# Darstellung der technischen und organisatorischen Maßnahmen bei der Auftragsverarbeitung/Sicherheit der Verarbeitung

|  |  |
| --- | --- |
| Unternehmen | Klicken oder tippen Sie hier, um Text einzugeben. |
| Stand | Klicken oder tippen Sie, um ein Datum einzugeben. |

1. **Datenschutz-Maßnahmen**

|  |  |
| --- | --- |
| Ist ein interner / externer Datenschutzbeauftragter bestellt? | |
|  | **ja**, dann bitte den Ansprechpartner für den Datenschutz angeben   Name: Klicken oder tippen Sie hier, um Text einzugeben. Kontaktdaten: Klicken oder tippen Sie hier, um Text einzugeben. |
|  | **nein**, dann bitte begründen Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Mitarbeiter nachweislich über Datenschutz und Datensicherheit  geschult bzw. informiert |
|  | Mitarbeiter nachweislich geschult und auf Vertraulichkeit (Datengeheimnis),  ggf. auf das Fernmeldegeheimnis und die Wahrung von Berufsgeheimnissen, verpflichtet |
|  | Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener vorhanden |
|  | Datensicherheitskonzept/ Informationssicherheitsmanagement vorhanden |
|  | Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen  (z. B. technisch unterstützt oder durch Externe) |
|  | Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am Klicken oder tippen Sie, um ein Datum einzugeben.und Bestätigung s. Anlage …) |
|  | Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am  tt.mm.jjjj und Bestätigung s. Anlage …) |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**2.1 Zutrittskontrolle**

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Alarmanlage |  | Empfang mit Anmeldung |
|  | Automatisches Zutrittskontrollsystem, Ausweisleser |  | Werkschutz/Pförtner |
|  | Türsicherung (elektrischer Türöffner, Zahlenschloss usw.) |  | Sorgfältige Auswahl von Wachpersonal |
|  | Sicherheitsschlösser |  | Sorgfältige Auswahl von Reinigungs-personal |
|  | Chipkarten-/Transponder-Schließsystem |  | Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.) |
|  | biometrische Kontrollsysteme (Fingerabdrücke o. ä.) |  | Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden |
|  | Manuelles Schließsystem | Sind schriftliche Zutrittsregelungen vorhanden? | |
|  | Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.) |  | ja, im Dokument (z. B. im Daten-  schutzhandbuch): |
|  | Magnetschleusen |  | nein |
|  | Lichtschranke/Bewegungsmelder |  |  |
|  | Feuerfeste Türen |  |  |
|  | Absicherung von Gebäudeschächten |  |  |
|  | Fenstervergitterung |  |  |
|  | Panzerglas |  |  |
|  | Videoüberwachung der Zugänge |  |  |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**2.2 Zugangskontrolle**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Authentifikation mit Benutzername/Passwort |  | Erstellen von Benutzerprofilen |
|  | Chipkarte mit PIN/Passwort |  | Mobile Device Policy |
|  | Automatische Sperrung des Arbeitsplatzes |  | Allg. Richtlinie Datenschutz und / oder Sicherheit |
|  | Biometrisches Merkmal mit PIN/Passwort | Passwortvergabe | |
|  | Einsatz von VPN-Technologie |  | Komplexität des Passworts |
|  | Firewall |  | Definierte Wechselfristen |
|  | Anti-Viren-Software |  | Anzahl der Fehleingaben beschränkt |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**2.3 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Protokollierung der Vernichtung |  | Schriftliches Berechtigungskonzept vorhanden |
|  | Einsatz von Akten-/Daten-trägervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399 |  | Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen |
|  | Gesicherte Nutzung von USB-Schnittstellen |  | Verwaltung der Rechte durch System-Administrator |
|  | physische Löschung von Datenträgern vor Wiederverwendung |  | Anzahl der Administratoren auf das "Notwendigste" reduziert |
|  | Verschlüsselung von Datenträgern |  | Sichere Aufbewahrung von Datenträgern |
|  | ordnungsgemäße Vernichtung von Datenträgern |  | Löschungskonzept für Daten |
|  | Verschlüsselung von Smartphone-Inhalten |  |  |
|  | Verschlüsselung von mobilen Datenträgern |  |  |
|  | Protokollierung von Zugriffen auf  Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten |  |  |
|  | Die Protokolle werden ausgewertet, zeitlicher Abstand: |  |  |
| Klicken oder tippen Sie hier, um Text einzugeben. | |  |  |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**2.4 Trennungskontrolle**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Trennung von Produktiv- und Testsystem |  | Versehen der Datensätze mit Zweckattributen/Datenfeldern |
|  | physikalisch getrennte Speicherung auf gesonderten Systemen oder  Datenträgern |  | Trennung von Daten verschiedener Auftraggeber |
|  | Logische Mandantentrennung (softwareseitig) |  | Festlegung Technologie von Datenbankrechten |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der

Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen“, insbes. eines Identifizierungsschlüssels, möglich ist.

Ja  Nein

**2.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

Ja  Nein

**3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

**3.1 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | E-Mail-Verschlüsselung |  | Erstellen einer Übersicht von Datenträgern, Aus- und Eingang |
|  | Einrichtungen von Standleitungen bzw. VPN-Tunneln |  | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw.  Verschlüsselung |
|  | Firewall |  | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen |
|  | Sicherung von Datenträgertransporten (verschließbare Transportbehälter)  auch für Papier |  | Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und  Fahrzeugen |
|  | Nutzung von Signaturverfahren |  | Protokollierung von Übermittlungen |
|  | Bereitstellung über verschlüsselte  Verbindungen wie sftp, https |  |  |
|  | Protokollierung der Zugriffe und Abrufe |  |  |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**3.2 Eingabekontrolle/Verarbeitungskontrolle**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Protokollauswertungsroutinen/-systeme vorhanden |  | Aufbewahrung von Formularen, von denen Daten in automatisierte  Verarbeitungen übernommen worden sind |
|  | Manuelle oder automatisierte Kontrolle der Protokolle |  | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |
|  |  |  | Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden |
|  |  |  | Übersicht, mit welchen Programmen  welche Daten eingegeben, geändert oder gelöscht werden können |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**3.3 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 Verzeichnisses von Verarbeitungstätigkeiten

Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

Zulässigkeit eines Datentransfers in Drittländer ist gegeben

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**3.4 Auftragskontrolle**

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

Vorhandene Vereinbarungen zur Auftragsdatenverarbeitung

Kontrolle der Vertragsausführung

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Regelung zu Wartungen (speziell Fernwartung)

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**4.1 Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

|  |  |  |  |
| --- | --- | --- | --- |
| Technische Maßnahmen | | Organisatorische Maßnahmen | |
|  | Feuer- und Rauchmeldeanlagen |  | Konzept für Katastrophenfall vorhanden |
|  | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen |  | Testen von Datenwiederherstellung |
|  | Unterbrechungsfreie Stromversorgung (USV) |  | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |
|  | Überspannungsschutz |  | Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort) |
|  | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |  |  |
|  | Schutzsteckdosenleisten in Serverräumen |  |  |
|  | Klimaanlage in Serverräumen |  |  |
|  | Feuerlöschgeräte in Serverräumen |  |  |
|  | Schutz gegen Umwelteinflüsse (Sturm, Wasser) |  |  |
|  | Virenschutzsystem |  |  |
|  | Spiegelung von Festplatten (z. B. RAID-Verfahren) |  |  |

Weitere Maßnahmen bitte hier eintragen:

|  |  |
| --- | --- |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |
|  | Klicken oder tippen Sie hier, um Text einzugeben. |

**4.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)**

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Redundante Systemauslegung

Ausfallsicherheits-/Hochverfügbarkeitskonzept

Einsatz fehlertoleranter Software

Schutz vor Überlast und Denial of Service-Angriffen

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

Datenschutz-Management

Incident-Response-Management

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

**Vom Auftraggeber auszufüllen:**

Geprüft am Klicken oder tippen Sie hier, um Text einzugeben. durch Klicken oder tippen Sie hier, um Text einzugeben.

*Ergebnis(se):*

Es besteht noch Klärungsbedarf zu Klicken oder tippen Sie hier, um Text einzugeben.

Die TOM sind für den angestrebten Schutzzweck ausreichend.