**Beispiele für technische und organisatorische Maßnahmen**

(davon müssen nur die genannt werden, die gegeben sind, dass hier wäre nur von Großunternehmen zu leisten, also einfach als Anregung verstehen)

**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

**Zutrittskontrolle**

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)

☐ Sicherheitstüren / -fenster

☐ Gitter vor Fenstern/Türen

☐ Zaunanlagen

☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

☐ Werkschutz, Pförtner

☐ Alarmanlage

☐ Videoüberwachung

☐ Spezielle Schutzvorkehrungen des Serverraums

☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern

☐ Nicht-reversible Vernichtung von Datenträgern

☐ Mitarbeiter- und Berechtigungsausweise

☐ Sperrbereiche

☐ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten,

Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

☐ Andere Maßnahmen: [Bitte ergänzen]

**Zugangskontrolle**

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

☐ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk

☐ Autorisierungsprozess für Zugangsberechtigungen

☐ Begrenzung der befugten Benutzer

☐ Single Sign-On

☐ BIOS-Passwörter

☐ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und

Aktualisierungsintervall)

☐ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor

unbefugtem Zugriff

☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.

☐ Protokollierung des Zugangs

☐ Zusätzlicher Login für bestimmte Anwendungen

☐ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität

☐ Firewall

☐ Andere Maßnahmen: [Bitte ergänzen]

**Zugriffskontrolle**

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

☐ Verwaltung und Dokumentation von differenzierten Berechtigungen

☐ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und

Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.

☐ Auswertungen/Protokollierungen von Datenverarbeitungen

☐ Autorisierungsprozess für Berechtigungen

☐ Genehmigungsroutinen

☐ Profile/Rollen

☐ Verschlüsselung von Datenträgern

☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf mobile

Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention System/DLP)

☐ Mobile Device Management (MDM)

☐ Vier-Augen-Prinzip

☐ Funktionstrennung (Segregation of Duties)

☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399

☐ Nicht-reversible Löschung von Datenträgern

☐ Sichtschutzfolien für mobile Datenverarbeitungsanlagen

☐ Andere Maßnahmen: [Bitte ergänzen]

**Trennungskontrolle**

Folgende stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken

☐ Verarbeitung auf mindestens logisch getrennten Systemen

☐ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☐ Mandantenfähigkeit von IT-Systemen

☐ Verwendung von Testdaten

☐ Trennung von Entwicklungs- und Produktionsumgebung

☐ Andere Maßnahmen: [Bitte ergänzen]

**Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

Die Verarbeitung von Daten erfolgt so, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

[Bitte das Verfahren zur Pseudonymisierung kurz und verständlich darstellen]

**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

**Weitergabekontrolle**

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☐ Verschlüsselung von E-Mail oder E-Mail-Anhängen

☐ Verschlüsselung von Datenträgern

☐ Gesicherter File Transfer oder sonstiger Datentransport

☐ Physikalische Transportsicherung

☐ Verpackungs- und Versandvorschriften

☐ Qualifizierte elektronische Signatur

☐ Verschlüsseltes WLAN

☐ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber,

Challenge-Response, Rückrufautomatik, Einmal-Passwort)

☐ Mobile Device Management (MDM)

☐ Data Loss Prevention System (DLP)

☐ Regelung zum Umgang mit mobilen Datenträgern (z.B. Laptop, USB-Stick, Mobiltelefon)

☐ Protokollierung von Datenübertragung oder Datentransport

☐ Protokollierung von lesenden Zugriffen

☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

☐ Andere Maßnahmen: [Bitte ergänzen]

**Eingabekontrolle**

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

☐ Zugriffsrechte

☐ Systemseitige Protokollierungen

☐ Dokumenten Management System (DMS) / Enterprise Content Management System (ECMS)

mit Änderungshistorie

☐ Sicherheits-/Protokollierungssoftware

☐ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

☐ Vieraugenprinzip

☐ Data Loss Prevention System (DLP)

☐ Andere Maßnahmen: [Bitte ergänzen]

**Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

☐ Sicherheitskonzept für Software- und IT-Anwendungen

☐ Backup Verfahren

☐ Aufbewahrungsprozess für Backups (z.B. brandgeschützter Safe, getrennter Brandabschnitt)

☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk

☐ Bedarfsgerechtes Einspielen von Sicherheits-Updates

☐ Spiegeln von Festplatten

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente

☐ Brand- und/oder Löschwasserschutz des Serverraums

☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten

☐ Klimatisierter Serverraum

☐ Virenschutz

☐ Firewall

☐ Notfallplan

☐ Erfolgreiche Notfallübungen

☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

☐ Andere Maßnahmen: [Bitte ausführen]

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**

**Datenschutz-Management**

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☐ Datenschutzleitbild des Anbieters

☐ Datenschutz-Richtlinie des Anbieters

☐ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen

zur Datensicherheit (z.B.: UHB der Sparkasse)

☐ Benennung eines Datenschutzbeauftragten

☐ Verpflichtung der Mitarbeiter auf die Vertraulichkeit

☐ Hinreichende Schulungen der Mitarbeiter im Datenschutz

☐ Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

☐ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

☐ Externe Prüfung oder Auditierung

☐ Andere Maßnahmen: [Bitte ausführen]

**Management bei Datenschutzverletzungen**

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den

Aufsichtsbehörden (Art. 33 DSGVO)

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber

betroffenen Personen (Art. 34 DSGVO)

☐ Andere Maßnahmen: [Bitte ausführen]

**Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

[Bitte Beispiele benennen]

**Auftragskontrolle**

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Auftraggebers verarbeitet werden:

☐ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten

der Parteien

☐ Prozess zur Erteilung und/oder Befolgung von Weisungen

☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung

☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Anbieter

☐ Unabhängige Auditierung der Weisungsgebundenheit

☐ Verpflichtung der Beschäftigten auf die Vertraulichkeit

☐ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen

☐ formalisiertes Auftragsmanagement

☐ dokumentiertes Verfahren zur Auswahl von Unterauftragnehmern

☐ standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern

☐ Andere Maßnahmen: [Bitte ergänzen]