Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) für das Produkt „Website“ (Erstellung, Hosting und Betrieb der Website des Auftraggebers)

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 erstellt für den Auftraggeber dessen Website, stellt sie im Internet bereit (Hosting) und betreibt sie einschließlich des Kontakt- bzw. Anfrageformulars (Hauptvertrag: Angebot / Auftrag vom). Dabei verarbeitet er personenbezogene Daten der Besucher der Website 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 grundsätzlich in einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Die Website wird über das weltweite Auslieferungsnetz des Hosting-Anbieters ausgeliefert; dabei ist eine Verarbeitung in Drittländern, insbesondere den USA, möglich. Sie erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO (siehe Anlage 3). Eine darüber hinausgehende Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

§ 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 Inhalten und Funktionen der Website (z. B. Felder des Anfrageformulars, Empfänger der Anfragen). 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 seine **Domain-Registrierung** und sein **E-Mail-Postfach**, an das Anfragen weitergeleitet werden.

§ 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 Impressum und Datenschutzerklärung seiner Website. Der Auftragnehmer stellt die technischen Angaben dafür zur Verfügung (eingesetzte Dienste, Speicherfristen, Formularfelder); die Rechtstexte selbst stellt der Auftraggeber, soweit nichts anderes vereinbart ist.

(2) Der Auftraggeber stellt sicher, dass er die Rechte an den gelieferten Inhalten hat und dass abgebildete Personen (z. B. Mitarbeitende auf Teamfotos) der Veröffentlichung zugestimmt haben.

(3) Sollen Dienste Dritter eingebunden werden, die Daten der Besucher verarbeiten oder eine Einwilligung erfordern (z. B. Besucherstatistik, Karten, Videos, Chat), wird dies vorher in Textform vereinbart und in Anlage 1 und 3 ergänzt.

(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 werden Anfragen aus dem Formular und Server-Protokolle automatisch nach den Fristen in Anlage 1 gelöscht.

(2) Nach Ende des Hauptvertrags nimmt der Auftragnehmer die Website vom Netz und löscht alle im Auftrag verarbeiteten personenbezogenen Daten innerhalb von **30 Tagen** – es sei denn, eine gesetzliche Pflicht zur Speicherung besteht. Die Übergabe der Website bzw. ihrer Inhalte richtet sich nach dem Hauptvertrag (Regelung bei Kündigung des Hostings noch festlegen). Die Löschung bestätigt der Auftragnehmer in Textform.

(3) Anfragen, die bereits an das Postfach des Auftraggebers weitergeleitet wurden, 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

Bereitstellung der Website des Auftraggebers im Internet (Hosting, Auslieferung, Schutz vor Angriffen und Missbrauch), Entgegennahme von Anfragen über das Kontakt- bzw. Anfrageformular und deren Weiterleitung an den Auftraggeber, Pflege von Inhalten im Auftrag sowie Fehlersuche und Wartung.

Vereinbarter Umfang (bitte ankreuzen)

- ☐ Hosting und Betrieb der Website
- ☐ Kontakt- bzw. Anfrageformular
- ☐ Weiterleitung der Anfragen per E-Mail über das Postfach des Auftragnehmers (Unterauftragsverarbeiter Nr. 3)
- ☐ Pflege von Inhalten im Auftrag (z. B. Teamfotos, Referenzen)

Online-Terminbuchung und weitere Automatisierungen auf der Website sind nicht Gegenstand dieser Vereinbarung; dafür gilt die Vereinbarung des jeweiligen Produkts.

Kategorien betroffener Personen

- Besucher der Website
- Interessenten und Kunden des Auftraggebers, die das Anfrageformular nutzen
- Mitarbeitende und Ansprechpartner des Auftraggebers, soweit sie auf der Website genannt oder abgebildet sind

Arten personenbezogener Daten

BEREICH	DATEN
Server-Protokolle	IP-Adresse, Zeitpunkt, aufgerufene Seite, übertragene Datenmenge, Browser und Betriebssystem, zuvor besuchte Seite (Referrer), Statuscode
Anfrageformular	Name, E-Mail-Adresse, Telefonnummer, Anliegen/Freitext, ggf. Ort bzw. Anschrift des Auftrags, Zeitpunkt und Bestätigung des Datenschutzhinweises
Inhalte der Website	Namen, Fotos und Funktionen von Mitarbeitenden und Ansprechpartnern des Auftraggebers, soweit geliefert
Technische Daten	Zeitstempel, interne Kennungen, Fehlermeldungen, Schutzmerkmale gegen Spam (z. B. Anzahl der Anfragen je IP-Adresse in kurzer Zeit)

Die Website setzt standardmäßig **keine Cookies zu Werbe- oder Statistikzwecken** und bindet keine Tracking-Dienste ein. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht planmäßig verarbeitet.

Art der Verarbeitung

Erheben, Speichern, Übermitteln an den Auftraggeber, Verwenden zum Schutz der Website, Löschen.

Speicherorte und Löschfristen

ORT	INHALT UND FRIST
Hosting-Plattform (Vercel, Funktionsregion Frankfurt)	Server-Protokolle: automatische Löschung nach der Frist des Plattform-Tarifs (derzeit höchstens _____ Tage). Formulardaten werden auf der Plattform nur zur Weiterleitung verarbeitet und nicht dauerhaft gespeichert.
Automatisierungsplattform (n8n Cloud, EU)	Anfragen und Versandprotokolle: automatische Löschung **90 Tage** nach Eingang (abweichende Frist: _____ Tage).
Quellcode-Verwaltung (GitHub)	Inhalte der Website (Texte, Bilder) bis zum Ende des Hauptvertrags; keine Besucher- oder Formulardaten.
E-Mail-Postfach des Auftraggebers	Weitergeleitete Anfragen verbleiben beim Auftraggeber (eigener Vertrag mit dem E-Mail-Anbieter).

