Sabia GmbH
Stuckstrasse 10, 12435 Berlin
E-Mail: founders@sabia.de
Tel: +49 (0) 152 59229752

Vertrag über die Auftragsverarbeitung

nach Art. 28 DSGVO („AVV“) – Anlage 2 zu den Nutzungsbedingungen Sabia OS

Fassung 1.0 · Stand: 11. August 2026

zwischen dem Kunden im Sinne der Nutzungsbedingungen Sabia OS – im Folgenden: „Auftraggeber“ – und der Sabia GmbH, Stuckstraße 10, 12435 Berlin, vertreten durch die Geschäftsführer Lukas Wagner und Patrick Alex – im Folgenden: „Auftragnehmer“ –.

Dieser Vertrag ist Anlage 2 der Nutzungsbedingungen Sabia OS. Er kommt mit dem Abschluss des Nutzungsvertrages im Buchungsprozess (§ 3 der Nutzungsbedingungen) zwischen den Parteien zustande, ohne dass es einer gesonderten Unterzeichnung bedarf.

§ 1 Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem Vertrag über die Nutzung der Software „Sabia OS“ (im Folgenden: „Hauptvertrag“) ist es erforderlich, dass der Auftragnehmer personenbezogene Daten verarbeitet, für die der Auftraggeber Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften ist (im Folgenden: „Auftraggeber-Daten“). Zu den Auftraggeber-Daten gehören auch Inhalte, die bei der Nutzung der KI- und Sprachfunktionen entstehen oder dort eingegeben werden, insbesondere Eingaben, Chatverläufe, Sprachaufnahmen und die daraus erzeugten Transkripte, sowie Sitzungsaufzeichnungen aus der Produktanalyse, soweit sie Auftraggeber-Daten wiedergeben. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen der Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrages vor.

§ 2 Umfang der Beauftragung

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn; ihm obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1 zu diesem Vertrag.

(3) Dem Auftragnehmer bleibt es vorbehalten, Auftraggeber-Daten so zu anonymisieren oder zu aggregieren, dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und sie in dieser Form zum Zweck der bedarfsgerechten Gestaltung, Weiterentwicklung und Optimierung sowie der Erbringung des nach dem Hauptvertrag vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass derart anonymisierte bzw. aggregierte Daten keine Auftraggeber-Daten im Sinne dieses Vertrages mehr sind.

(4) Die Verarbeitung der Auftraggeber-Daten findet grundsätzlich in der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Sollen Auftraggeber-Daten durch den Auftragnehmer oder seine Unterauftragnehmer außerhalb des EWR verarbeitet werden, ist dies nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (siehe § 7 Abs. 4 und 5).

§ 3 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den dokumentierten Weisungen des Auftraggebers, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrages festgelegt und dokumentiert. Einzelweisungen, die hiervon abweichen oder zusätzliche Anforderungen aufstellen, bedürfen der Textform und einer vorherigen Abstimmung mit dem Auftragnehmer; hierdurch entstehende nachgewiesene Mehraufwände kann der Auftragnehmer angemessen in Rechnung stellen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder anwendbares Datenschutzrecht verstößt, informiert er den Auftraggeber unverzüglich und ist berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber sie geändert oder die rechtlichen Bedenken ausgeräumt hat. Eine Weisung, die nach Auffassung des Auftragnehmers offensichtlich gegen datenschutzrechtliche Vorschriften verstößt, darf der Auftragnehmer ablehnen; die Bestätigung der Weisung durch den Auftraggeber begründet keine Ausführungspflicht.

§ 4 Verantwortlichkeit des Auftraggebers

(1) Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Personen und die Rechtmäßigkeit der Verarbeitung verantwortlich. Er stellt insbesondere sicher, dass die betroffenen Personen nach Art. 12 ff. DSGVO informiert werden und dass für die Verarbeitung – bei besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) insbesondere nach Art. 9 DSGVO – eine tragfähige Rechtsgrundlage besteht. Für die Freistellung von Ansprüchen Dritter gilt § 13 Abs. 2.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seiner Weisungen feststellt.

