SONNKOENIG.

SONNKOENIG.

Auftragsverarbeitungsvertrag

Fassung Oktober 2026 nach Art. 28 DSGVO
Anlage zu Ziffer 34 der AGB

VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG NACH ART. 28 DSGVO

zwischen dem Kunden als Verantwortlichem (im Folgenden „Kunde“) und der SONN|n|KOENIG UG (haftungsbeschränkt) & Co. KG, Hauptstraße 99, 67433 Neustadt an der Weinstraße, als Auftragsverarbeiterin (im Folgenden „Agentur“).

Dieser Vertrag wird nach Ziffer 34.2 der Allgemeinen Geschäftsbedingungen der Agentur mit Annahme des Angebots Bestandteil des Vertrags über die beauftragten Leistungen (im Folgenden „Hauptvertrag“). Einer gesonderten Unterschrift bedarf es nicht. Auf Wunsch stellt die Agentur ein unterschriebenes Exemplar bereit.

1. Gegenstand und Dauer

1.1 Gegenstand
Die Agentur verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit dies zur Erbringung der Leistungen aus dem Hauptvertrag erforderlich ist oder ein Zugriff darauf bei der Leistungserbringung nicht ausgeschlossen werden kann. Gegenstand, Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

1.2 Dauer
Dieser Vertrag gilt für die Laufzeit des Hauptvertrags und darüber hinaus, bis die Agentur alle im Auftrag verarbeiteten Daten nach Ziffer 10 zurückgegeben oder gelöscht hat.

1.3 Rangfolge
In Fragen des Datenschutzes geht dieser Vertrag den Allgemeinen Geschäftsbedingungen vor. Im Übrigen gilt der Hauptvertrag.

1.4 Eigene Verarbeitungen
Nicht von diesem Vertrag erfasst sind Verarbeitungen, für die die Agentur selbst Verantwortliche ist, insbesondere ihre Vertragsabwicklung, ihre Kommunikation einschließlich der KI-Assistenz, ihre Buchhaltung und ihre Eigenwerbung (Ziffer 34.1 der AGB).

2. Weisungen

2.1 Verarbeitung nur auf Weisung
Die Agentur verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung in ein Drittland, es sei denn, sie ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt sie dem Kunden diese Pflicht vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

2.2 Form der Weisungen
Der Hauptvertrag und dieser Vertrag sind die erste Weisung. Weitere Weisungen erteilt der Kunde in Textform an hello@sonnkoenig.de. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform. Weisungsberechtigt sind die Geschäftsführung des Kunden und die Personen, die er der Agentur in Textform benennt.

2.3 Rechtswidrige Weisungen
Ist die Agentur der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist sie den Kunden unverzüglich darauf hin. Sie darf die Ausführung aussetzen, bis der Kunde die Weisung in Textform bestätigt oder ändert. Eine Rechtsberatung schuldet die Agentur nicht.

2.4 Weisungen mit Mehraufwand
Weisungen, die über die im Hauptvertrag vereinbarten Leistungen hinausgehen, sind Leistungsänderungen und werden nach Aufwand vergütet.

3. Vertraulichkeit

3.1 Verpflichtung der Beschäftigten
Die Agentur setzt für die Verarbeitung nur Personen ein, die sie zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

3.2 Zugriff nach Bedarf
Zugriff auf Daten des Kunden erhalten nur die Personen, die ihn für ihre Aufgabe im Projekt benötigen, und nur für dessen Dauer.

4. Sicherheit der Verarbeitung

4.1 Technische und organisatorische Maßnahmen
Die Agentur trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Sie berücksichtigt dabei den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die betroffenen Personen.

4.2 Weiterentwicklung
Die Agentur darf die Maßnahmen an die technische Entwicklung anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert sie und teilt sie dem Kunden auf Anfrage mit.

