

Datenschutzerklärung

SabiaOS

Fassung 1.0 · Stand: 11. August 2026

Die Software „SabiaOS“ (im Folgenden: „die Software“) wird von der Sabia GmbH, Stuckstraße 10, 12435 Berlin, Deutschland, vertreten durch die Geschäftsführer Lukas Wagner und Patrick Alex, E-Mail: datenschutz@sabia.de (im Folgenden: „Sabia“, „wir“ oder „uns“), als Software-as-a-Service für Finanzberatungsunternehmen und unabhängige Finanzberater bereitgestellt.

Diese Datenschutzerklärung informiert Sie darüber, welche personenbezogenen Daten wir als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO verarbeiten, wenn Sie die Software als Kunde oder Nutzer verwenden oder mit uns in Kontakt treten, und welche Rechte Ihnen zustehen. Sabia hat die Voraussetzungen einer Benennungspflicht nach Art. 37 DSGVO geprüft und derzeit keinen Datenschutzbeauftragten benannt; diese Prüfung wird bei Änderungen von Art, Umfang und Zwecken der Verarbeitung wiederholt. Anfragen zum Datenschutz richten Sie bitte an datenschutz@sabia.de.

1. Rollenverteilung: Daten Ihrer Endkunden

Soweit Sie oder Ihre Endkunden im Rahmen der Nutzung der Software personenbezogene Daten Ihrer Endkunden und Interessenten erfassen, eingeben oder über angebundene Schnittstellen (z. B. die PSD2-Kontoanbindung) abrufen lassen, sind Sie bzw. Ihr Unternehmen datenschutzrechtlich Verantwortlicher; Sabia verarbeitet diese Daten ausschließlich als Auftragsverarbeiter im Sinne des Art. 28 DSGVO. Dies gilt auch für Daten, die Endkunden über einen eigenen Zugang zur Mandanten-Web-App selbst eingeben oder dort abrufen lassen: Diese Verarbeitung erfolgt für Sie und in Ihrer Verantwortung. Die Einzelheiten regelt der Vertrag über die Auftragsverarbeitung (AVV), der Bestandteil des Nutzungsvertrages ist. Die Information der betroffenen Endkunden nach Art. 12 ff. DSGVO obliegt Ihnen. Die nachfolgenden Abschnitte betreffen die Verarbeitungen, für die Sabia selbst Verantwortlicher ist.

2. Bereitstellung der Software; Logfiles

Bei jedem Zugriff auf die Software werden automatisch Daten erhoben, die für die Bereitstellung und den sicheren Betrieb technisch erforderlich sind: IP-Adresse, Datum und Uhrzeit des Zugriffs, Typ und Version von Browser und Betriebssystem, Geräteinformationen, Referrer-URL sowie technische Protokolldaten des Servers.

Zwecke: Bereitstellung der Software und ihrer Funktionen, Gewährleistung von Stabilität und Sicherheit der Systeme, Vorbeugung und Beseitigung von Missbrauch und Fehlfunktionen. Rechtsgrundlagen: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an einem funktionsfähigen, sicheren Betrieb). Speicherdauer: solange dies für

den sicheren Betrieb und die Aufklärung von Störungen erforderlich ist; die konkrete Aufbewahrung richtet sich nach den Voreinstellungen der eingesetzten Hosting-Dienstleister. Bei sicherheitsrelevanten Vorfällen kann eine längere Speicherung zur Aufklärung erforderlich sein.

3. Registrierung und Nutzeraccounts

Zur Nutzung der Software legen Sie bzw. Ihre Mitarbeiter Nutzeraccounts an. Dabei verarbeiten wir insbesondere: Name, geschäftliche E-Mail-Adresse, Firmenname und -anschrift, Authentifizierungsdaten (Passwort-Hash, Login-Tokens) sowie Metadaten zur Kontoaktivität (z. B. Zeitpunkt des Logins).

Zwecke: Einrichtung und Verwaltung der Accounts, Authentifizierung, Durchsetzung der Nutzungsbedingungen, Kommunikation zu technischen oder rechtlichen Hinweisen und Updates. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO; gegenüber Mitarbeitern des Kunden zusätzlich Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Bereitstellung des Dienstes gegenüber dem Kunden). Speicherdauer: für die Dauer des Vertragsverhältnisses; danach Löschung oder Anonymisierung, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

4. Buchung und Zahlungsabwicklung (Stripe)

Die Buchung des Abonnements und die Zahlungsabwicklung erfolgen über den Zahlungsdienstleister Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland (mit Konzerngesellschaften, u. a. Stripe, Inc., USA). Ihre Zahlungsdaten (z. B. Bankverbindung oder Kreditkartendaten) geben Sie unmittelbar auf den Seiten von Stripe ein; Sabia erhält keine vollständigen Zahlungsdaten, sondern im Wesentlichen Bestätigungen, Statusinformationen und die für die Rechnungsstellung erforderlichen Angaben.

Zwecke: Vertragsschluss, Abrechnung und Zahlungsabwicklung, Erfüllung steuer- und handelsrechtlicher Pflichten. Rechtsgrundlagen: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) und Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Verpflichtungen). Soweit erforderlich, werden Rechnungsdaten an unsere Steuerberatung weitergegeben. Speicherdauer: nach Maßgabe der gesetzlichen Aufbewahrungsfristen. Weitere Informationen zur Verarbeitung durch Stripe: <https://stripe.com/de/privacy>.

5. KI- und Sprachfunktionen

Die Software enthält KI-Funktionen (insbesondere den KI-Mitarbeiter), die derzeit über Google Cloud Vertex AI (Google Ireland Limited, Dublin, Irland / Google LLC, USA) mit Modellen der Gemini-Familie über europäische Endpunkte bereitgestellt werden. Verarbeitet werden Ihre Eingaben (Prompts) sowie der zur Beantwortung erforderliche Kontext aus der Software. Nutzen Sie Sprachfunktionen, werden zusätzlich Sprachaufnahmen und die daraus erzeugten Transkripte über die Sprachdienste desselben Anbieters (Speech-to-Text, Text-to-Speech) verarbeitet. Soweit dabei Daten Ihrer Endkunden verarbeitet werden, geschieht dies in unserer Rolle als Auftragsverarbeiter nach Maßgabe des AVV (siehe Ziffer 1). Eine Nutzung der Eingaben zum Training der allgemeinen Modelle des Anbieters ist nach den von uns genutzten Vertragskonditionen ausgeschlossen.

Zwecke: Bereitstellung der KI- und Sprachfunktionen, Qualitätssicherung. Rechtsgrundlagen: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an einem funktionierenden, qualitativ hochwertigen Dienst). Speicherdauer: Ihre Eingaben, die Chatverläufe, die Aufrufe von Funktionen der Software sowie Sprachaufnahmen und die daraus erzeugten Transkripte

werden als Inhalte der Software behandelt und für die Dauer des Vertragsverhältnisses gespeichert; im Übrigen gilt Ziffer 12. Ein gesondertes, kürzer aufbewahrtes Protokoll der KI-Aufrufe führen wir nicht.

Der KI-Mitarbeiter kann eine Websuche über den Dienst Exa (Exa Labs, Inc., USA) durchführen, um in öffentlich zugänglichen Quellen zu recherchieren. Übermittelt wird dabei die jeweilige Suchanfrage. Der Assistent ist so konfiguriert, dass er ausschließlich sachbezogene Rechercheanfragen stellt und dabei keine personenbezogenen Mandantendaten verwendet; eine technische Garantie hierfür besteht nicht. Sie entscheiden als Verantwortlicher, welche Inhalte Sie in den Assistenten eingeben, und sollten keine personenbezogenen Daten Ihrer Mandanten in Rechercheanfragen einfließen lassen. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung). Die Websuche lässt sich auf Wunsch für Ihre Organisation deaktivieren.

