TOM – Technische und organisatorische Sicherheitsmassnahmen

Die Vertragspartner sind verpflichtet, die technischen und organisatorischen Sicherheitsmassnahmen festzulegen.

Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind Massnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

Konkretisierung der Einzelmassnahmen

Im Einzelnen werden folgende Massnahmen bestimmt:

1. Vertraulichkeit

1.1. Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die Sicherung von Räumlichkeiten erfolgt durch Zutrittsregelung (nur einzelnen Personen wird Zutritt gewährt), persönliche RFID-Karten, elektrische Türöffner, einen 24/7 Werkschutz, Alarmanlagen und Videoanlagen an allen Ein- und Ausgängen.

1.2. Zugangskontrolle

Keine unbefugte Systembenutzung. Es kommen ausschliesslich sichere Kennwörter zum Einsatz.

1.3. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems. Dazu kommen Berechtigungskonzepte zum Einsatz. Zugriffsrechte werden nach dem Deny-Allow-Prinzip erteilt und auf das nötigste beschränkt. Der Zugriff erfolgt stets verschlüsselt.

1.4. Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

2. Integrität

2.1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport. Dazu wird nach aktuellen wissenschaftlichen Erkenntnissen auf Verschlüsselung der Daten sowie Datenübertragung durch Virtual Private Networks (VPN) gesetzt.

2.2. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu werden Änderungen und Eingaben von Daten protokolliert.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch eine Backup-Strategie, eine unterbrechungsfreie Stromversorgung (USV), redundanter Hardware, Netztrennungen und dem Einsatz von Virenschutz und Firewalls.

3.2. Rasche Wiederherstellbarkeit

Sicherstellen rascher Wiederherstellung mithilfe regelmässigen Recovery Tests.

4. Verfahren zur regelmässigen Überprüfung

4.1. Voreinstellungen

Datenschutzfreundliche Voreinstellungen

4.2. Auftragskontrolle

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers. Dazu liegt eine eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement vor und etwaige Dienstleister werden nach strengen Kriterien ausgewählt. Es finden angemessene Kontrollen und Nachkontrollen statt.