Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Diese Vereinbarung zur Auftragsverarbeitung („AVV“) wird Bestandteil des Nutzungsvertrags durch Akzeptanz der Allgemeinen Geschäftsbedingungen der finban GmbH.

finban GmbH
Jägerstraße 27b
16540 Hohen Neuendorf
– nachfolgend „Auftragsverarbeiter“ –

und

dem jeweiligen Kunden, der mit dem Auftragsverarbeiter einen Vertrag über die Nutzung der SaaS-Plattform „finban“ schließt und den anwendbaren Allgemeinen Geschäftsbedingungen zustimmt,

– nachfolgend „Verantwortlicher“ –

– gemeinsam „Parteien“ –

§ 1 Gegenstand und Geltung

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Nutzung der SaaS-Plattform „finban“.

Diese Vereinbarung gilt nur, soweit der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Eigene Verarbeitungen des Auftragsverarbeiters, die nicht im Auftrag des Verantwortlichen erfolgen, sind nicht Gegenstand dieser Vereinbarung.

Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen ergeben sich aus Anlage 1.

§ 2 Verarbeitung auf dokumentierte Weisung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit nicht eine Verpflichtung zur Verarbeitung nach dem Recht der Europäischen Union oder eines Mitgliedstaats besteht, dem der Auftragsverarbeiter unterliegt. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Bestimmungen dieser Vereinbarung sowie des Hauptvertrags gelten als dokumentierte Weisungen des Verantwortlichen. Einzelweisungen des Verantwortlichen bedürfen mindestens der Textform.

Hält der Auftragsverarbeiter eine Weisung des Verantwortlichen für datenschutzrechtswidrig, weist er den Verantwortlichen unverzüglich darauf hin.

§ 3 Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die zum Zeitpunkt des Vertragsschlusses bestehenden technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2.

Der Auftragsverarbeiter ist berechtigt, die technischen und organisatorischen Maßnahmen fortzuentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 5 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen nachzukommen, soweit diese Anträge die im Rahmen dieser Vereinbarung erfolgende Verarbeitung betreffen.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, soweit diese Pflichten die im Rahmen dieser Vereinbarung erfolgende Verarbeitung unmittelbar betreffen und der Auftragsverarbeiter auf Basis der ihm verfügbaren Informationen dazu in der Lage ist.

Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter, sofern eine Zuordnung zum Verantwortlichen möglich ist.

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit diese die im Auftrag verarbeiteten Daten betrifft. Sofern zum Zeitpunkt der Erstmeldung noch nicht alle Informationen vorliegen, können diese schrittweise nachgereicht werden.

§ 7 Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt. Die jeweils aktuelle Liste der Unterauftragsverarbeiter ist abrufbar unter https://finban.io/avv/.

Der Auftragsverarbeiter informiert den Verantwortlichen in Textform über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Verantwortliche kann solchen Änderungen aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information in Textform widersprechen. Im Fall eines fristgerechten und berechtigten Widerspruchs ist der Verantwortliche berechtigt, den Hauptvertrag mit einer Frist von 30 Tagen zum Monatsende außerordentlich zu kündigen. Eine Verpflichtung des Auftragsverarbeiters, den beabsichtigten Unterauftragsverarbeiter im Einzelfall durch einen alternativen Anbieter zu ersetzen oder die Leistung für den Verantwortlichen abweichend von der allgemeinen Produktarchitektur zu erbringen, besteht nicht.

Der Auftragsverarbeiter bindet Unterauftragsverarbeiter nur auf Grundlage eines Vertrags ein, der ihnen im Wesentlichen dieselben Datenschutzpflichten auferlegt, wie sie in dieser Vereinbarung festgelegt sind.

Soweit ein Unterauftragsverarbeiter personenbezogene Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeitet, stellt der Auftragsverarbeiter sicher, dass ein geeigneter Transfermechanismus gemäß Kapitel V DSGVO besteht, insbesondere durch Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO oder aufgrund eines Angemessenheitsbeschlusses der Europäischen Kommission.

§ 8 Nachweise und Prüfungen

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser Vereinbarung nachzuweisen. Der Nachweis erfolgt vorrangig durch Vorlage geeigneter Unterlagen, Auskünfte, Zertifizierungen oder Prüfberichte auf remote oder digitalem Weg.

Soweit die vorgelegten Nachweise im Einzelfall aus nachvollziehbaren datenschutzrechtlichen Gründen nicht ausreichen, ist der Verantwortliche berechtigt, nach Vorankündigung von mindestens 14 Kalendertagen und während der üblichen Geschäftszeiten eine weitergehende Prüfung durchzuführen oder durch einen zur

Vertraulichkeit verpflichteten Dritten durchführen zu lassen. Prüfungen sind auf das erforderliche Maß zu beschränken, dürfen die Vertraulichkeit von Daten anderer Kunden des Auftragsverarbeiters nicht beeinträchtigen und haben auf Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters angemessen Rücksicht zu nehmen.