Die Ergebnisse der KI-Funktionen haben ausschließlich unterstützenden Charakter. Eine ausschließlich automatisierte Entscheidung im Sinne des Art. 22 DSGVO ist damit nicht verbunden (siehe Ziffer 15).

6. Kalendersynchronisation

Wenn Sie die Kalendersynchronisation aktivieren, verbinden wir auf Ihre Veranlassung Ihr Kalenderkonto bei Google (Google Ireland Limited, Irland) oder Microsoft (Microsoft Ireland Operations Limited, Irland). Verarbeitet werden dabei die für die Synchronisation erforderlichen Termini (u. a. Titel, Beschreibung, Zeitraum, Teilnehmende, Organisator, Ort und Konferenzdaten) sowie die zugehörigen Zugriffstoken. Die Verbindung umfasst auch schreibenden Zugriff: Termine können aus der Software heraus angelegt, geändert und abgesagt werden, auch durch den KI-Mitarbeiter auf Veranlassung eines Nutzers.

Zweck: Anzeige und Verknüpfung von Terminen mit Mandanten und Aufgaben in der Software sowie Anlage und Pflege von Terminen. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung); die Aktivierung selbst ist freiwillig. Speicherdauer: bis zur Trennung der Verbindung oder zur Löschung des Kontos; mit der Trennung werden die gespeicherten Termini und die Zugriffstoken gelöscht.

7. Digitale Signatur (Yousign / Youtrust)

Für die digitale Signatur von Dokumenten (z. B. der Geeignetheitserklärung) setzen wir den eIDAS-konformen Signatordienst der Yousign SAS, Caen, Frankreich, ein, die unter der Marke „Youtrust“ auftritt. Verarbeitet werden dabei die für die Signatur erforderlichen Daten der Unterzeichnenden (z. B. Name, E-Mail-Adresse, Zeitstempel, Signaturnachweise). Soweit Endkunden unterzeichnen, erfolgt die Verarbeitung im Auftrag des Kunden nach Maßgabe des AVV. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO. Die Verarbeitung findet in der EU statt; für Signaturnachweise gelten die Aufbewahrungsvorgaben der eIDAS-Verordnung.

8. Produktanalyse (PostHog)

Zur Verbesserung der Software erheben wir Nutzungsstatistiken mit PostHog (PostHog, Inc., USA; EU-Hosting in Frankfurt). Wir unterscheiden zwei Verarbeitungen:

- Serverseitige Ereignisse: Wir protokollieren, welche Funktionen der Software genutzt werden. Diese Ereignisse sind Ihrem Nutzerkonto und Ihrer Organisation zugeordnet und können hierzu Ihren Namen, Ihre E-Mail-Adresse und den Namen Ihres Unternehmens umfassen. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Analyse und Verbesserung des Dienstes sowie an der Erkennung von Fehlern und Missbrauch). Sie können dieser Verarbeitung nach Art. 21 DSGVO widersprechen (siehe Ziffer 13).
- Analyse im Browser einschließlich Sitzungsaufzeichnungen: Erfassung von Seitenaufrufen, Interaktionen und Sitzungsaufzeichnungen (Session Recordings). Die Aufzeichnungen geben den Bildschirminhalt wieder; Eingaben und angezeigte Inhalte werden dabei nicht maskiert. Sie können daher auch Inhalte aus der Mandantenverwaltung umfassen, einschließlich Finanz-, Konto- und Dokumentinhalten. Diese Erfassung wird ausschließlich nach Ihrer Einwilligung über den Cookie-Banner aktiviert und kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Rechtsgrundlage: § 25 Abs. 1 TDDDG und Art. 6 Abs. 1 lit. a DSGVO (Einwilligung).

Die Aufzeichnung erfolgt auch in der Mandanten-Web-App und dort ebenfalls nur nach Einwilligung der jeweiligen Endnutzerin oder des jeweiligen Endnutzers über den Cookie-Banner. Soweit dabei Daten von Endkunden unseres Kunden verarbeitet werden, geschieht dies in unserer Rolle als Auftragsverarbeiter nach Maßgabe des AVV (siehe Ziffer 1). Speicherdauer: solange dies für die Analyse und Verbesserung des Dienstes erforderlich ist; die konkrete Aufbewahrung richtet sich nach der bei PostHog eingestellten Aufbewahrungsfrist. Sitzungsaufzeichnungen werden von PostHog nach Ablauf der eingestellten Frist automatisch gelöscht.