5. Unterauftragsverarbeiter

5.1 Genehmigung
Der Kunde erteilt die allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Unterauftragsverarbeiter). Die in Anlage 3 genannten Unterauftragsverarbeiter gelten mit Abschluss dieses Vertrags als genehmigt.

5.2 Änderungen
Über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informiert die Agentur den Kunden mindestens 14 Tage vorher in Textform. Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Kann die Agentur den Widerspruch nicht berücksichtigen, können beide Seiten die betroffene Leistung zum Zeitpunkt des Wechsels kündigen.

5.3 Gleiche Pflichten
Die Agentur legt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet die Agentur gegenüber dem Kunden für dessen Pflichterfüllung nach Art. 28 Abs. 4 DSGVO.

5.4 Keine Unterauftragsverarbeitung
Keine Unterauftragsverarbeitung sind Nebenleistungen, die die Agentur bei Dritten in Anspruch nimmt, etwa Telekommunikation, Post- und Transportdienste, Reinigung oder Zahlungsverkehr. Ebenfalls keine Unterauftragsverarbeitung ist ein Hosting, das der Kunde nach Ziffer 18.1 der AGB unmittelbar beim Anbieter beauftragt; den dafür erforderlichen Auftragsverarbeitungsvertrag schließt der Kunde selbst mit dem Anbieter.

6. Verarbeitung in Drittländern

6.1 Grundlage
Eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses wie des EU-US Data Privacy Framework oder von Standardvertragsklauseln der EU-Kommission. Anlage 3 nennt die jeweilige Grundlage.

6.2 Wegfall
Entfällt eine Grundlage, stellt die Agentur auf eine andere zulässige Grundlage oder einen anderen Anbieter um und informiert den Kunden nach Ziffer 5.2.

7. Unterstützung des Kunden

7.1 Rechte der betroffenen Personen
Wendet sich eine betroffene Person mit einem Anliegen zu ihren Rechten unmittelbar an die Agentur, leitet die Agentur das Anliegen unverzüglich an den Kunden weiter. Sie beantwortet es nicht selbst, es sei denn, der Kunde weist sie dazu an. Die Agentur unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten.

7.2 Weitere Pflichten
Die Agentur unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Meldungen von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und der Konsultation der Aufsichtsbehörde.

7.3 Vergütung
Leistungen nach dieser Ziffer werden nach Aufwand vergütet, es sei denn, ihr Anlass liegt im Verantwortungsbereich der Agentur.

8. Verletzungen des Schutzes personenbezogener Daten

8.1 Meldung
Die Agentur meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten, die Daten aus diesem Auftrag betrifft, unverzüglich nach Kenntnis, möglichst innerhalb von 48 Stunden, in Textform an die zuletzt bekannte Kontaktadresse des Kunden.

8.2 Inhalt
Die Meldung enthält, soweit bekannt, eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien und Personen und ihrer ungefähren Zahl, der wahrscheinlichen Folgen sowie der ergriffenen oder vorgeschlagenen Maßnahmen und eine Kontaktstelle. Was noch nicht bekannt ist, reicht die Agentur schrittweise nach.

8.3 Maßnahmen
Die Agentur ergreift unverzüglich die erforderlichen Maßnahmen, um die Verletzung einzudämmen und mögliche nachteilige Folgen für die betroffenen Personen zu mindern. Meldungen an Aufsichtsbehörde und betroffene Personen nimmt der Kunde vor.

9. Nachweise und Kontrollen

9.1 Informationen
Die Agentur stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung. Der Nachweis kann insbesondere durch eine aktuelle Beschreibung der Maßnahmen nach Anlage 2, eine Selbstauskunft der Agentur sowie Zertifikate und Prüfberichte der Unterauftragsverarbeiter erbracht werden.

