Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Artikel 32 DSGVO.

# 1. Allgemeines

# 2. Vertraulichkeit

Zutrittskontrolle

Zugangskontrolle

Zugriffskontrolle

Trennung

Pseudonymisierung & Verschlüsselung

# 3. Integrität

Eingabekontrolle

Weitergabekontrolle

# 4. Verfügbarkeit und Belastbarkeit

# 5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Ausfüllhinweise zu den technischen und organisatorischen Maßnahmen

Die DSGVO geht im Artikel 32 davon aus, dass die Maßnahmen sehr detailliert und konkret beschrieben werden sollen. Es gilt abzuwägen, ob dies in der Genauigkeit im Vertrag mit dem Auftragsverarbeiter (Auftragnehmer) enthalten sein sollte. Wenn die Angaben im Vertrag für die Auftragsverarbeitung vereinfacht formuliert sind, ist es notwendig die Angaben im Verarbeitungsverzeichnis zu dokumentieren.

# 1. Vertraulichkeit

Zutrittskontrolle

☐ 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

Zugangskontrolle

☐ Passwortvergabe (Länge, Wechsel, Zeichen)

☐ 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

Zugriffskontrolle

☐ 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

Trennung

☐ 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

Pseudonymisierung & Verschlüsselung

# 2. Integrität

Eingabekontrolle

☐ 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

Weitergabekontrolle

☐ 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

# 3. Verfügbarkeit und Belastbarkeit

☐ 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

# 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

☐ Führung eines Verarbeitungsverzeichnisses

☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung

☐ Kontrolle der Vertragsausführung

☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐ Regelung zu Wartungen (speziell Fernwartung)