Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) für das Produkt „Google-Bewertungen“ (Bewertungsautomatisierung)

VERANTWORTLICHER (AUFTRAGGEBER)

Firma / Name

Anschrift

vertreten durch

– nachfolgend „Auftraggeber“ –

AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

Sinkaro, Inhaber Daniel Kieselbach

Anschrift

E-Mail: d.kieselbach@sinkaro.de · Telefon: +49 176 72154319

– nachfolgend „Auftragnehmer“ –

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer richtet für den Auftraggeber die Bewertungsautomatisierung „Google-Bewertungen“ ein und betreibt sie (Hauptvertrag: Angebot / Auftrag vom _____). Dabei verarbeitet er personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Art, Zweck und Umfang der Verarbeitung, die Art der Daten und die betroffenen Personen ergeben sich aus **Anlage 1**.

(2) Die Vereinbarung gilt für die Dauer des Hauptvertrags. Sie endet automatisch mit dessen Beendigung, soweit sich aus den Regelungen zur Löschung und Rückgabe (§ 10) nichts anderes ergibt.

(3) Die Verarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Eine Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 2 Weisungsrecht

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Auftraggeber diese Verpflichtung vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

(2) Die Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung und den gemeinsam festgelegten Einstellungen der Bewertungsautomatisierung (z. B. Texte, Wartezeit, Erinnerung, Sperrfrist, Wege der Einwilligung, Löschfristen). Weitere Weisungen erteilt der Auftraggeber in Textform (z. B. per E-Mail).

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 3 Vertraulichkeit

Der Auftragnehmer setzt bei der Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Pflicht zur Vertraulichkeit gilt auch nach Ende dieser Vereinbarung fort.

§ 4 Sicherheit der Verarbeitung

(1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in **Anlage 2** beschrieben sind, und hält sie für die Dauer der Vereinbarung aufrecht.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das vereinbarte Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen teilt er dem Auftraggeber mit.

§ 5 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt den Einsatz der in **Anlage 3** genannten Unterauftragsverarbeiter.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vorher in Textform über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung). Der Auftraggeber kann der Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb von zwei Wochen widersprechen. Kommt keine Einigung zustande, können beide Seiten den Hauptvertrag für das betroffene Produkt außerordentlich kündigen.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieser Vereinbarung entsprechen (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für deren Einhaltung.

(4) Keine Unterauftragsverarbeiter im Sinne dieser Vereinbarung sind Dienste, die der Auftraggeber selbst beauftragt und für die er eigene Verträge hat – insbesondere sein **E-Mail-Postfach** und sein **Google-Unternehmensprofil**; auf das Google-Profil greift der Auftragnehmer nicht zu (es wird nur der öffentliche Bewertungslink verwendet). Der Auftragnehmer greift darauf nur mit den vom Auftraggeber erteilten Zugängen und nur im Umfang dieser Vereinbarung zu.

§ 6 Rechte der betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Art. 12 bis 23 DSGVO, z. B. Auskunft, Berichtigung, Löschung). Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst, soweit der Auftraggeber nichts anderes anweist.

§ 7 Weitere Unterstützungspflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der ihm vorliegenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(2) 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 sie ihm vorliegen. Er ergreift unverzüglich Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

(3) Der Auftragnehmer hat nach eigener Prüfung keinen Datenschutzbeauftragten zu benennen, da die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG nicht vorliegen. Ansprechpartner für den Datenschutz ist der Inhaber (Kontakt siehe oben).

§ 8 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Information der betroffenen Personen (Datenschutzhinweis auf seiner Website) und für den Inhalt der Bewertungsanfragen. Der Auftragnehmer stellt einen Datenschutz-Textbaustein und einen Muster-Satz für die Einwilligung zur Verfügung.

(2) Bewertungsanfragen per E-Mail oder SMS dürfen nur mit vorheriger ausdrücklicher Einwilligung der betroffenen Person verschickt werden (§ 7 Abs. 2 UWG). Meldet der Auftraggeber eine schriftlich erteilte Einwilligung (z. B. Kreuz im Formular „Auftrag erledigt“), versichert er, dass sie vorliegt, freiwillig erteilt wurde und von ihm aufbewahrt wird. Der Auftraggeber bietet für Bewertungen keine Gegenleistung an und wählt die angefragten Kunden nicht nach ihrer Zufriedenheit aus (Richtlinien von Google).

