Anlage 1 - technisch, organisatorische Maßnahmen

1. **Zutrittskontrolle**
   Schutz vor unbefugten Zutritt zu Datenverarbeitungsanlagen
   - Alarmanlage
   - Protokollierung der Besucher
   - Personenkontrolle beim Portier
   - Chipkarten für das Zugangssystem
   - Videoüberwachung
   - Tragepflicht von Berechtigungsausweisen

2. **Zugangskontrolle**
   Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme benutzen:
   - Zuordnung von Benutzerrechten
   - Passwortvergabe auf Basis einer Passwortpolicy
   - Authentifizierungen mittels Benutzernamen und Passwort
   - Gehäuseverriegelung an den Serverracks
   - Benutzerprofile
   - Einsatz von VPN Technologie
   - Sicherheitsschlösser
   - Personenkontrolle beim Portier
   - Tragepflicht von Berechtigtenausweisen
   - Teilweiser Einsatz von Smartphone-Administrationsservices (Android)
   - Einsatz von Antivirensoftware
   - Einsatz von Firewalls

3. **Zugriffskontrolle**
   Maßnahmen, die gewährleisten, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
   - Beschränkung der Anzahl von Systemadministratoren auf ein notwendiges Minimum
   - Passwortrichtlinie (Passwortlänge)

4. **Pseudonymisierung**
   Maßnahmen, die sicherstellen, dass, sofern möglich, primäre Identifikationsmerkmale aus personenbezogenen Daten entfernt werden und diese gesondert gespeichert werden:
   - Google Analytics IP Pseudonymisierung

5. **Klassifikationsschema für Daten**
   Einteilung in geheim, vertraulich, intern und öffentlich.

6. **Weitergabekontrolle**
   Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
   - Einrichtung von Standleitungen und VPN Tunneln
   - Die Durchführung von physischen Transporten von Hardware erfolgt mit persönlicher Begleitung durch qualifiziertes hauseigenes Personal
   - Der Transport erfolgt in sicheren Transportbehältern.
   - Datenweitergaben erfolgen nur an berechtigte Dritte (Behörden) im Rahmen der gesetzlichen Vorgaben.

7. **Eingabekontrolle**
Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
- Protokollierung mittels Access Logs
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

8. **Verfügbarkeitskontrolle**
Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
- Unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmierung bei unberechtigten Zutritten
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Backups inkl. Recoverykonzept
- Notfallpläne
- Serverräume sind nicht unter sanitären Anlagen
- Schutzsteckdosen in Serverräumen

9. **Trennungsgebot**
Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.
- Festlegung von Datenbankrechten
- Logische softwareseitige Mandantentrennung
- Trennung von Entwicklungs-, Test- und Produktivsystem

10. **Wiederherstellbarkeit**
Maßnahmen, die sicherstellen, dass personenbezogene Daten rasch wiederhergestellt werden können:
- Backups
- Recoverykonzept

11. **Löschungsfristen**
Maßnahmen, die sicherstellen, dass personenbezogene Daten und Metadaten entsprechend gelöscht werden können wenn ihre gesetzlichen Aufbewahrungsfristen erloschen sind.

12. **Auftragskontrolle**
Maßnahmen, die sicherstellen, dass keine Auftragsverarbeitung ohne entsprechende Weisung des AUFTRAGGEBERs erfolgt:
- Auftragsverarbeitungsvereinbarung mit Lieferanten inkl. Adressatenkreis von Weisungsgebern und Weisungsempfängern
- Schriftliche Weisungen