EuroDaT GmbH

Datenschutzrichtlinie

Vertraulichkeit: EuroDaT-intern

A.Versionsverwaltung

Version	Datum	Bearbeiter	Änderungshinweise
1.0	13.2.2025	Dr. Alexander Alldridge	erste Version

Die Revisionierung aller Datenschutzdokumente erfolgt über die Google Workspace-Versionshistorie in der Dokumentbibliothek:

Aktuelle Version:

https://docs.google.com/document/d/11dWs-PitGl613yvNpUbPLnqPg1JM28GtmGv6yg_2ems/edit?usp=sharing

Inhaltsverzeichnis

B. Mitgeltende Unterlagen und Muster-Dokumente

Verbindliche Formulare und Vorlagen im Anhang dieser Richtlinie

Folgende Formulare und Unterlagen sind verbindlicher Bestandteil dieser Datenschutzrichtlinie:

- » Richtlinien
  - Risikomanagement im Informationssicherheitsmanagement (ISMS)
  - Richtlinie zum Business Continuity Management (BCM)
  - Richtlinie für Indentitäts- und Zugriffsmanagement
  - Richtlinie Dokumentenlenkung
  - Richtlinie zur Meldung von Informationssicherheitsvorfällen
  - Richtlinie – Lieferanten und Supplier
  - IT- Konzept Informationssicherheit
  - Informationssicherheitsrichtlinie

C. Datenschutzrichtlinie

1. Einleitung

Die gesetzliche Ausgestaltung des Datenschutzes in der EU-Datenschutz-Grundverordnung (DSGVO) und in anderen den Datenschutz reglementierenden Gesetzen verfolgt das abstrakte Ziel, die Wahrung der Persönlichkeitsrechte des Einzelnen sicherzustellen. Dies kann nur wirksam geschehen, wenn der Datenschutz fester Bestandteil der Organisation ist und wenn die Mitarbeiter aller Ebenen des Unternehmens über ihre Datenschutzpflichten und -verantwortung aufgeklärt und in eine entsprechend ausgerichtete Organisation eingebunden werden.

Die übergeordneten Ziele dieser Datenschutzrichtlinie sind generell die Unterstützung der Schaffung von Datenschutz sowie die Dokumentation aller diesbezüglichen Entscheidungen.

Die vorliegende Richtlinie beinhaltet die Zusammenstellung bzw. die Dokumentation aller für das Gebiet des Datenschutzes erlassenen und gültigen organisatorischen Regeln. Die konkreten Anweisungen für Stelleninhaber in der Mitarbeiter- und Vorgesetztenfunktion gehen aus den Regelungen/Richtlinien hervor.

1.1 Datenschutzziele

Die DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen.

Die EuroDaT GmbH misst dem Schutz der Privatsphäre ihrer Mitarbeiter und Geschäftspartner sowie damit einer vertrauensvollen Zusammenarbeit einen hohen Stellenwert zu.

Ziel im Datenschutz soll es sein, den Anforderungen der Datenschutzgesetze voll Rechnung tragen.

Die Schaffung und Aufrechterhaltung eines hohen Niveaus des Datenschutzbewusstseins der Anwender, die Unternehmensleitung und EDV-Mitarbeiter sind für die EuroDaT GmbH von hoher Bedeutung.

Das Datenschutzmanagement ist in der betrieblichen Organisation fest verankert. Der betriebliche Beauftragte für den Datenschutz überwacht im Auftrag der Geschäftsführung die Einhaltung des Datenschutzes.

1.2 Geltungsbereich

Die Ausführungen in dieser Datenschutzrichtlinie sind umfassend gültig und von der Geschäftsleitung veranlasst und genehmigt.

Die nachstehenden Organisationsanweisungen dieser Datenschutzrichtlinie gelten verbindlich für alle Vorgesetzten und Mitarbeiter/Beschäftigte der EuroDaT GmbH. Darüber hinaus sind die Vorschriften auch für externe Mitarbeiter – soweit anwendbar – gültig.

Um auch den Sicherheitsstandard der EuroDaT GmbH sicherzustellen, sind Teile dieser vorliegenden Richtlinie als Vertragsinhalte mit IT-Dienstleistern zu nutzen.

1.3 Legende zu farblichen Markierungen

Zur besseren Übersicht werden verschiedene Passagen farblich hervorgehoben:

Grün hinterlegte Passagen dienen der stärkeren Hervorhebung von Inhalten und der besseren Strukturierung der Inhalte.

Passagen, die gelb/orange hervorgehoben werden, gelten für sensible Informationen und sind als zusätzliche Maßnahmen gegenüber den Basis-Maßnahmen vorgegeben.

Passagen, die rot hervorgehoben werden, gelten für hochsensible Informationen und sind als zusätzliche Maßnahmen gegenüber den Basis-Maßnahmen vorgegeben.

2. Datenschutz-Organisation

2.1 Verantwortung für den Datenschutz

Kollektiv verantwortlich für die Gewährleistung des gesetzlichen Datenschutzes ist die Geschäftsführung. Jeder Mitarbeiter trägt aber in seinem Arbeitsbereich entsprechend der verbindlichen Richtlinien eigenständig auch Verantwortung für die Umsetzung des Datenschutzes.

Durch Vorgaben dieser Datenschutzrichtlinie sowie weiterer Richtlinien und Arbeitsanweisungen wird die Verantwortung auf die Geschäftsführung sowie an die betroffenen Mitarbeiter weitergeben, so dass jeder Mitarbeiter in seinem Arbeitsbereich für die Einhaltung des Datenschutzes verantwortlich ist. Die Geschäftsführung hat die Umsetzung zu kontrollieren und bei Abweichungen entweder eine Umsetzung einzufordern oder eine alternative Maßnahme mit der Geschäftsführung und dem Datenschutzbeauftragten abzustimmen, sofern die aktuelle Maßnahme nicht sinnvoll umsetzbar ist.

2.2 Der betriebliche Datenschutzbeauftragte

Es ist die Stelle des **Datenschutzbeauftragten (DSB)** eingerichtet worden. Er ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Es ist sicherzustellen, dass dieser bei seiner Aufgabenerfüllung ausreichend unterstützt wird.

Der Datenschutzbeauftragte überwacht im Auftrag der Geschäftsleitung die Einhaltung der Datenschutz-Bestimmungen.

Der Datenschutzbeauftragte wurde durch die EuroDaT GmbH extern bestellt. Das Datenschutz-Team besteht aus:

Dirk Thomas (interner Datenschutzkoordinator)

Beatriz Loos – (externe Datenschutzbeauftragte; SiDIT GmbH, Langgasse 20, 97261 Güntersleben)

2.3 Kooperationspartner des Datenschutzbeauftragten

Die Aufgabenzusammenarbeit zwischen den nachfolgenden Bereichen bzw. Funktionen und dem DSB sieht jeweils wie folgt aus:

IT-Bereich

Im Bereich der IT bzw- IT-Sicherheit wirkt der DSB projektbegleitend bei der Entwicklung und Einführung von IT-Programmen und -Prozessen sowie bei den technischen und organisatorischen Maßnahmen mit. Der IT-Bereich unterstützt den DSB wiederum bei der Umsetzung der gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen.

Fachabteilung / Geschäftsführung

Die jeweiligen Abteilungen unterstützen den DSB bei der Sachverhaltsaufklärung im Rahmen der Bearbeitung von Datenschutzbeschwerden sowie in der Durchsetzung der

Datenschutzregelungen. Auch hat die Geschäftsführung eine Verantwortung im Hinblick auf die Kontrolle von datenschutzrechtlichen Maßnahmen innerhalb der jeweiligen Abteilung.

Einkauf / Teilnahme an Ausschreibungen

Der Einkauf, begleitet durch die Geschäftsführung, unterstützt den DSB dahingehend, datenschutzrechtliche Anforderungen insbesondere beim Outsourcing einzuhalten. Auch hat der Einkauf den DSB in diesen Prozess frühzeitig zu involvieren. Der DSB unterstützt den Einkaufsbereich bei rechtlichen Fragestellungen (wie z. B. Vertragsprüfungen).

2.4 Rechenschaftspflicht

Jedes Unternehmen ist zur Führung einer Übersicht aller Verarbeitungstätigkeiten verpflichtet. Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann und hat die inhaltlichen Anforderungen des Artikels 30 DSGVO zu entsprechen.

Alle Verfahrensverantwortlichen/ leitende Mitarbeiter haben für ihren Verantwortungsbereich die Erhebung zu veranlassen und die ausgefüllten Formblätter an den Datenschutzbeauftragten zurückzusenden. Das Verzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Weitere Dokumentationspflichten

Neben der Führung des Verzeichnisses für Verarbeitungstätigkeiten bestehen u. a. noch folgende Dokumentationspflichten:

- Nachweis der Einhaltung der Prinzipien rechtmäßiger Verarbeitung (siehe Anlage 2)
- Nachweis der Einwilligung (siehe Anlage 2.2)
- Dokumentation von Datenschutzvorfällen (siehe Kapitel 8.3)
- Datenschutz-Folgenabschätzung (siehe Kapitel 5.3.3)
- Dokumentation geeigneter Drittlandsgarantien (siehe Kapitel 7 und 9.2.3)

2.5 Unabhängige Überprüfung

Die Implementierung des Datenschutzes, die im Wesentlichen durch das vorliegende, durch die Geschäftsleitung genehmigte Richtlinie vorgegeben ist, ist durch eine unabhängige, regelmäßige Überprüfung durch den Datenschutzbeauftragten vorzunehmen. Hierzu ist ein Prüfplan zu entwickeln, in dem auch die in Rubrik B und Kapitel 2.4 genannten Unterlagen hinsichtlich Aktualität und Verbesserungspotential einbezogen werden.

Es ist in regelmäßigen Abständen ein Datenschutz-Checkup durchzuführen, welches die derzeitigen Schwächen und Schwachstellen aufdeckt. Darauf aufbauend sind Maßnahmen zur Beseitigung zu erarbeiten und innerhalb dieser Richtlinie einzuarbeiten. Darüber hinaus ist eine Risikoanalyse durchzuführen, um die Risiken hinsichtlich des Geschäfts aufzudecken und bei den IT-Sicherheitsmaßnahmen zu berücksichtigen.

Die Ergebnisse der Überprüfungen sind der Geschäftsführung in geeigneter Form mitzuteilen.

3. Personal-Richtlinie

3.1 Schulung der Mitarbeiter

Es ist in jedem Organisationsbereich durch organisatorische Maßnahmen sicherzustellen, dass die mit den IT-Systemen Arbeitenden vor erstmaliger Nutzung an Schulungen zum Datenschutz teilnehmen.

Der Datenschutzbeauftragte bietet in regelmäßigen Abständen Datenschutzschulungen an.

Die Mitarbeiter sind ferner durch eine Richtlinie/durch Richtlinien über die für Sie wesentlichen Regelungen dieser Datenschutzrichtlinie zu informieren. Hierzu ist die Informationssicherheitsrichtlinie zu nutzen (siehe mitgeltende Unterlagen; Rubrik B).

3.2 Verpflichtung der Mitarbeiter

Mitarbeiter, die unmittelbar mit der Verarbeitung personenbezogener Daten beschäftigt sind, sind bei Einstellung auf das Datengeheimnis zu verpflichten.

Unter die im Unternehmen beschäftigten Mitarbeiter fallen auch Werkstudenten, Auszubildende und Praktikanten.

3.3 Anforderungen an die Verarbeitung von Beschäftigtendaten

3.3.1 Rechtliche Grundlagen

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die

- Entscheidung über die Begründung eines Beschäftigungsverhältnisses (Bewerbung)
  oder
- nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung
- oder Beendigung

erforderlich ist.

Eine Datenverarbeitung im Rahmen eines Beschäftigungsverhältnisses kann auch durch eine Einwilligung gerechtfertigt werden; hierbei ist jedoch das bestehende Abhängigkeitsverhältnis in besonderem Maße zu berücksichtigen.

Es existiert kein Konzern-Privileg, so dass künftig auch Mutter-, Schwester- und Tochter-Unternehmen als Externe zu betrachten sind. Sofern personenbezogene Beschäftigtendaten an eine verbundene Gesellschaft weitergeleitet oder ihr Zugriff gewährt werden soll, so ist zwingend der Datenschutzbeauftragte vorab einzubinden.

Es sind die Informationspflichten aus Kapitel 10.1 zu beachten.

Eine darüber hinaus gehende Datenerhebung, -verarbeitung und -nutzung von Beschäftigtendaten ist auch zur „Aufdeckung von Straftaten“ zulässig, wenn

- zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen,
- dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat,
- die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist

- und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt,
- insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Es ist sicherzustellen, dass der Datenschutzbeauftragte im Rahmen eines solchen Verfahrens frühzeitig involviert wird.

3.3.2 Bewerbungsverfahren

Innerhalb des Bewerbungsverfahrens ist auf eine sensible Behandlung der Unterlagen und Bewerbungsdaten zu achten. Es sind nur jenen Personen die Unterlagen zur Verfügung zu stellen, die an der Personalauswahl beteiligt sind, wie z. B. Personalbereich, Leiter der personaleinstellenden Abteilung und ggf. der Betriebsrat.

Es sind nur jene Informationen beim Betroffenen einzuholen, die für eine fundierte Personalentscheidung erforderlich sind. Im Zweifelsfall ist der Datenschutzbeauftragte zu kontaktieren.

Die Informationen sind direkt beim Bewerber einzuholen. Eine Recherche im Internet oder in sozialen Netzwerken ist nur in Ausnahmefällen zulässig, was zuvor stets mit dem Datenschutzbeauftragten zu klären ist.

Nach Ablauf des Bewerbungsverfahrens sind die Unterlagen dem (abgelehnten) Bewerber zeitnah zurückzusenden und elektronische Daten zu löschen (Klagefristen können abgewartet werden; maximal sechs Monate nach der Absage). Alternativ kann der Bewerber auch informiert werden, dass seine Unterlagen auch für künftige Stellenausschreibungen genutzt werden sollen und ihm ein Widerspruchsrecht eingeräumt werden.

3.3.3 Personaleinstellung und -verwaltung

Im Rahmen der Personalverwaltung sind nur jene Daten zu erheben, zu verarbeiten und zu nutzen, die für die Abwicklung des Arbeitsvertrags erforderlich sind. Im Zweifelsfall ist der Datenschutzbeauftragte zu kontaktieren.

Personalunterlagen (beispielsweise Personalakten) und Personaldaten sind sicher zu verwahren. Hierzu sind Schränke zu verschließen, Arbeitsplätze aufzuräumen und Arbeitsstationen/-rechner zu sperren. Ferner sind Personalakten regelmäßig dahingehend zu „bereinigen“, dass jene Unterlagen/Dokumente entnommen und (sicher) vernichtet werden, deren Aufbewahrung nicht mehr erforderlich ist.

3.3.4 Weitergabe von Beschäftigtendaten

Grundsätzlich sind die Anforderungen des Kapitel 10.2 zu beachten.

Eine Übermittlung von Personaldaten ist grundsätzlich nur durch die Geschäftsführung oder Leitung der Personalabteilung oder auf dessen Genehmigung zulässig.

Im Zweifelsfall ist der Datenschutzbeauftragte zu befragen.

3.3.5 Mitarbeiter-Befragungen und -Umfragen

Der Datenschutzbeauftragte ist frühzeitig in die Planung einzubinden.

4. Berechtigungen (Zutritt, Zugang, Zugriff)

4.1 Allgemeines

Der Zutritt zu den Räumlichkeiten, der Zugang zu den IT-Diensten und der Zugriff auf Informationen ist gegen Unbefugte zu schützen und zu kontrollieren (siehe Richtlinie Indentitäts- und Zugriffmanagement, Kapitel B.

4.2 Benutzerverwaltungsrichtlinien

Es ist festzulegen, welche Benutzer zum Zugriff autorisiert sind und wie ein Benutzer oder eine Gruppe auf die Datei oder das Verzeichnis zugreifen können. Ferner ist die Stellvertretung zu regeln (siehe Richtlinie Indentitäts- und Zugriffmanagement, Kapitel B).

4.3 Vergabe und Änderung von Zugriffsrechten

Zugriffsrechte sind restriktiv zu vergeben.

Die Rechtebeantragung obliegt dem jeweiligen Fachabteilungsleiter; diese Rechte werden durch den IT-Bereich vergeben (Pflichtentrennung):

» Die Zugriffsrechte werden von dem IT-Bereich nur auf Antrag eingeräumt.

Dabei sind folgende Regelungen zu beachten:

» Zugriffsrechte sind auf für die Aufgabenerfüllung notwendige Rechte zu beschränken.

» Es ist dokumentiert festzulegen, wer welche Daten lesen, löschen, hinzufügen oder verändern darf.

» Schreibrechte sind nur dann zu erteilen, wenn reine Leserechte nicht ausreichen. Soweit nicht ausdrücklich als Schreibrechte beantragt, erfolgt die Vergabe der Rechte lediglich in Form von Leserechten.

» Auch Administrator-Rollen sind auf das Minimum zu beschränken.

Bei einer Veränderung des Aufgabengebiets eines Stelleninhabers oder einer Versetzung ist von der jeweiligen Fachabteilung zu überprüfen, inwieweit die vorhandenen Rechte für die neue Aufgabenerfüllung noch erforderlich sind. Die Löschung von darüber hinausgehenden Rechten ist möglichst umgehend beim IT-Bereich zu beantragen. Idealerweise sind die Rechte der vorherigen Stelle zu löschen und neue zu beantragen.

Die Veränderung von Zugriffsrechten ist schriftlich zu beantragen.

Folgende Ereignisse machen Änderungen an den Zugriffsrechten zwingend erforderlich:

» Eine Prüfung ergibt eine Notwendigkeit zur Anpassung.

» Das Ausscheiden von Mitarbeitern oder der Einsatz in anderen Bereichen ist dem IT-Bereich unverzüglich durch den Personalbereich mitzuteilen, damit dieser umgehend alle Zugriffsrechte löschen kann.

» Eine längere Abwesenheit (mehr als 6 Wochen) von Mitarbeitern ist dem IT-Bereich von der zuständigen Personalabteilung mitzuteilen. Diese hat im Einzelfall eine Sperrung der Zugriffsrechte zu veranlassen.

» Bei befristeten Arbeitsverhältnissen (Zeitarbeitskräfte, Praktikanten etc.) sind die Zugriffsrechte nur mit zeitlicher Begrenzung zu beantragen und einzurichten.

Ausnahmen sind zu definieren, zu genehmigen und zu dokumentieren.