(3) Der Auftraggeber stellt dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung, soweit sie dem Auftragnehmer nicht selbst vorliegen.

Sabia GmbH
Geschäftsführer: Lukas Wagner, Patrick Alex
Amtsgericht Berlin (Charlottenburg), HRB 286212 B

§ 5 Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).

§ 6 Sicherheit der Verarbeitung

(1) Der Auftragnehmer ergreift gemäß Art. 32 DSGVO die erforderlichen, geeigneten technischen und organisatorischen Maßnahmen („TOMs“), die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen ein dem Risiko angemessenes Schutzniveau gewährleisten. Die bei Vertragsschluss getroffenen Maßnahmen sind in Anlage 3 beschrieben.

(2) Der Auftragnehmer darf die TOMs während der Laufzeit des Vertrages ändern und fortentwickeln, solange das vereinbarte Schutzniveau dadurch nicht unterschritten wird. Wesentliche Änderungen dokumentiert der Auftragnehmer.

§ 7 Inanspruchnahme weiterer Auftragsverarbeiter (Subunternehmer)

(1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die bei Vertragsschluss eingesetzten weiteren Auftragsverarbeiter ergeben sich aus Anlage 2.

(2) Der Auftragnehmer informiert den Auftraggeber in Textform (E-Mail genügt) über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter, in der Regel mindestens 14 Tage vor deren Einsatz. Der Auftraggeber kann im Einzelfall aus wichtigem, dem Auftragnehmer nachzuweisendem datenschutzrechtlichen Grund innerhalb von 14 Tagen nach Zugang der Information Einspruch erheben. Erhebt der Auftraggeber fristgerecht Einspruch, bemühen sich die Parteien um eine einvernehmliche Lösung; kommt eine solche nicht zustande, ist jede Partei berechtigt, den Hauptvertrag und diesen Vertrag mit Wirkung zum Ende des laufenden Abrechnungszeitraums zu kündigen.

(3) Der Auftragnehmer erlegt dem weiteren Auftragsverarbeiter im Wege eines Vertrages dieselben Datenschutzpflichten auf, wie sie ihm nach diesem Vertrag obliegen (Art. 28 Abs. 4 DSGVO). Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

(4) Die Genehmigung nach Abs. 1 gilt unter Einhaltung der Anforderungen des § 2 Abs. 4 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittland eingesetzt wird. In diesem Fall stellt der Auftragnehmer sicher, dass geeignete Garantien nach Art. 44 ff. DSGVO bestehen, insbesondere Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO) oder ein Angemessenheitsbeschluss (Art. 45 DSGVO).

(5) Für die USA hat die Europäische Kommission mit Beschluss vom 10.07.2023 entschieden, dass unter den Regelungen des EU-US Data Privacy Framework („DPF“) ein angemessenes Datenschutzniveau besteht (Angemessenheitsbeschluss, Art. 45 DSGVO). Soweit in Anlage 2 ausgewiesen, sind die eingesetzten Dienstleister nach dem DPF zertifiziert; ergänzend oder alternativ werden Standardvertragsklauseln vereinbart.

Sabia GmbH
Geschäftsführer: Lukas Wagner, Patrick Alex
Amtsgericht Berlin (Charlottenburg), HRB 286212 B

§ 8 Rechte der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen in zumutbarem Umfang dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen nach Art. 12 bis 22 DSGVO nachzukommen. Für Unterstützungsleistungen, die über die im Dienst bereitgestellten Funktionen (z. B. Export-, Berichtigungs- und Löschfunktionen) wesentlich hinausgehen, kann der Auftragnehmer Ersatz der nachzuweisenden, angemessenen Aufwände verlangen.

(2) Macht eine betroffene Person Rechte unmittelbar gegenüber dem Auftragnehmer geltend, leitet der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiter; die Beantwortung obliegt dem Auftraggeber.

