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. Zugriffskontrolle
Keine unbefugte Systembenutzung. Es kommen ausschliesslich sichere Kennwörter zum Einsatz.
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. Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

1.2. Zugangskontrolle
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.

1.3. Benutzerkontrolle
Unbefugte Personen können automatisierte Datenbearbeitungssysteme nicht mittels Datenübertragungseinrichtungen nutzen.

2. Verfügbarkeit und Integrität

2.1. Datenträgerkontrolle
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. Speicherkontrolle
Kein unbefugtes Speichern, Lesen, Ändern, Löschen oder Vernichten von Personendaten im Speicher. Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu werden Änderungen und Eingaben von Daten protokolliert.

2.3. Transportkontrolle
Kein unbefugtes Bekanntgeben von Personendaten oder Lesen, Kopieren, Verändern, Löschen oder Vernichten von Personendaten beim Transport von Datenträgern.

2.4. Wiederherstellung
Rasche Wiederherstellbarkeit von Personendaten und des Zugangs dazu bei einem physischen oder technischen Zwischenfall. 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.

2.5. Verfügbarkeit, Zuverlässigkeit und Datenitegrität
Sicherstellung der Verfübarkeit des automatiscierten Datenbearbeitungssystems, Meldung von Fehlfunktionen und Verhinderung der Schädigung gespeicherter Personendaten durch Fehlfunktionen des Systems.

2.6. Systemsicherheit
Stete Sicherstellung des neuesten Sicherheitsstandes von Betriebssystemen und Anwendungssoftware sowie Schliessung bekannter kritischer Lücken.

3. Nachvollziehbarkeit

3.1. Eingabekontrolle
Überprüfbarkeit der Eingabe oder Veränderung der Personendaten im automatisierten Datenbearbeitungssystem zum jeweiligen Zeitpunkt und durch die jeweilige Person.

3.2. Bekanntgabekontrolle
Überprüfbarkeit der Adressaten bei Bekanntgabegabe von Personendaten mit Hilfe von Einrichtungen zur Datenübertragung.

3.3. Erkennung und Beseitigung
Rasche Erkennung von Verletzungen der Datensicherheit und Ergreifung von Massnahmen zur Minderung oder Beseitigung der Folgen.

Zug, September 2023

Xelon AG
Poststrasse 15
CH-6300 Zug
info@xelon.ch
xelon.ch