4.4 Passwort-Richtlinien

Vorläufige Passwörter müssen Benutzern auf sichere Art übergeben werden. Die Verwendung von ungeschützten E-Mails ist zu vermeiden. Vorläufige Passwörter sind umgehend durch den Benutzer zu ändern (technisches Erzwingen der Änderung des Initialpassworts). Im Übrigen werden identitätsabhängige, passwortgeschützte Zugänge zu Anwendungen und Daten bereitgestellt. Das Passwort ist durch den Anwender nirgends zu notieren und ist niemandem mitzuteilen. Das Passwort darf nur dem Benutzer persönlich bekannt sein. Das Passwort des Administrators darf nur ihm bekannt sein; für den Vertretungsfall ist es versiegelt aufzubewahren.

Der Anwender/Administrator hat insbesondere die Informationssicherheitsleitlinie (Kapitel B) zu beachten

Passwörter sind bei jedem Anzeichen einer möglichen Kompromittierung des Systems oder Passworts unverzüglich zu ändern. Der Verdacht ist dem DSB zu melden (siehe Kapitel 9.2).

Zum Schutz von hochsensiblen Informationen ist die Nutzung einer Zwei-Faktor-Authentifizierung zu prüfen.

4.5 Zutrittskonzept

Firmengelände und/oder Firmengebäude sind so zu schützen, dass keine Unbefugten eintreten können. Hierzu sind diese Bereiche entweder stets verschlossen zu halten oder durch Empfangspersonal zu kontrollieren. Es sind Regeln festzulegen, unter welchen Bedingungen der Zutritt außerhalb der Geschäftszeiten möglich ist.

Gelände, Gebäude und Bereiche sind flankierend – je nach Schutzbedarf – durch Alarmanlage, Bewegungssensoren, Videoüberwachung etc. zu schützen.

Die Bereiche und/oder Büros, in denen sensible oder hochsensible Daten verarbeitet werden, sind mit einem Schließsystem auszustatten. Büros sind verschlossen zu halten, wenn diese unbesetzt sind.

Bei der Beantragung und Ausführung sind die o. g. Ziele der Zutrittsregelung und -kontrolle zu beachten.

Besucherregelungen

Personen, die – wie Besucher, Handwerker, Wartungs- und Reinigungspersonal – nicht der Institution angehören, dürfen nicht unbeaufsichtigt bleiben (außer in Räumen, die ausdrücklich dafür vorgesehen sind). Alle Mitarbeiter sind darauf hinzuweisen, dass sie

Betriebsfremde, die sie unbeaufsichtigt innerhalb des Unternehmens antreffen, von diesem Moment an unter ihre Obhut nehmen müssen.

5. Weitere technische und organisatorische Maßnahmen

5.1 Physikalische und umweltbezogene Sicherheit

In wirtschaftlich vertretbarem Umfang sind Objekte, Hard- und Software sowie die Daten/Informationen vor unbefugten Zutritt, vor unbefugter Nutzung oder Veränderung, vor Sabotage, vor Ausfall und Diebstahl zu sichern.

5.2 Beschaffung, Abnahme, Freigabe

5.2.1 Beschaffung von Hard- und Software

Soft- und Hardware darf nur beschafft werden, wenn sie den datenschutzrechtlichen Anforderungen genügt. Daher ist der Datenschutzbeauftragte frühzeitig in die Planungen einzubinden. Analoge Anforderungen bestehen auch für selbst erstellte Soft- und Hardware.

Abnahmekriterien für neue Informationssysteme, Updates und neue Versionen sind zu schaffen und geeignete Systemtests vor der Abnahme durchzuführen.

Sofern Software, Updates oder Patches über das Internet beschafft werden, so sind diese nur von vertrauenswürdigen Quellen und nur durch Berechtigte herunterzuladen. Diese Programme sind automatisch auf Viren zu untersuchen. Eine automatische Installation ohne vorherige Prüfung ist zu vermeiden.

Es sind die Vorgaben aus dem Kapitel 5.2.2, 5.3 und 5.4.2 zu beachten.

5.2.2 Entwicklung, zur Abnahme und Freigabe von Software

Zur Systementwicklung und -wartung sind Sicherheitsanforderungen zu analysieren und zu spezifizieren. Der Datenschutzbeauftragte ist frühzeitig einzubeziehen.

Es ist zwischen Entwicklungs-, Test- und Einsatzumgebung zu trennen. System- und Übernahmetests benötigen gewöhnlich erhebliche Mengen an Testdaten, die den Daten im laufenden System möglichst nahe kommen. Die Verwendung von personenbezogenen Echt-Daten aus Produktivsystemen ist zu vermeiden. Falls solche Informationen benutzt werden, sind sie vor dem Gebrauch zu anonymisieren.

5.3 Einführung von IT-Systemen

Der Datenschutzbeauftragte ist hierzu frühzeitig in die Planung einzubinden.

5.3.1 Risikobewertung

Sofern innerhalb des Systems personenbezogene Daten verarbeitet werden, so ist vorab eine Analyse der Risiken für die Rechte und Freiheiten natürlicher Personen durch den Datenschutzbeauftragten durchzuführen.

Dies gilt neben Neueinführungen von Systemen auch für Änderungen (Update, Upgrade, Ausweitung des Funktionsumfangs, Änderungen der technischen und organisatorischen Maßnahmen etc.), wenn hierdurch eine geänderte Risikobewertung zu erwarten ist.

Die Risikobewertung ist zu dokumentieren.

Hierzu ist gemeinsam mit dem Datenschutzbeauftragten ein Verfahren zu etablieren, welches die Risikobewertung objektiviert und operationalisiert. Das Verfahren orientiert sich an der Klassifizierung von Informationen (siehe Kapitel 4).

5.3.2 Datenschutz-Folgeabschätzung

Sofern das Ergebnis dieser Risikobewertung ist (siehe 6.3.1), das voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so muss vor der Inbetriebnahme des Systems vorab eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt werden.

Die Datenschutz-Folgenabschätzung ist zu dokumentieren.

Die Datenschutz-Folgenabschätzung erfolgt durch den Datenschutzbeauftragten. Daher ist dieser frühzeitig einzubinden.

Hierzu ist gemeinsam mit dem Datenschutzbeauftragten ein Verfahren zu etablieren, welche die Datenschutz-Folgenabschätzung objektiviert und operationalisiert.

Geht aus der Datenschutz-Folgenabschätzung hervor, dass trotz Maßnahmen zur Risikoeindämmung (technische und organisatorische Maßnahmen) hinsichtlich des beabsichtigten Verarbeitungsvorgangs ein hohes Risiko für die betroffene Person besteht, so ist die zuständige Aufsichtsbehörde zu konsultieren („Vorherige Konsultation“). Für die Kommunikation mit der Aufsichtsbehörde ist der Datenschutzbeauftragte zuständig.

5.3.3 Privacy by Design

Es sind frühzeitig geeignete technische und organisatorische Maßnahmen zur Umsetzung und zur Einhaltung der Datenschutzgrundsätze der DSGVO zu implementieren. Die konkreten organisatorischen und technischen Maßnahmen – wie z. B. Maßnahmen zur Pseudonymisierung – sind anhand einer Verhältnismäßigkeitsabwägung zu bestimmen.

Der Datenschutzbeauftragte ist hierzu frühzeitig in die Planung einzubinden.

5.3.4 Privacy by Default (Datenschutzfreundliche Voreinstellungen)

Neben den Anforderungen des Kapitels 5.3.3 sind auch geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass Voreinstellungen
– wie beispielsweise bei Online-Diensten – so ausgestaltet sind, dass nur die Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Der Datenschutzbeauftragte ist hierzu frühzeitig in die Planung einzubinden.

5.4 Wartungsvereinbarungen

5.4.1 Allgemeines

Um ein möglichst störungsfreies Arbeiten mit Hard- und Softwarekomponenten sicherzustellen, müssen diese ordnungsgemäß verwaltet und gewartet werden. Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden.

Generell ist eine „Wartung vor Ort“ einer „Fernwartung“ vorzuziehen.

Fernwartung darf nur über verschlüsselte Verbindungen stattfinden. Es sind möglichst restriktive Zugriffsrechte zu vergeben. Der Verbindungsaufbau eines Externen ist zu kontrollieren (z. B. im Beisein eines internen IT-Mitarbeiters oder durch temporäre Freigabe des Zugangs).

Externen darf generell erst dann Zugang gewährt werden, wenn ein Vertrag (inkl. Datenschutz- und Vertraulichkeitsvereinbarung) unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert (siehe Kapitel 7).

5.4.2 Update- und Patch-Management

Um Sicherheitslücken in den IT-Systeme zu schließen, sind zeitnah Sicherheits-Updates und -Patches einzuspielen. Hierbei sind mobile Geräte bzw. nicht dauerhaft mit dem internen IT-Netzwerk verbundene Geräte ebenfalls zu berücksichtigen.

5.4.3 Hardware-Wartung außer Haus

Soll Hardware außer Haus gewartet werden, ist Folgendes zu beachten:

- Es sind – sofern möglich – alle sensitiven Daten, die sich auf den Datenträgern befinden, vorher physikalisch zu löschen (dies gilt auch für alle Geräte mit Speichermedien wie z. B. PC, Fax- und Kopiergeräte mit Datenspeicher).
- Sofern möglich, sind vor dem Versand alle Passwörter zu ändern.
- Bei Versand oder Transport sind die zu reparierenden IT-Komponenten vor Beschädigungen und Diebstahl zu schützen.
- IT-Systeme oder Komponenten sind nach Rückgabe auf Vollständigkeit zu überprüfen. Alle Passwörter sind zu ändern. PC-Datenträger sind nach Rückgabe auf Malware zu überprüfen.

