Technische und Organisatorische Maßnahmen gemäß DSGVO

der

Musterfirma (bei Einzelunternehmen ist
zusätzlich der Inhaber zu nennen)
Musterstraße 1
12345 Musterstadt
- Verantwortlicher -

(Stand: _____)

Der vg. Verantwortliche hat die nachfolgend benannten technischen und organisatorischen Maßnahmen getroffen, um die Vorgaben der jeweils geltenden Datenschutzgesetze, insbesondere der EU-Datenschutzgrundverordnung (EU-DSGVO) und des Bundesdatenschutzgesetzes (BDSG), im Hinblick auf ein angemessenes Schutzniveau zu gewährleisten.

I. Pseudonymisierung gemäß Art. 32 Abs. 1 lit. a) DSGVO

Maßnahmen, die gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden TOMs unterliegen.	
☐ Bei Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und gesicherten (verschlüsselten) Systemen	☐
☐	☐
☐	☐

II. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	
☐ Alarmanlage	☐ Absicherung von Gebäudeschächten
☐ Automatisches Zugangskontrollsystem	☐ Chipkarten-/Transponder-Schließsystem
☐ Schließsystem mit Codesperre	☐ Manuelles Schließsystem
☐ Biometrische Zugangssperren	☐ Videoüberwachung der Zugänge
☐ Lichtschranken / Bewegungsmelder	☐ Sicherheitsschlösser
☐ Schlüsselregelung (Schlüsselausgabe mit Liste)	☐ Personenkontrolle beim Pförtner / Empfang
☐ Protokoll der Besucher (Besucherbuch)	☐ Sorgfältige Auswahl von Reinigungspersonal

☐	Sorgfältige Auswahl von Wachpersonal	☐	Mitarbeiter- und Besucherausweise
☐	Türen mit Knauf Außenseite	☐	Klingelanlage mit Kamera
☐	Besucher nur in Begleitung von Mitarbeitern	☐	
☐		☐	
☐		☐	

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

☐	Zuordnung und Verwaltung von Benutzerrechten	☐	Erstellung von Benutzerprofilen
☐	Passwortvergabe durch Admin	☐	Authentifizierung mit biometrischen Verfahren
☐	Authentifizierung mit Benutzername / Passwort	☐	Einsatz von VPN-Technologie
☐	Gehäuseverriegelungen	☐	Einsatz von Anti-Viren-Software
☐	Sperren von externen Schnittstellen (USB etc.)	☐	Einsatz einer Software-Firewall
☐	Einsatz einer Hardware-Firewall	☐	Konzept „Clean Desk“
☐	Passwortkonzept inkl. Manuelle Desktopsperre	☐	Verschlüsselung von Notebooks / Tablets
☐	Löschkonzept	☐	Verschlüsselung von Datenträgern
☐	Einsatz von Intrustion-Detection-Systemen	☐	Verschlüsselung von Smartphones
☐		☐	
☐		☐	

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☐	Erstellung eines Berechtigungskonzepts	☐	Verwaltung der Rechte durch Admin
☐	Einsatz eines Berechtigungskonzepts	☐	Minimale Anzahl an Administratoren
☐	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☐	Sichere Aufbewahrung von Datenträgern
☐	Physische Löschung von Datenträgern	☐	Vernichtung von Datenträgern (DIN 32757)

☐	Aktenschredder ab Stufe 3 (vertrauliche Daten)	☐	
☐		☐	
☐		☐	

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.			
☐	Physikalische Trennung (Systeme / Datenbaken / Datenträger)	☐	Logische Mandantentrennung (per Software)
☐	Einsatz eines Berechtigungskonzepts	☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern	☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☐	Festlegung von Datenbankrechten	☐	Trennung von Produktiv- und Testsystem
☐		☐	
☐		☐	

III. Integrität gemäß Art. 32 Abs. 1 lit. b DSGVO

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.			
☐	Einrichtungen von VPN-Tunneln	☐	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
☐	E-Mail-Verschlüsselung	☐	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	☐	Beim Transport: sichere Transportbehälter/-verpackungen/-fahrzeuge
☐	Verschlüsselte Verbindungen, z.B. https	☐	
☐		☐	
☐		☐	