(3) Der Auftraggeber sorgt dafür, dass in Freitextfeldern (z. B. Positionstexte, Hinweise) keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO (z. B. Gesundheitsdaten) erfasst werden, soweit

dies nicht ausdrücklich vereinbart ist.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 9 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. Inspektionen werden mit angemessener Frist, in der Regel mindestens zwei Wochen, angekündigt und während der üblichen Geschäftszeiten ohne vermeidbare Störung des Betriebs durchgeführt. Bei Unterauftragsverarbeitern kann der Nachweis auch durch deren Zertifikate, Prüfberichte oder Auftragsverarbeitungsverträge erbracht werden.

§ 10 Löschung und Rückgabe

(1) Während der Laufzeit löscht die Bewertungsautomatisierung abgeschlossene Anfragen und Versandprotokolle automatisch nach der vereinbarten Frist (Standard: **90 Tage**), Nachweise von Einwilligungen nach **3 Jahren** (siehe Anlage 1).

(2) Nach Ende des Hauptvertrags löscht der Auftragnehmer alle im Auftrag verarbeiteten Daten innerhalb von **30 Tagen** und entfernt seine Zugänge zum Postfach des Auftraggebers; Zustimmungs-Seite und Links in versandten Nachrichten werden ungültig – es sei denn, eine gesetzliche Pflicht zur Speicherung besteht. Auf Wunsch übergibt er dem Auftraggeber vorher eine Kopie der noch vorhandenen Daten in einem gängigen Format (z. B. CSV) – insbesondere die Nachweise der Einwilligungen und die Sperrliste. Die Löschung bestätigt er in Textform.

(3) Nachrichten im Postfach und Bewertungen im Google-Profil des Auftraggebers verbleiben beim Auftraggeber und sind von der Löschung nach Absatz 2 nicht betroffen.

§ 11 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrags, soweit diese Vereinbarung nichts anderes bestimmt.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Bei Widersprüchen geht diese Vereinbarung in Fragen des Datenschutzes dem Hauptvertrag vor.

(2) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem Gewollten und den Anforderungen des Art. 28 DSGVO am nächsten kommt.

(3) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Ort, Datum	Ort, Datum
Auftraggeber (Unterschrift, Name in Druckbuchstaben)	Auftragnehmer – Sinkaro, Daniel Kieselbach

Anlage 1 Einzelheiten der Verarbeitung

Gegenstand und Zweck

Automatisierte Bitte um eine Google-Bewertung für den Auftraggeber: Entgegennahme erledigter Aufträge (aus dem Produkt „Zahlungserinnerung & Mahnung“, über ein Formular oder eine Schnittstelle), Verwaltung und Nachweis der Einwilligungen der Kunden (Häkchen auf der Angebots-Annahmeseite, Zustimmungs-Seite mit Bestätigung per E-Mail, vom Auftraggeber gemeldete schriftliche Einwilligung), Versand der Bitte und höchstens einer Erinnerung, Weiterleitung zum Bewertungsformular bei Google mit Zählung des Klicks, Abmeldung und Sperrliste, Monatsbericht an den Auftraggeber sowie Protokollierung des Versands.

Vereinbarter Umfang (bitte ankreuzen)

- ☐ Formular „Auftrag erledigt“ von Sinkaro
- ☐ Auslöser „Rechnung bezahlt“ (AV-Vertrag „Zahlungen“ gilt zusätzlich)
- ☐ Einwilligung auf der Angebots-Annahmeseite (AV-Vertrag „Angebote“ gilt zusätzlich)
- ☐ Zustimmungs-Seite mit QR-Code (Double-Opt-in)
- ☐ Bitte zusätzlich per SMS (Unterauftragsverarbeiter Nr. 2)
- ☐ Schnittstelle zur Software / Website des Auftraggebers

Kategorien betroffener Personen

- Kunden des Auftraggebers mit erledigtem Auftrag (Privatpersonen sowie Ansprechpartner von Firmen)
- Personen, die über die Zustimmungs-Seite eine Einwilligung abgeben
- Mitarbeitende und Ansprechpartner des Auftraggebers (Name, geschäftliche Kontaktdaten)

