

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

Auftraggeber	
Anschrift	
Vertretungsberechtigte Person	
Kontakt / E-Mail	
Auftragsverarbeiter	Newsite GmbH, Kienberger Allee 4, 12529 Schönefeld, vertreten durch Alexander Klein
Leistung	☐ Newsite PraxisAssist ☐ Newsite Recruit
Hauptvertrag	
Datum Hauptvertrag	
Vertragsbeginn	
Optionale Kanäle	☐ E-Mail ☐ Telegram ☐ WhatsApp/SMS

Diese Vereinbarung ist Bestandteil des Hauptvertrags. Sie konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien, soweit Newsite personenbezogene Daten im Auftrag verarbeitet. Bei Widersprüchen haben die spezielleren Datenschutzregelungen dieser Vereinbarung Vorrang.

Vor Unterzeichnung sind Kundendaten, beauftragte Leistungen und aktivierte optionale Kanäle zu vervollständigen. Die Vorlage ersetzt keine individuelle Rechtsberatung.

1. Gegenstand und Dauer

Newsite verarbeitet die in den Anlagen beschriebenen personenbezogenen Daten ausschließlich zur Erbringung der ausgewählten Leistung und nur im dokumentierten Auftrag des Auftraggebers.

Die Verarbeitung beginnt mit dem im Hauptvertrag vereinbarten Leistungsbeginn und endet mit dessen Beendigung, sofern keine gesetzlichen Pflichten oder dokumentierten Weisungen eine abweichende Dauer vorgeben.

Art, Zweck, Kategorien betroffener Personen, Datenarten und die konkrete Dauer sind in Anlage 1 beschrieben.

2. Weisungen und Zweckbindung

Newsite verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers. Der Hauptvertrag, diese Vereinbarung, freigegebene Einstellungen im Kundenportal und in Textform erteilte Einzelweisungen gelten als dokumentierte Weisungen.

Eine Verarbeitung zu eigenen Zwecken findet nicht statt, soweit Newsite nicht für klar abgegrenzte eigene Pflichten, insbesondere Vertragsverwaltung, Abrechnung, IT-Sicherheit oder Rechtsverteidigung, selbst verantwortlich ist.

Hält Newsite eine Weisung für datenschutzwidrig, informiert Newsite den Auftraggeber unverzüglich. Die Ausführung kann bis zur Bestätigung oder Änderung der Weisung ausgesetzt werden.

3. Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen, die Festlegung von Löschfristen und die Zulässigkeit der erteilten Weisungen verantwortlich.

Der Auftraggeber konfiguriert nur erforderliche Datenfelder und Zugriffe, hält Benutzer- und Rollenangaben aktuell und meldet Änderungen oder Sicherheitsverdachte ohne schuldhaftes Zögern.

Besondere Kategorien personenbezogener Daten dürfen nur verarbeitet werden, wenn hierfür eine tragfähige Rechtsgrundlage und angemessene Schutzmaßnahmen bestehen.

4. Vertraulichkeit und Zugriffssteuerung

Newsite setzt nur Personen ein, die auf Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind.

Zugriffe werden nach Rollen und Erforderlichkeit vergeben. Administrative Zugriffe werden auf das notwendige Maß begrenzt und für Betrieb, Support oder Sicherheit protokolliert.

Der Auftraggeber bleibt für die sichere Verwaltung seiner Benutzerkonten, Endgeräte und Zugangsdaten verantwortlich.

5. Technische und organisatorische Maßnahmen

Newsite trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Verarbeitungsrisiken und der besonderen Sensibilität von Gesundheits- und Bewerbungsdaten.

Newsite darf Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau nicht abgesenkt wird. Wesentliche Änderungen werden dokumentiert.

6. Unterauftragsverarbeiter

Der Auftraggeber erteilt eine allgemeine schriftliche Genehmigung für die in Anlage 3 aufgeführten Unterauftragsverarbeiter und die dort bezeichneten Verarbeitungstätigkeiten.

Newsite informiert den Auftraggeber grundsätzlich mindestens 30 Tage vor der geplanten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann aus nachvollziehbaren Datenschutzgründen innerhalb von 14 Tagen widersprechen. Die Parteien suchen eine angemessene Lösung; ist dies nicht möglich, gelten die Kündigungsrechte des Hauptvertrags.

Newsite verpflichtet Unterauftragsverarbeiter zu im Wesentlichen gleichwertigen Datenschutzpflichten. Drittlandübermittlungen erfolgen nur bei Vorliegen der Voraussetzungen der Art. 44 ff. DSGVO, etwa aufgrund eines Angemessenheitsbeschlusses oder geeigneter Garantien einschließlich EU-Standardvertragsklauseln.