5.4.4 Einsatz eines Fernwartungs-Tools

Ein Fernwartungs-Tool erlaubt den Fernzugriff auf PCs und deren Fernsteuerung. Hierzu werden Bildschirminhalte sowie Tastatureingaben und Mausbewegungen über das Netzwerk übertragen. Hierbei sind folgende Einstellungen bei der Konfiguration vorzunehmen:

- Administratoren müssen sich bei der Verbindungsaufnahme durch Eingabe eines Passworts authentifizieren,
- Mitarbeiter müssen Verbindungswünsche von Administratoren explizit in einem Dialogfenster bestätigen – erfolgt keine Bestätigung, darf kein Fernzugriff möglich sein,
- Einstellungen des Fernwartungs-Servers können nur von Administratoren geändert werden.

Ferner sind folgende Aspekte zu beachten:

- Für die Übermittlung sind Verschlüsselungsverfahren zu etablieren, wenn auf Rechner zugegriffen werden soll, auf denen personenbezogene Daten mit hoher Sensibilität verarbeitet werden.

- » Auch sind alle beteiligten Rechner über restriktiv konfigurierte Firewalls zu schützen.
- » Die (unverschlüsselte) Übertragung über offene Netze wie das Internet ist zu verhindern.
- » Eine Fernwartung durch Dritte
  - ist nur auf Basis expliziter Datenschutz- und Vertraulichkeitsvereinbarungen mit dem Dienstleister zulässig (siehe Kapitel 8).
  - bedarf einer Prüfung der Integrität durch einen internen IT-Mitarbeiter nach erfolgter Wartung.

Wartungsvorgänge sind anhand eines Wartungsprotokolls nachvollziehbar zu gestalten.

5.5 Maßnahmen zum Schutz vor bösartiger Software (Viren-/Malware-Schutz)

Um die Datenbestände vor Viren und anderer schadenstiftender Software (Malware) zu schützen, sind folgende Maßnahmen zu treffen:

- » Ein- und ausgehende E-Mails sind zentral und ggf. auch lokal auf Viren hin zu prüfen. Gleiches gilt für Downloads und für das Anschließen externer Datenträger.
- » Die Mitarbeiter sind hinsichtlich der Tatsache zu sensibilisieren, dass auch ein guter Virenscanner keinen 100%-igen Schutz darstellt.
- » Die Funktion des Browsers, heruntergeladene Daten automatisch zu öffnen, ist zu deaktivieren.
- » Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren).
- » Aktive Inhalte im Browser sind technisch soweit wie möglich zu unterdrücken.

Erst nach Einführung einer geeigneten Firewall darf der Anschluss an ein externes Netz erfolgen. Die Firewall ist so zu konfigurieren und zu administrieren, dass sie einen effektiven Schutz darstellt und Manipulationen verhindert werden.

- » Bei der Firewall sind die Filterregeln so restriktiv wie möglich zu wählen („Alles was nicht erlaubt ist, ist verboten“). Jedoch nicht derart, dass der Benutzer durch eine Vielzahl von Meldungen belästigt und in seiner Arbeit beeinträchtigt wird.
- » Auch die weiteren Komponenten, die der Kommunikation zwischen geschütztem/internen und ungeschütztem/externen Netz dienen, müssen sicher implementiert werden.

Die zentralen Netzwerk-Komponenten sind regelmäßig auf Integrität zu prüfen.

Begleitend sollten Intrusion Detection/Prevention Systeme eingesetzt sowie Sicherheits-Updates und Patches möglichst zeitnah installiert werden (siehe auch Kapitel 5.4.2).

5.6 Protokolldatenerfassung und -auswertung

Es gilt, dass generell festgelegt werden muss,
» *was wann und auf welche Weise zu protokollieren ist,*
» *wann und durch wen diese Protokolle auszuwerten,*
» *wie sie zu schützen sowie*
» *wann diese zu löschen sind.*

5.6.1 Protokolldatenerfassung

Die am Server mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. Es sind alle sicherheitsrelevanten Ereignisse zu protokollieren. In regelmäßigen Abständen muss der Administrator die Protokolldateien der Server überprüfen. Zumeist sind folgende Ereignisse ausreichend:

- Erfolgreiche/gescheiterte An- und Abmeldeversuche
- Gescheiterte Datei- und Objektzugriffe
- Gescheiterte Nutzung von Benutzerrechten
- Erfolgreiche/gescheiterte Versuche der Benutzer- und Gruppenverwaltung
- Erfolgreiche/gescheiterte Versuche der Sicherheitsrichtlinienänderung
- Erfolgreiche/gescheiterte Versuche des Neustartens und Herunterfahrens

Wie viele Ereignisse darüber hinaus protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab. Je höher dieser ist, desto mehr sollte protokolliert werden. Es sind sämtliche Aktivitäten im Administrationsmodus bzw. mit Administratorenrechten aufzuzeichnen.

Bei der Verarbeitung von personenbezogenen Daten sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zur Umsetzung der datenschutzrechtlichen Vorgaben zu protokollieren:

- Eingabe von Daten
- Datenübermittlungen
- Benutzung von automatisierten Abrufverfahren
- Löschung von Daten

Auf Protokolldaten sind nur sehr restriktive Zugriffsrechte zu vergeben.

Bei Systemen mit hochsensiblen Daten ist zu prüfen, ob auch die Einsichtnahme der Daten protokolliert werden sollte.

5.6.2 Speicherdauer von Protokollen

Die Protokolldaten sind manipulationssicher, zeitnah verfügbar und gemäß den gesetzlichen Anforderungen aufzubewahren.

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, besteht eine Löschungspflicht, sofern es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien gibt. Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbart werden können und

- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen nur kürzere Speicherfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten. Zur spezifischen Definition der Speicherdauer ist der Datenschutzbeauftragte zu kontaktieren.

Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokoll-dateien beachtet werden müssen.

5.7 Verfügbarkeitssicherung

5.7.1 Verfügbarkeit der Infrastruktur

Es sind Maßnahmen zu ergreifen, die eine angemessene Verfügbarkeit der zentralen IT-Einrichtungen wie Serverraum/Rechenzentrum sicherstellen.

5.7.2 Datensicherungen und Backup

Die Erstellung eines Datensicherungskonzepts ist erforderlich.

Zur Vermeidung von Datenverlusten sind regelmäßig Datensicherungen durchzuführen. Es sind Richtlinien zu treffen, welche Daten wann von wem zu sichern sind. Mit einer regelmäßigen Datensicherung muss erreicht werden, dass möglichst zeitnah durch die Rekonstruktion der verschiedenen Daten/Informationen der IT-Betrieb wieder anlaufen kann. Ferner sind regelmäßige Rücksicherungstests durchzuführen.

In Bereichen, in denen nur kurze Ausfallzeiten akzeptiert werden, sind die Daten auf zwei, in unterschiedlichen Brandabschnitten befindlichen Servern zu spiegeln.

Neben der Datenspiegelung sind noch weitere Maßnahmen gegen den Datenverlust umzusetzen.

Es sind regelmäßige Wiederherstellungstests durchzuführen.

Es darf nur ein Zugriff durch Berechtigte ermöglicht werden.

5.8 Kryptographie

Verschlüsselungsmöglichkeiten sind – sofern notwendig – technisch einzurichten.

Die Mitarbeiter haben für die Nutzung insbesondere die Regelungen des Kapitel 6 zu beachten.

Es ist festzulegen, wo kryptographische Maßnahmen sinnvoll einzusetzen sind, welche Art

von Maßnahmen zur Anwendung kommen sollen und für welchen Zweck und welche Geschäftsprozesse sie eingesetzt werden sollen.

Für mobile Datenträger (Laptops, USB-Sticks, Smartphones etc.), auf denen sensible bzw. personenbezogene Daten gespeichert werden, sind sichere Verschlüsselungstechniken einzusetzen.

Für die Übermittlung von Daten und Datenträger mit hochsensiblen Informationen sind sichere Verschlüsselungstechniken einzusetzen.

5.9 Sichere Kommunikation (VPN, WLAN)

Für den Zugriff auf Daten und auf das Netzwerk ist ein Virtuelles Privates Netz (VPN) einzurichten. Ein VPN ist ein Netz, das physisch in der Regel über das Internet betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs sind unter Zuhilfenahme aktueller kryptographischer Verfahren in der Lage, die Integrität und Vertraulichkeit von Daten zu schützen.

Für den Einsatz eines VPN ist ein entsprechendes Sicherheitskonzept zu erstellen. Der Datenschutzbeauftragte ist schon in der Planungsphase einzubinden.

Bei der Nutzung drahtloser Kommunikation (WLAN) ist eine Risikoeinschätzung vorzunehmen. Es sind die gängigen Sicherheitsmechanismen umzusetzen, wozu mindestens kryptographische Verfahren nach dem aktuellen Stand gehören. Für den Einsatz eines WLAN-Netzwerks ist ein entsprechendes Sicherheitskonzept zu erstellen. Der Datenschutzbeauftragte ist schon in der Planungsphase einzubinden.

5.10 Sichere Vernichtung von Datenträgern/Unterlagen

5.10.1 Vernichtung von Datenträgern/Unterlagen

Unterlagen und Datenträger, die schützenswerte Daten enthalten (z. B. CDs, DVDs, USB-Sticks, Festplatten, Fax- oder Kopiergeräte, Mobile Devices wie Smartphones oder Tablets), sind so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind.

Bei der Organisation der Vernichtung von Datenträgern (Papier und maschinell lesbare Datenträger) ist die DIN 66399 zu beachten. Die Schutzklassen und Sicherheitsstufen sind in Abhängigkeit von der Klassifizierung der Daten zu wählen:

5.10.2 Vernichtung durch Dritte

Sofern keine (interne) sichere Entsorgung durchgeführt werden kann, ist mit der Entsorgung ein Dienstleistungsunternehmen zu beauftragen.

Nicht mehr benötigte Dokumentationen sind bis zur Abholung bzw. zur Vernichtung durch einen externen Dienstleister sicher zu verwahren, in der Form, dass Unbefugte auf die Unterlagen nicht zugreifen können. Es darf generell erst dann Zugang zu den Daten/Datenträgern gewährt werden, wenn ein schriftlicher Vertrag unterschrieben wurde, der alle Bedingungen definiert. Hierzu ist Kapitel 8 zu beachten.

6. Arbeitsplatzorientierte Sicherheitsmaßnahmen

6.1 Sonderregelungen: Mobile Devices (Laptops, Smartphone etc.)

Es sind generell mindestens die gleichen Sicherheitsmaßnahmen wie bei den Geräten, die mit dem gleichen Zweck am Standort der Organisation verwendet werden, zu ergreifen. Hierzu zählt auch eine zentrale Verwaltung/Administration/Fernwartung der Geräte durch die IT.

Die nachfolgenden Vorgaben gelten insbesondere für den Fall, dass auf Mobile Devices mindestens sensible Daten verarbeitet werden.

Es ist grundsätzlich verboten, private Geräte für dienstliche Zwecke bzw. dienstliche Datenverarbeitung zu nutzen. Ein Abweichen bedarf einer Risikoanalyse und der schriftlichen Genehmigung durch die Geschäftsführung.

Die mobile Arbeit durch die Mitarbeiter wird von der Geschäftsleitung für bestimmte Stellen genehmigt und sollte vom DSB begleitet werden.

Jedem Mitarbeiter ist bei Übergabe eines Mobile Devices vor der Benutzung die entsprechende Richtlinie (für Laptops oder Smartphones) durch die IT zu übergeben, welche unterzeichnet in der Personalakte aufbewahrt wird (siehe mitgeltende Unterlagen; Rubrik B).

Es sind – sofern technisch realisierbar – klare Regeln für die Nutzung aufzustellen und dem Schutzzweck entsprechende Schutzmaßnahmen einzusetzen. Hierbei sind z. B. folgende Maßnahmen zu treffen:

- Es sind Verschlüsselungsverfahren zum Schutz der Daten auf dem Mobile Device zu installieren.
- Nicht erforderliche Kommunikationsfunktionen sind zu deaktivieren. Es sind klare Vorgaben zur Nutzung von Hotspots etc. zu erstellen.
- Die Aufhebung von Berechtigungen, Zugriffsrechten und die Rückgabe der Geräte, wenn die mobile Arbeit beendet ist, sind festzulegen.
- Geräte und Datenträger, die aus den Geschäftsräumen mitgenommen wurden, dürfen an öffentlichen Orten wie auch in Fahrzeugen nicht unbeaufsichtigt gelassen werden.
- Die Einsichtnahme durch Unbefugte ist zu verhindern. Dies kann z. B. durch die Nutzung von Sichtschutzfolien erreicht werden.

Für die Nutzung von Smartphones, Tablets etc. sind aufgrund der besonderen Beschaffenheit der Systeme in der Regel spezielle Regelungen und Sicherheitsmaßnahmen erforderlich. Hierzu ist zuvor eine Risikoanalyse von IT-Abteilung unter Beteiligung des Datenschutzbeauftragten zu erstellen.

Grundsätzlich sollten auf Mobile Devices keine bzw. so wenige personenbezogene Daten wie möglich gespeichert und verarbeitet werden.

6.2 Sonderregelungen: Home Office

Vor der Einrichtung eines Home Office ist grundsätzlich eine Risikoanalyse durchzuführen, in der neben dem potenziellen Nutzen auch die Gefahren, mögliche Sicherheitsmaßnahmen und Rest-Risiken betrachtet werden. Eine Freigabe hat durch die Geschäftsführung zu erfolgen.

Es sind generell bei den im Home Office betriebenen Geräten mindestens die gleichen Sicherheitsmaßnahmen wie bei den Geräten, die mit dem gleichen Zweck am Standort der Organisation verwendet werden, zu ergreifen. Hierzu zählt auch eine zentrale Verwaltung der Geräte durch die IT und Vorgaben zur Raumnutzung.

Trotz der Bereitstellung von Equipment durch den Arbeitgeber im heimischen Umfeld gilt auch hier grundsätzlich, dass die private Nutzung und die Nutzung des dienstlichen Equipments von Familienangehörigen nicht zulässig ist.

Es sind analoge Regelungen zur Nutzung von Mobile Devices zu erlassen (siehe Kapitel 7.3).

6.3 E-Mail

Sollen zwischen zwei oder mehreren Kommunikationspartnern Daten elektronisch ausgetauscht werden, so sind zum ordnungsgemäßen Austausch folgende Punkte zu beachten:

- » Versand
  - Die Adressierung von E-Mails muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden.
  - Es ist Kapitel 7.5.2 zum Schutz der Datenübertragung zu beachten.
  - Sofern E-Mails – bspw. in Form eines Newsletters – an mehrere Empfänger versandt werden, sind Verteilerlisten oder die „BCC-Option“ zu nutzen, so dass der Empfänger nicht die komplette Empfängerliste einsehen kann. Diese Funktion ist den Mitarbeitern technisch zu ermöglichen.
  - Es sollte beim Versand von E-Mails stets berücksichtigt werden, dass E-Mails ggf. automatisch an einen Vertreter weitergeleitet werden.
- » Weiterleitung / Bestätigung
  - Es ist untersagt, dienstliche Daten und/oder E-Mails auf einen privaten E-Mail-Account um- oder weiterzuleiten.
  - Bei einer automatischen Weiterleitung von E-Mails ist die Vertraulichkeit zu gewährleisten, indem sichergestellt wird, dass alle Empfänger die E-Mails auch lesen dürfen.

7. Outsourcing

Ein Outsourcing liegt dann vor, wenn es sich bei dem Auftraggeber und -nehmer um rechtlich voneinander selbstständige, unabhängige Unternehmen handelt.

Es existiert kein „Konzern-Privileg“ (d. h. zwei Unternehmen eines Konzerns sind wie „Dritte“ zu betrachten und haben keine Sonder-Privilegien).

Als Beispiele gelten:

- Wartung und Betrieb von IT-Systemen (Software, Hosting, Cloud-Dienste etc.)
- Archivierung von Daten auf optischen Datenträgern,
- Personalabrechnung,
- Lettershop,
- externes Rechenzentrum oder
- Vernichtung von Datenträgern/Unterlagen.

Es gilt zu beachten, dass die nachfolgenden Anforderungen bereits dann zu berücksichtigen sind, wenn der Zugriff auf personenbezogene Daten nicht auszuschließen ist bzw. theoretisch möglich ist.

7.1 Zugang von Fremdunternehmen

7.1.1 Kritikalität der externen Datenverarbeitung

Zur einerseits angemessenen sowie andererseits gesetzeskonformen Umsetzung der Anforderungen des Datenschutzes ist eine Kategorisierung der externen Datenverarbeitung im Hinblick auf die Kritikalität vorzunehmen.

7.1.2 Auswahl des Fremdunternehmens

Es ist notwendig, den Auftragnehmer sorgfältig auszuwählen. Im Rahmen der sorgfältigen Auswahl ist zu entscheiden, ob der Auftragnehmer insgesamt vertrauenswürdig ist. Dabei ist die Lieferanten-Richtlinie zu berücksichtigen.

Es sind die Regelungen im Kapitel 7.2 zu beachten.

7.1.3 Richtlinie zur Sicherheit beim Zugang durch Fremdunternehmen

Fremdunternehmen darf generell erst dann Zugang zu Informationen und Informationsverarbeitungsgeräten eingeräumt werden, wenn die entsprechenden Maßnahmen implementiert worden sind und ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang inkl. der zu treffenden technisch-organisatorischen Maßnahmen definiert. Auch hat dieser Vertrag eine Vertraulichkeits- und Datenschutzvereinbarung zu enthalten.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind sämtliche eingerichtete Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Hierbei besteht eine Benachrichtigungspflicht durch die Fachbereiche an den IT-Bereich. Außerdem ist der Ausscheidende explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.

Daten, die im Rahmen des Outsourcings extern gespeichert wurden, sind nach Abschluss des Auftrags vollständig und sicher zu löschen. Dies ist durch den Auftraggeber zu kontrollieren.

7.1.4 Verträge mit Fremdunternehmen

Die Fremdunternehmen sind auf die Einhaltung der Datenschutzvorschriften zu verpflichten

Die gilt für jegliche Arten von Dienstleistungen, bei denen personenbezogene Daten durch das Fremdunternehmen zur Kenntnis genommen werden können (unerheblich, ob Daten übermittelt, per Remote-Zugriff eingesehen oder im Rahmen des Leasings oder der Datenvernichtung zumindest theoretisch zur Kenntnis gelangen können).

Auftragsverarbeitungsverträge sind grundsätzlich von der Datenschutzbeauftragten zu prüfen.

7.2 Auftragsverarbeitung

Eine Auftragsdatenverarbeitung ist die Inanspruchnahme von externen Dienstleistungsfunktionen durch den Verantwortlichen.