Arten personenbezogener Daten

BEREICH	DATEN
Kontaktdaten	Name, E-Mail-Adresse, ggf. Mobilnummer und Einwilligung zur SMS
Auftragsdaten	Auftrags- bzw. Rechnungsnummer, Zeitpunkt „Auftrag erledigt“, Quelle der Meldung
Einwilligungen	Zeitpunkt, Quelle (z. B. „Häkchen bei Annahme des Angebots AN-…“), bei Webseiten zusätzlich IP-Adresse und Browserkennung, bei der Zustimmungs-Seite Zeitpunkt und IP-Adresse der Bestätigung; Widerruf
Vorgangsdaten	Status (geplant, verschickt, erinnert, geklickt, abgemeldet, ohne Einwilligung), Zeitpunkte von Bitte, Erinnerung und Klick
Sperrliste	E-Mail-Adresse bzw. Mobilnummer abgemeldeter Personen, Zeitpunkt der Abmeldung
Kommunikation	Inhalt, Betreff, Empfänger und Zeitpunkt versandter Nachrichten (E-Mail, ggf. SMS); Monatsbericht an den Auftraggeber
Technische Daten	Zeitstempel, interne Kennungen, Zugangsschlüssel der Links, Fehlermeldungen

Inhalte der Bewertungen bei Google werden nicht verarbeitet; Google verarbeitet sie in eigener Verantwortung. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht planmäßig verarbeitet.

Art der Verarbeitung

Erheben, Speichern, Abgleichen (Einwilligung, Sperrliste, Sperrfrist), Verwenden zum Versand von Nachrichten, Weiterleiten zu Google, Auswerten in zusammengefasster Form (Monatsbericht), Übermitteln an den Auftraggeber, Löschen.

Speicherorte und Löschfristen

ORT	INHALT UND FRIST

Automatisierungsplattform (n8n Cloud, EU)	Anfragen und Versandprotokolle: automatische Löschung **90 Tage** nach Abschluss bzw. Versand (abweichende Frist: _____ Tage). Nachweise der Einwilligungen: **3 Jahre** nach Erteilung, danach Löschung 90 Tage später. Unbestätigte Zustimmungen der Zustimmungs-Seite: nach 3 Tagen unwirksam, Löschung 90 Tage später. Sperrliste: für die Dauer des Hauptvertrags (Beachtung des Widerspruchs). Monatskennzahlen ohne Personenbezug: 13 Monate. Technische Ausführungsprotokolle der Plattform: nach der Frist des Plattform-Tarifs (derzeit höchstens _____ Tage).
E-Mail-Postfach des Auftraggebers	Gesendete Nachrichten, Antworten der Kunden und Monatsberichte verbleiben beim Auftraggeber.
Unterlagen des Auftraggebers	Schriftliche Einwilligungen (Auftrag, Arbeitszettel) bewahrt der Auftraggeber selbst auf.

Anlage 2 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- **Zutritts- und Zugangskontrolle:** Es werden keine eigenen Server betrieben. Die Plattform läuft in Rechenzentren des Anbieters in der EU (siehe Anlage 3). Zugang zur Plattform nur für den Auftragnehmer, geschützt durch individuelles, starkes Passwort und Zwei-Faktor-Anmeldung. Arbeitsgeräte sind verschlüsselt und mit Sperrbildschirm gesichert.
- **Zugriffskontrolle:** Der Zugang zum Postfach des Auftraggebers (App-Passwort) wird ausschließlich im verschlüsselten Zugangsdaten-Speicher der Plattform hinterlegt, nicht in Klartext und nicht auf Arbeitsgeräten. Der Auftraggeber kann ihn jederzeit selbst widerrufen. Ein Zugang zum Google-Konto des Auftraggebers wird nicht benötigt.
- **Trennung:** Daten verschiedener Auftraggeber werden über eine eindeutige Kennung je Auftraggeber logisch getrennt verarbeitet; jeder Auftraggeber hat einen eigenen Ablauf mit eigenen Einstellungen und eigenen Zugangsdaten.
- **Schutz der Links:** Bewertungs- und Abmeldelinks enthalten zufällige, nicht erratbare Schlüssel je Vorgang. Das Aufrufen der Abmelde- und Bestätigungsseiten zeigt nur an; Änderungen werden erst nach einem bewussten Klick ausgeführt, automatische Link-Prüfungen von Mailprogrammen lösen nichts aus. Schnittstellen sind durch geheime Schlüssel gesichert.
- **Zustimmungs-Seite:** Einwilligungen werden erst nach Bestätigung per E-Mail wirksam (Double-Opt-in); Schutz vor automatisierten Eintragungen durch eine Falle für Bots, Begrenzung der Anzahl offener Zustimmungen und keine doppelte Bestätigungsmail an dieselbe Adresse innerhalb von 30 Minuten.