9. Kontakt und Support

Bei Kontaktaufnahme per E-Mail oder über Supportkanäle verarbeiten wir Ihre Angaben (Name, E-Mail-Adresse, Inhalt der Anfrage) zur Bearbeitung der Anfrage und für etwaige Anschlussfragen. Rechtsgrundlagen: Art. 6 Abs. 1 lit. b DSGVO bzw. Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an effizienter Kommunikation). Speicherdauer: bis zur abschließenden Bearbeitung; darüber hinaus nur nach Maßgabe gesetzlicher Aufbewahrungspflichten.

10. Empfänger der Daten

Wir geben personenbezogene Daten nur weiter, soweit dies in dieser Datenschutzerklärung beschrieben, zur Vertragserfüllung erforderlich, gesetzlich zulässig oder von Ihnen gestattet ist. Wir setzen folgende Dienstleister ein, mit denen – soweit sie als Auftragsverarbeiter tätig sind – Verträge nach Art. 28 DSGVO bestehen:

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

- Resend, Inc., USA – Versand von Transaktions- und Einladungs-E-Mails – Standardvertragsklauseln;
- Slack Technologies (Salesforce, Inc.), USA – interne Benachrichtigungen zu Support-, Registrierungs- und Exportvorgängen – DPF, ergänzend Standardvertragsklauseln;
- Google Ireland Limited / Google LLC – KI-Funktionen über Google Cloud Vertex AI sowie Sprachdienste; Kalendersynchronisation – DPF (Google LLC), ergänzend Standardvertragsklauseln;
- Microsoft Ireland Operations Limited – Kalendersynchronisation, sofern aktiviert – Verarbeitung in der EU bzw. Standardvertragsklauseln;
- WealthAPI GmbH, Deutschland – PSD2-Kontoinformationen (regulierter Kontoinformationsdienst) – Verarbeitung in der EU;
- Yousign SAS, Frankreich – elektronische Signatur – Verarbeitung in der EU;
- Exa Labs, Inc., USA – Websuche des KI-Mitarbeiters – Standardvertragsklauseln;
- PostHog, Inc., USA – Produktanalyse – EU-Hosting (Frankfurt), DPF, ergänzend Standardvertragsklauseln;
- Stripe Payments Europe, Ltd., Irland (mit Konzerngesellschaften, u. a. in den USA) – Zahlungsabwicklung – DPF bzw. Standardvertragsklauseln; Stripe verarbeitet Zahlungsdaten teilweise in eigener Verantwortlichkeit.

Darüber hinaus können Daten an unsere Steuer- und Rechtsberater sowie – bei gesetzlicher Verpflichtung oder zur Rechtsverfolgung – an Behörden und Gerichte weitergegeben werden (Art. 6 Abs. 1 lit. c und f DSGVO).

11. Datenübermittlungen in Drittländer

Soweit die vorgenannten Dienstleister Daten in Ländern außerhalb des Europäischen Wirtschaftsraums (insbesondere in den USA) verarbeiten, erfolgt dies auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission zum EU-US Data Privacy Framework (Art. 45 DSGVO), von Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO) oder – in Ausnahmefällen – nach Art. 49 DSGVO. Eine Kopie der jeweils einschlägigen Garantien stellen wir auf Anfrage zur Verfügung.

12. Speicherdauer

Wir löschen oder anonymisieren personenbezogene Daten, sobald sie für die genannten Zwecke nicht mehr erforderlich sind. Eine feste Frist lässt sich nicht für jede Verarbeitung angeben; maßgeblich sind die folgenden Kriterien:

- Konto- und Nutzungsdaten: für die Dauer des Vertragsverhältnisses und darüber hinaus, solange dies für die Abwicklung des Vertrages erforderlich ist;
- Inhalte, die Sie in der Software verwalten (Mandantendaten): für die Dauer des Vertragsverhältnisses; nach dessen Ende nach Maßgabe des AVV;
- Server- und Zugriffsprotokolle: solange dies für den sicheren Betrieb und die Aufklärung von Störungen erforderlich ist, nach Maßgabe der Voreinstellungen der eingesetzten Hosting-Dienstleister;

- Eingaben, Chatverläufe, Sprachaufnahmen und Transkripte der KI- und Sprachfunktionen: wie die übrigen Inhalte, für die Dauer des Vertragsverhältnisses;
- Produktanalyse einschließlich Sitzungsaufzeichnungen: solange dies für die Analyse und Verbesserung des Dienstes erforderlich ist, nach Maßgabe der beim Anbieter eingestellten Aufbewahrungsfrist;
- Sicherungskopien (Backups): bis zum turnusmäßigen Überschreiben durch den Hosting-Dienstleister;
- Rechnungs- und Buchhaltungsdaten: nach Maßgabe der gesetzlichen Aufbewahrungsfristen.

Darüber hinaus speichern wir personenbezogene Daten, solange gesetzliche Aufbewahrungspflichten bestehen oder die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist; maßgeblich sind insoweit die gesetzlichen Verjährungsfristen. Auf Anfrage teilen wir Ihnen die für eine bestimmte Verarbeitung konkret geltende Aufbewahrung mit.

13. Ihre Rechte als betroffene Person

Sie haben gegenüber Sabia das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO) und Datenübertragbarkeit (Art. 20 DSGVO) sowie das Recht, eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen (Art. 7 Abs. 3 DSGVO). Zur Ausübung Ihrer Rechte genügt eine formlose Mitteilung an datenschutz@sabia.de.

Widerspruchsrecht (Art. 21 DSGVO): Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt, Widerspruch einzulegen. Wir verarbeiten die Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Beschwerderecht: Sie haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren (Art. 77 DSGVO). Für Sabia zuständig ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Friedrichstraße 219, 10969 Berlin, www.datenschutz-berlin.de.

14. Pflicht zur Bereitstellung von Daten

Die Bereitstellung der für Buchung, Registrierung und Vertragserfüllung erforderlichen Daten ist für die Nutzung der Software erforderlich; ohne diese Daten kann der Vertrag nicht durchgeführt werden. Die Nutzung einzelner Funktionen (z. B. KI-Funktionen, Signatur, Kontoanbindung) ist freiwillig; ohne die jeweilige Nutzung bzw. Einwilligung stehen lediglich die entsprechenden Funktionen nicht zur Verfügung.

15. Keine automatisierte Entscheidungsfindung

Eine ausschließlich auf automatisierter Verarbeitung – einschließlich Profiling – beruhende Entscheidungsfindung im Sinne des Art. 22 DSGVO, die Ihnen gegenüber rechtliche Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt, findet nicht statt.

16. Datensicherheit

Wir setzen technische und organisatorische Maßnahmen nach dem Stand der Technik ein, um Ihre Daten gegen unbefugte Zugriffe, Verlust und Manipulation zu schützen, insbesondere TLS-Verschlüsselung der Datenübertragung, verschlüsselte Speicherung, rollenbasierte Zugriffsbeschränkungen nach dem Need-to-know-Prinzip, Zwei-Faktor-Authentifizierung für administrative Zugänge sowie regelmäßige Datensicherungen. Für Ihre eigenen Nutzerkonten steht die Zwei-Faktor-Authentifizierung als Option zur Verfügung; wir empfehlen ihre Aktivierung.

17. Änderungen dieser Datenschutzerklärung

Wir passen diese Datenschutzerklärung an, wenn sich die Rechtslage, die Rechtsprechung oder unser Dienst ändert. Die jeweils aktuelle Fassung ist innerhalb der Software abrufbar; über wesentliche Änderungen informieren wir Sie zusätzlich per E-Mail oder im Dienst.