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

1. Vertraulichkeit

- **Zutritts- und Zugangskontrolle:** Es werden keine eigenen Server betrieben. Die Website läuft auf der Plattform des Hosting-Anbieters (siehe Anlage 3). Zugang zu Hosting, Automatisierungsplattform und Quellcode nur für den Auftragnehmer, geschützt durch individuelles, starkes Passwort und Zwei-Faktor-Anmeldung. Arbeitsgeräte sind verschlüsselt und mit Sperrbildschirm gesichert.
- **Zugriffskontrolle:** Zugangsdaten und Schlüssel (z. B. für die Weiterleitung der Anfragen) liegen ausschließlich als geschützte Umgebungsvariablen bzw. im verschlüsselten Zugangsdaten-Speicher der Plattformen, nicht im Quellcode.
- **Trennung:** Jede Kunden-Website ist ein eigenes Projekt mit eigener Konfiguration; Anfragen werden über eine eindeutige Kennung je Auftraggeber getrennt verarbeitet.

2. Integrität

- **Weitergabekontrolle:** Die Website ist ausschließlich verschlüsselt erreichbar (HTTPS/TLS); Übertragungen zwischen den Plattformen und der E-Mail-Versand erfolgen verschlüsselt. Keine Weitergabe an Dritte außer an die Unterauftragsverarbeiter nach Anlage 3 und an den Auftraggeber.
- **Eingabekontrolle:** Änderungen an der Website erfolgen ausschließlich durch den Auftragnehmer über eine Versionsverwaltung; jede Veröffentlichung ist nachvollziehbar und kann zurückgenommen werden.
- **Schutz des Formulars:** Prüfung der Eingaben auf dem Server, Begrenzung der Anfragen je IP-Adresse, unsichtbares Prüffeld gegen automatisierte Einsendungen.

3. Verfügbarkeit und Belastbarkeit

- Betrieb auf einer professionell gehosteten Plattform mit weltweitem Auslieferungsnetz und Schutz gegen Überlastungsangriffe durch den Anbieter.
- Jede veröffentlichte Version bleibt gespeichert; bei Fehlern kann sofort auf eine frühere Version zurückgeschaltet werden.
- Schlägt die Weiterleitung einer Anfrage fehl, sieht der Besucher einen Hinweis mit alternativen Kontaktwegen (Telefon, E-Mail); der Fehler wird protokolliert, Fehler auf der Automatisierungsplattform melden sich beim Auftragnehmer per Alarm.

4. Datenschutz durch Technikgestaltung und Löschung

- Datenminimierung: Das Formular fragt nur ab, was für die Bearbeitung der Anfrage nötig ist; keine Nutzung der Daten für Werbung oder eigene Zwecke des Auftragnehmers.
- Schriften und Bilder werden von der eigenen Domain ausgeliefert, nicht von Servern Dritter.
- Datenschutzfreundliche Voreinstellungen: kein Tracking, keine Cookies zu Werbe- oder Statistikzwecken; Dienste Dritter nur nach Vereinbarung (§ 8 Abs. 3).
- 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 Plattformen oder der Unterauftragsverarbeiter.
- Regelmäßige Aktualisierung der eingesetzten Software-Bibliotheken; Auswertung von Fehler- und Alarmmeldungen; Dokumentation von Datenschutzvorfällen.

Anlage 3 Genehmigte Unterauftragsverarbeiter

NR.	UNTERNEHMEN	LEISTUNG	ORT DER VERARBEITUNG
1	**Vercel Inc.** 440 N Barranca Ave #4133 Covina, CA 91723, USA	Hosting und Auslieferung der Website, Ausführung der Server-Funktionen (z. B. Anfrageformular), Server-Protokolle	Server-Funktionen in Frankfurt am Main (Deutschland); Auslieferung über das weltweite Netz des Anbieters, Übermittlung in die USA möglich. Grundlage: EU-US Data Privacy Framework und Standardvertragsklauseln im Auftragsverarbeitungsvertrag des Anbieters (Zertifizierung vor Abschluss prüfen).
2	**n8n GmbH** Novalisstr. 10, 10115 Berlin HRB 212509 B, AG Charlottenburg	Entgegennahme und Weiterleitung der Anfragen aus dem Formular, Versandprotokoll	EU – Rechenzentrum in Frankfurt am Main (Deutschland) laut Anbieter. n8n setzt seinerseits Unterauftragsverarbeiter ein (u. a. für das Hosting); Liste im Datenschutzbereich von n8n.
3	**IONOS SE** Elgendorfer Str. 57, 56410 Montabaur	Versand der weitergeleiteten Anfragen per E-Mail – **nur wenn die Weiterleitung über das Postfach des Auftragnehmers vereinbart ist** (Anlage 1)	Deutschland / EU
4	**GitHub, Inc.** 88 Colin P. Kelly Jr. Street San Francisco, CA 94107, USA	Versionsverwaltung des Quellcodes und der Inhalte der Website (keine Besucher- oder Formulardaten)	USA. Grundlage: EU-US Data Privacy Framework und Standardvertragsklauseln im Auftragsverarbeitungsvertrag des Anbieters (prüfen).

> **Nicht als Unterauftragsverarbeiter eingesetzt:** der Domain-Anbieter und der E-Mail-Anbieter des Auftraggebers – diese Dienste nutzt der Auftraggeber auf Grundlage eigener Verträge (§ 5 Abs. 4). Nutzt der Auftraggeber zusätzlich ein Automatisierungsprodukt (z. B. Online-Termine), gilt dafür die Vereinbarung des jeweiligen Produkts.

Kontakt für Datenschutzfragen

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