Sofern kein begründeter Anlass besteht, soll eine weitergehende Prüfung nicht häufiger als einmal pro Kalenderjahr erfolgen. Die angemessenen Kosten einer vom Verantwortlichen veranlassten Prüfung, die über die Vorlage von Dokumenten und Auskünften hinausgeht, trägt der Verantwortliche.

§ 9 Rückgabe und Löschung

Nach Beendigung der vertragsgegenständlichen Leistungen löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen die im Auftrag verarbeiteten personenbezogenen Daten zurück, sofern keine gesetzliche Verpflichtung zur weiteren Speicherung besteht. Ein Verlangen auf Rückgabe ist innerhalb von 14 Tagen nach Vertragsende in Textform geltend zu machen. Geht innerhalb dieser Frist kein Verlangen auf Rückgabe ein, ist der Auftragsverarbeiter berechtigt, die personenbezogenen Daten zu löschen. Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format, soweit dies technisch mit vertretbarem Aufwand möglich ist.

Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters bleiben unberührt. In diesem Fall beschränkt der Auftragsverarbeiter die Verarbeitung der betroffenen Daten auf die Erfüllung der gesetzlichen Aufbewahrungspflicht.

Löschungen in Backup- und Wiederherstellungssystemen erfolgen im Rahmen der üblichen Überschreib- und Löschzyklen, soweit eine sofortige Löschung dort nicht mit vertretbarem Aufwand möglich ist.

§ 10 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform.

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Im Übrigen gelten die gesetzlichen Vorschriften der DSGVO.

Anlage 1 – Gegenstand, Dauer, Art und Zweck der Verarbeitung

1. Gegenstand der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Zusammenhang mit der Bereitstellung und Nutzung der SaaS-Plattform „finban“.

2. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des zwischen den Parteien bestehenden Vertrags über die Nutzung von finban sowie bis zur vollständigen Rückgabe oder Löschung der personenbezogenen Daten nach Maßgabe dieser Vereinbarung.

3. Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt zur Bereitstellung der SaaS-Plattform „finban“ für Liquiditätsplanung, Budgetierung, Forecasting, Finanzanalysen und Berichte.

Die Verarbeitung umfasst insbesondere: die Bereitstellung und Verwaltung von Benutzerkonten und Zugriffsrechten; den Import, die Entgegennahme, Synchronisation und Verarbeitung von Daten aus vom Verantwortlichen aktivierten Datenquellen, Integrationen und Importfunktionen; die Strukturierung, Kategorisierung, Auswertung und Darstellung dieser Daten innerhalb der Anwendung; die Erstellung von Planungen, Prognosen, Übersichten und Berichten; sowie den technischen Betrieb der Plattform einschließlich Hosting, Datensicherung, Fehlerbehebung und anlassbezogener technischer Unterstützung.

Die Verarbeitung umfasst alle hierfür erforderlichen Verarbeitungsvorgänge im Sinne des Art. 4 Nr. 2 DSGVO.

4. Kategorien personenbezogener Daten

Welche Kategorien personenbezogener Daten Gegenstand der Verarbeitung sind, hängt davon ab, welche Daten der Verantwortliche über die Plattform, aktivierte Integrationen, Importfunktionen oder optionale Module einbringt. In Betracht kommen insbesondere:

- Benutzer- und Registrierungsdaten (Name, E-Mail-Adresse, Login-Daten, rollenbezogene Angaben);
- Finanz- und Transaktionsdaten (Banktransaktionen, Zahlungen, Rechnungen, Beträge, Fälligkeitsdaten);
- Stamm- und Geschäftspartnerdaten (Firmenname, Kunden-ID, IBAN/BIC, Kontaktdaten);
- Planungs- und Auswertungsdaten (Budget-, Forecast- und Szenariodaten);
- Personaldaten, soweit das Modul Personalplanung genutzt wird (insbesondere Mitarbeitername, Personalkosten, Vollzeit-/Teilzeitstatus, Vertragsbeginn, Vertragsende, Abteilung, Rolle und zugehörige Notizen);
- Vertragsbezogene Daten, soweit das Modul Vertragsmanagement genutzt wird (insbesondere Vertrags- und Kosteninformationen, Laufzeiten sowie Dateien und Inhalte, soweit diese vom Verantwortlichen importiert oder hochgeladen werden);
- vom Verantwortlichen eingegebene Freitextinhalte, Dateien und sonstige Nutzerinhalte.

5. Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personengruppen betroffen sein: Nutzer und Beschäftigte des Verantwortlichen; Ansprechpartner, Kunden, Interessenten, Lieferanten und sonstige Geschäftspartner des Verantwortlichen; Debitoren, Kreditoren sowie sonstige Zahlungsbeteiligte; sonstige Personen, deren Daten der Verantwortliche über aktivierte Integrationen, Importfunktionen, Freitextfelder oder Dateien in die Plattform einbringt.

6. Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sind nicht Gegenstand der vorgesehenen Verarbeitung.

Anlage 2 – Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Zugriffs- und Berechtigungskontrolle

Der Zugang zu Systemen, mit denen personenbezogene Daten verarbeitet werden, ist auf berechtigte Personen beschränkt. Für Nutzerkonten ist eine Multi-Faktor-Authentifizierung (MFA) verpflichtend. Der administrative Zugang zu Cloud-Infrastruktur und Produktivsystemen ist durch MFA abgesichert und auf einen kleinen Kreis berechtigter Personen beschränkt. Zugriffe auf produktive Kundendaten erfolgen nur, soweit dies zur Vertragserfüllung, Fehleranalyse, Sicherheit, Wartung oder anlassbezogenen Unterstützung erforderlich ist. Berechtigungen werden nach funktionalen Erfordernissen vergeben und bei Bedarf angepasst oder entzogen.

2. Vertraulichkeit und Übermittlungsschutz

Personen, die mit der Verarbeitung personenbezogener Daten befasst sind, sind zur Vertraulichkeit verpflichtet oder unterliegen einer entsprechenden gesetzlichen Verschwiegenheitspflicht. Personenbezogene Daten werden bei der elektronischen Übertragung mittels TLS-Verschlüsselung geschützt. Daten-Backups und im Datei-Speicher abgelegte personenbezogene Daten werden serverseitig mit AES-256 verschlüsselt. Der Zugriff auf produktive Datenbanken ist durch Zugriffskontrollen, Netzwerktrennung und Multi-Faktor-Authentifizierung abgesichert.

3. System- und Datentrennung

Produktiv-, Test- und Entwicklungsumgebungen werden voneinander getrennt betrieben. Personenbezogene Daten werden nur im Rahmen der jeweils vorgesehenen Zwecke und Funktionen verarbeitet.

4. Verfügbarkeit und Belastbarkeit

Der Auftragsverarbeiter trifft Maßnahmen zur Sicherstellung der Verfügbarkeit der verarbeiteten Daten und Systeme. Es bestehen automatisierte Datensicherungs- und Wiederherstellungsmaßnahmen. Die Plattform wird auf einer Infrastruktur betrieben, die nach anerkannten internationalen Standards zertifiziert ist (insbesondere ISO/IEC 27001).

5. Integrität und Nachvollziehbarkeit

Der Auftragsverarbeiter trifft Maßnahmen, um unbefugte Veränderungen von Daten und Systemen zu verhindern. Änderungen an Berechtigungen, Konfigurationen und technischen Systemen erfolgen kontrolliert und nach internen Zuständigkeiten. Sicherheitsrelevante Systemereignisse, einschließlich Anmeldungen, fehlgeschlagener Authentifizierungsversuche und administrativer Aktionen, werden protokolliert und in angemessenem Umfang nachvollziehbar gemacht.

6. Überprüfung und Fortentwicklung

Der Auftragsverarbeiter überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen in angemessenen Abständen und entwickelt sie bei Bedarf fort.

7. Verarbeitungsort

Die produktive Verarbeitung personenbezogener Daten erfolgt über die hierfür eingesetzte Infrastruktur des Auftragsverarbeiters. Soweit in Anlage 3 Unterauftragsverarbeiter benannt sind, erfolgt deren Einbindung nur im Rahmen der dort beschriebenen Leistungen.

Anlage 3 – Unterauftragsverarbeiter

Stand zum Zeitpunkt des Vertragsschlusses:

Amazon Web Services (AWS)

Hosting, Speicherung und technische Bereitstellung der Plattform sowie Speicherung von Produktdaten, Vertragsdaten und Dateien. Verarbeitungsort: Deutschland/Frankfurt.

finAPI

Abruf und Verarbeitung von Banktransaktionen sowie PayPal-Daten im Rahmen vom Verantwortlichen aktivierter Integrationen. Verarbeitungsort: Deutschland.

Unified

Verarbeitung von Daten aus vom Verantwortlichen aktivierten Drittintegrationen. Verarbeitungsort: Kanada. Transfermechanismus: Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO.

Intercom

Support- und Kommunikationsplattform; Verarbeitung von Registrierungsdaten sowie Inhalten aus Supportanfragen (Nachrichten, Anhänge, freiwillig übermittelte Screenshots), soweit vom Kunden im Supportkontext übermittelt. Verarbeitungsort: USA. Transfermechanismus: EU-U.S. Data Privacy Framework (DPF).

Brevo

Versand produktbezogener E-Mails, insbesondere für Registrierung, Passwort-Reset, Einladungen und Benachrichtigungen. Verarbeitungsort: Europäische Union.