7. Unterstützung des Auftraggebers

Newsite unterstützt den Auftraggeber im angemessenen Umfang bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Anfragen betroffener Personen werden ohne Weisung nicht inhaltlich beantwortet, sondern an den Auftraggeber weitergeleitet.

Newsite unterstützt bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen, bei Datenschutz-Folgenabschätzungen und, soweit erforderlich, bei Konsultationen der Aufsichtsbehörde. Ein außergewöhnlicher, nicht von Newsite verursachter Zusatzaufwand kann nach vorheriger Abstimmung vergütet werden.

8. Datenschutzverletzungen

Newsite informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, die die Auftragsverarbeitung betrifft. Soweit praktisch möglich, erfolgt eine Erstinformation innerhalb von 24 Stunden.

Die Mitteilung enthält die verfügbaren Angaben zu Art und Umfang, betroffenen Daten und Personen, wahrscheinlichen Folgen, ergriffenen oder vorgeschlagenen Maßnahmen sowie eine Kontaktstelle. Noch nicht verfügbare Angaben werden nachgereicht.

Die gesetzliche Bewertung und Meldung gegenüber Behörden oder betroffenen Personen obliegt dem Auftraggeber, soweit er Verantwortlicher ist.

9. Nachweise und Kontrollen

Newsite stellt die zum Nachweis der Einhaltung erforderlichen Informationen bereit. Der Auftraggeber kann nach angemessener Vorankündigung und grundsätzlich einmal jährlich Kontrollen selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen, sofern Geschäftsgeheimnisse, Sicherheit und Rechte anderer Kunden gewahrt bleiben.

Vor-Ort-Prüfungen sind auf erforderliche Bereiche und Geschäftszeiten zu beschränken. Gleichwertige Nachweise, Prüfberichte oder standardisierte Sicherheitsauskünfte sollen vorrangig genutzt werden.

10. Rückgabe und Löschung

Nach Ende der Leistung löscht oder gibt Newsite die Auftragsdaten nach Wahl des Auftraggebers zurück, soweit keine gesetzliche Aufbewahrungspflicht besteht. Produktivdaten werden nach dem in Anlage 4 beschriebenen Verfahren entfernt.

Sicherungen werden im Rahmen des regulären Sicherungszyklus überschrieben oder gelöscht und bis dahin gesperrt sowie nur für Wiederherstellungszwecke verarbeitet.

Der Auftraggeber exportiert erforderliche Daten vor Vertragsende über die vorgesehenen Funktionen oder beauftragt Newsite rechtzeitig in Textform.

11. Rangfolge, Laufzeit und Schlussbestimmungen

Diese Vereinbarung gilt für die Dauer der Auftragsverarbeitung. Änderungen bedürfen mindestens der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist.

Die Haftung richtet sich nach Art. 82 DSGVO und den zulässigen Regelungen des Hauptvertrags. Gesetzliche Rechte betroffener Personen bleiben unberührt.

Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen sie durch eine wirksame Regelung, die dem Zweck möglichst nahekommt.

Anlage 1 – Beschreibung der Verarbeitung

A. Newsite PraxisAssist

Gegenstand/Zweck	Telefonische und digitale Aufnahme, Strukturierung, Priorisierung und Übergabe administrativer Praxisanliegen; Portal, Website-Widget, Kalender- und PVS-Übergaben je Setup.
Betroffene Personen	Patienten, Anrufende, Angehörige, Bevollmächtigte, Praxismitarbeiter, Ärzte, Interessenten und Supportkontakte.
Datenkategorien	Stamm- und Kontaktdaten; Rufnummern; Termin-, Rezept-, Überweisungs-, Rückruf-, AU/eAU- und sonstige Anliegen; Gesundheitsangaben; Kommunikations-, Ticket-, Rollen-, Protokoll- und Sicherheitsdaten.
Besondere Kategorien	Gesundheitsdaten nach Art. 9 DSGVO, soweit sie durch Anrufende mitgeteilt oder für die Praxisübergabe erforderlich sind.
Verarbeitung	Erheben, Erfassen, Ordnen, Transkribieren, Strukturieren, Speichern, Anzeigen, Übermitteln auf Weisung, Sperren und Löschen.
Audiodaten	Kurzzeitige Verarbeitung zur Transkription; keine dauerhafte Rohaufnahme im Standard-Telefonkern. Strukturierte Zusammenfassungen und Vorgänge werden in Deutschland/EU gespeichert.
Dauer	Laufzeit des Hauptvertrags; Vorgangs- und Löschfristen nach Praxiskonfiguration und Anlage 4.

