Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Anlage 2: Technisch-organisatorische Maßnahmen

nach Art. 25 Abs. 1 und Art. 32 Datenschutz-Grundverordnung (DSGVO) Stand: 01.06.2026

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Manuelles Schließsystem, Sicherheitsschlösser
- Zutrittskontrolle
- Verantwortliche Person für die Vergabe der Berechtigungen und Schlüsselvergabe, inkl. Vertretungsregelung
- Ständige Erreichbarkeit einer Schlüsselperson, auch an Wochenenden
- Zugang externer Dienstleister nur nach Freigabe

Zugangskontrolle
Keine unbefugte Systembenutzung:

- Identifizierung und Authentifizierung des Nutzers
- Kennwortverfahren (Sonderzeichen, Mindestlänge, 12 Stellen inkl. Groß- und Kleinbuchstaben, regelmäßiger Wechsel und Wiederverwendbarkeit erst nach mehreren Generationen)
- Regelungen bei Ausscheiden eines Mitarbeiters
- Automatische Sperrung des Bildschirms
- Verschlüsselung von Datenträgern

Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

- Differenzierte Berechtigungen (Profile, Rollen, Objekte)
- Anzahl der Administratoren auf das Notwendigste reduziert
- Verantwortliche Person für die Vergabe der Berechtigungen inkl. Vertretungsregelung
- Regelungen bei Ausscheiden eines Mitarbeiters
- Zugriff auf interne Systeme ausschließlich über gesicherte Netzwerksegmente und Firewall-geschützte Übergänge
- Einsatz von VPN-Technologie (IPSec-VPN über LANCOM-Netzwerkinfrastruktur)
- Ordnungsgemäße Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Anti-Viren-Software
- Einsatz von Software- & Hardware-Firewall

Trennbarkeit
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Logische Mandantentrennung/ Zweckbindung
- Erstellung einer Berechtigungsübersicht

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Verarbeitung personenbezogener Daten in einer Weise, dass sie ohne zusätzliche Informationen nicht einer spezifischen betroffenen Person zugeordnet werden können, sofern diese
- Informationen gesondert und geschützt aufbewahrt werden
- Soweit der jeweilige Verarbeitungsvorgang dies zulässt, werden personenbezogene Daten pseudonymisiert oder anderweitig datenschutzfreundlich verarbeitet

Datenschutz-Management

- Regelmäßige interne Tests mit Dokumentation der Ergebnisse
- Regelmäßige Datenschutzaudits
- Regelmäßige Schulungen der Mitarbeitenden zu Datenschutz und IT-Sicherheit
- Sensibilisierung der Mitarbeitenden für den Umgang mit personenbezogenen Daten

Incident-Response-Management
IT relevante Aspekte einer Prüfung von Datenschutz Compliance:

- Dokumentation der Meldeprozesse
- Notfallpläne
- Regelmäßige Kontrollen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Technische und organisatorische Maßnahmen gewährleisten, dass nur für den Verarbeitungszweck erforderliche personenbezogene Daten verarbeitet werden
- Vorgaben im Systementwicklungsprozess oder Systemanpassung
- Arbeitsanweisungen und Schulungen zur Nutzung der Systeme
- Differenziertes Berechtigungskonzept
- Definition der Speicherfristen

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Fernzugriff ausschließlich über gesicherte VPN-Verbindungen
- Verschlüsselung der Datenübertragung mittels TLS 1.2 oder höher
- Datenschutzgerechte Entsorgung von Datenträgern (intern/extern)

Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (Protokollierung im System)

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Backup- & Recoverykonzept über Business IaaS-Backup des Rechenzentrums
- Backup-Historie: 14 Tage
- Redundantes Backupsystem vorhanden
- Sicherungsintervall: bis zu vier Sicherungen täglich
- Spiegeln von Festplatten, RAID-System
- Testen der Datenwiederherstellung
- Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort (externer Server bei vertraglich gebundenem Unterauftragnehmer)
- Schutzsteckdosen in Serverräumen
- Notfallplan
- Firewall-System
- Virenschutzsoftware

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Gewährleisten, dass einzelne Systeme im Störfall wiederhergestellt werden können:

- Standardisierte und dokumentierte Backup- und Wiederherstellungsverfahren
- Einsatz kurzfristig zu beschaffender Standard-Hardware
- Einsatz virtueller Server
- Regelmäßiges Testen der Wiederherstellbarkeit der Daten
- Notfallpläne

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Auftragskontrolle

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:
- Eindeutige Vertragsgestaltung nach Art. 28 DS-GVO - Auftragsverarbeitung
- Auswahl des Unterauftragnehmers unter Sorgfaltsgesichtspunkten
- Vorabüberzeugungspflicht
- Formalisiertes Auftragsmanagement
- Verpflichtung der Mitarbeitenden auf Vertraulichkeit nach Art. 28 Abs. 3 lit. b DSGVO