Vertrag

über die Verarbeitung personenbezogener Daten

- nachfolgend „AV-Vertrag“ genannt -

zwischen

dem Kunden

- nachfolgend „**Auftraggeber**“ oder „Verantwortlicher“-

und

Klein & Rose GmbH
Hanauer Landstraße 186
60314 Frankfurt am Main

- nachfolgend „**Auftragnehmer**“ oder „Auftragsverarbeiter“ -

einzeln oder gemeinsam auch „**Partei**“ und/oder „**Parteien**“

1 BEGRIFFSBESTIMMUNGEN

Im Sinne dieses AV-Vertrages bezeichnet der Ausdruck

(1) „**Auftragsverarbeiter“**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet; „Auftragsverarbeiter“ ist die im Vorstehenden als „Auftragsverarbeiter“ bezeichnete Vertragspartei.

(2) „**Dritter**“: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

(3) „**Hauptvertrag**“: Der Vertrag über die Erbringung der vom Verantwortlichen beauftragten und vom Auftragsverarbeiter erbrachten Agenturleistungen, inklusive der diesem Vertrag zu Grunde liegenden AGB des Auftragsverarbeiters.

(4) „**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; „Verantwortlicher“ ist die im Vorstehenden als „Verantwortlicher“ bezeichnete Vertragspartei, die hier allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, die diesem AV-Vertrag zu Grunde liegen.

(5) „**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(6) „**personenbezogene Daten**“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(7) „**weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter**“ den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

(8) „**Sub-Unterauftragsverarbeiter**“ den Vertragspartner des weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich dieses AV-Vertrags beauftragt wird.

2 GEGENSTAND DES VERTRAGS, RECHTSGRUNDLAGE

(1) **[Gegenstand des Vertrags]** Gegenstand des Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung im Zusammenhang mit der Erbringung von Agenturleistungen gemäß dem Hauptvertrag.

(2) **[Konkretisierung der Verarbeitung]** Aus dem Hauptvertrag in Verbindung mit **Annex 1** dieses AV-Vertrages ergeben sich Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen. Der Verantwortliche gewährt dem Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen wie in **Annex 1** dieses AV-Vertrages beschrieben.

3 RECHTE UND PFLICHTEN DES VERANTWORTLICHEN

(1) **[Zulässigkeit der Datenverarbeitung]** Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Verantwortliche verantwortlich. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

(2) **[Weisungen]** Der Auftragsverarbeiter wird personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. 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.

(3) **[Ausgleich Mehrleistung]** Soweit im Hauptvertrag Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarung zu Leistungsänderungen im Hauptvertrag getroffen wurde, werden Weisungen und Maßnahmen, die eine Abweichung zu den in diesem AV-Vertrag oder im Hauptvertrag festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind –soweit nicht ausdrücklich anders vereinbart- bei Mehraufwand für den Auftragsverarbeiter gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert ver-

ständigen. Soweit nicht ausdrücklich anders vereinbart, kann der Auftragsverarbeiter für Unterstützungsleistungen nach Ziffer 3 (4), (5) und Ziffer 4 (3), (4) dieses AV-Vertrages eine gesonderte Vergütung verlangen.

(5) **[Überprüfungen, Inspektionen]** Der Verantwortliche kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesem AV-Vertrag niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage von Nachweisen beim Auftragsverarbeiter in Form von marktüblichen Zertifizierungen und / oder Eigenerklärungen des Auftragsverarbeiters kontrollieren.

(6) **[Unterstützung durch den Verantwortlichen]** Der Verantwortliche wird im Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Verantwortliche wird im Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei der Prüfung möglicher Verstöße und bei Abwehr von Ansprüchen betroffener Personen oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

4 RECHTE UND PFLICHTEN DES AUFTRAGSVERARBEITERS

(1) **[Datenverarbeitung]** Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten im Rahmen des getroffenen Vertrags und nach Weisung des Verantwortlichen entsprechend der Regelung des Ziffer 3 Abs. 2. Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(2) **[Leistungsort]** Der Auftragsverarbeiter wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder in einem sogenannten Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter. Die zum Zeitpunkt der Auftragserteilung vereinbarten Leistungsstandorte sind in **Annex 1 und 3** dieses AV-Vertrages dargestellt. Soweit der Auftragsverarbeiter personenbezogene Daten in ein sogenanntes Drittland übermittelt, wird er die Anforderungen der Art. 44 ff. DS-GVO beachten.

