

newsite

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

Auftraggeber	[Kunde / Praxis / Einrichtung, Anschrift, Vertretungsberechtigte Person]
Auftragsverarbeiter	Newsite GmbH, Kienberger Allee 4, 12529 Schönefeld, vertreten durch Alexander Klein
Leistung	☐ PraxisAssist AI ☐ Newsite Recruit ☐ beide Leistungen
Hauptvertrag	[Bezeichnung und Datum]
Vertragsbeginn	[Datum]

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.

Vertragsstatus: Kundenspezifische Angaben, aktivierte Kanäle und Unterauftragsverarbeiter müssen vor Unterzeichnung vervollständigt werden. 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, 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 konkret 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, zum Beispiel 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 von betroffenen 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. PraxisAssist AI

Gegenstand/Zweck	Telefonische und digitale Aufnahme, Strukturierung, Priorisierung und Übergabe administrativer Praxisanliegen; Portal, 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 durch Anrufende mitgeteilt oder für die Praxisübergabe erforderlich.
Verarbeitung	Erheben, Erfassen, Ordnen, Transkribieren, Strukturieren, Speichern, Anzeigen, Übermitteln auf Weisung, Sperren und Löschen.
Audiodaten	Kurzzeitige Verarbeitung für lokale Transkription; keine dauerhafte Rohaufnahme im Standard-Telefonkern. Strukturierte Zusammenfassung und Vorgang werden in Deutschland/EU gespeichert.
Dauer	Laufzeit des Hauptvertrags; Vorgangs- und Löschfristen nach Praxiskonfiguration und Anlage 4.

B. Newsite Recruit

Gegenstand/Zweck	Bewerberkommunikation, Unterlagenannahme und Vollständigkeitsprüfung, strukturierte Vorqualifizierung, Terminierung, Reporting und Übergabe an den vom Kunden bestimmten Recruiting-Prozess oder 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, zum Beispiel Gesundheitsangaben oder Angaben, aus denen besondere Kategorien hervorgehen können.
Verarbeitung	Erheben, Erfassen, OCR-Auslesen, Zuordnen, Strukturieren, Speichern, Bereitstellen, Exportieren/Übermitteln auf Weisung, Sperren und Löschen.
Originalunterlagen	Speicherung und Dokumentenauslesung auf der 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/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, optionale TOTP-Zwei-Faktor-Authentifizierung, Sperren nach Fehlversuchen und administrative Trennung.
Zugriffskontrolle	Mandanten- und Rollenprüfung im Backend, minimale Berechtigungen, getrennte interne Secrets, Audit-Protokolle und regelmäßige Überprüfung von Konten und Integrationen.
Übertragungskontroll e	TLS für Webzugriffe; signierte beziehungsweise secret-geschützte Webhooks; dokumentierte Zielsysteme; Datenminimierung bei Benachrichtigungen; Drittlandübermittlung nur mit dokumentierter Grundlage.
Eingabekontrolle	Zeitstempel, Benutzer-/Rollenbezug und Audit-Ereignisse für wesentliche Portal-, Freigabe-, Integrations- und Sicherheitsaktionen.
Verfügbarkeitskontroll e	Systemd-Neustartregeln, Health-Checks, Ressourcenüberwachung, Firewall, Fail2ban, 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 Entscheidung; keine automatische Personalentscheidung; keine Originalunterlagen im regulären externen LLM-Chat; keine Patienten-Klarangaben in operativen Telegram-PVS-Alarmen.
Löschung	Status- und fristabhängige Löschung aus Datenbank und Dateispeicher; Session-Ablauf; kurzzeitige Telefon-Audiodateien werden nach Transkription entfernt; Backups werden zyklisch überschrieben.
Sicherheitsprüfung	Code- und Konfigurationsprüfungen, Abhängigkeits-Scans, Protokollauswertung, Last- und Wiederherstellungstests sowie dokumentiertes Incident-Verfahren.

Genehmigte Unterauftragsverarbeiter - Anlage 3

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

Anbieter	Leistung	Daten	Ort/Garantie	Status
Hetzner Online GmbH, DE	Cloud-/Serverinfrastruktur	Produktiv-, Datenbank-, Datei- und Sicherungsdaten	Deutschland/EU	Kern
IONOS Cloud GmbH, Deutschland	Primäre generative KI-Textfunktionen	Erforderliche Chatfrage und freigegebener Kontext; keine Originaldatei	Deutschland; zustandslos; kein Modelltraining	Nach Aktivierung und Abnahme
Anthropic, PBC, USA	Begrenzte KI-Textfunktionen	Erforderliche Chatfrage und Kontext; keine Originaldatei	Drittland; DPA/SCC; Standard-API grundsätzlich 30 Tage	Übergangs-Fallback; nach IONOS-Abnahme aus
Neue Medien Münnich, DE	E-Mail-Transport über kasserver.com	Empfänger, Betreff, Nachricht, Anhänge nach Weisung	Deutschland/EU	Recruit/E-Mail
Telegram Messenger Inc.	Optionalen Messenger-/Betriebskanal	Nur für aktivierte Kanäle; operative Alarme datenminimiert	Mögliche Drittlandverarbeitung; kundenspezifisch prüfen	Optional
Meta Platforms Ireland Ltd.	WhatsApp Business Cloud API	Kontakt-, Nachrichten- und optionale Dateiinhalte	EU/ggf. Drittland nach Meta-Bedingungen	Optional, derzeit nicht Standard

Hinweise zur KI-Verarbeitung

Die produktive Datenhaltung und die Originalunterlagen liegen in Deutschland/EU. Generative Textfunktionen nutzen primär den IONOS AI Model Hub in Deutschland. Übermittelt wird nur der erforderliche, möglichst minimierte oder pseudonymisierte Textkontext. Nach Anbieterangaben erfolgt die Inferenz zustandslos und ohne Nutzung zum Modelltraining.

Bis zur technischen Aktivierung und dokumentierten Abnahme des IONOS-Primärpfads kann Anthropic, PBC, USA, als ausdrücklich konfigurierbarer Übergangs-Fallback eingesetzt werden. Für diesen möglichen Drittlandpfad gelten DPA und, soweit erforderlich, EU-Standardvertragsklauseln. Nach erfolgreicher IONOS-Abnahme wird der Fallback deaktiviert. Änderungen werden nach Ziffer 6 dokumentiert und nicht stillschweigend vorgenommen.

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-Telefonkern nur kurzzeitig bis Transkription und Antwort; Tickets/Vorgänge nach Praxisregel; Konten bis Vertragsende und anschließender technischer Abwicklung.
Recruit	Abgeschlossene/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	Gesperpte 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. Offene Platzhalter und aktivierte optionale Dienste sind vor Unterzeichnung zu vervollständigen.

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

Rechtsgrundlagen und Orientierung

Art. 28 und 32 DSGVO: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679>

EU-Standardvertragsklauseln Verantwortlicher/Auftragsverarbeiter, Beschluss (EU) 2021/915:

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915>

Formulierungshilfe des Bayerischen Landesamts für Datenschutzaufsicht:

https://www.lida.bayern.de/media/muster/formulierungshilfe_av.pdf