Anlage 2:
Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Im Folgenden werden die 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.

1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Da die Verarbeitung der Daten im Auftrag aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben kann von einer Pseudonymisierung abgesehen werden. Die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen bilden einen ausreichenden Schutz der vorhandenen Daten.

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

Vertraulichkeit der verwendeten Systeme und Dienste schützen. Sie sollen verhindern, dass es zu unbefugter oder unrechtmäßiger Verarbeitung kommt.

2.1 Zutrittskontrolle

Ziel ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Hiermit ist der räumliche Zugang zu dem Gebäude gemeint.

Maßnahmen:

- **Schlüssel**
  Es liegt eine Dokumentation der Vergabe der Schlüssel vor – jeder Mitarbeiter hat die Schlüsselübergabe unterzeichnet und wurde über die einhergehenden Rechte und Pflichten aufgeklärt – der letzte Mitarbeiter der das Gebäude verlässt verschließt die Tür
- **Zutrittskontrolle für Serverraum**
  Sicherheitstürgriff mit Zahlenschloss an der Eingangstür zum Serverraum vorhanden
- **Begleitung von Besuchern durch Mitarbeiter**
  Besucher werden durch die Mitarbeiter begleitet – alle Bereiche mit sensiblen Dokumenten/Daten sind durch Sicherheitstürgriffe mit Zahlenschloss gesichert – Computer sind bei Verlassen des Arbeitsplatzes zu sperren bzw. eine automatische Sperre des Bildschirmes ist bei jedem PC nach Ablauf eines Zeitlimits eingerichtet
- **Schutz von Außenfenstern durch automatische Rollos**
  Die Rollos sind programmiert und fahren am Abend automatisch nach unten sodass die Fenster über Nacht geschützt sind.

2.2 Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen unbefugter Personen in das EDV-System selbst.

Maßnahmen:

- **Sichere Kennwörter**
  Kennwörter sollten mindestens acht Zeichen beinhalten. Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern sind zu kombinieren. Passwort ohne persönlichen Bezug.
- **Automatische Sperrmechanismen**
  Computer sind bei Verlassen des Arbeitsplatzes zu sperren bzw. eine automatische Sperre des Bildschirmes ist bei jedem PC nach Ablauf von 15 Minuten eingerichtet
- **Einsatz sicherer Löschprogramme**
  Dies wird bei der Entsorgung von Altgeräten durch ein Fachunternehmen gewährleistet.

2.3. Zugriffskontrolle

Es muss gewährleistet werden, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Maßnahmen:

- **Dateizugriff auf Basis einer Leseberechtigung**
- **Benutzerkennung mit Passwort**
- **gesicherte Schnittstellen - Schutz durch Firewall und Virenschutz**
- **Protokollierung Dateizugriff**

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

Integrität umfasst, dass die von Ihnen erhobenen Daten nicht unbeabsichtigt oder beabsichtigt geändert oder zerstört werden können (Fälschungssicherheit).

3.1 Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- **Art der Übertragung von Daten**
- **Sicherung bei der elektronischen Übertragung**

    - Zum Teilen von Daten mit personenbezogenen via Cloud/KOMvista
    - Virtual Private Networks (VPN)
    - Firewall
    - Fax-Protokoll

3.2 Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden können.

Maßnahmen:

- **Trennung der Daten**
- **getrennte Ordnerstrukturen**
- **getrennte Datenbanken**

3.3 Eingabekontrolle

Es muss sichergestellt werden, dass nachträglich überprüft werden kann ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

Maßnahmen:

- **Protokollierung Dateizugriff**
- **Benutzeridentifikation**
- **Dateizugriff auf Basis einer Leseberechtigung**

3.4 Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden.

Maßnahmen:

- **Weisungsbefugnisse festlegen**
- **Vor-Ort Kontrollen/Stichprobenprüfung/Kontrollrechte**

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

Daten und die zur Verarbeitung notwendigen Systeme sollen stets dann verfügbar sein, wenn sie benötigt werden.

4.1 Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Maßnahmen:

- **Brandschutzmaßnahmen**
- **Überspannungsschutz**
- **RAID (Festplattenspiegelung)**
- **Backupkonzept**
- **Virenschutzkonzept**

- **Firewall**
- **Schutz vor Diebstahl**
- **Sichere Entsorgung**

4.2 Belastbarkeit

Datenverarbeitungssysteme und -dienste müssen auch belastbar sein. Die IT muss widerstandsfähig aufgestellt sein, um starke Beanspruchung überstehen zu können ohne gänzlich zusammenzubrechen. (Zum Beispiel können zu viele gleichzeitige Zugriffsanfragen auf den Webserver die Systeme belasten (Denial of Service) – Cyberangriff)

Maßnahmen:

- **Schutz gegen DDoS- Angriffe**
- **RAID-Systeme**

5 Wiederherstellung der Verfügbarkeit bei Zwischenfall (Art. 32 Abs. 1 lit. c DS-GVO)

Kommt es trotz der obigen TOMs DSGVO zu Systemstörungen oder einem IT-Ausfall, muss das Unternehmen in der Lage sein, die Daten schnellstmöglich wiederherzustellen und die Systeme alsbald wieder einsatzbereit zu haben.

Maßnahmen:

- **Backupkonzept**
- **IT-Notfallplan**
- **Überspannungsschutz (USV)**
- **Virenscanner**
- **Firewall**

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

Die Maßnahmen zu Datenschutz und Datensicherheit müssen regelmäßig dahingehend überprüft werden, ob sie ihren Zweck noch erfüllen und auf dem derzeitigen Stand der Technik sind. Einen bestimmten Turnus zur Überprüfung schreibt der Gesetzgeber nicht vor. Daher wird Kontrolle der technischen und organisatorischen Maßnahmen festgelegt vom Datenschutzbeauftragten festgelegt, die alle ein bis drei Jahre stattfindet. Mitarbeiter werden zum Umgang mit personenbezogenen Daten sensibilisiert.