

Vertrag über die Auftragsverarbeitung personenbezogener Daten

Zwischen **Ihnen** (einschließlich aller verbundenen Unternehmen i.S.d. §§ 15 ff. AktG)

- nachfolgend bezeichnet als „**Auftraggeber**“ -

und

*Brune Medizintechnik
Otto-Schott-Str. 21
73431 Aalen*

vertreten durch

Herrn Jürgen Brune

- nachfolgend bezeichnet als „**Auftragnehmer**“ -

1 Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten, im Rahmen der Fernwartung, Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.
- (3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer selbst erfolgt nicht generell bei Zustandekommen der Verbindung. Sie bezieht sich auf die mögliche Einsichtnahme in z.B. Kunden- oder Patientendaten bei gegebenenfalls geöffneten Anwendungen während der Durchführung der Fernwartung. Der Umfang der Verarbeitung selbst ist in dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“) geregelt.

2.2 Dauer

Dieser Vertrag ist in seiner Laufzeit unbegrenzt und kommt bei allen zukünftigen Rechtsgeschäften der Parteien zur Anwendung. Die Verarbeitung beginnt im Einzelfall mit der Zustimmung zu den Nutzungsbedingungen des Unterauftragnehmers TeamViewer durch einen Mitarbeiter des Auftraggebers und endet mit der Beendigung der Fernzugriffs-Verbindung.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung durch den Auftragnehmer ist folgender Art: Kenntnisnahme von Daten

Die Verarbeitung durch den Auftragnehmer dient folgendem Zweck: Der Erfüllung des Hauptvertrages in Hinblick auf eine reibungslose Auftragsabwicklung aus Kundensicht.

Neben dem Auftragnehmer wird auch der Unterauftragnehmer TeamViewer personenbezogene Daten des Auftraggebers verarbeiten, um die Nutzung der bereitgestellten Software und Services nach dokumentierten Weisungen (im Rahmen der Produktfunktionalität) des Auftraggebers und/oder seiner Benutzer zu ermöglichen.

Dies umfasst im Wesentlichen die Verarbeitung der übertragenen Inhalte sowie das Management der Inhalte des Benutzerkontos.

Bei der Nutzung wird TeamViewer die folgenden Verarbeitungen im Auftrag durchführen:

- Verarbeitung der Daten im Benutzerkonto, insbesondere Speicherung und Zugänglichmachung der Daten für andere Benutzer im Rahmen einer Verbindung, z.B. Name, Kontakte, E-Mail-Adresse, Profilbild sowie Inhaltsdaten der Verbindungen, z.B. Chat.
- Übermittlung der vom jeweiligen Benutzer übertragenen Inhaltsdaten an andere Benutzer innerhalb einer Remote-Verbindung oder Sitzung (Bildschirm, übermittelten Daten und Dateien sowie alle anderen sonstigen ausgetauschten Informationen).
- Übermittlung der verschlüsselter Kundenkontodaten
- Die Verarbeitung außerhalb des Geltungsbereichs dieses AVVs wird in der jeweiligen Datenschutzzinformation beschrieben.

3.2 Art der Daten

Im Zusammenhang mit TeamViewer Core werden die folgenden Arten von personenbezogenen Daten von TeamViewer als Unterauftragsverarbeiter verarbeitet:

- Inhaltsdaten, die während einer Verbindung zwischen TeamViewer-Clients ausgetauscht werden, z.B. Video- und Audiostream (Bildschirmansichten und Benutzerkamera), Dateitransfers, Text-Chat, Fernsteuerungsbefehle, Ticketinhalte, Whiteboard, sowie personenbezogene Daten, die für die Herstellung der Verbindung erforderlich sind.
- Benutzerkontoinformationen, z.B. TeamViewer ID, Benutzername, Anzeigename, E-Mail-Adresse, IP-Adresse, Profilbild (optional), Spracheinstellung, Meeting-ID, Standort, Passwort. Die Domäne des Auftraggebers sowie das Alter des Kontos (z.B. "älter als 6 Monate") werden dem Sitzungshost vor der Verbindung als Teil der Sicherheitsfunktion "Showing Supporter Data During Connection" angezeigt.
- Personenbezogene Daten in Verbindung mit der Benutzerkontoverwaltung und -administration, z.B. Speichern und Freigeben von Benutzerprofilen, Kontodetails, Freundesliste, Kontaktinformationen, Chat-Verlauf, Dateianhänge.
- Personenbezogene Daten im Zusammenhang mit der Verwaltung und dem Management des Firmenprofils, z.B. Firmenprofil, Firmenrichtlinien, Zuordnungen zu Benutzerkonten, Verwaltung des Benutzerzugangs, Verbindungsberichte.
- Push-Benachrichtigungen, wie von den Benutzern initiiert.
- Personenbezogene Daten im Zusammenhang mit der Planung von Besprechungen sowie der Outlook-Integration (z.B. Uhrzeit und Datum von Besprechungen, Teilnehmer usw.).

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Der Auftraggeber (soweit personenbezogene Daten des Kunden gemäß Ziffer 3.2 verarbeitet werden) und ggf. die die Benutzer des Auftraggebers
- Die Verbindungspartner beim Auftragnehmer
- Dritte, deren personenbezogene Daten vom Auftraggeber in einer Verbindung unter Umständen offenbart werden können (z.B. Patientendaten in während der Fernwartung geöffneten Anwendungen)

4 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen.
- (7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (9) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt:
Marcel Hoffmann
brune-medizintechnik@aantispy.de
Tel. 07361 5986-30

5 Technische und organisatorische Maßnahmen

- (1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (3) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (4) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften oder vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen.
- (5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen,

- der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
 - (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
 - (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (3) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10 Beendigung des Auftrags

- (1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.
- (2) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

11 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

12 Haftung

- (1) Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

- (2) Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.
- (3) Nummer (2) gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

14 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Für Nebenabreden ist die Schriftform erforderlich.
- (3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 – technische und organisatorische Maßnahmen

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. Maßnahmen zur Sicherung des Zutritts zu Grundstück oder Gebäudes sind vorhanden. Ja Nein
2. Mitarbeiter sind auf das Datengeheimnis verpflichtet oder in ähnlicher Weise zum Stillschweigen verpflichtet. Ja Nein
3. Mitarbeiter müssen sich bei der Benutzung von IT-Systemen mit Benutzername und Passwort anmelden oder durch ein mindestens gleichwertiges System authentifizieren. Ja Nein
4. Schutz vor Schadsoftware ist mindestens gewährleistet durch Viren-Scanner und Firewall. Ja Nein
5. Es erfolgen regelmäßige Backups. Ja Nein