**Technische und organisatorische Maßnahmen**

**gem. Art. 32 DSGVO**

(bitte wählen Sie einzelne auf Sie zutreffende Maßnahmen durch Anklicken aus)

**Maßnahmen zur Pseudonymisierung (Art. 25 Abs. 1 DSGVO) und Verschlüsselung personenbezogener Daten – Art. 32 Abs. 1 a) DSGVO**

Schaffung von eineindeutigen Identifizierungsmerkmalen (z.B. Personen-Nummern anhand zufälliger Zeichenfolge)

Identifizierung von Datensätzen mit IDs (statt Klarnamen und anderen personenbezogenen Merkmalen)

keine Eingabe von nicht pseudonymen Daten möglich (z.B. nur Nicknames statt Klarnamen)

automatische Pseudonymisierung bei Eingabe neuer Datensätze (z.B. automatische Vergabe einer Personen-Nummer)

Verschlüsselung von Dateien

Verschlüsselung von mobilen Endgeräten (Smartphones, Laptops etc.)

gesicherte Datenweitergabe (SSL, FTPS, TLS etc.)

gesichertes WLAN

sonstiges:

**Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität – Art. 32 Abs. 1 b) DSGVO**

**Zutrittskontrolle:**

- kein unbefugter Zutritt zu Datenverarbeitungsanlagen -

Sicherheitsschlösser/-türen/-fenster

Ausweis- / Magnet- / Chipkarten

Alarmanlage

Schlüsselvergabe / -verwaltung / -dokumentation

Zutrittsregelungen für Besucher

Wachdienst / Pförtner

Videoüberwachung

Gebäudesicherung durch Zäune, Pforten etc.

sonstiges:

**Zugangs-/ Zugriffskontrolle:**

- keine unbefugte Systemnutzung und unbefugtes Lesen, Schreiben, Kopieren, Verändern, Entfernen von personenbezogenen Daten innerhalb des Systems -

Passwort-Authentifizierung

Zwei-Faktoren-Authentifizierung / Multi-Factor-Authentifizierung

sichere Passwörter / Anforderungen an Passwörter (z.B. Sonderzeichen, Mindestlänge, regelmäßige Änderung)

automatische Sperrung nach Fehlversuchen der Passworteingabe

Berechtigungs- / Rollenkonzept

Zugangssperre durch Bildschirmschoner

Protokollierung des Zugangs/Zugriffs

Verschlüsselung von Datenträgern

aktueller Virenschutz

aktuelle Softwareversionen

Firewalls (Hard-/Software)

Einsatz von VPN (Virtual Private Networks)

ordnungsgemäße Vernichtung von Datenträgern

sonstiges:

**Weitergabekontrolle:**

- kein unbefugtes Lesen, Schreiben, Kopieren, Verändern, Entfernen von personenbezogenen Daten bei elektronischer Übertragung -

Festlegung und Dokumentation der Empfänger

Übermittlungsprotokolle

Verschlüsselung von Datenträgern und Verbindungen

Weitergabeberechtigungen

elektronische Signatur

Regelungen zur Datenträgervernichtung

Regelungen zur sicheren Löschung vom Speichermedium

Regelungen zur sicheren Lagerung und Versand von Datenträgern

Regelungen zum Gebrauch von mobilen Datenträgern (CDs, USB-Sticks, etc.)

sonstiges:

**Eingabekontrolle:**

- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind -

Protokollierung von Dateneingaben, -änderungen und -löschungen

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

Berechtigungskonzept zur Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten

sonstiges:

**Trennungskontrolle:**

- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können -

physische Trennung der Daten (hardwareseitig)

logische Trennung der Daten (softwareseitig)

Mandanten-Trennung

Trennung Produktiv- und Testsystem

bei Pseudonymisierung: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten System

sonstiges:

**Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme – Art. 32 Abs. 1 b) DSGVO**

**Verfügbarkeitskontrolle:**

- Schutz gegen zufällige Zerstörung oder Verlust personenbezogener Daten -

Back-Up-Strategie (online/offline, onsite/offsite)

unterbrechungsfreie Stromversorgung (USV)

Notfallkonzept für den Bedarfsfall

sonstiges:

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen – Art. 32 Abs. 1 d) DSGVO**

**Auftragskontrolle:**

- Auftragsverarbeitung nur entsprechend den Weisungen des Auftraggebers -

Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten

Schriftliche Festlegung der Weisungen (Vertrag gem. Art. 28 Abs. 3 DSGVO)

Prozess zur Weiterleitung von Betroffenenanfragen

Kontrolle der Einhaltung bei Auftragnehmern

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

sonstiges:

**Sonstige Verfahren:**

Datenschutz-Management

Datenschutz-Schulungen

Datensicherheitskonzept

Incident-Response-Management

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Zweckbindungskontrolle (regelmäßige Überprüfung des Verwendungszwecks)

sonstiges:

**Begleitende Maßnahmen:**

**Datenschutz auf Mitarbeiterebene:**

Vertrauens-/Verschwiegenheitsverpflichtung

Regelungen Home-Office

Regelungen zur Nutzung privater mobiler Endgeräte (Smartphones, Laptops etc.)

Regelungen betrieblicher Internet/E-Mail-Nutzung

Schulungen

sonstiges:

**Archivierung, Löschung, Entsorgung und Einschränkung Verarbeitung:**

Archivierungs-, Lösch- und Entsorgungskonzept mit festgelegten Zuständigkeiten

einfache Löschung ohne Überschreiben

randomisiertes Überschreiben

Fernlöschung (z.B. mobile Endgeräte)

mechanische Deformierung (Schreddern) von Datenträgern (Papier, DVD, CD etc.)

Zerstörung von Datenträgern vor Entsorgung

Auswahl von Entsorgungsdienstleistern unter Sorgfaltsgesichtspunkten

Protokollierung der Löschvorgänge

automatische Löschung von Datensätzen nach festgelegter Frist

Unterrichtung der Mitarbeiter über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für Geräteentsorgung und Entsorgungsdienstleister

sonstiges:

**Wahrung der Betroffenenrechte:**

Konzept zur Wahrung der Rechte der Betroffenen (Auskunft, Korrektur, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen

sonstiges:

**Notfallkonzept**

Konzept über unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung)

sonstiges:

**genehmigte Regelungen/Zertifikate:**

interne Verhaltensregeln gem. Art. 40 DSGVO

Zertifizierung gem. Art. 42 DSGVO

sonstiges:

**Sonstige Maßnahmen:**

**Haftungsausschluss:**

Diese Mustervorlage dient als Formulierungshilfe und ist entsprechend den Anforderungen an die DSGVO möglichst verständlich formuliert. Jedoch sollten Sie das Muster nur nach sorgfältiger Prüfung und Anpassung auf Ihren spezifischen Einzelfall und nach Ihren eigenen Anforderungen anwenden und ggf. ergänzen und erweitern. Lassen Sie sich im Zweifel rechtlich beraten.