Technische und organisatorische Maßnahmen (Anlage 1 zur Auftragsverarbeitung)

1. Verantwortliche Stelle

Anqa IT-Security GmbH
Edmund-Rumpler-Straße 5
51149 Köln

www.anqa-itsecurity.de

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

2.1 Zutrittskontrolle:
Chipkarten-/Transponder-Schließsystem, Personenkontrolle beim Pförtner/Empfang, biometrische Zugangssperren, manuelles Schließsystem, Schlüsselregelung/Schlüsselbuch, Alarmanlage

2.2 Zugangskontrolle:
Authentifikation mit Benutzer + Passwort, Einsatz von Anti-Viren-Software, Einsatz von Firewalls, Einsatz von VPN-Technologie, Verschlüsselung von Datenträgern, Verschlüsselung von Smartphones, Passwortvergabe/Passwortregeln, Benutzerberechtigungen verwalten, Personenkontrolle beim Pförtner/Empfang

2.3 Zugriffskontrolle:
Einsatz von Aktenvernichtern, Erstellen eines Berechtigungskonzepts, physische Löschung von Datenträgern vor deren Wiederverwendung, Passwortrichtlinie inkl. Länge und Wechsel, Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten, Verschlüsselung von Datenträgern, sichere Aufbewahrung von Datenträgern, Verschlüsselung von Smartphones, Verwaltung der Benutzerrechte durch Systemadministratoren

2.4 Trennungskontrolle bei pseudonymisierten Daten:
Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System, Erstellen eines Berechtigungskonzepts, Festlegung von Datenbankrechten, logische Mandantentrennung (softwareseitig), physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern, Trennung von Produktiv- und Testsystem, Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):
Eine Pseudonymisierung findet standardmäßig nicht statt, kann jedoch auf Kundenwunsch umgesetzt werden.

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

3.1 Weitergabekontrolle:
Einrichtung von VPN-Tunneln, sorgfältige Auswahl von Transportpersonal & -fahrzeugen, sichere Transportbehälter/-verpackungen

3.2 Eingabekontrolle:
Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen), Protokollierung der Eingabe, Änderung und Löschung von Daten, Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

4.1 Verfügbarkeitskontrolle:
Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort, unterbrechungsfreie Stromversorgung (USV), Erstellen eines Backup- & Recoverykonzepts, Testen von Datenwiederherstellung, Alarmmeldung bei unberechtigten Zutritten in Serverräumen (SOC Frankfurt / ISO27001), Feuer- und Rauchmeldeanlagen, Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen (SOC Frankfurt / ISO27001)

4.1.1 Aufbewahrungsort:
Anqa IT-Security GmbH, Edmund-Rumpler-Straße 5, 51149 Köln, Deutschland:
- Vertriebliche Dokumente (Angebote, Auftragsbestätigungen, Rechnungen, Lieferscheine)
- Zugehörige Ansprechpartner des Kunden
- Kontaktdaten / Adressen / Koordinaten / Telefonnummern
- Netzwerktechnische Daten der Kunden:
    - IP Adressen / Subnetze
    - E-Mailadressen / Verteiler
    - Namen (z.B. für VPN-User)

4.1.2 Aufbewahrungsort:
Rechenzentrum Frankfurt („SOC“, ISO27001):
- Spiegelung der Konfiguration der Network Box Firewall des Kunden:
    - Adresse / Koordinaten
    - Netzwerktechnische Daten (siehe 4.1.1 Aufbewahrungsort)

4.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):
Testen von Datenwiederherstellung, regelmäßige Überprüfung (1x pro Woche), ob Daten auf Fileservern fehlerfrei abgerufen werden können

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

5.1 Datenschutz-Management:
Hiermit erklärt die Firma Anqa IT-Security GmbH (Edmund-Rumpler-Straße 5, 51149 Köln), dass alle Mitarbeiter auf das Datengeheimnis verpflichtet wurden. Insbesondere ist der Zugriff auf die Konfigurationsdateien und Schlüssel auf ausschließlich die Mitarbeiter des technischen Supports beschränkt. AQ hat einen externen Datenschutzbeauftragten bestellt.

5.2 Incident-Response-Management:
Es liegt eine Handlungsanweisung für Notfälle und für IT-Sicherheitsvorfälle vor.

5.3 Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DS-GVO):
Es wird bei der Verwendung von personenbezogenen Daten darauf geachtet, dass nur Daten erhoben werden, die für die Vertragsdurchführung notwendig sind.

5.4 Auftragskontrolle:
Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DSGVO.