Der Auftraggeber bleibt für die Einhaltung der Vorschriften über den Datenschutz verantwortlich.

Die Einhaltung der Vorgaben des Kapitels 7.1 ***und*** *die Einbeziehung der Datenschutzbeauftragten sind erforderlich.*

Sofern Dienstleistungen in Rahmen einer Auftragsverarbeitung angeboten werden („Auftragsverarbeiter“), so sind die vorgenannten Regelungen analog anzuwenden. Ferner gilt im Rahmen der Dienstleistung auch das Kapitel 2.4.1; auch hat der Auftragsverarbeiter die rechtliche Verpflichtung an der Gestaltung ausreichender Sicherheitsmaßnahmen (insbesondere Kapitel 4 und 5) und der Umsetzung der Rechte der Betroffenen (Kapitel 10) mitzuwirken.

Somit ist diese Richtlinie auch bei den angebotenen Dienstleistungen im Rahmen der Auftragsdatenverarbeitung hinzuzuziehen.

8 Notfallvorsorge und Umgang mit Vorfällen

8.1 Notfall- und Katastrophenmanagement

Es sind Richtlinien für Notfall-, Katastrophen- und Wiederanlaufplanung zu erstellen.

Der IT-Bereich ist neben der Erstellung auch für die Pflege und für Änderungen verantwortlich.

Das Notfall- und Kontinuitätsmanagement muss regelmäßig auf seine Aktualität und Wirksamkeit geprüft sowie hinsichtlich Effektivität und Effizienz der Maßnahmen analysiert werden.

8.2 Meldung sicherheitsrelevanter Ereignisse

Es ist ein formales, verbindliches Verfahren für die Meldung sicherheitsrelevanter Ereignisse zu etablieren und an die Mitarbeiter zu kommunizieren.

Alle sicherheitsrelevanten Ereignisse (wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung, usw.) sind **sofort** an den IT-Bereich zu melden. Dort ist die Meldung zu prüfen und etwaige Schritte zur Behebung der Probleme einzuleiten.

Der Nutzer darf keine eigenen Aufklärungsversuche unternehmen, da evtl. wertvolle Hinweise und Spuren verwischt werden oder verloren gehen könnten.

Es sind etwaige Meldepflichten (siehe Kapitel 8.3) zu prüfen. Hierzu hat der IT-Bereich unverzüglich den Datenschutzbeauftragten zu informieren.

8.3 Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

8.3.1 Meldepflicht gegenüber der Aufsichtsbehörde

Im Falle einer Datenschutzverletzung ist die Verletzung unverzüglich (d. h. „ohne schuldhaftes Zögern“, § 121 BGB) – möglichst aber binnen 72 Stunden nach Konsultation des externen Datenschutzbeauftragten – ggf. der zuständigen Aufsichtsbehörde mitzuteilen.

Erfolgt die Meldung nicht innerhalb von 72 Stunden, so ist der Mitteilung außerdem eine Begründung für die Verzögerung beizufügen.

Zur Beurteilung, ob ein meldepflichtiger Tatbestand vorliegt, sind sowohl Geschäftsführung als auch die Datenschutzbeauftragte einzubinden.

8.3.2 Benachrichtigungspflicht gegenüber betroffenen Personen

Hat eine Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so ist die betroffene Person unverzüglich über die Verletzung zu benachrichtigen.

Zur Beurteilung, ob ein benachrichtigungspflichtiger Tatbestand vorliegt, sind sowohl Geschäftsführung als auch die Datenschutzbeauftragte einzubinden.

9 Anforderungen an die personenbezogene Datenverarbeitung

9.1 Erhebung und Verarbeitung von personenbezogenen Daten

Bei der Erhebung und Verarbeitung von personenbezogenen Daten sind die Grundsätze der Datenverarbeitung zu beachten.

Sofern erstmal personenbezogene Daten erhoben und/oder verarbeitet werden, ist die Datenschutzbeauftragte einzubinden.

9.2 Weitergabe von personenbezogenen Daten

Grundsätzlich gilt, dass eine (interne und externe) Weitergabe von personenbezogenen Daten ausschließlich dann zulässig ist, wenn eine Rechtsgrundlage dies explizit erlaubt.

9.2.1 Interne Weitergabe

Sensible Informationen sind nur dann weiterzugeben, wenn eine betriebliche Notwendigkeit zur Kenntnisnahme besteht. Bestehende Zugangs-/Zugriffsrechte geben bei der internen Weitergabe (also an Kollegen) Anhaltspunkte. Insbesondere bei der Weitergabe an abteilungsfremde Stellen ist eine vorherige Prüfung u. a. der Zweckbindung vorzunehmen.

Die Weitergabe hochsensibler Daten bedarf ferner der vorherigen Genehmigung durch den Vorgesetzten.

9.2.2 Weitergabe an Externe

Die Übermittlung von personenbezogenen Daten an Dritte unterliegt einem Verbot mit Erlaubnisvorbehalt. Wenn personenbezogene Daten an Dritte übermittelt werden, so ist zuvor die Zulässigkeit zu überprüfen. Der Empfänger ist zur sensiblen Behandlung und zur Zweckbindung zu verpflichten.

Es ist sicherzustellen, dass personenbezogene Daten nicht unbeabsichtigt oder gar infolge einer arglistigen Täuschung übermittelt werden. Damit ist die Weitergabe von personenbezogenen Daten über Telefon oder Telefax in der Regel ausgeschlossen oder zumindest problematisch, wenn die Identität des Gegenübers nicht zweifelsfrei festzustellen ist.

Die Weitergabe hochsensibler Daten bedarf ferner der vorherigen Genehmigung durchdie Geschäftsführung.

Die Verantwortung für die Zulässigkeit und Sicherheit der Übermittlung trägt die übermittelnde Stelle.

9.2.3 Weitergabe an Externe im Ausland

Die Übermittlung ins Ausland oder an zwischen- oder überstaatliche Stellen ist zu unterlassen, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Für die Übermittlung personenbezogener Daten an Stellen

- in anderen Mitgliedstaaten der Europäischen Union (EU) oder in andere Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR),
- in Länder mit einem durch die EU-Kommission anerkannten Datenschutzniveau oder
- der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten die gleichen Regelungen wie bei einer Übermittlung innerhalb Deutschlands.

Bei Datenempfängern, deren Länder kein angemessenes Datenschutzniveau gewährleisten (wie in den meisten Außer-EU-Staaten, wie z. B. USA oder China), sind spezielle Maßnahmen wie der Abschluss von Verträgen, die durch die EU-Kommission vorgegeben sind, zu ergreifen. Alternativ ist im Rahmen eines konzerninternen Datenaustausch der Abschluss von „Binding Corporate Rules“ (konzernweit verbindliche Regelungen) möglich.

Aufgrund der hohen Komplexität und Brisanz ist in diesem Fall die Datenschutzbeauftragte zwingend einzuschalten.

9.3 Veröffentlichung von personenbezogenen Daten

Grundsätzlich bedarf es bei der Veröffentlichung von personenbezogenen Daten (inkl. Fotos) der Einwilligung des Betroffenen.

Nur soweit die Veröffentlichung die erforderliche Erreichbarkeit und damit die Erfüllung der Arbeitspflicht des Mitarbeiters sicherstellt, darf eine Bekanntgabe der Basiskommunikationsdaten (und ggf. funktionsrelevanter Zusatzdaten) – ohne entsprechende Einwilligung – erfolgen. In Betracht kommen somit ausschließlich Mitarbeiter, zu deren Aufgabengebiet ein entsprechender Außenkontakt oder besondere Entscheidungsbefugnis gehören bzw. die eine Repräsentationsfunktion zugunsten des Unternehmens ausüben.

Allgemein betrachtet muss das Bedürfnis nach entsprechender Kontaktaufnahme durch Dritte bestehen. Bei rein intern Tätigen – wie etwa Registratur, Botendiensten, Schreibdiensten – besteht keine Notwendigkeit und damit keine Rechtsgrundlage zur Veröffentlichung der Arbeitnehmerdaten.

Zu den rechtmäßig veröffentlichten Basiskontaktdaten zählen:

- Name und Aufgabenbereich
- dienstliche Anschrift
- dienstliche Telefon- und Faxnummer
- dienstliche E-Mail-Adresse.

Zur Veröffentlichung der o. g. Fotos muss grundsätzlich eine Einwilligung eingeholt werden.

Sofern Fremd-Bilder eingekauft/genutzt werden, sind die vom Fotografen auferlegten Nutzungsbedingungen zu beachten. Bei der Beauftragung eines Fotografen (z. B. bei eigenen Veranstaltungen) sind die Nutzungsrechte vertraglich festzulegen.

9.4 Datenverarbeitung von Kunden und anderen Vertragspartnern

9.4.1 Rechtliche Grundlagen

Personenbezogene Daten eines Kunden, Lieferanten oder anderen Vertragspartners dürfen für Zwecke des Vertragsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Abwicklung des Vertragsverhältnisses erforderlich ist (beispielsweise Lieferung oder Rechnungsstellung).

9.4.2 Nutzung zu Werbezwecken

Werbung ist jede Äußerung mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen zu fördern. Die Steigerung des Imagewerts kann hierbei zumindest indirekt dieses Ziel ebenfalls verfolgen.

Die Direktwerbung ist allerdings nur zulässig, wenn die betroffene Person der Datenverarbeitung nicht widersprochen hat.

