DigitalAnstehen.

# Vertrag zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) für die Nutzung der digitalen Warteschlange „DigitalAnstehen“

zwischen

**AUFTRAGGEBER (VERANTWORTLICHER)**

_____

_____

_____

_____

Firma, Anschrift, Ansprechpartner

**AUFTRAGNEHMER (AUFTRAGSVERARBEITER)**

Julian Reiter
Gedankraum
Anschrift siehe gedankraum.de/impressum
E-Mail: info@gedankraum.de
Web: digitalanstehen.de

## § 1 Gegenstand und Dauer

1. Der Auftragnehmer stellt dem Auftraggeber die Software „DigitalAnstehen“ als Online-Dienst bereit. Damit betreibt der Auftraggeber digitale Warteschlangen (z. B. auf Messen, in Praxen, Ämtern oder bei Veranstaltungen). Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.
2. Dieser Vertrag gilt für alle Warteschlangen, die der Auftraggeber bei DigitalAnstehen anlegt oder bucht, einschließlich des kostenlosen Testlaufs. Er gilt, solange der Auftragnehmer für den Auftraggeber Daten verarbeitet, und endet ohne gesonderte Kündigung, wenn alle Daten nach § 9 gelöscht sind.
3. Die Leistungsbeschreibung und die Preise ergeben sich aus der Buchung und den Angaben auf digitalanstehen.de. Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes vor.

## § 2 Art und Zweck der Verarbeitung, Art der Daten, Betroffene

| | |
|---|---|
| **Zweck** | Verwaltung einer Warteschlange: Vergabe von Wartenummern, Anzeige von Position und Wartezeit, Aufruf und Benachrichtigung der Wartenden, Auswertung der Wartezeiten; optional Erfassung von Einwilligungen in Werbung per E-Mail („Leads“) und Beantwortung von Fragen durch einen KI-Assistenten. |
| **Betroffene Personen** | Besucher, Kunden, Patienten oder Interessenten des Auftraggebers, die sich in eine Warteschlange einreihen; Mitarbeiter des Auftraggebers, die die Warteschlange bedienen. |
| **Datenarten** | • Wartedaten: Wartenummer, Status, Zeitpunkte (angestellt, aufgerufen, beendet), Schalter, gewählte Sprache<br>• Antworten auf vom Auftraggeber festgelegte Felder (z. B. „Anzahl Personen“, „Gewünschte Demo“), auch während der Wartezeit, sowie ein optionaler Name, den Mitarbeiter manuell eintragen |

| | |
|---|---|
| | • Bewertung und Gesprächsnotiz, die Mitarbeiter des Auftraggebers nach dem Gespräch erfassen<br>• freiwillige Kontaktdaten für Benachrichtigungen: Mobilnummer oder E-Mail-Adresse<br>• nur bei eingeschalteter Lead-Erfassung und nach ausdrücklicher Einwilligung: E-Mail-Adresse, optional Name und Firma, Wortlaut und Zeitpunkt der Einwilligung, Zeitpunkt der Bestätigung<br>• Nachrichten an den KI-Assistenten, soweit Besucher ihn nutzen<br>• technische Daten: IP-Adresse ausschließlich als gekürzter, gesalzener Hashwert zur Missbrauchsabwehr |
| **Besondere Kategorien** | Der Dienst ist nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) vorgesehen. Der Auftraggeber legt keine Felder an, mit denen z. B. Gesundheitsdaten oder Behandlungsgründe abgefragt werden. Für den Betrieb genügen Wartenummern; Namen sind nicht erforderlich. |

## § 3 Weisungen des Auftraggebers

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet; in diesem Fall teilt er dem Auftraggeber dies vorher mit, soweit das Gesetz es nicht verbietet.
2. Die Weisungen ergeben sich aus diesem Vertrag und aus den Einstellungen, die der Auftraggeber in der Verwaltung seiner Warteschlange vornimmt (z. B. Felder, Benachrichtigungsarten, Lead-Erfassung, Nachfass-Mail, Löschen von Einträgen). Richtet der Auftraggeber eine CRM-Anbindung oder einen Webhook ein, übermittelt der Auftragnehmer bestätigte Leads auf dessen Weisung an das vom Auftraggeber gewählte System; dieses ist kein Unterauftragsverarbeiter des Auftragnehmers. Weitere Weisungen erteilt der Auftraggeber in Textform an info@gedankraum.de.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin und darf ihre Ausführung bis zur Bestätigung aussetzen.

