

# Anlage 2

## Vereinbarung zur Auftragsverarbeitung (Art. 28 DS-GVO)

zwischen

**Audicon GmbH**, Toulouser Allee 19a, 40211 Düsseldorf,

- im Folgenden „Auftragsverarbeiter“ genannt -

u n d

---

- im Folgenden „Verantwortlicher“ genannt -

### **Präambel**

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Sinne des Art. 4 Ziff. 1 Datenschutzgrundverordnung („DS-GVO“) im Auftrag des Verantwortlichen. Zu diesem Zwecke schließen die Parteien die nachstehende Vereinbarung über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO:

## § 1 Vertragsgegenstand

- 1.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Inhalt des Vertrages ist die Regelung sämtlicher datenschutzrechtlicher Fragen zwischen dem Auftragsverarbeiter und dem Verantwortlichen.
  
- 1.2 Gegenstand der Datenverarbeitung sind folgende Vorgänge:  
  
Im Rahmen seiner Tätigkeit wird der Auftragsverarbeiter solche Daten des GoBD-Exports aus dem ERP-System von Mandanten des Verantwortlichen verarbeiten, die zur Erstellung einer Datenanalyse nach Vorgaben des Verantwortlichen auf Basis einer zwischen den Parteien geschlossenen Rahmenvereinbarung erforderlich sind.
  
- 1.3 Die Dauer des Auftrages ist auf die Dauer der Erbringung der Leistungen gemäß Einzelauftrag befristet.
  
- 1.4 Im Rahmen der vereinbarten Verarbeitung von personenbezogenen Daten nimmt der Auftragsverarbeiter folgende Aufgaben wahr: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten. Der genaue Umfang, Art und Zweck der Datenverarbeitung ist in den jeweiligen Einzelaufträgen näher beschrieben.
  
- 1.5 Die vertraglich vereinbarte Datenverarbeitung findet bei dem Auftragsverarbeiter ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen oder in Textform erfolgenden Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

## § 2

### **Art der verarbeiteten personenbezogenen Daten, Kategorien betroffener Personen**

- 2.1 Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-Kategorien:

Stamm- und Transaktionsdaten des ERP-Systems der von dem Verantwortlichen benannten Mandanten, die auch zur Datenträgerüberlassung (Z3-Zugriff) im Rahmen einer Außenprüfung (Betriebsprüfung) durch die Finanzbehörden angefordert werden.

Eine detaillierte Auflistung der Daten, die durch den Auftragsverarbeiter im Rahmen seiner Tätigkeit verarbeitet werden, ergibt sich aus dem Datenanforderungsblatt, das dem Verantwortlichen nach Bekanntgabe des beim Mandanten eingesetzten ERP-Systems zugesandt wird.

- 2.2 Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

Mandanten des Verantwortlichen

## § 3

### **Rechte und Pflichten des Verantwortlichen**

- 3.1 Der Verantwortliche ist ausschließlich verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverarbeitungsverhältnisses durchzuführenden Verarbeitung durch den Auftragsverarbeiter im Hinblick auf die Regelungen der DS-GVO und anderer etwaig neben der DS-GVO geltenden datenschutzrechtlichen Vorschriften. Ebenso ist der Verantwortliche für die Wahrung der Rechte der betroffenen Personen gemäß Art. 12 ff. DS-GVO verantwortlich.

- 3.2 Der Verantwortliche erteilt alle Aufträge, Teilaufträge und/oder Weisungen schriftlich oder in dokumentierter Textform. Mündliche Weisungen sind unverzüglich schriftlich oder in dokumentierter Textform zu bestätigen.
- 3.3 Der Verantwortliche ist berechtigt, Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen zu verlangen. Die Parteien werden diese sodann gemeinsam abstimmen und schriftlich oder in dokumentierter Textform festhalten. Sofern von dem Verantwortlichen gewünschte Verfahrensänderungen für den Auftragsverarbeiter technisch nicht oder nur mit wirtschaftlich hohem Aufwand umsetzbar sind, ist der Auftragsverarbeiter berechtigt, von dem Vertragsverhältnis zurückzutreten und eine weitere Verarbeitung abzulehnen.
- 3.4 Der Verantwortliche hat im Rahmen der Auftragsverarbeitung das Recht, Überprüfungen bei dem Auftragsverarbeiter durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er ist dabei berechtigt, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Soweit sich der Verantwortliche zur Durchführung von Kontrollen der Hilfe Dritter bedienen möchte, ist er hierzu nur berechtigt, soweit die eingesetzten, nicht zum Unternehmen des Verantwortlichen gehörenden natürlichen oder juristischen Personen einer gesetzlichen beruflichen Verschwiegenheitspflicht unterfallen. Soweit andere Dritte mit Kontrollen befasst werden sollen, steht dem Auftragsverarbeiter das Recht zu, Kontrollpersonen abzulehnen, soweit diese direkt oder indirekt Mitbewerber des Auftragsverarbeiters sind oder zum Auftragsverarbeiter in einem direkten oder indirekten Wettbewerbsverhältnis stehen. Dies gilt auch, soweit die mit Kontrollen beauftragten Dritten ihrerseits als verbundenen Unternehmen eines direkten oder indirekten Mitbewerbers des Auftragsverarbeiters gelten.
- 3.5 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

## § 4

### Pflichten des Auftragsverarbeiters

- 4.1 Der Auftragsverarbeiter verpflichtet sich, die gesetzlichen Pflichten gemäß Art. 28 - 33 DS-GVO einzuhalten.
- 4.2 Der Auftragsverarbeiter verarbeitet personenbezogene Daten, die ihm von dem Verantwortlichen übermittelt wurden, ausschließlich im Rahmen der vertraglich festgelegten Weisungen und der speziellen Einzelweisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere, insbesondere eigene Zwecke und bewahrt sie nicht länger auf, als es der Verantwortliche bestimmt.
- 4.3 Der Auftragsverarbeiter sichert dem Verantwortlichen zu, dass die für den Verantwortlichen verarbeiteten Daten von anderen Datenbeständen strikt getrennt werden.
- 4.4 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen Datenschutzvorschriften verstößt, hat er den Verantwortlichen unverzüglich schriftlich oder in dokumentierter Textform darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Weisungsberechtigten beim Verantwortlichen bestätigt oder geändert wird.
- 4.5 Die Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 2 lit. b, 29, 32 DS-GVO wird gewahrt. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Verpflichtung zur Vertraulichkeit

gilt auch nach Beendigung des Auftrags fort. Der Auftragsverarbeiter wird die Einhaltung der datenschutzrechtlichen Bestimmungen durch seine Mitarbeiter während der Durchführung der Arbeiten überwachen.

- 4.6 Der Auftragsverarbeiter verpflichtet sich zur Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen, die in der **Anlage** zu dieser Vereinbarung festgehalten sind, gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DS- GVO.

Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen gemäß der **Anlage** zu dieser Vereinbarung, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

- 4.7 Der Auftragsverarbeiter führt das Verzeichnis der Verarbeitungstätigkeit gemäß Art. 30 Abs. 2 DS-GVO und stellt dies auf Anfrage dem Verantwortlichen zur Verfügung. Der Verantwortliche stellt dem Auftragsverarbeiter die hierzu erforderlichen Informationen zur Verfügung. Der Auftragsverarbeiter wird den Verantwortlichen auf dessen ausdrücklichen Wunsch bei der Erstellung des Verzeichnisses nach Art. 30 Abs. 1 DS-GVO unterstützen. Der Verantwortliche erstattet dem Auftragsverarbeiter die durch diese Unterstützung entstandenen Kosten.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32-36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten. Der Verantwortliche erstattet dem Auftragsverarbeiter die durch diese Unterstützung entstandenen Kosten.

Ebenso unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12-22 DS-GVO. Eigene Auskünfte gegenüber betroffenen Personen wird der Auftragsverarbeiter nur auf ausdrückliche Weisung des Verantwortlichen erteilen.

4.8 Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Unterlagen und Daten betroffen sind. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4.9 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei dem Auftragsverarbeiter ermittelt.

Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, wird ihn der Auftragsverarbeiter nach besten Kräften unterstützen. Der Verantwortliche erstattet dem Auftragsverarbeiter die durch diese Unterstützung entstehenden Kosten.

4.10 Als Datenschutzbeauftragter ist bei dem Auftragsverarbeiter Herr Jürgen Recha, c/o interev GmbH, Robert-Koch-Straße 26, 30853 Langenhagen bestellt. Die Kontaktdaten des Datenschutzbeauftragten lauten: Tel. 0511/89798410 E-Mail: juergen.recha@interev.de. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

## **§ 5**

### **Weisungsrechte des Verantwortlichen**

5.1 Dem Verantwortlichen wird im Rahmen der Auftragsverarbeitung durch den Auftragsverarbeiter ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung eingeräumt, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und etwaig erforderliche Verfahrensänderungen sind von den Parteien einvernehmlich zu vereinbaren und in schriftlicher oder elektronischer Form zu dokumentieren.

- 5.2 Etwaig erfolgende mündliche Weisungen sind nur dann verbindlich, wenn der Verantwortliche diese unverzüglich schriftlich oder in einer dokumentierten elektronischen Form bestätigt.
- 5.3 Sofern der Auftragsverarbeiter zum Ersatz eines Schadens verpflichtet ist, der aufgrund einer Weisung des Verantwortlichen verursacht wurde oder sonst von diesem zu vertreten ist, stellt der Verantwortliche den Auftragsverarbeiter im Innenverhältnis frei.
- 5.4 Für den Fall, dass der Verantwortliche Einzelweisungen erteilen sollte, die über die gesetzlichen Anforderungen hinausgehen, werden die Parteien eine gesonderte Regelung zu den mit der Einzelweisung verbundenen Kosten beim Auftragsverarbeiter treffen. Die nach Maßgabe solcher Einzelweisungen entstehenden Kosten wird der Verantwortliche tragen.

## **§ 6**

### **Rückgabe und Löschung übergebener Daten**

- 6.1 Dem Auftragsverarbeiter ist es nicht gestattet, ohne ausdrückliche Zustimmung des Verantwortlichen Kopien oder Duplikate der Daten zu erstellen. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.
- 6.2 Nach Abschluss der von dem Auftragsverarbeiter zu erbringenden Dienstleistungen oder nach schriftlicher oder in dokumentierter Textform gehaltener Aufforderung durch den Verantwortlichen, spätestens jedoch mit Beendigung der Dienstleistungsvereinbarung zwischen den Parteien hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorherigen Vereinbarungen mit dem Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.



- 6.3 Die Parteien vereinbaren, dass die Löschung und Vernichtung von Daten so zu erfolgen hat, dass diese nicht wiederhergestellt werden können.

Sollte die Löschung von Daten nicht oder nur mit einem unverhältnismäßig hohen Aufwand möglich sein, tritt an die Stelle der Löschung der Information die Einschränkung der Verarbeitung entsprechend der Regelungen in Art. 18 DS-GVO.

- 6.4 Sofern gesetzliche oder behördliche Anordnungen bzw. Regelungen existieren, die einer Vernichtung oder Lösung der personenbezogenen Daten entgegenstehen, wird diese durch den Auftragsverarbeiter nicht erfolgen. Der Auftragsverarbeiter wird den Verantwortlichen insoweit schriftlich oder in dokumentierter Textform informieren.

- 6.5 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende jedoch dem Verantwortlichen übergeben.

## § 7

### **Unterbeauftragung**

- 7.1 Der Auftragsverarbeiter wird die Tätigkeiten nach Maßgabe dieser Vereinbarung grundsätzlich selbst, das heißt mit eigenen Mitarbeitern erbringen. Die Beauftragung Dritter mit der Datenverarbeitung ist nicht beabsichtigt.

- 7.2 Gleichwohl kommen die Parteien überein, dass der Auftragsverarbeiter nach vorheriger schriftlicher oder in dokumentierter Textform erteilter Zustimmung des Verantwortlichen berechtigt ist, die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter in (nachfolgend „Unterauftragnehmer“) erbringen lassen. Nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung gelten Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder Wartungen und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität

und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

Der Auftragsverarbeiter ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der von dem Verantwortlichen erlangten Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Beauftragung eines Unterauftragnehmers hat durch den Auftragsverarbeiter schriftlich zu erfolgen. Eine Beauftragung von Unterauftragnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

- 7.3 Der Auftragsverarbeiter verpflichtet sich, Unterauftragnehmer in gleicher Weise zu verpflichten, wie es in dieser Vereinbarung vorgesehen ist. Der Auftragsverarbeiter stellt vertraglich sicher, dass die dem Verantwortlichen eingeräumten Rechte, insbesondere die Kontrollrechte, durch diesen auch gegenüber einem Unterauftragnehmer wahrgenommen werden können. Dem Auftragsverarbeiter ist es nicht gestattet, im Zusammenhang mit der Begründung von Unterauftragsverhältnissen die in diesem Vertrag festgelegten Grundsätze zu unterschreiten. Die Vereinbarung darüber hinaus gehender Pflichten des Unterauftragnehmers ist jedoch zulässig. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Verlangen Auskunft über die aktuell eingesetzten Unterauftragnehmer und die Vereinbarungen zwischen dem Auftragsverarbeiter und dem jeweiligen Unterauftragnehmer zu erteilen.
- 7.4 Eine weitere Auslagerung von Rechten und Pflichten durch den Unterauftragnehmer ist nur bei ausdrücklicher schriftlicher oder in dokumentierter Textform erteilter Zustimmung des Verantwortlichen zulässig. Sofern die Zustimmung des Verantwortlichen vorliegt, wird der Unterauftragnehmer dafür Sorge tragen, dass sämtliche vertraglichen Regelungen in der Vertragskette auch dem weiteren Unterauftragnehmer auferlegt werden.
- 7.5 Bei Mängeln in der Datenverarbeitung des Unterauftragnehmers (z. B. Nichteinhaltung von Datenschutzbestimmungen) oder bei nicht ordnungsgemäßer Berücksichtigung

von Kontroll- und Überprüfungsrechten des Verantwortlichen durch den Unterauftragnehmer, hat der Verantwortliche das Recht vom Auftragsverarbeiter zu verlangen, dass die Verarbeitung oder Nutzung personenbezogener Daten des Verantwortlichen nicht mehr von dem Unterauftragnehmer durchgeführt wird.

## § 8

### Rechte betroffener Personen

- 8.1 Der Auftragsverarbeiter darf die Daten, die er im Auftrag verarbeitet, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken.
- 8.2 Soweit sich eine betroffene Person diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird dieser das Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Die Beantwortung des Ersuchens gegenüber der betroffenen Person erfolgt durch den Verantwortlichen. Der Auftragsverarbeiter ist berechtigt, die betroffene Person entsprechend zu unterrichten.

## § 9

### Technische und organisatorische Maßnahmen

- 9.1 Zwischen den Parteien besteht Einvernehmen, dass die in der *Anlage* festgelegten technischen und organisatorischen Maßnahmen für die Vertragsbeziehung der Parteien verbindlich festgelegt werden.

Der Auftragsverarbeiter hat damit die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere i. V. m. Art. 5 Abs. 1, Abs. 2 DSGVO hergestellt. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Art, der Umfang und die Zwecke der

Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 BS-GVO zu berücksichtigen.

- 9.2 Zwischen den Parteien besteht Einvernehmen, dass die technischen und organisatorischen Maßnahmen nach Maßgabe des jeweiligen technischen Fortschrittes und der Weiterentwicklung zu überprüfen sind. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen jedoch nicht unterschritten werden. Entsprechende Änderungen sind dem Verantwortlichen vorab anzuzeigen und in der Folge zu dokumentieren.
- 9.3 Soweit die bei dem Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich schriftlich oder in dokumentierter Textform. Entsprechendes gilt für Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen und/oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

## **§ 10**

### **Haftung**

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Vereinbarung zur Auftragsverarbeitung gelten die gesetzlichen Vorschriften, insbesondere Art. 82 Abs. 2 Satz 2 sowie Art. 82 Abs. 3 DS-GVO, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

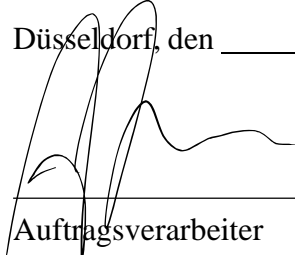
**§ 11**  
**Schlussbestimmungen**

- 11.1 Änderungen und Ergänzungen dieser Vereinbarung und ihrer Bestandteile bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für einen Verzicht auf das Schriftformerfordernis selbst.
- 11.2 Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Düsseldorf.
- 11.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien werden im Falle einer unwirksamen und/oder undurchführbaren Bestimmung unverzüglich sämtliche Anstrengungen unternehmen, um eine Anpassung der unwirksam oder undurchführbaren Bestimmung zu erreichen. Gleiches gilt für den Fall einer Regelungslücke.

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_  
Verantwortlichen

Düsseldorf, den \_\_\_\_\_

  
\_\_\_\_\_  
Auftragsverarbeiter  
Axel Zimmermann

**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:**

Allgemein: Der Zutritt zu den Räumlichkeiten der Audicon GmbH erfolgt über eine Identifikation via Key-Card oder im Beisein eines autorisierten Mitarbeiters.

Besucherregelung: Vorhanden – Besucher werden erfasst und tragen einen Ausweis.

Dokumentierte Schlüsselvergabe: Vorhanden – Key-Card nur nach Ausgabe durch die Administration, Erfassung von Key-Card-Nummer, Name und Datum.

Sicherheitsschlösser: Vorhanden

Konzept zur Gebäudesicherheit: Am Gebäudeeingang gibt es ein elektronisches Zugangserfassungssystem. Die Tür öffnet sich für MitarbeiterInnen über individuelle Key-Cards. Die Tür öffnet sich für Besucher, wenn der Empfangsmitarbeiter nach Sichtung des Besuchers über die am Gebäude befindliche Kamera einen Knopf betätigt. Zu den Räumlichkeiten der Audicon GmbH gibt es einen Büroeinheitszugang.

### **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

Es besteht ein Berechtigungskonzept zum Serverraum.

Die MitarbeiterInnen der Audicon GmbH müssen Ihre Passwörter im Abstand von 90 Tagen wechseln. Dabei sind die letzten 10 gewählten Passwörter nicht zulässig. Bei der Wahl der Passwörter gibt es eine Komplexitätsanforderung (min. 8 Zeichen – Zahlen, Buchstaben, Groß-/Kleinschreibung). Firewall und Virenschutz werden eingesetzt.

### **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.

Die Überwachung und Protokollierung von Systemzugriffen erfolgt über ein Standard-Protokoll des Windows-Servers, Firewall-Protokolle sowie AV-Protokolle.

**Weitergabekontrolle:**

Die verschlüsselte Datenübertragung erfolgt über SSL-VPN-Systeme.

Die Verpflichtung der MitarbeiterInnen der Audicon GmbH auf Vertraulichkeit ist vertraglich geregelt.

**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.

Eine unterbrechungsfreie Stromversorgung (USV) für Serversysteme ist gewährleistet, klimatisierte Serverräume sind gegeben. Feuer- bzw. Rauchmeldeanlagen innerhalb der Räumlichkeiten der Audicon GmbH sind mit einer zentralen Brandmeldeanlage verknüpft. Ein Backup- und Recoverykonzept ist vorhanden (unabhängige Backup-Standorte, replizierend). Auch ein Notfallplan ist vorhanden.



### **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