2. Integrität

- **Weitergabekontrolle:** Übertragungen erfolgen verschlüsselt (HTTPS/TLS; E-Mail-Versand über SSL/TLS). Keine Weitergabe an Dritte außer an die Unterauftragsverarbeiter nach Anlage 3 und an die betroffene Person selbst; Google erhält vom Auftragnehmer keine Daten (der Kunde wird nur weitergeleitet).
- **Eingabekontrolle:** Jede versandte Nachricht wird mit Empfänger, Inhalt, Zeitpunkt und Ergebnis protokolliert; jede Einwilligung mit Zeitpunkt, Quelle und Nachweis gespeichert. Änderungen an Abläufen und Einstellungen erfolgen ausschließlich durch den Auftragnehmer über eine versionierte Konfiguration.
- **Schutz vor unzulässigem Versand:** Ohne gespeicherte Einwilligung wird keine Bitte verschickt; Adressen auf der Sperrliste werden vor jedem Versand geprüft; je Kunde höchstens eine Bitte innerhalb der vereinbarten Sperrfrist.
- **Testbetrieb:** Vor dem Livegang laufen Tests mit einer Freigabeliste – echte Nachrichten gehen dann nur an vom Auftraggeber benannte Testadressen.

3. Verfügbarkeit und Belastbarkeit

- Betrieb auf einer professionell gehosteten Plattform mit Datensicherung durch den Anbieter.
- Automatische Wiederholung bei Versandstörungen; schlägt der Versand endgültig fehl, wird der Auftragnehmer sofort per Alarm benachrichtigt.
- Täglicher Lauf (werktags): fällige Bitten und Erinnerungen werden nachgeholt, abgelaufene Zustimmungen und Nachweise beendet.

4. Datenschutz durch Technikgestaltung und Löschung

- Datenminimierung: nur Name, Kontaktdaten und Auftragsbezug; keine Inhalte der Bewertungen; keine Nutzung für Werbung oder eigene Zwecke des Auftragnehmers.
- Höchstens eine Erinnerung; Ende sofort bei Klick oder Abmeldung. Eine Einwilligung wird für genau eine Bitte verwendet.
- Automatische Löschung nach Anlage 1; Löschung aller Daten nach Vertragsende (§ 10).

5. Verfahren zur regelmäßigen Überprüfung

- Überprüfung der Maßnahmen mindestens jährlich sowie bei wesentlichen Änderungen der Plattform oder der Unterauftragsverarbeiter.
- Auswertung von Fehler- und Alarmmeldungen; Dokumentation von Datenschutzvorfällen.

Anlage 3 Genehmigte Unterauftragsverarbeiter

NR.	UNTERNEHMEN	LEISTUNG	ORT DER VERARBEITUNG
1	**n8n GmbH** Novalisstr. 10, 10115 Berlin HRB 212509 B, AG Charlottenburg	Betrieb der Automatisierungsplattform (n8n Cloud): Ausführung der Abläufe, Zustimmungs- und Abmeldeseiten, Speicherung von Vorgängen, Einwilligungen und Protokollen, Zugangsdaten-Speicher	EU – Rechenzentrum in Frankfurt am Main (Deutschland) laut Anbieter. n8n setzt seinerseits Unterauftragsverarbeiter ein (u. a. für das Hosting); Liste im Datenschutzbereich von n8n.
2	**seven communications GmbH & Co. KG** Willestr. 4-6, 24103 Kiel HRA 11707 KI, AG Kiel	Versand von SMS – **nur wenn SMS vereinbart sind** (Anlage 1)	Deutschland / EU

> **Nicht als Unterauftragsverarbeiter eingesetzt:** der E-Mail-Anbieter des Auftraggebers und Google (Unternehmensprofil und Bewertungen) – diese Dienste nutzt der Auftraggeber bzw. der Kunde auf Grundlage eigener Verträge (§ 5 Abs. 4). Für Angebote und Rechnungen gelten die Vereinbarungen zu den Produkten „Angebote & Nachfassen“ bzw. „Zahlungserinnerung & Mahnung“.

Kontakt für Datenschutzfragen

Sinkaro · Daniel Kieselbach · d.kieselbach@sinkaro.de · +49 176 72154319