Anlage 1

Allgemeine technische und organisatorische Maßnahmen

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

a) Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Umsetzung durch: Manuelles und elektronisches Schließsystem (Chipkarte, Schlüssel); Besuche durch Geschäftspartner nur in Ausnahmefällen und begleitet durch Fachpersonal; Sorgfältige Auswahl des Reinigungspersonals und der Reinigungsfirma; Serverraum wird durch eigenes Fachpersonal gereinigt; Einbruchmeldeanlage; Tür zum Serverraum mit Türknauf

b) Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Umsetzung durch: sichere Kennwörter (nach festgelegten Regeln, min. 12 Zeichen) für Nutzer-Accounts; automatische Sperrmechanismen; Zwei-Faktor-Authentifizierung; Verschlüsselung von Datenbanken, Datenträgern und mobilen Endgeräten, VPN- oder TLS-Verbindungen mit Angabe von Benutzername und Passwort; SSO; Netzwerksegmentierung

c) Zugriffskontrolle / Benutzerkontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Umsetzung durch: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte; Protokollierung von Zugriffen; Authentifizierungs- und Verschlüsselungsverfahren; sichere Kennwörter; automatische Sperrmechanismen; eingeschränkte Anzahl und Regelungen von Administratorenkonten

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Umsetzung durch: getrennte Zugriffsrechte; physische Datentrennung; Verwendung mandantenfähiger Systeme; Trennung von Produktiv- und Entwicklungs- / Testsystemen

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

a) Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Umsetzung durch: Verschlüsselung (min. AES 256 und SHA2 256); Virtual Private Networks (VPN); E-Mail-Verschlüsselung per SSL/TLS 1.2; Nutzung elektronische Signatur

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umsetzung durch: Protokollierung; Dokumentenmanagement; Dokumentation von Ein- und Ausgang (Ticketsystem)

3. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Umsetzung durch: Schreibschutz/Versionskontrolle; Backup-Strategie; Virenschutz (XDR-Variante mit aktivem Eingreifen); Firewall; Systemwartung/Belastungstests; Updates; Notfallpläne; Feuer-/Rauchmelder; Feuerlöscher; Überspannungsschutz; regelmäßige Wiederherstellungstests

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

Für Schweizer Aufträge umfasst die regelmäßige Überprüfung zusätzlich die fortlaufende Beurteilung von Schutzbedarf und Risiken nach DSG/DSV sowie die Wirksamkeit der Maßnahmen zur Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit.

a) Datenschutz-Management

Umsetzung durch: Sicherheitsricht- und -leitlinien sind definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert; Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (IT-Leiter und Datenschutzbeauftragter); konsequente Einbindung des DSB bei Sicherheitsfragen; ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema; Datenschutzschulungen finden für neue Beschäftigte zeitnah nach Aufnahme

des Beschäftigungsverhältnisses statt; Kontrolle durch externen Datenschutzbeauftragten

b) Incident-Response-Management

Umsetzung durch: Dokumentierte Ab-/ Aufarbeitung von Informationssicherheitsvorfällen; IT-Notfallplanung

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

Umsetzung durch: Umsetzung Passwortrichtlinie; automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen / Verhinderung der Auswahl schwacher Passwörter bei Anwendungen; Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT (z. B. bei Vergessen des Passworts) muss eine Passwortänderung durch den Nutzer erfolgen; Auto-Start von externen Medien deaktivieren; Anwendungen an Endgeräten möglichst ohne Administratorenrechte ausführen; Hardware-Verschlüsselung mobiler Endgeräte

d) Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers

Umsetzung durch: Eindeutige Vertragsgestaltung; Unterweisung der Mitarbeiter; formalisiertes Auftragsmanagement; strenge Auswahl des Dienstleisters; Nachkontrollen; Nachweis von Zertifikaten und Audits; Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht.