Allgemeine technische und organisatorische Maßnahmen

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

- **Zutrittskontrolle**
  Es erfolgt kein unbefugter Zutritt zu Datenverarbeitungsanlagen
  - Schlüsselregelung, dokumentierte Vergabe, unterschiedliche Rechte
  - Videoüberwachung der Zugänge und des Firmengeländes;

- **Zugangskontrolle**
  Keine unbefugte Systembenutzung
  - sichere Kennwörter
  - Verschlüsselung von Datenträgern
  - Verschlüsselung von Laptops und Rechnern

- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
  Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
  Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt in der Firma zerstört.
  beim Hosting Service mit root und FTP Zugriff
  Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
  beim sonstigen Hosting
  Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
  beim Hosting Service mit root und FTP Zugriff
  Die Trennungskontrolle obliegt dem Auftraggeber.
  beim sonstigen Hosting
  Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.

- **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;
beim Hosting Service mit root und FTP Zugriff
Für die Pseudonymisierung ist der Auftraggeber verantwortlich.

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

- **Weitergabekontrolle**
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der - Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

- **Eingabekontrolle**
  bei internen Verwaltungssystemen des Auftragnehmers
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.
  beim sonstigen Hosting
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

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

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
  - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
  - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
  - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
  - Monitoring aller relevanten Server.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Dauerhaft aktiver DDoS-Schutz.
  beim Hosting Service mit root und FTP Zugriff
  - Datensicherung obliegt dem Auftraggeber.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Dauerhaft aktiver DDoS-Schutz.
  beim sonstigen Hosting
  - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten
  - Einsatz von Festplattenspiegelung.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Dauerhaft aktiver DDoS-Schutz

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
  Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- **Auftragskontrolle**
  Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers.
  - eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement
  - strenge Auswahl des Dienstleisters
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Computer Zentrum Strausberg GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt.