

Vertrag zur Auftragsverarbeitung

Version 1.0 · gilt ab 25. Oktober 2026 · Stand Oktober 2026

Wenn du in finflow Daten von Kunden, Interessenten, Tippgebern oder Mitarbeitenden verarbeitest, tun wir das in deinem Auftrag. Dieser Vertrag regelt nach Art. 28 DSGVO, wie wir mit diesen Daten umgehen. Er gilt zusammen mit den AGB und wird mit ihnen Vertragsbestandteil.

Vertragsparteien

Dieser Vertrag gilt zwischen dem Kunden, der finflow nutzt („Auftraggeber“, „du“), und der finflow GmbH, Am Sandtorkai 27, 20457 Hamburg („Auftragnehmer“, „wir“). Begriffe wie „personenbezogene Daten“, „Verarbeitung“ oder „Unterauftragsverarbeiter“ haben die Bedeutung aus Art. 4 DSGVO.

1. Gegenstand und Dauer

1.1 Wir verarbeiten personenbezogene Daten für dich, um dir finflow nach dem Hauptvertrag (den AGB und deiner Buchung) bereitzustellen. Gegenstand, Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen beschreibt Anlage 1.

1.2 Dieser Vertrag gilt, solange wir für dich personenbezogene Daten verarbeiten. Er endet nicht vor Abschluss der Löschung oder Rückgabe nach Ziffer 11.

2. Ort der Verarbeitung

2.1 Wir verarbeiten die Daten in der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Die Datenbank von finflow wird in Frankfurt am Main betrieben.

2.2 Eine Verarbeitung außerhalb dieser Staaten erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, etwa auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission oder der EU-Standardvertragsklauseln. Welche Unterauftragsverarbeiter das betrifft, steht in Anlage 3.

3. Weisungen

3.1 Wir verarbeiten die Daten nur auf deine dokumentierte Weisung. Deine Weisungen ergeben sich aus diesem Vertrag, dem Hauptvertrag und der Art, wie du finflow einstellt und nutzt, etwa wenn du eine Übergabe an ein angebundenes System auslöst. Weitere Weisungen erteilst du in Textform.

3.2 Sind wir nach dem Recht der EU oder eines Mitgliedstaats zu einer anderen Verarbeitung verpflichtet, teilen wir dir das vorher mit, soweit das Recht eine solche Mitteilung nicht verbietet.

3.3 Halten wir eine Weisung für rechtswidrig, sagen wir es dir unverzüglich. Wir dürfen die Ausführung aussetzen, bis du die Weisung bestätigst oder änderst.

3.4 Weisungen nehmen bei uns die in Anlage 1 genannten Personen entgegen. Auf deiner Seite darf jede Person Weisungen erteilen, die dich insoweit vertreten kann, etwa die Geschäftsführung oder Inhaber und Admins in finflow.

4. Vertraulichkeit

Alle Personen, die bei uns Zugriff auf deine Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht. Sie erhalten nur den Zugriff, den sie für ihre Aufgabe brauchen. Die Pflicht gilt über das Ende ihrer Tätigkeit hinaus.

5. Sicherheit der Verarbeitung

5.1 Wir treffen technische und organisatorische Maßnahmen nach Art. 32 DSGVO, die dem Risiko der Verarbeitung angemessen sind. Sie stehen in Anlage 2 und sind verbindlich.

5.2 Wir dürfen die Maßnahmen an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentieren wir und teilen sie dir auf Anfrage mit.

6. Unterauftragsverarbeiter

6.1 Du erlaubst uns, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten stehen in Anlage 3 und gelten als genehmigt.

6.2 Wollen wir einen Unterauftragsverarbeiter hinzunehmen oder ersetzen, informieren wir dich mindestens vier Wochen vorher in Textform. Du kannst der Änderung innerhalb dieser Frist aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Können wir dem Einwand nicht abhelfen, dürfen beide Seiten den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

6.3 Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht. Wir bleiben dir gegenüber für seine Pflichten verantwortlich.

6.4 Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Systeme, die du selbst mit finflow verbindest und an die finflow auf deine Weisung Daten übermittelt, etwa CRM-Systeme, Maklersoftware oder dein E-Mail- und Kalenderanbieter. Für sie bist du verantwortlich und schließt bei Bedarf eigene Verträge.

7. Unterstützung

7.1 Wir unterstützen dich mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 22 DSGVO zu beantworten, etwa auf Auskunft, Berichtigung oder Löschung. Viele dieser Schritte kannst du direkt in finflow erledigen.

7.2 Wendet sich eine betroffene Person direkt an uns, leiten wir die Anfrage unverzüglich an dich weiter und beantworten sie nicht selbst, außer du weist uns dazu an.

7.3 Wir unterstützen dich bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen nach Datenschutzverletzungen, bei Datenschutz-Folgenabschätzungen und bei der Konsultation der Aufsichtsbehörde (Art. 32 bis 36 DSGVO), jeweils mit den Informationen, die uns zur Verfügung stehen.

8. Verletzungen des Schutzes personenbezogener Daten

8.1 Erfahren wir von einer Verletzung des Schutzes deiner Daten, informieren wir dich unverzüglich. Die Mitteilung enthält, soweit bekannt, die Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der Personen und Datensätze, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen.

8.2 Wir ergreifen sofort die nötigen Maßnahmen, um die Daten zu sichern und mögliche Folgen zu begrenzen, und stimmen das weitere Vorgehen mit dir ab.

9. Nachweise und Kontrollen

9.1 Wir stellen dir auf Anfrage die Informationen bereit, die nötig sind, um die Einhaltung dieses Vertrags nachzuweisen, etwa aktuelle Dokumentationen der Maßnahmen aus Anlage 2.

9.2 Du oder ein von dir beauftragter, zur Verschwiegenheit verpflichteter Prüfer dürfen die Einhaltung nach vorheriger Ankündigung mit angemessener Frist während unserer Geschäftszeiten überprüfen, in der Regel einmal im Jahr und zusätzlich aus konkretem Anlass. Die Prüfung darf den Betrieb nicht unverhältnismäßig stören und muss die Vertraulichkeit der Daten anderer Kunden wahren.

9.3 Prüft uns eine Aufsichtsbehörde zu Verarbeitungen nach diesem Vertrag, informieren wir dich über das Ergebnis, soweit es dich betrifft.

10. Kontaktperson für Datenschutz

Fragen zu diesem Vertrag richtest du an hello@finflow.io. Wir haben derzeit keinen Datenschutzbeauftragten benannt. Sobald wir einen benennen, teilen wir dir seine Kontaktdaten mit.

11. Löschung und Rückgabe

11.1 Nach dem Ende des Hauptvertrags speichern wir deine Daten noch höchstens einen Monat, damit du sie exportieren kannst, oder im Einzelfall bis zu einem Export- oder Löschdatum, das du uns nennst. Danach löschen wir sie einschließlich vorhandener Kopien, soweit nicht das Recht der EU oder eines Mitgliedstaats eine Speicherung vorschreibt. In Datensicherungen enthaltene Daten werden im Rahmen der regelmäßigen Rotation überschrieben.

11.2 Auf Wunsch bestätigen wir dir die Löschung in Textform.

12. Haftung

Für Schäden aus einer Verletzung der DSGVO haften die Parteien nach Art. 82 DSGVO. Im Verhältnis zueinander gelten im Übrigen die Haftungsregeln des Hauptvertrags.

13. Schlussbestimmungen

13.1 Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor.

13.2 Der Vertrag wird elektronisch geschlossen, indem du den AGB bei der Buchung zustimmst oder ihn in finflow bestätigst. Die Textform nach Art. 28 Abs. 9 DSGVO ist damit gewahrt. Änderungen bedürfen ebenfalls der Textform.

13.3 Ein Zurückbehaltungsrecht an deinen Daten ist ausgeschlossen. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. Es gilt deutsches Recht; Gerichtsstand ist der des Hauptvertrags.

Anlage 1: Gegenstand der Verarbeitung

Zweck und Art der Verarbeitung

Bereitstellung der Software finflow für Kreditvermittler und ihre Vertriebsorganisationen: Betrieb, Hosting, Wartung, Support und Weiterentwicklung. Dazu gehören das Erheben, Speichern, Ordnen, Anzeigen, Auswerten, Übermitteln auf Weisung und Löschen von Daten in diesen Bereichen:

- Workspace: Kontakte und Unternehmen, Kalender und Aufgaben, E-Mail, Chat, Dokumente;
- Leadflow: Anbindung von Tippgebern, Empfang von Finanzierungsanfragen mit Einwilligung, Vergütungsregeln;

- Salesflow: Qualifizierung von Anfragen bis zur Übergabe;
- Organisation: Standorte, Rollen und Rechte der Nutzer;
- Vela: KI-gestützte Aufbereitung von Anfragen mit einem Score für Vollständigkeit und Machbarkeit; Vela prüft nicht die Kreditwürdigkeit einer Person und entscheidet nicht über Personen oder Verträge;
- Übermittlung an Systeme, die du verbindest, wenn du sie auslöst oder einstellst.

Kategorien betroffener Personen

- Nutzer des Auftraggebers, etwa Mitarbeitende, freie Berater und Standortleitungen;
- Tippgeber und deren Ansprechpersonen, etwa Immobilienmakler;
- Finanzierungsinteressenten, Kunden und deren Mitantragsteller;
- sonstige Geschäftskontakte des Auftraggebers.

Arten personenbezogener Daten

- Kontakt- und Stammdaten, etwa Name, Anschrift, E-Mail, Telefonnummer, Unternehmen, Rolle;
- Angaben zum Finanzierungsvorhaben, etwa Finanzierungswunsch, Objektdaten, Kaufpreis, Eigenkapital und Unterlagen, die der Auftraggeber oder Interessenten hochladen;
- Einwilligungen und deren Nachweise;
- Kommunikationsinhalte aus E-Mail, Chat und Notizen;
- Vergütungsvereinbarungen und -abrechnungen mit Tippgebern;
- Nutzungs- und Protokolldaten, etwa Anmeldungen, Aktivitäten, IP-Adressen;
- Eingaben und Ergebnisse der KI-Funktionen.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeiten wir nur, wenn du sie selbst in finflow einstellst. Dafür ist finflow nicht vorgesehen.

Weisungsempfänger beim Auftragnehmer

Christian Kunde (Geschäftsführer) und Marcus Schmidt (CTO), erreichbar über hello@finflow.io.

Anlage 2: Technische und organisatorische Maßnahmen

Für die Verarbeitung nach diesem Vertrag gelten die folgenden Maßnahmen nach Art. 32 DSGVO.

Vertraulichkeit

- Betrieb der Anwendung und Datenhaltung ausschließlich in Rechenzentren in Deutschland: Anwendung bei Hetzner in Nürnberg, Datenbank und Dateispeicher bei Supabase in Frankfurt am Main. Physischer Zutritt zu den Rechenzentren nur nach den Kontrollen der Anbieter; Hetzner ist nach

eigenen Angaben nach ISO/IEC 27001 zertifiziert, Supabase nach eigenen Angaben nach SOC 2 Typ II geprüft.

- Anmeldung an finflow mit persönlichem Zugang und Zwei-Faktor-Anmeldung.
- Rollen und Rechte in finflow: Jede Person sieht und bearbeitet nur, was ihre Rolle erlaubt, etwa eigene Datensätze, den eigenen Standort oder alles.
- Strikte Trennung der Daten verschiedener Kunden (Mandantentrennung).
- Zugriff des finflow-Teams auf Kundendaten nur, soweit es für Betrieb und Support nötig ist, mit persönlichen Zugängen.

Integrität

- Verschlüsselte Übertragung aller Daten zwischen Endgerät und finflow sowie zwischen den Systemen (TLS).
- Verschlüsselte Speicherung der Daten.
- Protokollierung sicherheitsrelevanter Ereignisse wie Anmeldungen; Aufbewahrung der Protokolle für 90 Tage.

Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherungen, getrennt vom laufenden Betrieb gespeichert.
- Überwachung der Verfügbarkeit mit dem Ziel von 99,9 % im Monatsmittel.
- Einspielen von Sicherheitsupdates ohne vermeidbare Verzögerung.

Organisation und Überprüfung

- Verpflichtung aller Personen mit Datenzugriff auf Vertraulichkeit.
- Einsatz von Unterauftragsverarbeitern nur mit Vertrag nach Art. 28 DSGVO.
- Überprüfung und Anpassung der Maßnahmen, wenn sich Technik, Risiken oder die Verarbeitung ändern.

Anlage 3: Unterauftragsverarbeiter

- **Hetzner Online GmbH**, Industriestr. 25, 91710 Gunzenhausen, Deutschland: Hosting der Anwendung. Ort: Rechenzentrum Nürnberg, Deutschland.
- **Supabase Inc.**, USA: Betrieb der Datenbank und Dateispeicherung. Ort: Europäische Union, Frankfurt am Main. Für mögliche Zugriffe aus den USA, etwa im Support, gelten die EU-Standardvertragsklauseln.
- **Anthropic, PBC**, 548 Market Street, PMB 90375, San Francisco, CA 94104, USA: Sprachmodelle für Vela. Ort: USA. Grundlage: Datenverarbeitungsbedingungen von Anthropic mit EU-Standardvertragsklauseln. Eingaben und Ergebnisse werden nicht zum Training von Modellen verwendet.

- **Google Ireland Limited**, Gordon House, Barrow Street, Dublin 4, Irland: Versand von E-Mails aus finflow (Google Workspace). Eine Übermittlung an die Google LLC in den USA ist möglich; sie ist nach dem EU-U.S. Data Privacy Framework zertifiziert.
- **Plus Five Five, Inc. (Resend)**, 2261 Market Street #5039, San Francisco, CA 94114, USA: Versand von E-Mails aus finflow. Versand über Server in der EU (Irland); für Übermittlungen in die USA gelten die EU-Standardvertragsklauseln.