SIBEL LANG CONSULTING

Vertrag über die Verarbeitung personenbezogener Daten

nachfolgend „AV-Vertrag“ genannt

zwischen

dem Kunden

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

und

Sibel Lang
Sibel Lang Consulting
c/o Rechtsanwaltskanzlei Yilmaz Öndemir
Wilhelm-Leuschner-Straße 41
60329 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**“ den Vertrag über die Erbringung der vom Verantwortlichen beauftragten und vom Auftragsverarbeiter erbrachten Beratungs- und Umsetzungsleistungen, 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) „**Gesundheitsdaten**“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15, Art. 9 DS-GVO);

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

(9) „**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 Beratungs- und Umsetzungsleistungen 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 verständigen.

(4) **[Unterstützungsleistungen]** Soweit nicht ausdrücklich anders vereinbart, kann der Auftragsverarbeiter für Unterstützungsleistungen nach Ziffer 3 (5) und Ziffer 4 (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 die 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 den Auftragsverarbeiter bei der Prüfung möglicher Verstöße und bei

der Abwehr von Ansprüchen betroffener Personen oder Dritter 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 in Ziffer 3 (2). Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befassten 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) **[Löschung und Rückgabe]** Nach Abschluss der Leistungen löscht der Auftragsverarbeiter die personenbezogenen Daten des Verantwortlichen oder gibt sie nach dessen Wahl zurück, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Zugänge zu Systemen des Verantwortlichen gibt der Auftragsverarbeiter nach Abschluss der Leistungen zurück.

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 UND SCHWEIGEPFLICHT

Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Soweit der Auftragsverarbeiter dabei Kenntnis von Geheimnissen erhält, die der ärztlichen oder einer vergleichbaren beruflichen Schweigepflicht unterliegen, wirkt er an der beruflichen Tätigkeit des Verantwortlichen im Sinne von § 203 Abs. 3 StGB mit und ist zur Verschwie-

genheit verpflichtet. Der Verantwortliche weist den Auftragsverarbeiter hiermit auf die strafrechtlichen Folgen einer Verletzung dieser Pflicht hin. Der Auftragsverarbeiter verpflichtet von ihm eingesetzte Unterauftragsverarbeiter, soweit diese Kenntnis von solchen Geheimnissen erlangen können, in gleicher Weise.

7 UNTERAUFTRAGSVERARBEITER

(1) **[Befugnis]** Der Auftragsverarbeiter darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) 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 Auftragsverarbeiters]** 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 Regelungen dieses Vertrages im Wesentlichen entsprechen.

8 VERTRAGSDAUER, KÜNDIGUNG

Diese Vereinbarung gilt für die Dauer des Hauptvertrages.

9 KONTAKTAUFNAHME MIT DEM AUFTRAGSVERARBEITER

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

Sibel Lang Consulting
c/o Rechtsanwaltskanzlei Yilmaz Öndemir
Wilhelm-Leuschner-Straße 41
60329 Frankfurt am Main
hallo@sibel-lang.de

zu richten.

10 HAFTUNG

Die Haftung für Schäden, die durch eine nicht der DS-GVO und geltenden Datenschutzbestimmungen entsprechende Verarbeitung verursacht werden, 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. Der 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. Der 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. Der 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. Ziffer 7 (Änderungen beim Einsatz von Unterauftragsverarbeitern) bleibt unberührt.

(3) **[Gerichtsstand]** Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem AV-Vertrag ist Frankfurt am Main, soweit eine Gerichtsstandsvereinbarung gesetzlich zulässig ist. Dieser gilt vorbehaltlich eines etwaigen ausschließlichen gesetzlichen Gerichtsstandes.

(4) **[Geltendes Recht]** Bezüglich des geltenden Rechts 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 Leistungen:

	Leistung	Beschreibung und Gegenstand der Verarbeitung
1	Webdesign, -Entwicklung und Web-Hosting	Konzeption, Erstellung, Betrieb und Pflege der Praxis-Website oder Landingpage, technisch wie inhaltlich, einschließlich Kontakt- und Anfrageformularen
2	Einrichtung digitaler Systeme	Einrichtung und Anbindung von Online-Terminbuchung, Buchungssystemen, KI-Telefon- und Sprachassistenten und Automatisierungen im Konto des Verantwortlichen beim jeweiligen Anbieter
3	Beratung, Analysen und Befragungen	Auswertung von Praxis- und Leistungskennzahlen, Durchführung und Auswertung von Mitarbeiter- und Patientenbefragungen, Workshops und Schulungen
4	Website-Analyse	Cookielose Reichweitenmessung der Website des Verantwortlichen