9.5 Online-Dienste

9.5.1 Bereitstellung einer Internetpräsenz

Bei der Datenerhebung auf der Internetpräsenz ist der Datensparsamkeitsgedanke zu berücksichtigen. So ist bspw. beim Abonnieren eines Newsletters vom Betroffenen nur die E-Mail-Adresse oder auch bei weiteren Kontaktformularen so wenige Daten wie erforderlich abzufragen.

Sofern E-Commerce-Angebote bereitgestellt oder sensible Daten beispielsweise im Rahmen von Kontaktformularen übermittelt werden sollen, so sind entsprechende Sicherheitsmaßnahmen hinsichtlich Authentizität oder Vertraulichkeit einzurichten (z. B. Einsatz von Kryptographie und SSL/TSL-Protokollen).

Die Weiterleitung auf fremde Internetseiten sind entsprechend dem Nutzer anzuzeigen (Nennung der URL der Zielseite und Öffnen in einem separaten Browser-Fenster/-Tab oder Nutzung einer sog. Redirect-Seite mit entsprechendem Weiterleitungs-Hinweis).

Dies schließt auch die Einbindung von Plugins, wie beispielsweise Tools zum Teilen von Inhalten mit sozialen Netzwerken (z. B. „Like“-Button), oder „embedded content“ wie beispielsweise zur Anfahrtsbeschreibung (z. B. Google Maps) oder Video-Darstellung (z. B. Youtube) ein; hierbei ist zwingend der Datenschutzbeauftragte zu involvieren.

Die Nutzung bzw. der Einsatz von Cookies ist zu vermeiden.

Es sollten nur Tracking-Tools zur Analyse der Besucheraktivitäten genutzt werden, die auf dem eigenen Webserver installiert werden können sowie Anonymisierungs- und Widerspruchsmöglichkeiten bieten. Hierbei ist der Datenschutzbeauftragte vorab einzubinden.

Sofern technisch – innerhalb des CMS der Internetpräsenz – möglich, sind die Datenschutzeinstellung der Browser zu akzeptieren (z. B. „do not track“).

9.5.2 Social Media

Die Nutzung jeglicher sozialer Netzwerke/Social-Media-Dienste (wie z. B. LinkedIn) und/oder das Angebot von Inhalten auf anderen Plattformen sind nur nach Genehmigung der Geschäftsführung zulässig. Bei Erlaubnis der Nutzung sind Regelungen hierzu zu erarbeiten.

Die Nutzung dieser Dienste ist auch im privaten Umfeld (beispielsweise in der Freizeit) so zu gestalten, dass weder sensible Informationen (textuell oder bildlich) noch Informationen in sozialen Netzwerken veröffentlicht werden, die dem Unternehmen schaden könnten.

10 Gewährleistung der Rechte des Betroffenen

An die Mitarbeiter, die im Rahmen ihrer dienstlichen Aufgaben mit Mitarbeiter-, Kunden- oder Lieferantendaten oder anderen personenbezogenen Daten in Berührung kommen bzw. an die Leiter der jeweiligen Abteilung können sich Betroffene wenden, die aufgrund der Datenschutzbestimmungen von ihren Rechten Gebrauch machen.

Die Datenschutzvorschriften geben dem Betroffenen folgende Rechte:

10.1 Informationspflichten (Art. 13, 14 DSGVO)

Werden personenbezogene Daten bei der betroffenen Person erhoben, so sind der betroffenen Person die in den Artikel 13 DSGVO zum Zeitpunkt der Datenerhebung mitzuteilen.

Hierzu sind entsprechende Informationsblätter in Kooperation mit dem DSB durch die Verfahrensverantwortlichen zu erstellen.

Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, so sind der betroffenen Person diese Informationen innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, mitzuteilen.

Die Informationspflicht besteht nicht, wenn

- die betroffene Person bereits über die Informationen verfügt.
- die Erteilung der Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. In diesen Fällen sind allerdings geeignete Maßnahmen zum Schutz der betroffenen Personen, einschließlich der Bereitstellung der Informationen für die Öffentlichkeit, zu ergreifen.
- die personenbezogenen Daten einem Berufsgeheimnis unterliegen.

Näheres zu den gesetzlichen Anforderungen sind der Anlage 3 in Rubrik E zu entnehmen.

10.2 Auskunftsrecht (Art. 15 DSGVO)

Auf Verlangen ist gegenüber der betroffenen Person zu bestätigen, dass die sie betreffende personenbezogene Daten verarbeitet werden. Ferner ist der betroffenen Person auf Verlangen Auskunft zu erteilen.

Sofern ein Betroffener sein Auskunftsrecht einfordert, so ist dem Betroffenen ein Informationsschreiben zukommen zu lassen und der Datenschutzbeauftragte zu informieren. Dieser hat die Zulässigkeit des Auskunftsersuchens zu prüfen.

Bei einer elektronischen Beauskunftung ist eine sichere Datenübertragung sicherzustellen.

10.3 Berichtigung der Daten (Art. 16 DSGVO)

Auf Verlangen der betroffenen Person sind unrichtige personenbezogene Daten unverzüglich zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Über die Berichtigung sind alle Empfänger der von der Berichtigung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen

Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

10.4 Löschung der Daten (Art. 17 DSGVO)

Auf Verlangen der betroffenen Person sind die sie betreffenden personenbezogenen Daten unverzüglich zu löschen, wenn die Anforderungen des Artikels 17 DSGVO erfüllt sind.

Über die Löschung sind alle Empfänger der von der Löschung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

Der Datenschutzbeauftragte hat die Notwendigkeit der Löschung zu prüfen.

Wurden die zu löschenden personenbezogenen Daten öffentlich gemacht, so sind die anderen Verantwortlichen, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass die betroffene Person die Löschung aller Links zu den zu löschenden personenbezogenen Daten oder von Kopien oder Replikationen der personenbezogenen Daten verlangt hat.

10.5 Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Einschränkung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Wurde die Verarbeitung eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden.

Im Falle einer Aufhebung der Einschränkung ist die betroffene Person zuvor von der Aufhebung zu unterrichten.

Über die Einschränkung der Verarbeitung sind alle Empfänger der von der Einschränkung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

Der Datenschutzbeauftragte hat die Notwendigkeit der Einschränkung zu prüfen.

10.6 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Auf Verlangen der betroffenen Person sind dieser die sie betreffenden und von ihr bereit gestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln.

Falls die betroffene Person dies verlangt, so sind die erwähnten personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln, wenn die Verarbeitung auf einer

Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Der Datenschutzbeauftragte ist hierbei einzubinden.

Bei einer elektronischen Übertragung der Daten ist eine sichere Übertragung sicherzustellen.

10.7 Widerspruchsrecht (Art. 21 DSGVO)

Die betroffene Person hat das Recht Widerspruch einzulegen. Die Gründe für Rechtmäßigkeit können der Anlage 4 in Rubrik E entnommen werden.

Werden personenbezogene verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung zum Zwecke der Direktwerbung einzulegen.

Der Datenschutzbeauftragte hat zu prüfen, ob der Widerspruch begründet ist und ihm stattgegeben werden muss.

10.8 Automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO)

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Der Datenschutzbeauftragte ist frühzeitig einzubinden.

11 Formale Richtlinien

11.1 Aktualitätsstand und Empfängerkreis

Die aktuelle Version dieser Datenschutzrichtlinie ist im Googel Workspace hinterlegt.

11.2 Verteilungsmodalitäten und Betriebsverfahren

Diese Datenschutzrichtlinie steht dem Datenschutzteam mit Schreibzugriff und allen Mitarbeitern lesend zur Verfügung.

11.3 Verantwortlicher für Pflege und Änderungsdienst

Für die inhaltliche Bearbeitung sowie für die Pflege und Änderung der Texte ist die externe Datenschutzbeauftragte auf Anfordern der Geschäftsführung zuständig.

Bei Bedarf ist diese Datenschutzrichtlinie zu überarbeiten und mindestens einmal im Jahr ist die Aktualität zu überprüfen. Änderungen sind durch die Geschäftsführung zu genehmigen.

D. Anlagen

1 Begriffsbestimmungen

Die EU-Datenschutz-Grundverordnung (DSGVO) definiert in Art. 4 verschiedene Begrifflichkeiten wie folgt:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen.

Besondere Kategorien sind personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Verantwortlicher ist die 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.

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Die folgenden Ausführungen sind Ergänzungen zu den jeweiligen Richtlinien in den vorangehenden Kapiteln des Handbuchs.

2 Datenschutzgrundsätze nach der DSGVO

Es sind bei der automatisierten und nicht-automatisierten Datenverarbeitung die folgenden Grundsätze zum Datenschutz zu verfolgen. Diese sind regelmäßig auf ihre Einhaltung hin zu prüfen. Die Einhaltung der Grundsätze ist nachzuweisen (Rechenschaftspflicht).

2.1 Prinzipien der personenbezogenen Datenverarbeitung gemäß DSGVO

*Die Verarbeitung personenbezogener Daten unterliegt einem **Verbot mit Erlaubnisvorbehalt**.*

Das bedeutet, dass die personenbezogene Datenverarbeitung nur dann zulässig ist, soweit ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (siehe 9.1.2). Die Zwecke der Verarbeitung personenbezogener Daten sind festzulegen. Es sind die Vorgaben gemäß Art. 5, Art. 6 DSGVO zu beachten.

Es sind die **Rechte der Betroffenen** zu gewährleisten.