## § 4 Pflichten des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Information der Betroffenen (Art. 13 DSGVO) und – bei der Lead-Erfassung – für einen zutreffenden Einwilligungstext, einen Link zu seiner eigenen Datenschutzerklärung und für eine Verwendung der Leads nur im Rahmen der erteilten Einwilligung.
2. Der Auftraggeber hält den geheimen Verwaltungs-Link vertraulich und gibt ihn nur an Personen weiter, die die Warteschlange bedienen sollen. Er informiert den Auftragnehmer unverzüglich, wenn der Link Unbefugten bekannt geworden sein könnte; der Auftragnehmer stellt dann einen neuen Link aus.

## § 5 Vertraulichkeit

Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Derzeit erbringt der Auftragnehmer die Leistung persönlich.

## § 6 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in **Anlage 1** beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er.

## § 7 Unterauftragsverarbeiter

1. Der Auftraggeber stimmt dem Einsatz der in **Anlage 2** genannten Unterauftragsverarbeiter zu.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vorher in Textform über die Hinzuziehung oder den Austausch eines Unterauftragsverarbeiters. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen; kann keine Lösung gefunden werden, darf er den Vertrag kündigen und erhält bereits gezahlte Entgelte für nicht genutzte Zeiträume anteilig zurück.
3. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Datenschutzniveau. Eine Übermittlung in Drittländer erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

## § 8 Unterstützung des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Beantwortung von Anträgen Betroffener (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). In der Verwaltung kann der Auftraggeber einzelne Einträge und Leads selbst löschen und als CSV-Datei exportieren. Erreicht ein Antrag den Auftragnehmer direkt, leitet er ihn unverzüglich weiter.
2. Betroffene können ihre Einwilligung in die Lead-Erfassung über den Link in der Bestätigungs-E-Mail selbst widerrufen; die Daten werden dann sofort gelöscht.
3. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, soweit dies für ihn zumutbar und mit den ihm vorliegenden Informationen möglich ist.
4. Verletzungen des Schutzes personenbezogener Daten meldet der Auftragnehmer dem Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.

## § 9 Löschung und Rückgabe

| Daten | Löschung |
|---|---|
| Mobilnummer oder E-Mail für Benachrichtigungen | automatisch, sobald der Eintrag abgeschlossen ist (bedient, nicht erschienen, verlassen, entfernt oder Tag beendet) |
| Leads mit Einwilligung | automatisch nach 90 Tagen; unbestätigte Leads nach 7 Tagen; bei Widerruf sofort; jederzeit durch den Auftraggeber in der Verwaltung |
| Wartedaten ohne Kontaktdaten (für die Statistik), Bewertungen und Gesprächsnotizen | automatisch nach spätestens 13 Monaten |
| Nachrichten an den KI-Assistenten | werden beim Auftragnehmer nicht gespeichert; der Gesprächsverlauf liegt nur im Browser des Besuchers für die Dauer der Sitzung |

| | |
|---|---|
| Alle Daten einer Warteschlange | auf Weisung des Auftraggebers innerhalb von 14 Tagen nach Vertragsende oder Anforderung; vorher stellt der Auftragnehmer die Daten auf Wunsch als CSV-Datei bereit |

Gesetzliche Aufbewahrungspflichten des Auftragnehmers (z. B. für Rechnungen) bleiben unberührt; sie betreffen nur Daten des Auftraggebers, nicht der Wartenden.

### § 10 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind, und ermöglicht Überprüfungen nach vorheriger Anmeldung mit angemessener Frist, zu üblichen Geschäftszeiten und ohne Störung des Betriebs. Die Überprüfung kann auch durch schriftliche Auskünfte erfolgen.

### § 11 Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die gesetzlichen Bestimmungen.
2. Änderungen und Ergänzungen bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.
3. Es gilt deutsches Recht.