9.2 Kontrollen vor Ort
Der Kunde oder ein von ihm beauftragter Prüfer kann sich nach Anmeldung mit einer Frist von mindestens 14 Tagen während der Servicezeiten von der Einhaltung dieses Vertrags überzeugen, ohne Anlass höchstens einmal im Kalenderjahr. Prüfer müssen zur Vertraulichkeit verpflichtet sein und dürfen nicht im Wettbewerb zur Agentur stehen. Die Kontrolle darf den Betrieb der Agentur und die Daten anderer Kunden nicht beeinträchtigen.

9.3 Kosten
Den Aufwand der Agentur für Kontrollen trägt der Kunde nach Aufwand, es sei denn, die Kontrolle ergibt einen wesentlichen Verstoß der Agentur gegen diesen Vertrag.

10. Rückgabe und Löschung

10.1 Wahl des Kunden
Nach Ende der Leistungen gibt die Agentur die im Auftrag verarbeiteten Daten nach Wahl des Kunden einmalig in einem bei ihr vorhandenen Standardformat zurück oder löscht sie, soweit nicht eine Pflicht zur Speicherung nach dem Recht der Union oder eines Mitgliedstaats besteht.

10.2 Frist
Teilt der Kunde seine Wahl nicht innerhalb von 30 Tagen nach Vertragsende in Textform mit, löscht die Agentur die Daten. Datensicherungen werden im regulären Rotationszyklus gelöscht. Auf Anfrage bestätigt die Agentur die Löschung in Textform.

10.3 Daten beim Kunden
Daten, die sich auf Systemen des Kunden oder eines von ihm beauftragten Anbieters befinden, verbleiben dort. Die Agentur entfernt ihre Zugänge zu diesen Systemen oder bittet den Kunden, sie zu sperren.

11. Pflichten des Kunden

11.1 Verantwortung
Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für Rechtsgrundlagen, Einwilligungen (auch nach § 25 TDDDG), seine

Datenschutzerklärung und die Wahrung der Rechte betroffener Personen. Er stellt sicher, dass er personenbezogene Daten rechtmäßig an die Agentur übermittelt.

11.2 Hinweise
Stellt der Kunde Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er die Agentur unverzüglich.

11.3 Zugangsdaten
Zugangsdaten übermittelt der Kunde nicht per E-Mail, sondern über einen verschlüsselten Einmal-Link, den die Agentur bereitstellt.

11.4 Besondere Kategorien
Daten besonderer Kategorien nach Art. 9 DSGVO und Daten über strafrechtliche Verurteilungen übermittelt der Kunde nur nach vorheriger Absprache in Textform.

12. Haftung und Vergütung

12.1 Haftung
Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Im Verhältnis der Parteien zueinander gelten die Haftungsregeln des Hauptvertrags (Ziffer 30 der AGB), soweit Art. 82 DSGVO nicht entgegensteht.

12.2 Vergütung
Die Pflichten aus diesem Vertrag sind mit der im Hauptvertrag vereinbarten Vergütung abgegolten, soweit dieser Vertrag nicht ausdrücklich eine Vergütung nach Aufwand vorsieht. Aufwand wird nach dem im Hauptvertrag vereinbarten Stundensatz berechnet. Prüfung, Verhandlung oder Verwendung von Vertragsmustern des Kunden erfolgen nach Aufwand.

13. Schlussbestimmungen

13.1 Form
Dieser Vertrag ist in einem elektronischen Format abgefasst (Art. 28 Abs. 9 DSGVO). Änderungen und Ergänzungen bedürfen der Textform.

13.2 Fassung
Es gilt die bei Annahme des Angebots gültige Fassung, auf deren Stand das Angebot hinweist. Eine neue Fassung gilt für laufende Verträge erst mit deren Verlängerung oder mit Zustimmung des Kunden. Änderungen der Anlage 3 richten sich nach Ziffer 5.2.