(3) **[Meldung von Zwischenfällen]** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

(4) **[Ausübung von Betroffenenrechten]** Abhängig von der Art der Verarbeitung wird der Auftragsverarbeiter den Verantwortlichen bei dessen Pflicht zur Beantwortung von Anträgen auf

Wahrnehmung der Betroffenenrechte nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Bei Bedarf werden sich die Vertragsparteien über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen. Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, leitet der Auftragsverarbeiter die Anfragen der betroffenen Person zeitnah an den Verantwortlichen weiter.

5 TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN

Der Verantwortliche und der Auftragsverarbeiter werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten. Die derzeit als geeignet angesehenen Maßnahmen des Auftragsverarbeiters sind in Annex 2 dieses AV-Vertrages beschrieben und werden als geeignete Maßnahmen vereinbart.

6 VERTRAULICHKEIT

Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren.

7 UNTERAUFTRAGSVERARBEITER

(1) **[Befugnis]** Der Auftragsverarbeiter darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unter-Auftragsverarbeiter) einsetzen.

(2) **[Gesonderte Genehmigung]** Für die in **Annex 3** dieses AV-Vertrages aufgeführten Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter gilt die Genehmigung des Verantwortlichen als erteilt.

(3) **[Allgemeine schriftliche Genehmigung]** Der Verantwortliche erteilt hiermit dem Auftragsverarbeiter die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter).

(4) **[Information bei Änderungen]** Der Auftragsverarbeiter informiert den Verantwortlichen schriftlich oder per E-Mail, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter mindestens 4 Wochen vor der beabsichtigten Änderung. Hierdurch erhält der Verantwortliche die Möglichkeit, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim Verantwortlichen Einspruch zu erheben. Der Verantwortliche wird die Genehmigung zur Einbindung weiterer Unterauftragsverarbeiter nicht ohne wichtigen Grund verweigern.

(5) **[Kündigungsrecht des Auftragsverarbeiter]** Dem Auftragsverarbeiter steht ein außerordentliches Kündigungsrecht des Hauptvertrages nach Maßgabe des Hauptvertrages – oder für den Fall, dass ein solches Kündigungsrecht im Hauptvertrag nicht eingeräumt wurde, ein außerordentliches Kündigungsrecht von 4 Wochen zum Monatsende - zu, wenn nach Auffassung des

Auftragsverarbeiters der Verantwortliche die Einbindung des Unterauftragsverarbeiters ohne wichtigen Grund verweigert oder dem Auftragsverarbeiter eine Leistungserbringung ohne den abgelehnten Unterauftragsverarbeiter nicht möglich ist.

(6) **[Auswahl von Unterauftragsverarbeitern]** Der Auftragsverarbeiter wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt. Der Auftragsverarbeiter wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen diesem Vertrag im Wesentlichen entsprechen.

8 VERTRAGSDAUER, KÜNDIGUNG

Diese Vereinbarung gilt für die Dauer des Hauptvertrages.

9 KONTAKTAUFNAHME MIT AUFTRAGSVERARBEITER

Anliegen betreffend diesen AV-Vertrag sind auf Seiten des Auftragsverarbeiters an

Klein & Rose GmbH
Hanauer Landstraße 186
60314 Frankfurt am Main
info@klein-rose.com

zu richten.

10 HAFTUNG

Die Haftung für Schäden, die durch eine nicht der DSGVO und geltenden Datenschutzbestimmungen entsprechende Verarbeitung verursacht, richtet sich nach den gesetzlichen Vorschriften.

11 SONSTIGES

(1) **[Gültigkeit des Vertrags]** Von der Ungültigkeit einer Bestimmung dieses AV-Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt.

(2) **[Änderungen des Vertrags]** Änderungen dieses AV-Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich in elektronischer Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst. Auftragsverarbeiter behält sich das Recht vor, diesen AV-Vertrag jederzeit zu ändern, wenn ein hinreichender Grund hierfür gegeben ist. Sachliche Gründe sind insbesondere im Falle der Veränderung der Gesetzeslage, der höchstrichterlichen Rechtsprechung oder der Marktgegebenheiten zu sehen. Auftragsverarbeiter wird den Verantwortlichen über die Änderung unter Angabe der Gründe mindestens 4 Wochen vor ihrem geplanten Wirksamwerden in Textform informieren. Der Verantwortliche kann den neuen Bedingungen bis spätestens 2 (zwei) Wochen vor dem geplanten Wirksamwerden widersprechen. Widerspricht er nicht, gilt seine Zustimmung als erteilt. Auftragsverarbeiter besitzt im Falle des Widerspruches des Verantwortlichen ein Wahlrecht, ob der Vertrag unter Fortgeltung der alten Bedingungen fortgesetzt oder

mit Datum des Wirksamwerdens der neuen Regelungen gekündigt wird. Ziff. 7 (Änderungen beim Einsatz von Unter-Auftragsverarbeitern) bleibt unberührt.