2. Arten und Kategorien von personenbezogenen Daten

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

	Leistung	Personenbezogene Daten
1	Webdesign, -Entwicklung und Web-Hosting	— personenbezogene Daten der Website-Besucher: Protokolldaten, Logfiles, IP-Adresse — im Falle von Kontakt- und Anfrageformularen: Kontakt- und Kommunikationsdaten (z. B. Name, Telefonnummer, E-Mail-Adresse, Anliegen) sowie gegebenenfalls Gesundheitsdaten, die Interessenten im Anliegen selbst angeben — personenbezogene Daten der auf der Website abgebildeten oder genannten Personen, z. B. Name, Foto, Qualifikation von Praxisinhabern und Mitarbeitenden
2	Einrichtung digitaler Systeme	— Stamm- und Kontaktdaten von Patientinnen und Patienten, soweit sie im System des Verantwortlichen sichtbar sind — Termindaten, gegebenenfalls mit Terminart oder Behandlungsanlass (Gesundheitsdaten) — Benutzer- und Kontaktdaten von Mitarbeitenden des Verantwortlichen
3	Beratung, Analysen und Befragungen	— Name, Funktion und Kontaktdaten von Mitarbeitenden — Antworten aus Mitarbeiter- und Patientenbefragungen, nach Möglichkeit anonymisiert — Leistungs- und Abrechnungskennzahlen, nach Möglichkeit ohne Personenbezug oder pseudonymisiert

4	Website-Analyse	— gekürzte, nicht gespeicherte IP-Adresse, Seitenaufrufe, Herkunftsseite, Gerätetyp, Browser und Land, ausschließlich in aggregierter Form

3. Kategorien betroffener Personen

Patientinnen und Patienten sowie Interessenten des Verantwortlichen, Besucher der Website des Verantwortlichen, Inhaber und Mitarbeitende des Verantwortlichen.

4. Leistungen, Verarbeitungszweck

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

5. Verarbeitungsort

Siehe Annex 2 und 3 des AV-Vertrages.

6. Besondere Kategorien personenbezogener Daten

Soweit besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO, insbesondere Gesundheitsdaten, verarbeitet werden, stellt der Verantwortliche die hierfür erforderliche Rechtsgrundlage sicher. Der Auftragsverarbeiter verarbeitet diese Daten nur, soweit es für die Leistung unvermeidbar ist, und trifft hierfür angemessene zusätzliche Schutzmaßnahmen, insbesondere Verschlüsselung bei Übertragung und Speicherung sowie eine strenge Zugriffsbeschränkung. Gesundheitsdaten werden nicht per unverschlüsselter E-Mail übermittelt.

Annex 2
Technische und organisatorische Sicherheitsmaßnahmen

Für die Bereitstellung der Leistungen gegenüber dem Verantwortlichen nimmt der Auftragsverarbeiter je nach Gegenstand der Leistung die technische Infrastruktur von Unterauftragsverarbeitern in Anspruch (vgl. Annex 3). Der Auftragsverarbeiter betreibt keine eigenen Server. Insoweit gelten, zusätzlich zu den TOMs des Auftragsverarbeiters, die TOMs des jeweiligen Unterauftragsverarbeiters. Im Übrigen gelten die nachfolgenden TOMs des Auftragsverarbeiters:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DS-GVO

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
☒ Abschließbare Arbeitsräume	☒ Kein Zutritt Unbefugter zum Arbeitsplatz
☒ Rechenzentren ausschließlich bei Unterauftragsverarbeitern (vgl. Annex 3)	☒ Endgeräte werden unterwegs nicht unbeaufsichtigt gelassen

1.2 Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername und Passwort	☒ Individuelle, starke Passwörter je Dienst
☒ Zwei-Faktor-Authentisierung bei allen Diensten, die sie anbieten	☒ Verwaltung der Zugangsdaten in einem Passwortmanager
☒ Verschlüsselung der Festplatten von Notebooks und Mobilgeräten	☒ Keine Weitergabe von Zugangsdaten
☒ Automatische Bildschirmsperre	
☒ Firewall und Virenschutz des Betriebssystems	
☒ Zeitnahe Sicherheitsupdates für Betriebssystem und Software	

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
☒ Eigene Benutzerkonten in Systemen des Verantwortlichen statt geteilter Zugänge	☒ Berechtigungen nur im für die Leistung erforderlichen Umfang

☒ Sichere Löschung nicht mehr benötigter Daten und Datenträger	☒ Rückgabe von Zugängen nach Abschluss der Leistung
☒ Aktenvernichter für Papierunterlagen	☒ Möglichst papierlose Arbeitsweise

