technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

- Organisation der Informationssicherheit
- Personalsicherheit
- Verwaltung der Werte
- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
- Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)
- Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    - Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
    - Zugangskontrolle: Keine unbefugte Systembenutzung
    - Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
    - Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
    - Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
    - Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    - Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
    - Belastbarkeitskontrolle: Fähigkeit der Systeme, mit risikobedingten Veränderungen umzugehen und Aufweisen einer Toleranz und Ausgleichsfähigkeit gegenüber Störungen
- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
    - Datenschutz-Management: System zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen
    - Incident-Response-Management: System zur Vorbereitung, Identifizierung und Meldung von Sicherheitsvorfällen
    - Datenschutzfreundliche Voreinstellungen:
    - Auftragskontrolle:
    - Datenschutzbeauftragter