Anlage 1 – Beschreibung der Verarbeitung

B. Newsite Recruit

Gegenstand/Zweck	Bewerberkommunikation, Unterlagenannahme und Vollständigkeitsprüfung, strukturierte Vorqualifizierung, Terminierung, Reporting und Übergabe an den vom Kunden bestimmten Recruiting-Prozess oder das ATS.
Betroffene Personen	Bewerber, Kandidaten, Talentpool-Kontakte, Interviewpartner, HR- und Fachbereichsmitarbeiter, Portalnutzer und Supportkontakte.
Datenkategorien	Stamm- und Kontaktdaten; Bewerbungsunterlagen; Qualifikation, Berufserfahrung und Verfügbarkeit; Kommunikations-, Termin-, Bewertungs-, Rollen-, Audit- und Sicherheitsdaten.
Besondere Kategorien	Nur soweit im Bewerbungsverfahren zulässig und erforderlich, etwa Gesundheitsangaben oder Angaben, aus denen besondere Kategorien hervorgehen können.
Verarbeitung	Erheben, Erfassen, OCR-Auslesen, Zuordnen, Strukturieren, Speichern, Bereitstellen, Exportieren oder Übermitteln auf Weisung, Sperren und Löschen.
Originalunterlagen	Speicherung und Dokumentenauslesung auf Newsite-Infrastruktur in Deutschland/EU. Keine standardmäßige Übermittlung der Originaldatei an ein US-Sprachmodell zur Vollständigkeitsprüfung.
Dauer	Laufzeit des Hauptvertrags; je Mandant und Verfahrensstatus festgelegte Frist, regelmäßig 180 Tage nach Abschluss oder Ablehnung, sofern keine andere dokumentierte Frist oder Talentpool-Einwilligung gilt.

Anlage 2 – Technische und organisatorische Maßnahmen

Zutrittskontrolle	Betrieb in professionellen Rechenzentren; physischer Zutritt wird durch den Infrastrukturprovider kontrolliert. Newsite betreibt keine frei zugänglichen Serverräume.
Zugangskontrolle	Individuelle Benutzerkonten, starke Passwort-Hashes, zeitlich begrenzte Sitzungen, rollenbasierte Rechte, TOTP-Zwei-Faktor-Authentifizierung für privilegierte Konten, Sperren nach Fehlversuchen und administrative Trennung.
Zugriffskontrolle	Mandanten- und Rollenprüfung im Backend, minimale Berechtigungen, getrennte interne Geheimnisse, Audit-Protokolle und regelmäßige Überprüfung von Konten und Integrationen.
Übertragungskontrolle	TLS für Webzugriffe; signierte oder geheimnisgeschützte Webhooks; dokumentierte Zielsysteme; Datenminimierung bei Benachrichtigungen; Drittlandübermittlung nur mit dokumentierter Grundlage.
Eingabekontrolle	Zeitstempel, Benutzer- oder Rollenbezug und Audit-Ereignisse für wesentliche Portal-, Freigabe-, Integrations- und Sicherheitsaktionen.
Verfügbarkeitskontrolle	Automatisierte Dienstneustarts, Health-Checks, Ressourcenüberwachung, Firewalls, Angriffsschutz, Kapazitätswarnungen, Datenbank- und Anwendungsbackups sowie dokumentierte Wiederherstellungsprüfungen.
Trennungsgebot	Mandantenkennungen und serverseitige Sichtbarkeitsprüfungen; getrennte Produktdatenbanken und Dienste; getrennte Entwicklungs-, Sicherungs- und Produktivartefakte.
Datenminimierung	Nur erforderliche Felder und Texte; keine medizinische oder automatische Personalentscheidung; keine Originalunterlagen im regulären externen LLM-Chat; keine Patienten-Klarangaben in operativen Alarmen.
Löschung	Status- und fristabhängige Löschung aus Datenbank und Dateispeicher; Sitzungsablauf; kurzzeitige Telefon-Audiodateien werden nach Transkription entfernt; Sicherungen werden zyklisch überschrieben.
Sicherheitsprüfung	Code- und Konfigurationsprüfungen, Abhängigkeits-Scans, Protokollauswertung, Last- und Wiederherstellungstests sowie ein dokumentiertes Incident-Verfahren.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Es gelten nur die für das beauftragte Produkt und die konkret aktivierten Kanäle erforderlichen Einträge. Optionale Dienste werden erst nach dokumentierter Weisung oder Aktivierung eingesetzt.