(3) Der Auftragnehmer ermöglicht es dem Auftraggeber, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken, oder nimmt dies auf dokumentierte Weisung des Auftraggebers selbst vor, wenn und soweit dies dem Auftraggeber mit den bereitgestellten Funktionen nicht selbst möglich ist.

§ 9 Melde- und Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer meldet dem Auftraggeber unverzüglich nach Bekanntwerden jede Verletzung des Schutzes personenbezogener Daten, die Auftraggeber-Daten betrifft (Art. 33 Abs. 2 DSGVO). Die Meldung enthält, soweit möglich, die in Art. 33 Abs. 3 DSGVO genannten Informationen. Der Auftragnehmer unterstützt den Auftraggeber in zumutbarem Umfang bei der Erfüllung seiner Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO.

(2) Der Auftragnehmer unterstützt den Auftraggeber in zumutbarem Umfang bei Datenschutz-Folgenabschätzungen und etwaigen vorherigen Konsultationen der Aufsichtsbehörden (Art. 35, 36 DSGVO). Für Unterstützungsleistungen nach diesem Absatz, die der Auftragnehmer nicht zu vertreten hat und die erheblichen Aufwand verursachen, kann er Ersatz der nachzuweisenden, angemessenen Aufwände verlangen.

§ 10 Löschung und Rückgabe von Auftraggeber-Daten

(1) Nach Beendigung des Hauptvertrages gibt der Auftragnehmer nach Wahl des Auftraggebers sämtliche Auftraggeber-Daten heraus (§ 5 Abs. 4 des Hauptvertrages) und/oder löscht sie, sofern nicht eine gesetzliche Verpflichtung zur weiteren Speicherung besteht. Ohne abweichende Weisung erfolgt die Löschung, sobald die Herausgabe abgeschlossen ist und die Daten für die Abwicklung des Vertrages nicht mehr benötigt werden, spätestens jedoch sechs Monate nach Vertragsende. Aus Sicherungskopien werden die Daten mit dem turnusmäßigen Überschreiben entfernt.

(2) Löscht der Auftraggeber einen einzelnen Endkunden, werden die vom Auftraggeber verwalteten Daten dieses Endkunden gelöscht. Verfügt der Endkunde über einen eigenen Zugang zur Mandanten-Web-App, gilt Folgendes: Besteht für diesen Endkunden eine weitere Beziehung zu einem anderen Auftraggeber des Auftragnehmers, wird lediglich die Verknüpfung zum löschenden Auftraggeber aufgehoben; der Zugang des Endkunden und die von ihm selbst eingegebenen sowie die über angebundene Schnittstellen abgerufenen Daten bleiben im Verhältnis zu dem oder den übrigen Auftraggebern bestehen. Besteht keine weitere solche Beziehung, wird der Zugang des Endkunden einschließlich dieser Daten nach Ablauf einer Karenzzeit von 30 Tagen gelöscht; der Auftragnehmer weist den Endkunden zu Beginn der Karenzzeit auf die bevorstehende Löschung und auf die

Möglichkeit hin, seine Daten zu exportieren. Der Auftragnehmer weist den Auftraggeber in der Software vor der Löschung auf die jeweilige Wirkung hin.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen, darf der Auftragnehmer auch nach Vertragsende aufbewahren. Auf Verlangen bestätigt der Auftragnehmer die Löschung in Textform.

§ 11 Nachweise und Überprüfungen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle erforderlichen und bei ihm vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrages, insbesondere die Umsetzung der TOMs, zu überprüfen, einschließlich durch Inspektionen. Inspektionen erfolgen nach rechtzeitiger Vorankündigung (in der Regel mindestens zwei Wochen) während der üblichen Geschäftszeiten, auf eigene Kosten des Auftraggebers, ohne Störung des Betriebsablaufs und unter strikter Wahrung der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers. Der Auftraggeber darf höchstens eine Überprüfung pro Kalenderjahr durchführen; anlassbezogene Überprüfungen nach einer Verletzung des Schutzes von Auftraggeber-Daten bleiben unberührt.

