Anlage:
Technische und organisatorische Maßnahmen
(CaseWare Cloud und Audicon GmbH)

gem. Art. 32 Abs. 1 DS-GVO

Im Rahmen der AudiconFactory wird für den Datenaustausch und die Kommunikation zwischen Auftraggeber (Kunde der AudiconFactory) und Auftragnehmer (Audicon GmbH) die Collaboration-Plattform CaseWare Cloud genutzt. Die direkte Bearbeitung der Aufträge erfolgt allerdings auf den Servern der Audicon GmbH. Daher beziehen sich die folgenden technischen und organisatorischen Maßnahmen auf den Service

1. **von CaseWare Cloud**
2. **der Audicon GmbH**

1. Verschlüsselung

Eine Verschlüsselung erfolgt in Abhängigkeit

- der Daten
- des Auftrags
- der Umsetzungsmöglichkeit

Die Verschlüsselung erfolgt mit angemessener Verschlüsselungstechnik in Abhängigkeit zu den technischen, organisatorischen und finanziellen Mitteln.

CaseWare Cloud

☒ Eine Verschlüsselung der Datentransfers ist bei dem vorliegenden Vertrag vereinbart: HTTPS

Audicon GmbH

☒ Eine Verschlüsselung erfolgt nicht.

2. Gewährleistung der Vertraulichkeit

Zutrittskontrolle:

Der Zutritt zu den Räumlichkeiten der Audicon GmbH erfolgt über eine Identifikation via Transponder oder im Beisein eines autorisierten Mitarbeiters.

Zugangskontrolle:

CaseWare Cloud
Die Verantwortlichkeit für die Passworteinstellungen liegt beim Administrator der AudiconFactory Instanz von CaseWare Cloud (Audicon Mitarbeiter). Derzeit gibt es kein Fälligkeitsdatum für das vom Kunden selbst gewählte Passwort.

Audicon GmbH
Die Passwortregelungen und der Passwortwechsel entsprechen der jeweils gültigen Regelung zum angemessenen Umgang.

Zugriffskontrolle:

CaseWare Cloud
Derzeit sind drei Audicon Mitarbeiter (Staff) als Administratoren angelegt. Sie haben Zugriff auf die Daten in CaseWare Cloud. Das eingestellte Rollenkonzept stellt sicher, dass Kunden (Contacts) ausschließlich Zugriff auf selbst hochgeladene sowie für sie freigegebene Daten haben, nicht jedoch Daten anderer Kunden einsehen können.

Audicon GmbH
Das Rollenkonzept ist in Gruppencluster organisiert. Die Vergabe erfolgt nach dem Minimalprinzip des Datenschutzrechts.

Belehrung der Mitarbeiter
Die Mitarbeiter werden mindestens jährlich mit angemessenen Maßnahmen über das aktuelle Datenschutzrecht unterrichtet.

Trennungskontrolle:
Die genutzten Systeme sind, soweit nötig, mandantenfähig. Die Zuordnung zu Mandant und Zugriffsrecht erfolgt über die Accounteinrichtung.

3. Gewährleistung der Integrität

Eingabekontrolle:

CaseWare Cloud
CaseWare Cloud hat eine journalisierte Historienverwaltung.

Audicon GmbH
Alle Datenbanken haben eine journalisierte Historienverwaltung.

4. Gewährleistung der Verfügbarkeit
Verfügbarkeitskontrolle:

CaseWare Cloud
Daten, die in CaseWare Cloud hochgeladen werden, befinden sich auf Servern innerhalb der EU. Die Daten werden drei Wochen nach Abschluss des Projektes gelöscht.

Audicon GmbH
In den Standorten werden Datensicherungen sowohl als Vollsicherung, aber auch als inkrementelle Sicherung gefahren. Die Datensicherungen verbleiben in Deutschland.

5. Gewährleistung der Belastbarkeit der Systeme
Durch entsprechende Daten-Backup-Systeme, dem entsprechenden Sicherungskonzept und aktuelle Device-Nutzung ist das IT-System ausreichend belastbar.

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall
Zur Sicherung der Daten während der Arbeitsphase werden diese angemessen gesichert. Ein Löschen dieser Datensicherungen erfolgt nach 3 Wochen.

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen
Durch interne IKS-Prüfungen, Review der Sicherungen und Kontrollen des Datenschutzbeauftragten erfolgt eine Analyse der technischen und organisatorischen Maßnahmen. Der PLAN-DO-CHECK-ACT-Zyklus kommt hier zum Einsatz.

8. Datenschutzbeauftragter
Der extern benannte Datenschutzbeauftragte ist:

Herr Jürgen Recha
interev GmbH
Robert-Koch-Straße 26
30853 Langenhagen
05 11 / 89 79 84 10