Anlage 1 zum Auftrag gemäß Art. 28 DSGVO: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

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

- **Zutrittskontrolle:** Maßnahmen, Unbefugte den Zugriff zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:
  - Zugänge zu den Büroräumen grundsätzlich verschlossen
  - Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels
  - Videoüberwachung in den angemieteten Bereichen in den Rechenzentren

  Zugangskontrolle: Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
  - Firewall, Intrusion Detection System
  - Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Kennwort
  - Zusätzliches Login für spezielle Applikationen
  - Kennwörter mit mehr als 8 Zeichen, bestehende aus Sonderzeichen, Groß-und Kleinbuchstaben sowie Zahlen
  - Home Partition der Arbeitsplatzrechner verschlüsselt
  - Zugang zur Applikation im Rechenzentrum nur über verschlüsselte Verbindung

- **Zugriffskontrolle:** Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigte ausschließlich auf ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernet werden können:
  - Benutzerrollen-/Gruppenkonzept
  - Erteilung und Verwaltung von Benutzerrechten voneinander getrennt
  - Überprüfung/Aktualisierung der Berechtigungen
  - Virenschutzprogramm mit automatischer Aktualisierung
  - Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung
  - Papier-Shredder für Dokumentenvernichtung
  - Regelmäßige Installation von Sicherheitsupdates, um unberechtigte Zugriffe zu verhindern

- **Trennungskontrolle:** Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
  - Firmendaten (Buchhaltung, Personenverwaltung etc) physikalisch getrennt
  - Trennung von Entwicklungs- und Produktionsumgebung

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

- **Weitergabekontrolle:** Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
  - Verschlüsselte Übertragung
  - Identifizierung / Authentifizierung

- **Eingabekontrolle:** Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  - Protokollierung bei Eingabe, Änderung und Löschung von Daten
  - Regelungen zum Zugriff und zur Löschung der Protokolle

3. Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b, c EU-DSGVO)

- **Verfügbarkeitskontrolle:** Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:
  - Alle Server stehen in Rechenzentren in Deutschland
  - Rechenzentren sind DIN ISO/IEC 27001-zertifiziert
    Schutzmaßnahmen:
    - Geeignete Zutrittskontrollsysteme
    - Videoüberwachung
    - Redundante unterbrechungsfreie Stromversorgung
    - Überspannungsschutz
    - Schutz gegen Feuer und Wassereintritt
    - Monitoring der Leitungskapazitäten
    - Intrusion Detection System (Dos/DDoS-Angriffe)
  - Redundante IT-Infrastruktur (z.B. durch Virtualisierung)
  - RAID-Festplattenspeicher
  - Datensicherungskonzept vorhandenen / Prüfung der Rücksicherung/Wiederherstellung
  - Virenscanner und Firewalls im Einsatz

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

- **Auftragskontrolle:** Maßnahmen, die gewährleisten, dass personenbezogene Daten im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
  - Zwischen Auftragnehmer und evtl. Unterauftragnehmer wird bei Bedarf ein AV-Vertrag geschlossen.

- **Datenschutz-Management:** Es ist ein Datenschutzmanagementsystem implementiert, mit dessen Hilfe die Nachweispflichten der EU-DSGVO und des BDSG-neu umgesetzt werden:
  - Rechtsgrundlagen der Verarbeitung, Art.6 DSGVO
  - Erteilung der Einwilligung, Art.7 DSGVO
  - Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art.12 DSGVO
  - Einhaltung der Informationspflichten, Art.13 DSGVO
  - Datenschutz durch Technik, Art.25 DSGVO
  - Auskunftsrecht der betroffenen Person, Art.15 DSGVO
  - Recht auf Berichtigung, Art.16 DSGVO
  - Recht auf Löschung, Art.17 DSGVO
  - Umsetzung der Speicherbegrenzung, Art.5 DSGVO
  - Umsetzung der Sicherheit der Verarbeitung, Art.32 DSGVO
  - Auflistung aller Auftragsverarbeiter, Art.30 Abs.2 DSGVO
  - Umgang mit Datenschutzverletzungen, Art.33 DSGVO
  - Darstellung der Meldepflicht an Aufsichtsbehörden, Art.33 DSGVO
  - Verwendung von Werkzeug Zertifizierung, Art.42 DSGVO

- Risikobewertung / Datenschutzfolgenabschätzung, Art.35 DSGVO
- Dokumentation von Audits

- **Incident-Response-Management:**
  - Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen, eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO):**
  - Es sind technisch-organisatorische Maßnahmen getroffen, die sicherzustellen, dass die Im Kundenbereich verarbeiteten Daten lt. den Vorgaben von Art. 25 Abs. 2 EU-DSGVO verarbeitet werden.