Anbieter	Leistung und Daten	Ort / Status
Hetzner Online GmbH, Deutschland	Cloud- und Serverinfrastruktur; Produktiv-, Datenbank-, Datei- und Sicherungsdaten.	Deutschland/EU · Kern
Mistral AI SAS, Frankreich	Aktuelle primäre generative KI-Textfunktionen; erforderliche Chatfrage und freigegebener minimierter Kontext, keine Originaldatei.	Frankreich (EU) · aktiv im Einsatz
Anthropic, PBC, USA	Begrenzte KI-Textfunktionen; erforderliche Chatfrage und minimierter Kontext, keine Originaldatei.	Drittland · DPA/SCC · konfigurierbarer Fallback
Neue Medien Münnich, Deutschland	E-Mail-Transport über kasserver.com; Empfänger, Betreff, Nachricht und Anhänge nach Weisung.	Deutschland/EU · E-Mail
Telegram Messenger Inc.	Optionaler Messenger- oder Betriebskanal; nur aktivierte Kanäle, operative Alarmer datenminimiert.	Mögliche Drittlandverarbeitung · optional
Meta Platforms Ireland Ltd.	WhatsApp Business Cloud API; Kontakt-, Nachrichten- und optionale Dateiinhalte.	EU/gegebenenfalls Drittland nach Meta-Bedingungen · optional

Hinweise zur KI-Verarbeitung

Produktive Datenhaltung und Originalunterlagen liegen in Deutschland. Generative Textfunktionen nutzen aktuell primär Mistral AI SAS mit Verarbeitung in Frankreich (Europäische Union). Übermittelt wird nur der erforderliche, möglichst minimierte oder pseudonymisierte Textkontext; Originaldateien werden nicht an ein Sprachmodell übertragen.

Fällt der aktive EU-Primärpfad aus, kann Anthropic, PBC, USA, als transparenter Fallback aktiviert sein. Für diesen Drittlandpfad gelten ein Auftragsverarbeitungsvertrag und, soweit erforderlich, EU-Standardvertragsklauseln nach Art. 46 DSGVO. Der Fallback lässt sich auf Wunsch des Auftraggebers deaktivieren; die Verarbeitung erfolgt dann ausschließlich über den EU-Primärpfad. Änderungen erfolgen nach Ziffer 6 und nicht stillschweigend.

Anlage 4 – Lösch- und Rückgabekonzept

Während der Laufzeit	Status- und kundenspezifische Fristen; Lösch- und Exportfunktionen im Portal; Protokollierung wesentlicher Vorgänge.
PraxisAssist	Roh-Audio im Standard-Telefonat nur kurzzeitig bis Transkription und Antwort; Tickets und Vorgänge nach Praxisregel; Konten bis Vertragsende und anschließender technischer Abwicklung.
Recruit	Abgeschlossene oder abgelehnte Verfahren nach Mandantenfrist, regelmäßig 180 Tage; Talentpool nur auf gesonderter Grundlage; Datenbankobjekte und zugehörige Dateien werden gemeinsam entfernt.
Vertragsende	Export auf Weisung; Löschung der Produktivdaten grundsätzlich innerhalb von 30 Tagen nach Ende und geklärter Rückgabe, soweit keine Pflicht zur Aufbewahrung besteht.
Sicherungen	Gesperrte Restkopien werden im regulären Sicherungszyklus überschrieben; keine erneute produktive Nutzung außer zur notwendigen Wiederherstellung.
Nachweis	Löschlauf- und Systemprotokolle beziehungsweise schriftliche Bestätigung auf angemessene Anfrage.

Unterzeichnung

Die Parteien bestätigen, die Vereinbarung einschließlich Anlagen gelesen zu haben. Kundendaten, beauftragte Leistungen und aktivierte optionale Dienste sind vor Unterzeichnung zu vervollständigen.

Auftraggeber	Newsite GmbH
	Ort, Datum: _____
	Alexander Klein, Geschäftsführer
	Unterschrift: _____

Rechtsgrundlagen und Orientierung

Art. 28 und 32 DSGVO: [EUR-Lex · Verordnung \(EU\) 2016/679](#)

EU-Standardvertragsklauseln: [Beschluss \(EU\) 2021/915](#)

Formulierungshilfe: [Bayerisches Landesamt für Datenschutzaufsicht](#)