(3) Beauftragt der Auftraggeber einen Dritten mit der Überprüfung, verpflichtet er diesen in Textform zur Verschwiegenheit und Geheimhaltung, es sei denn, der Dritte unterliegt einer beruflichen Verschwiegenheitspflicht. Ein Wettbewerber des Auftragnehmers darf nicht beauftragt werden.

(4) Nach Wahl des Auftragnehmers kann der Nachweis auch durch Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Datenschutzauditor) oder einer geeigneten Zertifizierung (z. B. ISO 27001, BSI-Grundschutz) erbracht werden, wenn dieser es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

(5) Der Auftragnehmer ist berechtigt, Informationen nicht zu offenbaren, die im Hinblick auf seine Geschäfte sensibel sind oder deren Offenbarung gegen gesetzliche oder vertragliche Pflichten verstoßen würde; Daten oder Informationen über andere Kunden des Auftragnehmers werden nicht zugänglich gemacht.

§ 12 Vertragsdauer und Kündigung

Laufzeit und Kündigung dieses Vertrages richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Beendigung des Hauptvertrages bewirkt automatisch auch die Beendigung dieses Vertrages; eine isolierte Kündigung dieses Vertrages ist ausgeschlossen. Pflichten, die ihrer Natur nach über das Vertragsende hinaus fortgelten (insbesondere §§ 5, 10), bleiben unberührt.

§ 13 Haftung

(1) Für die Haftung der Parteien nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen des Hauptvertrages. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

(2) Machen Dritte, einschließlich Aufsichtsbehörden, gegen den Auftragnehmer Ansprüche geltend oder verhängen Geldbußen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen seine Pflichten als Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer in dem Umfang frei, in dem der Auftraggeber Anteil an der Verantwortung für den Verstoß trägt. Entsprechendes gilt zugunsten des Auftraggebers bei schuldhaften Verstößen des Auftragnehmers.

Anlage 1: Gegenstand, Dauer, Art und Zweck der Verarbeitung; Datenarten; Kategorien betroffener Personen

Gegenstand und Dauer der Verarbeitung: Bereitstellung der Software „Sabia OS“ als Software-as-a-Service einschließlich der Einräumung von Speicherplatz für die Dauer des Hauptvertrages.

Art und Zweck der Verarbeitung: Hosting, Speicherung, Anzeige, Auswertung, Aufbereitung und Übermittlung der vom Auftraggeber, seinen Nutzern und seinen Endkunden eingegebenen bzw. über angebundene Schnittstellen abgerufenen Daten zum Zweck der Kundenverwaltung (CRM/CLM), der Vorbereitung und Dokumentation der Finanzberatung (u. a. Geeignetheitserklärung, Finanzplanung, Auswertungen und Reports), der Kommunikation und Aufgabenverwaltung sowie der Unterstützung des Auftraggebers durch KI-Funktionen.

Art der personenbezogenen Daten:

- Stammdaten und Kontaktdaten der Endkunden und Interessenten (z. B. Name, Anschrift, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Familienstand, Beruf);
- finanzielle Daten (z. B. Einkommen, Ausgaben, Konto-, Depot- und Transaktionsdaten aus der PSD2-Kontoanbindung, Vermögenswerte wie Immobilien, Beteiligungen und Wertpapiere, Verbindlichkeiten und Finanzierungen, Steuerdaten, Versicherungsschutz, Angaben zur Bonität);
- Daten aus der Beratungsdokumentation (z. B. Ziele, Kenntnisse und Erfahrungen, Risikobereitschaft, Geeignetheitserklärung, Finanzpläne und Szenarien);
- Dokumente und Inhalte des Dokumententresors sowie Kommunikations- und Verlaufsdaten (z. B. Notizen, Aufgaben, Historie);
- Kalenderdaten, sofern der Kunde die Kalendersynchronisation aktiviert (z. B. Termintitel und -beschreibung, Teilnehmende, Organisator, Ort, Konferenzdaten sowie die zugehörigen Zugriffstoken); die Anbindung umfasst auch schreibenden Zugriff auf den verbundenen Kalender;
- Audio- und Transkriptionsdaten, sofern der Kunde Sprachfunktionen nutzt (z. B. Sprachaufnahmen und daraus erzeugte Transkripte), sowie Eingaben und Chatverläufe der KI-Funktionen;
- Signaturdaten im Rahmen der digitalen Signatur (z. B. Name, E-Mail-Adresse, Zeitstempel, Nachweisdokumente);
- gegebenenfalls besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, soweit der Auftraggeber sie im Rahmen der Beratung erfasst (z. B. für Absicherungs- und Vorsorgeanalysen); die erforderliche Rechtsgrundlage nach Art. 9 DSGVO stellt der Auftraggeber sicher;

