# Dokumentation der Einhaltung der bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen

**Dieses ist eine mögliche Checkliste für den Nachweis gemäß § 30 Abs. 2 S. 4 DSG-EKD. Das Muster ist nicht abschließend und kann für den Einzelfall angepasst werden.**

**1. Maßnahmen zur Sicherstellung der Vertraulichkeit:**

* 1. **Maßnahmen, die Unbefugten den räumlichen Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet werden**

**a) Vorhandene Zutrittskontrollen zum Gebäude und den Büroräumen:**

ja / nein

/ Personenkontrolle durch Pförtner / Empfang am Eingang

/ Besucherregelung mit Ausgabe von Besucherausweisen

/ Videoüberwachung aller Gebäudezugänge

/ Einbruchsmeldeanlage, informiert wird: Namen eingeben

/ Schließsystem mit Berechtigungsregelung

/ Chipkarten-/Transponder-Schließsystem (z.B. RFID)

Protokollierung erfolgt für die Dauer von: Zeitraum eingeben

/ Regelungen zur Nachvollziehbarkeit der Schlüsselausgabe

/ Sonstiges: Text eingeben

**b) Vorhandene Zutrittskontrollen zum Serverraum:**

ja / nein

/ Personenbezogene Daten werden auf Server gespeichert

/ Gesonderte Zutrittsregelung für autorisiertes Personal

/ Der oder die Server befinden sich in der Dienststelle. Folgende Personen haben

Zutritt: Namen eingeben

/ Wird der Serverraum auch für andere Zwecke genutzt? Wenn ja,

welche: andere Zwecke angeben

/ Der oder die Server sind ausgelagert / angemietet:

1. Standort / Firma: Standort, Firma angeben

2. Standort / Firma: Standort, Firma angeben

/ Sonstiges: Text eingeben

* 1. **Maßnahmen, die Unbefugten die Nutzung der Datenverarbeitungssysteme und die Verarbeitung von personenbezogenen Daten verwehren**

**a) Vorhandene Zugangskontrollen zu den Datenverarbeitungssystemen:**

ja / nein

/ Die Systeme sind durch eine Firewall geschützt

/ Die Firewall wird regelmäßig aktualisiert. Durch:  eigene IT  Dienstleister

/ Der Zugriff von außen erfolgt über eine VPN-Verbindung

Zugang wird nach Zahl eingeben erfolglosen Anmeldeversuchen für Zahl eingeben Min. gesperrt

/ Authentifikation erfolgt durch Benutzername und Kennwort. Vorgaben sind:

mindestens:  6 Zeichen  8 Zeichen  10 Zeichen

zu verwenden sind:  Sonderzeichen  Ziffern  Groß-/Kleinschreibung

Gültigkeitsdauer:  90 Tage  bis 180 Tage  mehr als 180 Tage

/ Das IT System zwingt zur Einhaltung der o. a. Vorgaben

/ Authentifizierung mit biometrischen Verfahren

/ Datenträger werden verschlüsselt. Verschlüsselung erfolgt bei:

Notebooks  mobilen Datenträgern  Smartphones

/ Externe Schnittstellen (z.B. USB) werden auf mobilen Geräten gesperrt

/ Smartphones können durch zentrale Admin-Software zurückgesetzt werden

/ Einsatz von Anti-Viren-Software

/ Automatische Sperrmechanismen bei unautorisiertem Zugang

/ Protokollierung des Zugangs

/ Sonstiges: Text eingeben

**b) Vorhandene Zugriffskontrollen zu personenbezogenen Daten:**

ja / nein

/ Ein Berechtigungskonzept kommt zur Anwendung.

/ Die Rechtevergabe wird nachvollziehbar protokolliert.

Die Verwaltung der Rechte erfolgt durch: Namen eingeben

/ Physisches Löschen von Datenträgern vor Weiterverwendung

/ Vernichtung von Datenträgern nach DIN 66399 (ggf. über zertifizierte Dienst-

leister)

/ Protokollierung der Vernichtung

/ Sonstiges: Text eingeben.