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Vorschau- und Produktivumgebung bei Websites	☒ Getrennte Projekte und Ablagen je Kunde
☒ Logische Trennung der Kundendaten bei den Unterauftragsverarbeitern	

2. Integrität gem. Art. 32 Abs. 1 lit. b DS-GVO

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Transportverschlüsselung (TLS / HTTPS) für Websites, E-Mail und Cloud-Dienste	☒ Gesundheitsdaten nicht per unverschlüsselter E-Mail
☒ Freigabe von Dateien nur über zugriffsbeschränkte Links	☒ Übermittlung nur an die in Annex 3 genannten Stellen

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
☒ Versionsverwaltung aller Änderungen an Websites	☒ Nachvollziehbarkeit durch personenbezogene Benutzerkonten
☒ Protokollierung durch die eingesetzten Cloud-Dienste	

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DS-GVO

3.1 Verfügbarkeitskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Redundante Infrastruktur der Hosting-Anbieter	☒ Regelmäßige Datensicherung

☒ Wiederherstellbare Versionen aller Website-Stände	

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

4.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen mindestens jährlich	☒ Verpflichtung eingesetzter Dritter auf Vertraulichkeit und auf § 203 StGB

4.2 Vorfall- und Reaktions-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Firewall, Spamfilter und Virenschutz mit regelmäßiger Aktualisierung	☒ Unverzügliche Meldung von Vorfällen an den Verantwortlichen
	☒ Sofortiges Sperren und Ändern betroffener Zugänge

4.3 Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DS-GVO)

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Anonymisierung oder Pseudonymisierung, wo immer möglich
☒ Cookielose Reichweitenmessung	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Auswahl der Unterauftragsverarbeiter unter Sorgfaltsgesichtspunkten
	☒ Verträge zur Auftragsverarbeitung mit allen Unterauftragsverarbeitern
	☒ Regelung zum Einsatz weiterer Subunternehmer

Annex 3
Genehmigte Unterauftragsverarbeiter

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

Unternehmen	Services	Kontakt und Ort der Verarbeitung	Zweck	Kategorien von personenbezogenen Daten
Google	Google Workspace: Gmail, Google Drive, Google Meet	Google Ireland Ltd. Gordon House, Barrow Street, Dublin 4, Irland	Kommunikation mit dem Verantwortlichen, Ablage von Projektunterlagen, Videokonferenzen	siehe Annex 1, Ziff. 2, dort Nr. 1—3
Vercel	Hosting und Auslieferung von Websites	Vercel Inc. 440 N Barranca Ave #4133, Covina, CA 91723, USA	Betrieb der Website des Verantwortlichen	siehe Annex 1, Ziff. 2, dort Nr. 1
GitHub	Versionsverwaltung des Website-Quellcodes	GitHub B.V. Prins Bernhardplein 200, 1097 JB Amsterdam, Niederlande	Ablage und Versionierung der Website-Inhalte	siehe Annex 1, Ziff. 2, dort Nr. 1 (nur abgebildete oder genannte Personen)
Plausible	Cookielose Website-Analyse	Plausible Insights OÜ Västriku tn 2, 50403 Tartu, Estland; Server in der EU	Reichweitenmessung der Website des Verantwortlichen	siehe Annex 1, Ziff. 2, dort Nr. 4

Hinweis zu möglichen Datentransfers in die USA:
Soweit Unterauftragsverarbeiter mit Sitz in den USA eingesetzt werden oder Unterauftragsverarbeiter Daten in die USA übermitteln, sind diese Übermittlungen über EU-Standardvertragsklauseln gem. Art. 46 DS-GVO und, soweit zertifiziert, über das EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/list) abgesichert.

Informationen zu Sub-Unterauftragsverarbeitern

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

Google	https://workspace.google.com/terms/subprocessors.html
Vercel	https://vercel.com/legal/sub-processors
GitHub	https://docs.github.com/en/site-policy/privacy-policies/github-subprocessors
Plausible	https://plausible.io/dpa

Hinweis zu Software Dritter, die der Verantwortliche selbst beauftragt (z. B. Online-Terminbuchung, Buchungssysteme, KI-Telefonassistenten): Den Vertrag zur Auftragsverarbeitung schließt der Verantwortliche direkt mit dem jeweiligen Anbieter ab. Diese Anbieter sind keine Unterauftragsverarbeiter des Auftragsverarbeiters.

© Sibel Lang Consulting, Stand: Oktober 2026