**[Auf Briefbogen des Betriebs]**

**Muster**

**Technische und organisatorische Maßnahmen**

**1. Organisatorische Maßnahmen**

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?

☐ Nein

☐ Ja

Name: ………………………….

Funktion: ………………………

E-Mail: …………………………

Telefon: ………………………..

☐ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.

☐ Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.

☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).

☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.

☐ Ein Datenschutzkonzept ist vorhanden.

☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am \_\_\_\_\_\_\_und Bestätigung s. Anlage \_\_\_\_).

☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am \_\_\_\_\_\_und Bestätigung s. Anlage \_\_\_\_).

**2. Vertraulichkeit**

1. ***Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle***

*Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.*

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden

☐ Alarmanlage

☐ Automatisches Zutrittskontrollsystem, Ausweisleser

☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)

☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)

☐ Sicherheitsschlösser

☐ Chipkarten-/Transponder-Schließsystem

☐ Biometrie (Fingerabdrücke o. ä.)

☐ Manuelles Schließsystem

☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)

☐ Magnetschleusen

☐ Werkschutz/Pförtner

☐ Empfang mit Anmeldung

☐ Sorgfältige Auswahl von Wachpersonal

☐ Sorgfältige Auswahl von Reinigungspersonal

☐ Lichtschranke/Bewegungsmelder

☐ Feuerfeste Türen

☐ Absicherung von Gebäudeschächten

☐ Fenstervergitterung

☐ Panzerglas

☐ Videoüberwachung der Zugänge

1. ***Zugangs- und Benutzerkontrolle***

*Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

☐ Passwortvergabe

Länge des Passworts: … Zeichen

Wechselfristen: … Wochen/Monate

Anzahl der Fehleingaben: …

☐ Chipkarte mit PIN/Passwort

☐ Authentifikation mit Benutzername/Passwort

☐ Biometrisches Merkmal mit PIN/Passwort

☐ Einsatz von VPN-Technologie

☐ Verschlüsselung von Smartphone-Inhalten

☐ Verschlüsselung von mobilen Datenträgern

1. ***Zugriffskontrolle***

*Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

☐ Schriftliches Berechtigungskonzept vorhanden

☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen

☐ Verwaltung der Rechte durch System-Administrator

☐ Anzahl der Administratoren auf das "Notwendigste" reduziert

☐ Gesicherte Nutzung von USB-Schnittstellen

☐ Automatische Sperrung des Arbeitsplatzes

☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ….

☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399

☐ Verschlüsselung von Datenträgern

☐ Sichere Aufbewahrung von Datenträgern

☐ Ordnungsgemäße Vernichtung von Datenträgern

☐ Löschungskonzept für Daten

☐ Protokollierung der Vernichtung

1. ***Transport- und Übertragungskontrolle***

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektroni*schen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln

☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung

☐ E-Mail-Verschlüsselung

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☐ Protokollierung von Übermittlungen

☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang

☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen

☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

1. ***Auftragskontrolle***

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung

☐ Kontrolle der Vertragsausführung

☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐ Regelung zu Wartungen (speziell Fernwartung)

**3. Integrität**

1. ***Eingabekontrolle/Verarbeitungskontrolle***

*Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

☐ Protokollauswertungsroutinen/-systeme vorhanden

☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

1. ***Dokumentationskontrolle***

*Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.*

☐ Führung eines Verarbeitungsverzeichnisses

☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

**4. Verfügbarkeitskontrolle**

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.*

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Überspannungsschutz

☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)

☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☐ Feuer- und Rauchmeldeanlagen

☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

☐ Testen von Datenwiederherstellung

☐ Klimaanlage in Serverräumen

☐ Schutzsteckdosenleisten in Serverräumen

☐ Feuerlöschgeräte in Serverräumen

☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)

☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ Virenschutzsystem

☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)

☐ Konzept für Katastrophenfall vorhanden

**5. Trennungsgebot**

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Logische Mandantentrennung (softwareseitig)

☐ Trennung von Produktiv- und Testsystem

☐ Festlegung Technologie von Datenbankrechten

☐ Trennung von Daten verschiedener Auftraggeber