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	
☐ Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Erstellung einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
☐ 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
☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☐ Kontrolle der Protokolle
☐ Löschkonzept mit Zuständigkeiten	☐
☐	☐
☐	☐

IV. Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, sowie die gewährleisten, dass personenbezogene Daten rasch wiederhergestellt werden können.	
☐ Unterbrechungsfreie Stromversorgung (USV)	☐ Klimaanlage in Serverräumen
☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☐ Schutzsteckdosenleisten in Serverräumen
☐ Feuer- und Rauchmeldeanlagen	☐ Feuerlöschgeräte in Serverräumen
☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☐ Erstellung eines Backup- & Recoverykonzepts
☐ Testen von Datenwiederherstellung	☐ Erstellung und Tests eines Notfallplans
☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☐ Serverräume nicht unter sowie ohne sanitäre Anlagen
☐ Serverräume über der Wassergrenze (bei Hochwassergebieten)	☐ RAID-System / Spiegelung von Festplatten
☐ Videoüberwachung Serverraum	☐
☐	☐
☐	☐

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Art. 32 Abs. 1 lit. d) DSGVO

1. Datenschutz-Management

Maßnahmen, die die Einhaltung der Datenschutzvorgaben gewährleisten.			
☐	Installation eines internen oder externen Datenschutzbeauftragten, sofern entsprechende Pflicht besteht	☐	Regelmäßige Schulung der Mitarbeiter zum Datenschutzrecht
☐	Meldung des internen oder externen Datenschutzbeauftragten bei der Aufsichtsbehörde	☐	Verpflichtung der Mitarbeiter auf das Datengeheimnis
☐	Prüfung der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung sowie Durchführung im Bedarfsfall	☐	Installation eines Prozesses zur Erfüllung der Informationspflichten gem. Art. 13, 14 DSGVO
☐	Installation eines Prozesses zur Erfüllung der Auskunftspflicht gem. Art. 15 DSGVO	☐	Löschkonzept i.S.d. Art. 17 DSGVO
☐	Installation eines Prozesses zur Erfüllung der Pflichten gem. Art. 16 (Berichtigung) und 18 (Einschränkung der Verarbeitung) DSGVO	☐	Installation eines Prozesses zur Bearbeitung von Widersprüchen i.S.d. Art. 21 DSGVO
☐	Zentrale Dokumentation aller Verfahrensanweisungen zum Datenschutz nebst Zugriffsmöglichkeiten für die Mitarbeiter	☐	Erstellung eines IT-Sicherheitskonzeptes
☐	Regelmäßige Überprüfung der Wirksamkeit der getroffenen TOMs	☐	
☐		☐	
☐		☐	

2. Incident-Response-Management

Maßnahmen, die für den Fall bzw. im Falle einer Datenschutzverletzung zu ergreifen sind.			
☐	Dokumentation eines Prozesses zur Erkennung und (rechtzeitigen) Meldung von Datenschutzverletzungen inkl. Festlegung von Zuständigkeiten und Erstellung von Musterformularen (Meldung bei der Aufsichtsbehörde und/oder beim Betroffenen)	☐	Einschaltung des Datenschutzbeauftragten
☐	Regelmäßige Durchführung von Testsituationen einer Datenschutzverletzung	☐	Nachbearbeitung von Datenschutzverletzungen
☐		☐	
☐		☐	

3. Datenschutzfreundliche Voreinstellungen

Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

☐	Vorhaltung nur objektiv erforderlicher Checkboxen	☐	Keine Vorhaltung vorausgefüllter Checkboxen
☐		☐	
☐		☐	

4. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.			
☐	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	☐	Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☐	Dokumentierte Weisungen an den Auftragnehmer	☐	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
☐	Auftragnehmer hat Datenschutzbeauftragten bestellt, sofern entsprechende Pflicht besteht	☐	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	☐	Laufende Überprüfung des Auftragnehmers, seiner Tätigkeiten und seines Schutzniveaus
☐	Vertragsstrafen bei Verstößen	☐	Abschluss eines Auftragsverarbeitungsvertrages
☐	Vereinbarung zur Verwendung von Subunternehmern	☐	
☐		☐	
☐		☐	