Anlage 1 - Technische und organisatorische Maßnahmen des Auftragnehmers Ortho Caps GmbH gemäß Art 32 DSGVO

1. Vertraulichkeit

1.1. Zutrittskontrolle zum Büro

- Dritten/ Unbefugten wird der Zutritt verwehrt
- Alarmanlage
- Abgeschlossener Serverraum
- Festlegung befugter Personen durch Chip
- Anwesenheitskontrolle
- Schlüsselregelung
- Anmeldung und Begleitung von Besuchern. Es ist klar definiert, zu welchen Räumen Besucher Zutritt haben (Empfang, Besprechungsräume, Sanitärräume). In diesen Räumen befinden sich weder Datenverarbeitungsanlagen noch Papierakten.

1.2. Zugangs- und Zugriffskontrolle

Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, können nicht von Unbefugten genutzt werden. Es wird gewährleistet, dass nur autorisierte Mitarbeiter Zugang zu den Daten haben. Maßnahmen:

- Passwortkonzept
- Bildschirmsperren nach Inaktivität
- Berechtigungskonzept
- Hardware-Firewall zur Filterung des Datenverkehrs
- Aktuelle Browser und Antivirensoftware
- Verschlüsseltes WLAN-Netz, Gästezugang ausschließlich mit Internetfunktion
- Remotezugänge sind verschlüsselt, die Anzahl wird so gering wie möglich gehalten.
- Bei Ausscheiden von Mitarbeitern werden sämtliche Zugangs- und Zugriffsmöglichkeiten gesperrt.

- Datenschutzkonforme Löschung von personenbezogenen Daten. Dies betrifft sowohl Datenträger als auch Papierunterlagen.

1.3. Trennungskontrolle

Personenbezogene Daten werden logisch voneinander getrennt, sodass eine vollständige Löschung dieser Daten jederzeit möglich ist.

1.4. Pseudonymisierung

Eine Pseudonymisierung findet vor Weitergabe der Daten statt.

1.5. Verschlüsselung

Die Weitergabe von personenbezogenen Daten auf elektronischem Wege erfolgt ausschließlich verschlüsselt.

2. Integrität

Eingabekontrolle

Die Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind, orientieren sich an den Möglichkeiten der jeweils eingesetzten Software. Des Weiteren unterstützen Protokollierungssysteme und ein Dokumentenmanagementsystem die nachträgliche Überprüfung.

3. Auftragskontrolle

Auftragnehmer werden sorgfältig ausgewählt und mindestens einmal jährlich geprüft. Mit allen Auftragnehmern sind schriftliche Verträge zur Auftragsdatenverarbeitung abgeschlossen.

4. Verfügbarkeit und Belastbarkeit

Es wird sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Maßnahmen:

- Klimatisierung des Serverraums
- Brandschutzmaßnahmen
- Überspannungsschutz

- Unterbrechungsfreie Stromversorgung
- Backup-Konzept
- Virenschutz
- Schutz vor Diebstahl
- Notfallkonzept

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die vorstehenden Maßnahmen werden mindestens einmal jährlich geprüft, bewertet, evaluiert und bei Bedarf angepasst. Die Mitarbeiterschulung findet mindestens einmal jährlich statt. Unterauftragnehmer werden mindestens einmal jährlich geprüft bzw. evaluiert.

Es gibt ein Incident-Response-Konzept. Es gibt einen Prozess zur fristgerechten Beantwortung von Anfragen Betroffener.

Das Verzeichnis der Verarbeitungstätigkeiten wird laufend gepflegt, zum Beispiel wenn neue Verarbeitungen hinzukommen.

Datenschutzfreundliche Voreinstellungen: es werden grundsätzlich nur Daten erhoben, die erforderlich sind.

Die Maßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird.