Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) für das Produkt „Zahlungserinnerung & Mahnung“ (Zahlungsautomatisierung)

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 Zahlungsautomatisierung „Zahlungserinnerung & Mahnung“ 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 Zahlungsautomatisierung (z. B. Texte, Zahlungsziel, Zeitpunkte der Erinnerungen und Mahnungen, Freigabe, Löschfrist). 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**, sein **Rechnungsprogramm** (z. B. Lexware Office, sevDesk) und ggf. sein **Google-Kalender**. 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 z. B. auf seiner Website oder in der Rechnung), und für den Inhalt seiner Rechnungen, Erinnerungen und Mahnungen (z. B. Pflichtangaben, Fristen, Hinweise auf Verzugszinsen). Der Auftragnehmer stellt einen Datenschutz-Textbaustein zur Verfügung.

(2) Der Auftraggeber bewahrt Rechnungen, Stornorechnungen und Mahnungen in eigenen Unterlagen auf und gibt sie an seine Buchhaltung weiter. Die Zahlungsautomatisierung ist kein Archiv im Sinne handels- oder steuerrechtlicher Aufbewahrungspflichten. Für Nachrichten per SMS holt der Auftraggeber, soweit erforderlich, die Einwilligung der betroffenen Person ein.

(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 Zahlungsautomatisierung abgeschlossene Vorgänge und Versandprotokolle automatisch nach der vereinbarten Frist (Standard: **90 Tage**, 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 und ggf. zum Rechnungsprogramm des Auftraggebers; der Link zum Rechnungs-Editor wird 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). Die Löschung bestätigt er in Textform.

(3) Rechnungen im Rechnungsprogramm und Nachrichten im Postfach 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 Rechnungsstellung und Zahlungserinnerung für den Auftraggeber: Erstellung von Rechnungen und Stornorechnungen als PDF (über den Rechnungs-Editor, aus einem angenommenen Angebot des Produkts „Angebote & Nachfassen“ oder als wiederkehrende Monatsrechnung), Freigabe durch den Auftraggeber, Versand an den Kunden, Erfassung von Zahlungseingängen, Zahlungserinnerung und Mahnungen in Stufen bei ausbleibender Zahlung, Übernahme offener Rechnungen und Zahlungsstände aus dem Rechnungsprogramm des Auftraggebers, Information des Auftraggebers (Vorwarnungen, Belege, Wochenübersicht) sowie Protokollierung des Versands.

Vereinbarter Umfang (bitte ankreuzen)

- ☐ Rechnungs-Editor / Formulare von Sinkaro
- ☐ Rechnung aus angenommenem Angebot (AV-Vertrag „Angebote“ gilt zusätzlich)
- ☐ Übernahme aus Lexware Office (nur Lesezugriff)
- ☐ Übernahme aus sevDesk (nur Lesezugriff)
- ☐ Erinnerung zusätzlich per SMS (Unterauftragsverarbeiter Nr. 2)
- ☐ Antworten im Posteingang erkennen (IMAP)
- ☐ Weitermeldung „bezahlt“ an das Produkt „Google-Bewertungen“

Kategorien betroffener Personen

- Kunden des Auftraggebers, die eine Rechnung erhalten (Privatpersonen sowie Ansprechpartner von Firmen)
- Mitarbeitende und Ansprechpartner des Auftraggebers (Name, geschäftliche Kontaktdaten)

Arten personenbezogener Daten

BEREICH	DATEN
Kontaktdaten	Name, ggf. Firma, Anschrift, E-Mail-Adresse, ggf. Telefon-/Mobilnummer und SMS-Einwilligung
Rechnungsdaten	Rechnungsnummer, Rechnungs- und Leistungsdatum, Positionen (Leistung, Beschreibung, Menge, Einheit, Preis), Summen netto/USt./brutto, Zahlungsziel, Bezug zum Angebot, die erzeugten PDFs (Rechnung, Stornorechnung, Erinnerung, Mahnungen)
Zahlungsdaten	Zahlungseingänge (Datum, Betrag, Art der Erfassung), offener Betrag; keine Kontoverbindungen der Kunden
Vorgangsdaten	Status (Entwurf, versendet, erinnert, gemahnt, angehalten, pausiert, bezahlt, storniert), Zeitpunkte der Erinnerungen und Mahnungen, Vertragsdaten für Monatsrechnungen (Startdatum, Monatsbetrag)
Daten aus dem Rechnungsprogramm	nur bei vereinbarter Übernahme: Rechnungsliste (Nummer, Datum, Fälligkeit, Betrag, offener Betrag, Status) und E-Mail-Adresse bzw. Name des zugehörigen Kontakts
Kommunikation	Inhalt, Betreff, Empfänger und Zeitpunkt versandter Nachrichten (E-Mail, ggf. SMS)
Eingehende E-Mails	nur bei vereinbarter Antwort-Erkennung: neue E-Mails mit „Rechnung“ im Betreff – ausgewertet werden Absender und Betreff; der Inhalt wird nicht im Vorgang gespeichert, nur in den technischen Ausführungsprotokollen
Technische Daten	Zeitstempel, interne Kennungen, Zugangsschlüssel der Links, Fehlermeldungen

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht planmäßig verarbeitet.

Art der Verarbeitung

Erheben, Abrufen (aus dem Rechnungsprogramm), Speichern, Abgleichen, Erstellen von Dokumenten (PDF), Vergabe fortlaufender Rechnungsnummern, Verwenden zum Versand von Nachrichten, Übermitteln an den Auftraggeber und an die betroffene Person selbst, Löschen.