Sabia GmbH
Geschäftsführer: Lukas Wagner, Patrick Alex
Amtsgericht Berlin (Charlottenburg), HRB 286212 B

- Stammdaten und Nutzungsdaten der Nutzer (Mitarbeiter) des Auftraggebers im Rahmen der Seats.

Kategorien betroffener Personen: Endkunden und Interessenten (Leads) des Auftraggebers sowie gegebenenfalls deren Angehörige und wirtschaftlich Berechtigte; Mitarbeiter und sonstige Nutzer des Auftraggebers.

Anlage 2: Weitere Auftragsverarbeiter (Subunternehmer)

Die folgenden Unternehmen sind weitere Auftragsverarbeiter im Sinne des § 7 dieses Vertrages. Die jeweils aktuelle Fassung dieser Liste ist unter der vom Auftragnehmer benannten Internetadresse abrufbar; maßgeblich für Änderungen ist § 7 Abs. 2.

Infrastruktur und Betrieb

- Vercel Inc., San Francisco, USA – Hosting und Auslieferung der Web-Anwendung – EU-US Data Privacy Framework (zertifiziert), ergänzend Standardvertragsklauseln;
- Supabase, Inc., San Francisco, USA – Datenbank, Authentifizierung und Storage; Datenhaltung in der EU-Region Frankfurt (eu-central-1) – Standardvertragsklauseln für etwaigen administrativen Zugriff aus Drittländern;
- Upstash, Inc., USA – Caching und Ratenbegrenzung (Redis); Datenhaltung in der EU – Standardvertragsklauseln;

Kommunikation

- Resend, Inc., USA – Versand von Transaktions- und Einladungs-E-Mails (u. a. an Endkunden des Auftraggebers) – Standardvertragsklauseln;
- Slack Technologies (Salesforce, Inc.), USA – interne Benachrichtigungen des Auftragnehmers zu Support-, Registrierungs- und Exportvorgängen – EU-US Data Privacy Framework (zertifiziert), ergänzend Standardvertragsklauseln;

Fachliche Funktionen

- Google Ireland Limited, Dublin, Irland / Google LLC, USA – KI-Funktionen über Google Cloud Vertex AI (derzeit Modellfamilie Gemini) sowie Sprachverarbeitung (Speech-to-Text, Text-to-Speech), Verarbeitung über europäische Endpunkte – EU-US Data Privacy Framework (Google LLC zertifiziert), ergänzend Standardvertragsklauseln; eine Nutzung der Eingaben zum Training der allgemeinen Modelle des Anbieters ist nach den genutzten Vertragskonditionen ausgeschlossen;
- WealthAPI GmbH, Deutschland – Abruf von Konto-, Depot- und Transaktionsdaten (PSD2-Kontoinformationen) über eine regulierte Schnittstelle – Verarbeitung in der EU;
- Google Ireland Limited bzw. Microsoft Ireland Operations Limited – Kalendersynchronisation, sofern vom Auftraggeber aktiviert – Angemessenheitsbeschluss bzw. Standardvertragsklauseln;
- Yousign SAS, Caen, Frankreich, auftretend unter der Marke „Youtrust“ – elektronische Signatur (eIDAS-konform) – Verarbeitung in der EU;
- Exa Labs, Inc., USA – Websuche des KI-Mitarbeiters in öffentlich zugänglichen Quellen – Standardvertragsklauseln; übermittelt wird die jeweilige Suchanfrage. Der Auftragnehmer

konfiguriert den Assistenten so, dass Rechercheanfragen keine personenbezogenen Daten enthalten sollen; der Auftraggeber stellt seinerseits sicher, dass seine Nutzer keine personenbezogenen Daten in Rechercheanfragen eingeben (§ 7 Abs. 6 des Hauptvertrages). Die Funktion kann auf Weisung des Auftraggebers für dessen Organisation deaktiviert werden;