13.3 Recht und Gerichtsstand
Es gilt deutsches Recht. Für den Gerichtsstand gilt der Hauptvertrag.

13.4 Teilunwirksamkeit
Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung, insbesondere Art. 28 DSGVO.

ANLAGE 1 – GEGENSTAND, ART UND ZWECK DER VERARBEITUNG

Leistungen mit Verarbeitung im Auftrag

Welche der folgenden Leistungen im Einzelfall betroffen sind, ergibt sich aus dem Hauptvertrag.

- Erstellung, Relaunch und Pflege von Websites und Online-Shops mit Echtdaten, einschließlich Inhaltsübertragung und Migration
- Wartung, Updates, Datensicherung und Wiederherstellung
- Einrichtung und Betreuung von Kontakt-, Anfrage- und Bewerbungsformularen
- Analyse und Behebung von Fehlern, einschließlich Auswertung von Server- und Fehlerprotokollen
- Einrichtung und Auswertung von Webanalyse im Auftrag des Kunden
- Arbeit in Newsletter-, Social-Media-, Unternehmensprofilund Werbekonten des Kunden
- Pflege von Inhalten, etwa Stellenanzeigen, News, Projekte und Ansprechpartner

Arten personenbezogener Daten

- Kontaktdaten (Name, Anschrift, E-Mail-Adresse, Telefonnummer, Firma, Funktion)
- Inhalte von Anfragen, Nachrichten und Kommentaren
- Bewerbungsdaten (Lebenslauf, Zeugnisse, Anschreiben), soweit die Website Bewerbungen entgegennimmt
- Vertrags- und Bestelldaten (Bestellungen, Lieferanschriften, Rechnungsbezug; keine vollständigen Kartendaten)
- Nutzungs- und Protokolldaten (IP-Adresse, Zeitpunkt, aufgerufene Seiten, Geräte- und Browserangaben)
- Konto- und Zugangsdaten von Redakteuren, Mitgliedern und Kunden des Kunden
- Bild- und Tonaufnahmen von Personen, soweit der Kunde sie für seine Inhalte bereitstellt
- Profil- und Interaktionsdaten in Social-Media- und Werbekonten

Kategorien betroffener Personen

- Besucher der Websites und Kanäle des Kunden
- Kunden, Interessenten und Geschäftspartner des Kunden
- Bewerberinnen und Bewerber des Kunden
- Beschäftigte des Kunden
- Abonnenten, Follower und Mitglieder

Zweck

Die Verarbeitung dient ausschließlich der Erbringung der im Hauptvertrag vereinbarten Leistungen. Eine Verarbeitung zu eigenen Zwecken der Agentur findet nicht statt.

ANLAGE 2 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (ART. 32 DSGVO)

Vertraulichkeit

- Zutritt: Der Server der Agentur steht an einem nicht öffentlich bekannten Standort.
- Zugang: Jede Person arbeitet mit einem persönlichen Benutzerkonto. Die Festplatten aller Arbeitsrechner sind verschlüsselt.
- Zugriff: Jede Person erhält auf jedem System einen eigenen Benutzer mit der niedrigsten ausreichenden Rolle. Keine geteilten Zugänge, keine Sammelkonten. Freischaltung projektbezogen durch die Geschäftsführung, Entzug bei Projektende.
- Fernzugriff: Der Server der Agentur ist von außen nur mit Zwei-Faktor-Anmeldung für alle Konten erreichbar, mit automatischer Sperre nach Fehlversuchen und automatischen Sicherheitsupdates.
- Passwortverwaltung: Zugangsdaten zu Kundensystemen liegen ausschließlich in einem Passwortmanager mit Zwei-Faktor-Anmeldung und Datenhaltung in der EU, je Kunde in einem eigenen Bereich.
- Trennung: Daten verschiedener Kunden werden in getrennten Systemen, Zugängen und Ordnern verarbeitet.
- KI-Werkzeuge: Personenbezogene Daten aus Kundenprojekten gibt die Agentur nicht in KI-Werkzeuge ein. KI-Werkzeuge nutzt sie nur für Texte und Gestaltung auf Grundlage öffentlich zugänglicher Inhalte.

Integrität

- Weitergabe: Übertragung von Websites und Verwaltungsoberflächen ausschließlich verschlüsselt (TLS). Zugangsdaten nur über verschlüsselte Einmal-Links mit Ablauffrist, nie per E-Mail oder Dateiübertragung.

- Eingabe: Änderungen in Kundensystemen erfolgen über persönliche Benutzerkonten, sodass nachvollziehbar ist, wer was geändert hat, soweit das System dies protokolliert.

Verfügbarkeit und Belastbarkeit

- Monatliche Sicherung der betreuten Websites beim Hosting-Anbieter und zusätzlich verschlüsselt auf dem Server der Agentur.
- Prüfung der Wiederherstellbarkeit nach der vereinbarten Wartungsklasse.
- Sicherheitsupdates der betreuten Systeme im Rahmen der vereinbarten Wartung.
- Verfahren zur regelmäßigen Überprüfung
- Schriftliche Verpflichtung aller Beschäftigten auf Vertraulichkeit vor Aufnahme der Tätigkeit.
- Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO, einschließlich der Verarbeitungen im Auftrag.
- Auswahl von Unterauftragsverarbeitern nach ihren Garantien, Abschluss von Auftragsverarbeitungsverträgen, bei Drittlandbezug mit Standardvertragsklauseln oder Angemessenheitsbeschluss.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich und bei wesentlichen Änderungen.

ANLAGE 3 – UNTERAUFTRAGSVERARBEITER

Stand: Oktober 2026. Nicht jeder Dienst wird in jedem Auftrag eingesetzt. Änderungen kündigt die Agentur nach Ziffer 5.2 an.

- E-Mail und Server: webgo GmbH, Heidenkampsweg 81, 20097 Hamburg – E-Mail und eigene Systeme der Agentur – Verarbeitung in Deutschland
- Projektsteuerung: Mango Technologies, Inc. (ClickUp), San Diego, USA – Aufgaben, Kommentare und Dateien zum Projekt – Drittland USA: EU-US Data Privacy Framework bzw. Standardvertragsklauseln
- Passwortverwaltung: Bitwarden, Inc., Santa Barbara, USA – Verwahrung von Zugangsdaten und verschlüsselte Einmal-Links (Bitwarden Send) – Datenhaltung in der EU; Betreiber in den USA: EU-US Data Privacy Framework bzw. Standardvertragsklauseln
- Einmal-Links für Zugangsdaten: Apnotic, LLC (Password Pusher, EU-Instanz), USA – verschlüsselte Einmal-Links mit Ablauffrist – Datenhaltung in der EU; Betreiber in den USA: Standardvertragsklauseln
- Dateiübertragung: WeTransfer B.V., Amsterdam, Niederlande – Übertragung großer Dateien – Verarbeitung in der EU
- Videokonferenzen: Microsoft Ireland Operations Limited, Dublin, Irland (Microsoft Teams) – Termine und Bildschirmfreigabe – Verarbeitung in der EU; Drittlandbezug USA: EU-US Data Privacy Framework

Keine Unterauftragsverarbeitung ist ein Hosting, das der Kunde unmittelbar beim Anbieter beauftragt, etwa bei unserem Hosting-Partner phi.itservice (Ziffer 5.4). Lädt der Kunde zu Terminen über einen eigenen Dienst ein, gilt dessen Vertrag mit dem Kunden.

SONN|n|KOENIG UG & Co. KG
(haftungsbeschränkt)

Hauptstraße 99
67433 Neustadt an der Weinstraße
Amtsgericht Ludwigshafen am Rhein, HRA 62336
USt-IdNr.: DE324705467

Persönlich haftende Gesellschafterin:

SnK Verwaltungs UG
(haftungsbeschränkt)

Amtsgericht Ludwigshafen am Rhein HRB 69629,
vertreten durch den Geschäftsführer Sascha König

Stand: Oktober 2026