Bei der Verarbeitung von personenbezogenen Daten ist das Ziel zu verfolgen, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (**Datenvermeidung**). Dies ist auch bei der Gestaltung und der Auswahl von Datenverarbeitungssystemen zu beachten; Analoges gilt auch bei der nicht-automatisierten Verarbeitung personenbezogener Daten (beispielsweise im Rahmen von Fragebögen).

Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung dann Gebrauch zu machen, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (**Datensparsamkeit**).

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**).

Die Daten sind sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu halten. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (**Richtigkeit**).

Zudem müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (**Integrität** und **Vertraulichkeit**).

2.2 Einwilligungserklärung

Die Einwilligung hat ausdrücklich zu erfolgen und muss auf einer freien Entscheidung beruhen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

Der Betroffene ist bei der Einwilligung auf

- den vorgesehenen Zweck der Verarbeitung;

- mögliche Datenempfänger;
- die Möglichkeit des jederzeitigen Widerrufs;
- auf den Umstand, dass durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird;
- sowie – soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen – auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Die Erteilung der Einwilligung ist nachzuweisen. Die Einwilligung sollte daher schriftlich oder in einer anderen geeigneten (nachweisbaren) Form eingeholt werden.

2.3 Zweckbindung der Datenverarbeitung

Personenbezogene Daten dürfen nur zu dem Zweck weiter verarbeitet werden, zu dem sie auch erhoben wurden. Diese Zwecke sind zuvor eindeutig festzulegen.

2.4 Zweckänderung

Eine Weiterverarbeitung zu einem anderen Zweck ist neben der Einwilligung nur bei der Existenz eines gesetzlichen Erlaubnistatbestandes zulässig, oder wenn die Verarbeitung für andere Zwecke mit den ursprünglichen Zwecken nach einer Prüfung anhand folgender Kriterien vereinbar ist:

- Die Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

3 Informationspflichten (Art. 13, 14 DSGVO)

3.1 Daten werden direkt bei der betroffenen Person erhoben

Werden personenbezogene Daten bei der betroffenen Person erhoben, so sind der betroffenen Person die in den Artikeln 13 DSGVO zum Zeitpunkt der Datenerhebung mitzuteilen.

Die Informationsblätter haben folgende Informationen zu enthalten:

- Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters; sowie die Kontaktdaten des Datenschutzbeauftragten;
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen;
- Rechtsgrundlage für die Verarbeitung (wenn die Verarbeitung zur Wahrung von berechtigten Interessen erforderlich sein sollte, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- (sofern notwendig) Empfänger oder Kategorien von Empfängern;
- (sofern notwendig) Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln (inkl. Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder – im Falle von Übermittlungen gemäß Art. 46 oder Art. 47 oder Art. 49 Abs. 1 Unterabsatz 2 DSGVO – einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind);
- Speicherdauer oder falls dies nicht möglich ist: Kriterien für die Festlegung dieser Dauer;
- Bestehen eines Rechts
  - auf Auskunft sowie
  - auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie
  - des Rechts auf Datenübertragbarkeit;
- (sofern Verarbeitung auf einer Einwilligung beruht) Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Informationen darüber, ob
  - Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
  - die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte

» (sofern notwendig) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1, 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Ist beabsichtigt, dass die personenbezogenen Daten für einen anderen Zweck weiterverarbeitet werden als den, für den die personenbezogenen Daten erhoben wurden, so sind der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung zu stellen.

3.2 Daten werden nicht direkt bei der betroffenen Person erhoben

Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, so sind der betroffenen Person über die Informationen dieser Rubrik zusätzlich noch folgende Informationen innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, mitzuteilen:

» Kategorien personenbezogener Daten, die verarbeitet werden;

» Quelle, aus der die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, sind die Informationen spätestens zum Zeitpunkt der ersten Mitteilung an die betroffene Person zu erteilen.

Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, hat die Information spätestens zum Zeitpunkt der ersten Offenlegung zu erfolgen.

Ist beabsichtigt, dass die personenbezogenen Daten für einen anderen Zweck weiterverarbeitet werden als den, für den die personenbezogenen Daten erhoben wurden, so sind der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung zu stellen.

Die Informationspflicht besteht nicht, wenn

» und soweit die betroffene Person bereits über die Informationen verfügt.

» die Erteilung der Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. In diesen Fällen sind allerdings geeignete Maßnahmen zum Schutz der betroffenen Personen, einschließlich der Bereitstellung der Informationen für die Öffentlichkeit, zu ergreifen.

» die personenbezogenen Daten einem Berufsgeheimnis unterliegen.

4 Rechte der Betroffenen

4.1 Auskunftsrecht (Art. 15 DSGVO)

Auf Verlangen ist gegenüber der betroffenen Person zu bestätigen, dass die sie betreffende personenbezogenen Daten verarbeitet werden. Ferner ist der betroffenen Person auf Verlangen Auskunft zu erteilen.

Die Auskunft hat folgende Informationen zu enthalten:

- Verarbeitungszwecke;
- Kategorien personenbezogener Daten, die verarbeitet werden;
- (sofern notwendig) Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- Speicherdauer oder falls dies nicht möglich ist: Kriterien für die Festlegung dieser Dauer;
- Bestehen eines Rechts
  - auf Auskunft sowie
  - auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie
  - des Rechts auf Datenübertragbarkeit (siehe Kapitel 11.2 ff.);
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden: alle verfügbaren Informationen über die Herkunft der Daten;
- (sofern notwendig) Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1, 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

Der betroffenen Person ist eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, unter Beachtung der Rechte Dritter unentgeltlich bereitzustellen. So dürfen durch die Bereitstellung der Kopie z. B. keine Geschäftsgeheimnisse oder Rechte des geistigen Eigentums (Urheberechte, Markenrechte) beeinträchtigt werden. Sollte die betroffene Person mehrere Kopien wünschen, so kann hierfür ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangt werden. Wird der Antrag elektronisch gestellt, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

4.2 Berichtigung der Daten (Art. 16 DSGVO)

Auf Verlangen der betroffenen Person sind unrichtige personenbezogene Daten unverzüglich zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Über die Berichtigung sind alle Empfänger der von der Berichtigung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

4.3 Löschung der Daten (Art. 17 DSGVO)

4.3.1 Recht auf Löschung

Auf Verlangen der betroffenen Person sind die sie betreffenden personenbezogenen Daten unverzüglich zu löschen, wenn einer der folgenden Gründe gegeben ist:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt Widerspruch gegen die Verarbeitung zur Direktwerbung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben (Einwilligung eines Kindes).

Über die Löschung sind alle Empfänger der von der Löschung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

4.3.2 Recht auf Vergessenwerden

Wurden die zu löschenden personenbezogenen Daten öffentlich gemacht, so sind die anderen Verantwortlichen, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass die betroffene Person die Löschung aller Links zu den zu löschenden personenbezogenen Daten oder von Kopien oder Replikationen der personenbezogenen Daten verlangt hat.

4.3.3 Ausnahmen

Die Pflicht zur Löschung besteht nicht, soweit die Verarbeitung der personenbezogenen Daten in folgenden Fällen erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 h), i) DSGVO sowie Art. 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO, soweit das Recht auf Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

4.4 Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Einschränkung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Die Einschränkung der Verarbeitung hat zu erfolgen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Richtigkeit wird von der betroffenen Person bestritten (Einschränkung für eine Dauer, die es ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen);
- Verarbeitung ist unrechtmäßig, die betroffene Person lehnt aber die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten;
- Daten werden für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person benötigt sie jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;
- Widerspruch gegen die Verarbeitung durch betroffene Person (Einschränkung für eine Dauer der Prüfung, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen).

Wurde die Verarbeitung eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden.

Im Falle einer Aufhebung der Einschränkung ist die betroffene Person zuvor von der Aufhebung zu unterrichten.

Über die Einschränkung der Verarbeitung sind alle Empfänger der von der Einschränkung betroffenen personenbezogenen Daten zu unterrichten, soweit dies nicht unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist. Auf Verlangen der betroffenen Person ist diese über die Empfänger zu unterrichten.

4.5 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Auf Verlangen der betroffenen Person sind dieser die sie betreffenden und von ihr bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln.

Falls die betroffene Person dies verlangt, so sind die erwähnten personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln, wenn die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

4.6 Widerspruchsrecht (Art. 21 DSGVO)

Die betroffene Person hat das Recht aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, jederzeit gegen die Datenverarbeitung, die auf einer der folgenden Gründe beruht, Widerspruch einzulegen:

- Für eine im öffentlichen Interesse liegende oder in Ausübung öffentlicher Gewalt erfolgenden Verarbeitung oder
- Verarbeitungen im berechtigten Interesse des Verantwortlichen oder eines Dritten ohne überwiegende schutzwürdige Interessen der betroffenen Person.

Werden personenbezogene verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung zum Zwecke der Direktwerbung einzulegen.

4.7 Automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO)

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Gestattet sind automatisierte Entscheidungen in folgenden Einzelfällen, wobei die Ausnahmen grundsätzlich nicht für Entscheidungen auf besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO beruhen dürfen:

- Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags mit der betroffenen Person erforderlich,
- die automatisierte Entscheidung ist aufgrund von Rechtsvorschriften zulässig und diese Rechtsvorschriften enthalten angemessene Maßnahmen zur

Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

» die Entscheidung erfolgt mit ausdrücklicher Einwilligung der betroffenen Person.

Ist die automatisierte Entscheidung zur Vertragserfüllung erforderlich oder beruht sie auf einer Einwilligung, so sind geeignete Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren.