Vereinbarung über **Auftragsverarbeitung**

i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen dem Verantwortlichen

xxx

– nachfolgend Auftraggeber genannt –

und dem Auftragsverarbeiter

xxx

– nachfolgend Auftragnehmer genannt –

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Im Einzelnen sind die Angaben in **Anlage 1** Bestandteil der Datenverarbeitung.
Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen gemäß **Anlage 4** zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz--Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber in **Anlage 2** den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(11) Der Auftragnehmer benennt dem Auftraggeber in **Anlage 2** die Person(en), die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer in **Anlage 2** den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine

Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat. Für die in **Anlage 3** aufgeführten Unterauftragnehmer wird mit Unterzeichnung dieses Vertrages Zustimmung erteilt.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** aufgelisteten Subunternehmer durchgeführt. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Anlage 1: Gegenstand und Dauer der Verarbeitung, Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung
Anlage 2: Weisungsberechtigte Personen und Datenschutzbeauftragter
Anlage 3: Unterauftragnehmer mit Beschreibung der Leistungen / Teilleistungen
Anlage 4: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 3 Abs. 2)

Ort, Datum Unterschrift Auftragnehmer

Ort, Datum Unterschrift Auftraggeber

Anlage 1

Gegenstand der Verarbeitung

z.B. Fernwartung

Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung

Kategorien von Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
z.B. Adressdaten, Kommunikationsdaten, Userdaten, Plandaten, Projektdaten, Bilddaten, Tondaten, IT-Nutzungsdaten, Zeiterfassungsdaten, Vertragsdaten, Maschinendaten, Funktionsbezeichnung, Bankverbindungsdaten	z.B. Fernwartungszugriff zur Konfiguration, Wartung, Fehlersuche und Fehlerbehebung, Konfigurieren und Erstellen von Backups, Scandienstleistungen, Datenkonvertierungen	z.B. Mitarbeiter, Leiharbeiter, Praktikanten, Werkstudenten, Lieferanten

Anlage 2

Weisungsberechtigte Personen des Auftraggebers:

Vorname	Name	Telefonnummer
xxx		

Weisungsberechtigte Personen des Auftragnehmers

Vorname	Name	Telefonnummer
xxx		

Datenschutzbeauftragter/Ansprechpartner des Auftragnehmers

Vorname	Name	Telefonnummer
xxx		

Anlage 3

Unterauftragnehmer mit Beschreibung der Leistungen / Teilleistungen

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
xxx	

Anlage 4

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Zugangskontrolle (Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte):

- z.B. Alarmanlage
- Automatisches Zugangskontrollsystem
- Schließsystem mit Codesperre
- Lichtschranken / Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Wach- und Reinigungspersonal
- Absicherung von Gebäudeschächten
- Videoüberwachung
- Sicherheitsschlösser

Datenträgerkontrolle (Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern)

- z.B. Verwendung fester, verschließbarer Metallbehälter
- Versand der Datenträger als Wertsendung
- Keine Kennzeichnung der Behältnisse als Datenträger
- Abgleich der Risiken zwischen Spediteur und Postdienste
- Versandmappen bei hausinternem Transport fest verschließen

Speicherkontrolle (Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten)

- z.B. Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

Benutzerkontrolle (Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte)

- z.B. Zuordnung von Benutzerrechten
- Authentifikation mit Benutzername / Passwort
- Gehäuseverriegelungen
- Sperren von externen Schnittstellen (USB, etc.)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Wachpersonal
- Einsatz von Intrustion-Detection-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Anti-Viren-Software
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Verschlüsselung von mobilen Datenträgern
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Hard- und Softwarefirewalls

Zugriffskontrolle (Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben)

- z.B. Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das Notwendigste reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

Übertragungskontrolle (Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können)

- z.B. Verschlüsselung der Daten
- Passwortschutz einzelner Dokumente
- VPN-Tunnel
- Firewall, Virenschutz, Intrusion Detection
- System (IDS)
- Content-Filter, SSL-Scanner

Eingabekontrolle (Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind)

- z.B. Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

Transportkontrolle (Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden)

- z.B. Einrichtung von verschlüsselten VPN-Tunneln
- E-Mail-Verschlüsselung
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Wiederherstellbarkeit (Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)

- z.B. Erstellen eines Backup- & Recoverykonzepts
- Festplattenspiegelung nach Vereinbarung mit dem Auf- traggeber
- Testen von Datenwiederherstellung• Erstellen eines Notfallplans

Zuverlässigkeit (Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden)

- z.B. Unabhängig voneinander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

Datenintegrität (Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können)

- z.B. Erstellen eines Backup- & Recoverykonzepts
- Nachträgliche Feststellung inwieweit Daten verändert wurden (über Prüfsummen, Richtungsindikatoren oder Sequenznummern)
- Einführung von Audit-Trails
- Verwendung digitaler Signaturen

Auftragskontrolle (Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

- z.B. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafen bei Verstößen
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit

- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeitskontrolle (Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind)

- z.B. Temperatur- und Feuchtigkeitsüberwachung in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- und Recoverykonzepts
- Erstellen eines Notfallsplans

Trennbarkeit (Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können)

- z.B. Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Trennung von Produktiv- und Testsystem