Ort, Datum, Unterschrift Auftraggeber

Ort, Datum, Unterschrift Auftragnehmer
Julian Reiter

# Anlage 1
# Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

**Vertraulichkeit**

- **Zutritt:** Die Server stehen in einem Rechenzentrum des Hosting-Anbieters in Deutschland (Anlage 2). Zutrittskontrolle, Überwachung und Brandschutz stellt der Anbieter sicher.
- **Zugang zum Server:** Administration ausschließlich über verschlüsselte Verbindungen (SSH) durch den Auftragnehmer persönlich. Zugangsdaten und Programmschlüssel liegen außerhalb des öffentlichen Webverzeichnisses.
- **Zugriff auf die Verwaltung:** nur mit einem geheimen, zufällig erzeugten Verwaltungs-Link (256 Bit). Jede Warteschlange hat ihren eigenen Link; Daten anderer Kunden sind darüber nicht erreichbar.
- **Zugriff für Besucher:** Besucher sehen nur ihren eigenen Eintrag über ein zufälliges Kennzeichen (128 Bit). Öffentliche Anzeigen zeigen nur Wartenummern, keine Namen oder Kontaktdaten.
- **Datensparsamkeit:** Für die Teilnahme sind keine Namen, Konten oder Apps nötig. Kontaktdaten sind freiwillig. IP-Adressen werden nicht im Klartext gespeichert, sondern nur als gesalzener Hashwert zur Begrenzung von Missbrauch.
- **Trennung:** Die Daten aller Kunden liegen logisch getrennt nach Warteschlange; jede Abfrage ist an die jeweilige Warteschlange gebunden.

**Integrität**

- **Übertragung:** Alle Seiten und Schnittstellen sind nur verschlüsselt per HTTPS (TLS) erreichbar. SMS werden über eine verschlüsselte Schnittstelle an den SMS-Dienstleister übergeben.
- **Eingaben:** Alle Eingaben werden serverseitig geprüft und begrenzt; Datenbankzugriffe erfolgen über vorbereitete Abfragen (Schutz vor SQL-Injection), Ausgaben werden maskiert.
- **Missbrauchsschutz:** Begrenzung der Anfragen je Gerät und Zeitraum für Anmeldungen, KI-Assistent und Anfragen.
- **Nachweis von Einwilligungen:** Bei Leads werden Wortlaut, Zeitpunkt der Einwilligung und – bei Double-Opt-in – Zeitpunkt der Bestätigung gespeichert.

**Verfügbarkeit und Belastbarkeit**

- Betrieb auf einem Server mit Speicherreserven und regelmäßigen Sicherheitsupdates des Betriebssystems.
- Vor Änderungen an der Software werden Sicherungskopien der betroffenen Dateien und Datenbanktabellen erstellt.
- Fällt die Benachrichtigung per SMS oder E-Mail aus, bleibt die Warteschlange über die Besucherseite und die Bildschirm-Anzeige nutzbar.

**Verfahren zur regelmäßigen Überprüfung**

- Automatische Löschung nach den Fristen in § 9.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich und bei wesentlichen Änderungen der Software.

# Anlage 2
# Unterauftragsverarbeiter

| Unternehmen | Leistung | Ort der Verarbeitung |
|---|---|---|
| netcup GmbH<br>Daimlerstraße 25<br>76185 Karlsruhe | Hosting des Servers (Webseiten, Datenbank, E-Mail-Versand) | Deutschland |
| seven communications GmbH & Co. KG (seven.io)<br>Willestr. 4–6<br>24103 Kiel | Versand von SMS-Benachrichtigungen; nur wenn ein Besucher SMS wählt (Mobilnummer und Nachrichtentext) | Deutschland |
| Anthropic, PBC<br>San Francisco, USA | KI-Assistent „Claude“; nur wenn ein Besucher dem Assistenten eine Frage stellt (Frage, Name der Warteschlange, Position und Wartezeit; keine Kontaktdaten) | USA; Übermittlung auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO) bzw. der EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) |

Bindet der Auftraggeber auf der Warteseite ein Video von YouTube oder Vimeo ein, wird es erst nach einem Klick des Besuchers geladen; die Verantwortung für diese Einbindung liegt beim Auftraggeber. Der Auftraggeber kann die SMS-Benachrichtigung in der Verwaltung abschalten und den KI-Assistenten auf Anfrage für seine Warteschlange abschalten lassen; die betreffenden Unterauftragsverarbeiter erhalten dann keine Daten aus seiner Warteschlange.