarbeiter nicht im gleichen Rechtsraum wie das Unternehmen befindet.

12.1.5 Überprüfung

Das Unternehmen MUSS seine AV überprüfen.

Dies KANN durch sachverständige Dritte geschehen.

Der Nachweis KANN durch Zertifikate (z. B. gemäß dieser Richtlinien), Attestate oder sonstige Bestätigungen erbracht werden.

Wenn bei einzelnen AV eine andere Vorgehensweise notwendig ist, so MÜSSEN die folgende Anforderungen erfüllt werden:

1. Bei jedem betroffenen AV wird jährlich ein Drittel der zu ihm ausgelagerten Verarbeitungen überprüft.
2. Die zu überprüfenden Verarbeitungen werden nach dem Zufallsprinzip ausgewählt.
3. Wenn die Prüfung ergibt, dass bei mehr als die Hälfte der überprüften Verarbeitungen eines AV Mängel bestehen, werden alle an den AV ausgelagerten Verarbeitungen überprüft.
4. Die Verarbeitungen werden anhand der Ergebnisse und Erkenntnisse der Prüfung zeitnah überarbeitet und geprüft, bis sie mängelfrei sind.
5. Die Durchführung und die Ergebnisse der Prüfung werden dokumentiert.

12.2 Als Auftragnehmer

Wenn Verarbeitungen angeboten werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung hilft dem Unternehmen, Haftungsrisiken vorzubeugen.

12.2.1 Vertragsgestaltung

Für jede Verarbeitung MUSS ein Vertrag mit dem Verantwortlichen gemäß Abschnitt 12.1.4 geschlossen werden.

12.2.2 Zertifizierungen

Auftragsverarbeiter SOLLTEN ihre Eignung durch entsprechende Zertifizierungen, beispielsweise nach diesen Richtlinien, nachweisen.

13 Datenschutzvorfälle

Eine angemessene Reaktion auf Datenschutzvorfälle ermöglicht es einem Unternehmen, Schäden schnell einzudämmen und beheben zu können sowie gesetzliche Anforderungen zu erfüllen. Deshalb ist es notwendig, angemessen auf Datenschutzvorfälle vorbereitet zu sein.

13.1 Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS der Umgang mit Datenschutzvorfällen in einer Richtlinie festgelegt werden.

Die DS-Richtlinie MUSS folgende Punkte sicherstellen:

1. Der Begriff des Datenschutzvorfalls wird klar definiert.

   Hierbei SOLLTE aufgezählt werden, welche Auffälligkeiten zur Meldung eines potentiellen Datenschutzvorfalles führen müssen.

2. Jeder Mitarbeiter meldet mögliche Datenschutzvorfälle an den DSM.
3. Der DSM untersucht in Zusammenarbeit mit dem DSB (falls bestellt) und ggf. den Eigentümern der betroffenen Verarbeitungen (siehe Abschnitt 4.6), dem IT-Verantwortlichen, den Administratoren und den entsprechenden Auftragsverarbeitern (siehe Kapitel 12), Datenschutzvorfälle vordringlich.
4. Es wird definiert, in welchen Fällen das Topmanagement über Datenschutzvorfälle informiert wird.
5. Es wird definiert, wie das Unternehmen intern und nach außen über akute und bewältigte Datenschutzvorfälle kommuniziert.

13.2 Erkennen

Das Unternehmen SOLLTE Maßnahmen implementieren, die es ermöglichen, Datenschutzvorfälle zu erkennen, wie z. B.

1. *technische Überwachung der IT-Infrastruktur (wie z. B. Intrusion Detection Systeme (IDS), Sensor-Systeme (Honeypots), überwachen der Zugriffe auf besonders sensible Dateien, oder erfassen und auswerten von Logmeldungen)*
2. *einrichten von anonymen Meldewegen für Mitarbeiter, Kunden und/oder Öffentlichkeit.*

13.3 Reaktion

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten eines Datenschutzvorfalls folgende Reaktionen in der angegebenen Reihenfolge sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
3. Der Vorfall wird durch Sofortmaßnahmen eingedämmt.
4. Der Vorfall wird dokumentiert, insbesondere
   a. welche Daten von welchen Personenkategorien betroffen sind
   b. wie hoch die Anzahl der Betroffenen und der Datensätze ist
   c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung
   d. eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen
   e. ggf. Maßnahmen für die Abmilderungen der möglichen negativen Folgen
5. Beweismittel werden gesichert.
6. Der Schaden wird behoben und die regulären Geschäftsprozesse wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.
8. Es wird ermittelt, ob eine gesetzliche Meldepflicht besteht und welche Vorgaben und Fristen hierbei eingehalten werden müssen.

9. Es wird geprüft, ob das Unternehmen die Betroffenen benachrichtigen oder eine öffentliche Bekanntmachung veranlassen muss.

Bei geringfügigen Vorfällen SOLLTE es möglich sein, die Punkte 2, 3, 5, 6 und 7 vorzeitig zu beenden oder auszulassen.

14 Datenmanagement

Es besteht die gesetzliche Verpflichtung, nicht mehr benötigte personenbezogene Daten zu löschen. Hierfür ist ein strukturiertes Vorgehen notwendig.

14.1 Löschen

Das Unternehmen MUSS seine gesetzlichen Löschpflichten erfüllen.

Dies SOLLTE auf Basis eines anerkannten Standards wie z. B. DIN 66398 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die folgenden Anforderungen erfüllt:

1. Für jede Datenkategorie wird gemäß der in Abschnitt 10.8.1 definierten Bedingungen eine Vorgehensweise definiert, wie und in welchem Rhythmus nach zu löschenden Daten gesucht wird und wie eine Löschung zu erfolgen hat.

   Datenkategorien mit gleichen oder ähnlichen Anforderungen KÖNNEN zusammengefasst werden.
2. Es werden der aktive Datenbestand und die archivierten Daten erfasst.
3. Der Suchlauf, das Löschen sowie auftretende Fehler werden, sofern technisch möglich, protokolliert.

14.2 Anonymisieren, Pseudonymisieren, Verschlüsseln

Wenn personenbezogene Daten zu ihrem Schutz anonymisiert, pseudonymisiert oder verschlüsselt werden, SOLLTEN Vorgehensweisen analog zu Abschnitt 14.1 etabliert werden.

Anhang A

A.1 Verfahren

Das Unternehmen MUSS die in diesen Richtlinien geforderten Verfahren planen, steuern und stetig verbessern.

Dies SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 geschehen.

Wenn eine andere Vorgehensweise gewählt wird, so MÜSSEN folgende Anforderungen erfüllt werden:

1. Es wird definiert, wer für die Durchführung verantwortlich ist.
2. Verfahren werden in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form definiert, dokumentiert und bekannt gegeben.
3. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit und Effektivität erkannt werden.
4. Umsetzung, Angemessenheit und Effektivität werden jährlich bei einem Drittel der Verfahren überprüft. Die zu überprüfenden Verfahren werden nach dem Zufallsprinzip ausgewählt. Wenn die jährliche Überprüfung ergibt, dass mehr als die Hälfte der überprüften Verfahren mängelbehaftet ist, werden alle Verfahren überprüft.

A.2 Risikoanalyse und -behandlung

Das Unternehmen MUSS die in diesen Richtlinien geforderten Risikoanalysen durchführen und erkannte Risiken zeitnah und angemessen behandeln.

Dies SOLLTE im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wie BSI-Standard 200-3, ISO/IEC 27005 oder ISO 31000 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

A.2.1 Risikoanalyse

Eine Risikoanalyse MUSS folgende Anforderungen erfüllen:

1. Die Dokumentation beinhaltet das Vorgehen für das Identifizieren und Bewerten von Risiken.
2. Die Vorgehensweise gewährleistet, dass Bedrohungen und Schwachstellen zuverlässig erkannt werden können.
3. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden und deren Eintrittswahrscheinlichkeit.
4. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

A.2.2 Risikobehandlung

Identifizierte Risiken MÜSSEN zeitnah und priorisiert behandelt werden, indem geeignete Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken (z. B. durch den Abschluss einer Versicherung) definiert, dokumentiert und umgesetzt werden.

Die Umsetzung MUSS kontrolliert und auf Wirksamkeit geprüft werden.

Wenn Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert und dies dokumentiert werden.

A.2.3 Wiederholung und Anpassung

Risikoanalysen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.

Risikoanalysen MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn einer der folgenden Faktoren auftritt:

1. Der Gegenstand der Risikoanalyse hat sich wesentlich verändert (z. B. die Hardware, die Software oder die Konfiguration eines IT-Systems).
2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
3. Die Gefährdungslage hat sich erhöht (z. B. wenn eine neue Gefährdung bekannt wurde oder eine bestehende Gefährdung sich wesentlich erhöht hat).