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:
Manuelles Schließsystem / Codesperre, Sicherheitsschlösser, Schlüsselregelung/Schlüsselbuch, Alarmanlage, umzäuntes Gelände mit verschlossenem Tor, Bewegungsmelder, Sicherung der Verteilerräume, Besucher werden durch Beschäftigte in Empfang genommen, Besucher sind während des Besuchs in Begleitung, abgeschlossener Serverraum, Rechenzentrum in Frankfurt, Zutrittsdokumentation in Serverräume, Sicherung der
– Verteilerräume, Zugänge zum Serverraume sind begrenzt, Regelungen für Zutritt zu Serverräumen externer Personen.

2.2 Zugangskontrolle:
Authentifikation mit Benutzer und Passwort, Authentifikation mit biometrischen Daten (optional), Nutzung von Benutzerprofilen, Verwaltung von Benutzerberechtigungen, Regeln zur Passwortvergabe, Mindestanforderungen an Passwort-Komplexität (Mind. 12-16 Zeichen, Groß/Kleinbuchstaben), Regelung für den Umgang mit Passwörtern, Zwei-Faktor-Authentifizierung, Einsatz von Anti-Viren-Software, Einsatz von Firewalls, Einsatz von VPN-Technologie inkl. Zwei-Faktor-Authentifizierung, gesichertes WLAN, separates Gäste-WLAN, autorisierte Geräte bekommen logischen Zugang zum Netzwerk, regelmäßige Penetrationstests, Verschlüsselung von Datenträgern, Verschlüsselung von Smartphones, sorgfältige Auswahl von Reinigungspersonal.

2.3 Zugriffskontrolle:
Einsatz von Aktenvernichtern, Nutzung eines Berechtigungskonzepts, regelmäßige Prüfung des Berechtigungskonzepts, Verwaltung der Benutzerrechte durch Systemadministratoren, Anzahl der Administratoren auf das Mindeste begrenzt, sichere Entsorgung und Wiederverwendung von Speichermedien, sichere Aufbewahrung von Datenträgern, Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten), Sperren beim Verlassen des Platzes ist Pflicht, Clean Desk, Passwortrichtlinie, Verschlüsselung von Datenträgern, Verschlüsselung von Smartphones.

2.4 Trennungskontrolle:
– Nutzung eines Berechtigungskonzepts, Festlegung von Datenbankrechten, logische Mandantentrennung (softwareseitig), physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern, Trennung von Produktiv- und Testsystem, ausschließliche Nutzung fiktiver Daten für Testzwecke.

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:
Nutzung von VPN-Tunneln inkl. Zwei-Faktor-Authentifizierung, Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen, Maßnahmen bei Mitarbeiteraustritt, Prüfung der Rechtmäßigkeit der Weitergabe von Daten, Verpflichtung der Mitarbeiter auf das Datengeheimnis, sorgfältige Auswahl von Transportpersonal und Transportfahrzeugen, sichere Transportbehälter/ -verpackungen, revisionssichere Protokollierung.

3.2 Eingabekontrolle:
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen), Protokollierung der Eingabe, Änderung und Löschung von Daten, Eingabekontrolldaten sind zweckbestimmt, Protokollierung genutzter Dienste, Schutz gegen Manipulation, anlassbezogene Auswertung von Protokolldaten.

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

4.1 Verfügbarkeitskontrolle:
Backup- & Recovery-Konzept, feste Prozesse zur Datensicherung, Backup-Rechenzentrum (SOC Frankfurt / ISO 27001), Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort, Backup-Datenträger sind verschlüsselt, Kapazitätsplanung für die Datensicherung, zuständige Personen für Datensicherung, Testen von Datenwiederherstellung, Alarmmeldung bei unberechtigten Zutritten in Serverräumen (SOC Frankfurt / ISO 27001), Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen (SOC Frankfurt / ISO 27001), Unterbrechungsfreie Stromversorgung (USV), Serverräume nicht unter sanitären Anlagen, Feuerlöschgeräte in Serverräumen, Feuer- und Rauchmeldeanlagen, IT-Risiken sind über Versicherungen abgedeckt, Risiko- und Schwachstellenanalyse.

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):
Backup- & Recovery-Konzept, 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:
Beschäftigte geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, anderweitiges dokumentiertes Sicherheitskonzept, externer Datenschutzbeauftragter, Software-Lösungen für Datenschutz-Management im Einsatz, formalisierter Prozess zur Bearbeitung von Auskunftsanfragen betroffener Personen, jährliche Überprüfung der technischen Schutzmaßnahmen, Mitarbeiterzugriff auf zentrale Datenschutzdokumentation.

5.2 Incident-Response-Management:
Handlungsanweisung für IT-Sicherheitsvorfälle, Dokumentation von Sicherheitsvorfällen und Datenpannen, Einbindung des DSB in Sicherheitsvorfälle und Datenpannen, Einsatz einer Firewall mit regelmäßiger Aktualisierung, Einsatz von Spamfiltern mit regelmäßiger Aktualisierung, Einsatz von Virenscannern mit regelmäßiger Aktualisierung, Intrusion Detection System (IDS), Intrusion Prevention System (IPS).

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, einfache Ausübung des Widerrufrechts durch technische Maßnahmen.

5.4 Auftragskontrolle:
Ausreichende Ressourcen für Datenschutzmanagementsystem, Datenschutzbeauftragter, auszusondernde Hardware wird sicher zerstört, Hard- und Softwareprodukte aus seriösen Quellen, Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28.