Analyse

- PostHog, Inc., San Francisco, USA – Produktanalyse einschließlich Sitzungsaufzeichnungen ohne Maskierung von Eingaben und angezeigten Inhalten; hierbei können Auftraggeber-Daten einschließlich Inhalten verarbeitet werden. Die Aufzeichnung im Browser erfolgt ausschließlich nach Einwilligung der jeweiligen Nutzerin oder des jeweiligen Nutzers; EU-Hosting (Frankfurt) – EU-US Data Privacy Framework (zertifiziert), ergänzend Standardvertragsklauseln.

Der Zahlungsdienstleister Stripe verarbeitet ausschließlich Daten des Auftraggebers zur Zahlungsabwicklung des Hauptvertrages und ist insoweit kein Subunternehmer im Sinne dieses Vertrages.

Anlage 3: Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zugangskontrolle: Authentifizierung sämtlicher Nutzer mit persönlichen Zugangsdaten; Zwei-Faktor-Authentifizierung für administrative Zugänge des Auftragnehmers und der eingesetzten Dienstleister; für Nutzer des Auftraggebers steht die Zwei-Faktor-Authentifizierung als Option zur Verfügung; rollenbasierte Berechtigungen nach dem Need-to-know-Prinzip;
- Zugriffskontrolle: Protokollierung administrativer Zugriffe; getrennte Berechtigungen für Produktions- und Entwicklungsumgebungen; unverzüglicher Entzug von Berechtigungen beim Ausscheiden von Mitarbeitern;
- Trennungskontrolle: logische Mandantentrennung der Kundendaten in der Datenbank; Trennung von Produktiv- und Testdaten;
- Zutrittskontrolle: Das Hosting erfolgt in zertifizierten Rechenzentren der eingesetzten Dienstleister (u. a. Zutrittskontrollen, Videoüberwachung, Sicherheitspersonal).

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle: Verschlüsselung der Datenübertragung nach dem Stand der Technik (TLS); Verschlüsselung gespeicherter Daten (Encryption at Rest) bei den eingesetzten Hosting-Dienstleistern;
- Eingabekontrolle: Protokollierung wesentlicher Änderungen an Daten und Konfigurationen; Nachvollziehbarkeit durch Verlaufs- und Aktivitätshistorien.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- regelmäßige, automatisierte Backups der Datenbank durch den eingesetzten Hosting-Dienstleister; Wiederherstellung nach dessen Standardverfahren; redundante Infrastruktur der eingesetzten Dienstleister; Schutzmaßnahmen gegen Angriffe (u. a. Firewalls und DDoS-Schutz auf Ebene der Dienstleister); Monitoring und Alarmierung. Konkrete Wiederherstellungszeiten (RTO/RPO) sind nicht zugesagt, soweit sie nicht gesondert vereinbart werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Datenschutz-Management mit regelmäßiger Überprüfung der TOMs; Incident-Response-Prozess zur Erkennung, Bewertung und Meldung von Sicherheitsvorfällen; sorgfältige Auswahl und regelmäßige Überprüfung der Unterauftragnehmer einschließlich Abschluss von Verträgen nach Art. 28 DSGVO; Verpflichtung der Mitarbeiter auf Vertraulichkeit und regelmäßige Sensibilisierung.

Sabia GmbH
Geschäftsführer: Lukas Wagner, Patrick Alex
Amtsgericht Berlin (Charlottenburg), HRB 286212 B