(3) **[Gerichtsstand]** Der alleinige Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem AV-Vertrag ist Frankfurt. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

(4) **[Geltendes Recht]** Bezüglich geltendem Recht und Gerichtsstand gelten die Regelungen aus dem Hauptvertrag.

(5) **[Vorrangregelung]** Bei Widersprüchen zwischen den Bestimmungen dieses Vertrags und Bestimmungen sonstiger Vereinbarungen, insbesondere des Hauptvertrags, sind die Bestimmungen dieses AV-Vertrags maßgebend. Im Übrigen bleiben die Bestimmungen des Hauptvertrags unberührt und gelten für diesen AV-Vertrag entsprechend.

Annexe:

Nachstehende Annexe sind feste Bestandteile dieser Vereinbarung:

Annex 1: Einzelheiten der Datenverarbeitung

Annex 2: Technische und organisatorische Sicherheitsmaßnahmen

Annex 3: Genehmigte Unterauftragsverarbeiter

Annex 1

Einzelheiten der Datenverarbeitung

1. Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung richtet sich nach den im Hauptvertrag beauftragten Agenturleistungen:

	Agenturleistung	Beschreibung und Gegenstand der Verarbeitung
1	Video- und Fotoproduktion	Erstellung von Foto- und Videomaterial (z.B. Imagefilme, Fotoserien von Firmenfeiern)
2	Social Media Marketing	Ausspielen von Inhalten auf Social Media (z.B. Werbung, Reels, etc.)
3	Printdesign	Erstellung von Druckmedien
4	Webhosting	Einrichtung, Betrieb und Pflege von Webseiten, sowohl technisch wie inhaltich
5	Lead-Generierung / Patienten-Anfragen	Aufbau und Betrieb einer Landingpage mit Anfrage- bzw. Kontaktformular zur Gewinnung von Patienten-Anfragen fuer den Verantwortlichen. Erfassung und Speicherung der Formular-Eingaben in einer Datenbank zum Abruf durch den Verantwortlichen sowie Sofort-Benachrichtigung des Verantwortlichen ueber neue Anfragen.

2. Arten und Kategorien von personenbezogenen Daten

Die Art und die Kategorien der betroffenen personenbezogenen Daten richten sich nach den im Hauptvertrag konkret beauftragten Agenturleistungen im jeweiligen Einzelfall:

	Agenturleistung	Personenbezogene Daten
1	Video- und Fotoproduktion	- personenbezogene Daten der abgebildeten und / oder aufgezeichneten Personen, wie z.B.: Aussehen, Stimme, Name, etc.
2	Social Media Marketing	- personenbezogene Daten der Besucher der Social Media Profile der Kunden, wie z.B.: Profilname, Kommunikationsdaten, Nutzerverhalten
3	Printdesign	- personenbezogene Daten der abgebildeten Personen, wie z.B.: Aussehen, Name
4	Webhosting	- personenbezogene Daten der Webseiten-Besucher: Protokolldaten, Logfiles, IP-Adresse

		- im Falle des Einsatzes von Cookies: die mit Hilfe der Cookies verarbeiteten und generierten personenbezogenen Daten, wie z.B.: IP-Adresse, Nutzerverhalten, Statistiken - im Falle des Einsatzes von Kommunikationstools wie Kontaktanfragemasken: Kommunikationsdaten, Kontaktdaten der Webseiten-Besucher - Sämtliche Inhaltsdaten, die über die gehostete Website des Kunden verarbeitet und hochgeladen werden, wie z.B. im Falle einer Bewerberplattform: personenbezogene Daten von Bewerbern des Kunden wie z.B. Name, Adresse, Lebenslauf, Foto, Zeugnisse, Gehaltswunsch, Telefonnummer, Profildaten aus Social-Media-Netzwerk
5	Lead-Generierung / Patienten-Anfragen	- - Kontakt- und Kommunikationsdaten der Interessenten (z. B. Name, Telefonnummer, E-Mail-Adresse, Nachricht/Anliegen) - - Besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO (Gesundheitsdaten): Angaben der Interessenten zu ihrer zahnmedizinischen Situation bzw. ihrem Behandlungswunsch (z. B. fehlende/lockere Zaehne, vorhandene Prothese, Interesse an festsitzendem Zahnersatz) - - technische Daten der Webseiten-Besucher (IP-Adresse, Protokolldaten)