Speicherorte und Löschfristen

ORT	INHALT UND FRIST
Automatisierungsplattform (n8n Cloud, EU)	Vorgänge und Versandprotokolle: automatische Löschung **90 Tage** nach Abschluss eines Vorgangs bzw. nach Versand (abweichende Frist: _____ Tage). Technische Ausführungsprotokolle der Plattform: automatische Löschung nach der Frist des Plattform-Tarifs (derzeit höchstens _____ Tage). Die PDFs werden bei jedem Versand neu erzeugt und nicht gesondert gespeichert. Ausgenommen ist der Zähler des Nummernkreises (nur Jahr und letzte Nummer, ohne personenbezogene Daten).
Rechnungsprogramm des Auftraggebers	Rechnungen, Zahlungen und Kontakte verbleiben beim Auftraggeber (eigener Vertrag mit dem Anbieter); der Auftragnehmer liest nur.
E-Mail-Postfach des Auftraggebers	Gesendete Nachrichten, Antworten der Kunden und die Beleg-Mails mit den Rechnungs-PDFs verbleiben beim Auftraggeber.

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:** Zugänge zum Postfach und zum Rechnungsprogramm des Auftraggebers (App-Passwort, API-Schlüssel) werden ausschließlich im verschlüsselten Zugangsdaten-Speicher der Plattform hinterlegt, nicht in Klartext und nicht auf Arbeitsgeräten. Den API-Schlüssel erstellt der Auftraggeber selbst; die Automatisierung ruft damit nur Rechnungen und Kontakte ab und schreibt nichts in das Rechnungsprogramm. Der Auftraggeber kann alle Zugänge jederzeit selbst widerrufen.
- **Antwort-Erkennung (falls vereinbart):** Der Zugang zum Posteingang wird ausschließlich zum Lesen genutzt. Abgerufen werden nur neue E-Mails mit „Rechnung“ im Betreff; sie bleiben ungelesen und werden weder verschoben noch gelöscht. Abwesenheitsnotizen und Rundschreiben werden verworfen.
- **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:** Der Rechnungs-Editor ist nur über einen Link mit geheimem Schlüssel je Auftraggeber erreichbar; der Schlüssel kann jederzeit ausgetauscht werden. Links in den Nachrichten an den Auftraggeber (Freigeben, Bezahlt, Nicht mahnen, Stornieren, Pausieren) enthalten zufällige, nicht erratbare Schlüssel je Vorgang. Kunden erhalten keine Links mit Handlungsmöglichkeiten. Das Aufrufen eines Links zeigt nur an; Änderungen werden erst nach einem bewussten Klick auf „Absenden“ ausgeführt, automatische Link-Prüfungen von Mailprogrammen lösen nichts aus. Schnittstellen sind durch geheime Schlüssel gesichert.

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.
- **Eingabekontrolle:** Jede versandte Nachricht wird mit Empfänger, Inhalt, Zeitpunkt und Ergebnis protokolliert; Zahlungseingänge werden mit Datum, Betrag und Art der Erfassung gespeichert. Rechnungsnummern werden fortlaufend und lückenlos vergeben; verworfene Entwürfe verbrauchen keine Nummer, versendete Rechnungen werden nur durch Stornorechnung aufgehoben. Änderungen an Abläufen und Einstellungen erfolgen ausschließlich durch den Auftragnehmer über eine versionierte Konfiguration.
- **Vier-Augen-Prinzip:** Neue Rechnungen gehen standardmäßig erst nach Freigabe durch den Auftraggeber an den Kunden; vor jeder Erinnerung und Mahnung erhält der Auftraggeber eine Vorwarnung und kann sie anhalten.
- **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 Sicherheitslauf: fällige Erinnerungen und Mahnungen werden nachgeholt (nur an Werktagen), der Abgleich mit dem Rechnungsprogramm wird ausgeführt. Ist das Rechnungsprogramm nicht erreichbar, wird der Auftraggeber informiert; bereits bekannte Vorgänge laufen weiter.

4. Datenschutz durch Technikgestaltung und Löschung

- Datenminimierung: nur die für Rechnungsversand und Zahlungserinnerung nötigen Daten; aus dem Rechnungsprogramm nur Rechnungen ab dem Tag der Einrichtung und die E-Mail-Adresse des Kontakts; keine Kontodaten der Kunden; keine Nutzung für Werbung oder eigene Zwecke des Auftragnehmers.
- Erinnerungen und Mahnungen enden automatisch nach der letzten Stufe sowie sofort bei Zahlung, Storno oder wenn der Auftraggeber sie anhält.
- 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, Erzeugung der PDFs, Speicherung von Vorgängen 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-Erinnerungen – **nur wenn SMS vereinbart sind** (Anlage 1)	Deutschland / EU

> **Nicht als Unterauftragsverarbeiter eingesetzt:** der E-Mail-Anbieter des Auftraggebers, sein Rechnungsprogramm (z. B. Lexware Office der Haufe-Lexware GmbH & Co. KG, sevDesk der sevDesk GmbH) und ggf. Google (Kalender) – diese Dienste nutzt der Auftraggeber auf Grundlage eigener Verträge (§ 5 Abs. 4). Für die Angebotsabwicklung gilt die Vereinbarung zum Produkt „Angebote & Nachfassen“.

Kontakt für Datenschutzfragen

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