**1.3 Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle)**

ja / nein

/ Trennung von Produktiv- und Testsystemen

/ Mandantentrennung

/ Physikalisch getrennte Speicherung auf gesonderten Systemen oder

Datenträgern

/ Logische Mandantentrennung (softwareseitig)

/ Nutzung von Berechtigungskonzepten

/ Sonstiges: Text eingeben

**2. Maßnahmen zur Sicherstellung der Integrität (Unversehrtheit von Daten)**

**Maßnahmen zur nachträglichen Feststellung, ob und von wem Daten eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)**

ja / nein

/ Vergabe und Dokumentation von Rechten zur Eingabe, Änderung und Löschung

von Daten auf Basis eines Berechtigungskonzepts inklusive Vererbungslogik

/ Protokollierung der Eingabe, der Änderung und der Löschung von Daten auf

Basis individueller Benutzernamen

/ Sonstiges: Text eingeben

**3. Maßnahmen zur Sicherstellung der Verfügbarkeit**

**Maßnahmen, die eine Zerstörung personenbezogener Daten verhindern, bzw. eine Wiederherstellung sicherstellen (Verfügbarkeitskontrolle)**

ja / nein

/ Serverraum ist hochwassergeschützt

/ Serverraum befindet sich nicht unter sanitären Anlagen

/ Serverraum ist klimatisiert

/ Temperatur und Feuchtigkeit im Serverraum werden überwacht

/ Brandmeldeanlage ist vorhanden

/ Überspannungsschutz ist vorhanden

/ Unterbrechungsfreie Stromversorgung (USV) ist vorhanden

/ Notstromaggregat ist vorhanden

/ Alarmmeldung bei unberechtigten Zutritten zum Serverraum

/ Festplattenspiegelung (RAID System) ist eingerichtet

/ Backup- & Wiederherstellungskonzept ist vorhanden

Backup erfolgt:  täglich  wöchentlich  monatlich

/ Test einer Datenwiederherstellung erfolgt regelmäßig

/ Backup-Datei/en sind verschlüsselt

/ Datensicherung wird von den Servern räumlich getrennt aufbewahrt:

Separater Brandabschnitt

Anderer Standort

/ Prozesse für Software- und Patchmaßnahmen sind vorhanden

werden regelmäßig durchgeführt

werden dokumentiert

werden durch eigene IT durchgeführt

werden von einem Dienstleister durchgeführt

/ Notfallplan ist vorhanden (z.B. bei Brand, Hardwaredefekt)

/ Sonstiges: Text eigeben

**4. Maßnahmen zur sicheren Datenübertragung**

**Maßnahmen, die sicherstellen, dass bei Übertragungen Unbefugte die Daten nicht lesen, kopieren, verändern oder entfernen können. (Weitergabekontrolle)**

ja / nein

/ Die Datenübertragung erfolgt für alle in diesem Auftrag relevanten Vorgänge

elektronisch und zwar verschlüsselt per:

Transportverschlüsselung

VPN-Tunnel (Virtual Private Network)

TLS/SSL (Transport Layer Security / Secure Sockets Layer)

SFTP (Secure File Transfer Protocol)

Ende-zu-Ende Verschlüsselung

SMime (Secure Multipurpose Internet Mail Extensions)

PGP (Pretty Good Privacy)

WinZip-Dateianhang an einer E-Mail

evtl. weitere oben noch nicht aufgeführte Maßnahmen

/ Abruf- und Übermittlungsvorgänge werden nachvollziehbar protokolliert und

aufbewahrt:  dauerhaft  bis Auftragsende  bis Datum auswählen

/ Transport erfolgt physisch sicher verpackt auf einem Datenträger

/ Sonstiges: evtl. zusätzlichen Text eingeben