3. Leistungen, Verarbeitungszweck:

Siehe Annex 1, Ziff. 1 und 2 des AV-Vertrages sowie im Übrigen den Hauptvertrag

4. Verarbeitungsort:

Siehe Annex 2 und 3 des AV-Vertrages

5. Besondere Kategorien personenbezogener Daten: Soweit im Rahmen der Lead-Generierung besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO (insbesondere Gesundheitsdaten) verarbeitet werden, stellt der Verantwortliche die hierfuer erforderliche ausdrueckliche Einwilligung der betroffenen Personen (Art. 9 Abs. 2 lit. a DS-GVO) sicher. Der Auftragsverarbeiter trifft fuer diese Daten angemessene zusaetzliche Schutzmassnahmen, insbesondere Verschluesselung bei Uebertragung und Speicherung sowie eine strenge Zugriffsbeschraenkung.

Annex 2

Technische und organisatorische Sicherheitsmaßnahmen

Für die Bereitstellung der Leistungen gegenüber dem Verantwortlichen nimmt der Auftragsverarbeiter teilweise – je nach Gegenstand der Leistung – die technische Infrastruktur von Unter-Auftragsverarbeitern in Anspruch (vgl. Annex 3). Insoweit gelten – zusätzlich zu den TOMs des Auftragsverarbeiters – die TOMs des jeweiligen Unter-Auftragsverarbeiters. Im Übrigen gelten die nachfolgenden TOMs des Auftragsverarbeiters:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Biometrische Zugangssperren	☒ Empfang / Rezeption
☒ Chipkarte / Transpondersysteme	☒ Besucherkontrolle / Protokollierung
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl des Wachpersonals
	☒ Sorgfalt bei Auswahl Reinigungsdienste

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername & Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Firewall	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Viren-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Intrusion Detection Systems	☒ Allgemeine Richtline Datenschutz und / oder Sicherheit
☒ Mobile Device Management	
☒ Einsatz von VPN bei Remote-Zugriffen	
☒ BIOS Schutz (separates Passwort)	
☒ Automatische Desktopsperre	
☒ Verschlüsselung von Notebooks / Tablets	

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines 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.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichter (insb. DIN 66399)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Datenschutztresor

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger	☒ Festlegung von Datenbankrechten

2. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann an, an welche

Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	
☒ Protokollierung der Zugriffe und Abrufe	

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherheitsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Serverraum Löschanlage	☒ Kontrolle des Sicherheitsvorgangs
☒ USV	
☒ Schutzsteckdosenleisten Serverraum	
☒ RAID System / Festplattenspiegelung	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	
	☒ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich

4.2. Vorfall- und Reaktions-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☒ Intrusion Detection System (IDS)	
☒ Intrusion Prevention System (IPS)	

4.3. Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung der Betroffenenrechte durch technische Maßnahmen	

4.4. Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
	☒ Regelung zum Einsatz weiterer Subunternehmer

Annex 3

Genehmigte Unter-Aauftragsverarbeiter

Der Auftragsverarbeiter darf die folgenden Unter-Auftragsverarbeiter für die folgenden Leistungen an den folgenden Verarbeitungsorten einsetzen:

Unternehmen	**Services**	**Kontakt und Ort der Verarbeitung**	**Zweck**	**Kategorien von personenbezogenen Daten**
Webflow	Webflow: SaaS für die Erstellung und das Hosting von Webseiten	Webflow, Inc. 398 11th St. Fl 2, San Francisco, California, 94103, USA	SaaS für die Erstellung und das Hosting von Webseiten	siehe Annex 1, Ziff. 2, dort Nr. 4
Celonis	Make.com: iPaaS für die Verknüpfung der im Rahmen der Agenturleistungen verwendeten Software / Tools	Celonis Inc. One World Trade Center, 87th Floor, New York, NY, 10007, USA	iPaaS für die Verknüpfung der im Rahmen der Agenturleistungen verwendeten Software / Tools	siehe Annex 1, Ziff. 2, dort Nr. 1-4
Google	Google Sheets: SaaS für Tabellenkonfiguration	Google Ireland Ltd. Gordon House Barow Street, Dublin 4, Irland	SaaS für Tabellenkonfigurationen und Aufbereitung von Inhaltsdaten	siehe Annex 1, Ziff. 2, dort Nr. 1-4
Microsoft	Office 365: Outlook, SharePoint, OneDrive, Teams	Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park, Leopardstown Dublin 18, Ireland	SaaS für die Kommunikation mit dem Kunden	siehe Annex 1, Ziff. 2, dort Nr. 1-4
Perspective	SaaS für die Unterstützung zur Leadgenerierung	Perspective Software GmbH, Müggelstraße 22, 10247 Berlin	SaaS für die Unterstützung zur Leadgenerierung	siehe Annex 1, Ziff. 2, dort Nr. 2
Supabase Inc.	Backend-/Datenbank-Dienst (PostgreSQL, Authentifizierung) zur Speicherung der ueber die Landingpage erhobenen Anfrage-Daten	Supabase Inc., USA. Datenhaltung in der EU-Region (Frankfurt, eu-central-1). Drittlandtransfer abgesichert ueber Supabase-DPA und EU-Standardvertragsklauseln.	Speicherung und Verwaltung der Patienten-Anfragen	siehe Annex 1, Ziff. 2, Nr. 5 (inkl. Gesundheitsdaten Art. 9)
Hosting-Anbieter der Landingpage (z. B. Vercel Inc. / Netlify Inc. / Cloudflare Inc.)	Hosting und Auslieferung der Landingpage (Frontend, Astro)	EU-Region waehlen; DPA und EU-Standardvertragsklauseln.	Hosting der Landingpage	siehe Annex 1, Ziff. 2, Nr. 5

SuperX GmbH (Marke Superchat) - WhatsApp Business Solution Provider	Versand von WhatsApp-Nachrichten ueber die WhatsApp Business Platform: (a) interne Sofort-Benachrichtigung der Praxis ueber neue Anfragen zur schnellen Rueckruf-Reaktion (neutraler Hinweis ohne Gesundheitsdetails), (b) geplant: Terminbestaetigung/-erinnerung an Patienten	SuperX GmbH, Prenzlauer Allee 242-247, 10405 Berlin (Haus 7). Datenhaltung in der EU (laut Anbieter Frankfurt am Main; im Superchat-AVV bestaetigen). Nutzt 360dialog GmbH (Berlin) und Meta (WhatsApp) als Unter-Unterauftragsverarbeiter.	WhatsApp-Benachrichtigungen (interne Lead-Meldung sowie geplante Patiententermine)	Kontakt-/Kommunikationsdaten; interne Lead-Meldung als neutraler Hinweis ohne Gesundheitsdetails

Hinweis zu möglichen Datentransfers in die USA:
Ergaenzung (Stand Juni 2026): Supabase Inc. (USA) sowie der eingesetzte Hosting-Anbieter der Landingpage verarbeiten in der EU-Region; etwaige Drittland-Transfers werden ueber EU-Standardvertragsklauseln gem. Art. 46 DS-GVO und - soweit zertifiziert - das EU-US Data Privacy Framework abgesichert. Der eingesetzte WhatsApp-Anbieter SuperX GmbH (Superchat) ist EU-gehostet; ueber die WhatsApp Business Platform kann Meta als Empfaenger fungieren (US-Transfer ueber Data Privacy Framework).

Folgende Unternehmen sind – Stand Februar 2024 – in den USA gemäß EU-US Data Privacy Agreement zertifiziert (https://www.dataprivacyframework.gov/list): Microsoft Corporation (für HR Data und Non-HR Data), Google LLC (für HR Data und Non-HR Data), Webflow Inc (Non-HR Data), Celonis Inc (für HR Data und Non-HR Data).

Informationen zu Unter-Unterauftragsverarbeitern

Die Unter-Auftragsverarbeiter (s. oben) können je nach Einzelfall und Situation die unter den nachfolgenden Links aufgeführten Dienstleister als deren Auftragsverarbeiter einsetzen:

Webflow	https://webflow.com/legal/subprocessors
Celonis	https://www.make.com/en/sub-processors.pdf
Google	https://cloud.google.com/terms/subprocessors
Microsoft	https://servicetrust.microsoft.com/DocumentPage/6471c92a-d274-4188-914a-033aa3efb296
Perspective	Auf Anfrage
Supabase	https://supabase.com/legal/subprocessors

SuperX GmbH (Superchat, WhatsApp-BSP)	Sub-Prozessoren u. a. 360dialog GmbH und Meta; gemaess Superchat-AVV/Website

Hinweis zum Einsatz von Tracking-Pixeln (z. B. Meta-Pixel): Soweit auf der Landingpage Tracking-Technologien des Anbieters Meta (Meta Platforms Ireland Ltd.) eingesetzt werden, besteht insoweit eine gemeinsame Verantwortlichkeit gem. Art. 26 DS-GVO zwischen dem fuer die Schaltung Verantwortlichen und Meta. Diese gemeinsame Verantwortlichkeit ist nicht Gegenstand dieses AV-Vertrages; sie wird ueber die Vertragsbedingungen von Meta (Controller Addendum) sowie die Einwilligung der Nutzer (Cookie-Banner) gesondert geregelt. An Meta werden keine Gesundheitsdaten und keine Formularinhalte uebertragen.