Anlage 1

Allgemeine technische und organisatorische Maßnahmen nach DS-GVO

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

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch RFID-Transponder, Schlüssel, elektrische Türöffner, Alarmanlage, Videoanlage.
- **Zugangskontrolle**
  Keine unbefugte Systembenutzung durch (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.
- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.
- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch Trennung nach Bereichen (Entwicklung, Support, Verwaltung).
- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

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

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN) und elektronische Signatur.
- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Protokollierung.

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

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Netzwerküberwachung und Firewall
- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)**
  Gewährleistet durch Reserve-Systeme für kritische Systeme und tägliche Spiegelung der Produktivsysteme

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

- **Datenschutz-Management**
  Festlegung von Verantwortlichkeiten, Umsetzung und Kontrolle geeigneter Prozesse, Melde- und Freigabeprozess, Umsetzung von Schulungsmaßnahmen, Verpflichtung auf Vertraulichkeit, Regelungen zur internen Aufgabenverteilung, Beachtung von Funktionstrennung und -zuordnung, Einführung einer geeigneten Vertreterregelung
- **Datenschutz-Zertifizierung**
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**
  Zugriffsrechte auf personenbezogene Datenbereich sind bei neuen Benutzern defaultmäßig deaktiviert.
- **Auftragskontrolle**
  Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch eindeutige Vertragsgestaltung und formalisiertes Auftragsmanagement.