

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO – eigenapp Fibu

Fassung 1.0 vom 20.10.2026

Vertragsparteien

Auftraggeber (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO) ist die Gesellschaft, für die dieser Vertrag in eigenapp Fibu abgeschlossen wird. Firma, Anschrift, Register sowie Name und Funktion der handelnden Person stehen im Abschlussnachweis, der Bestandteil dieses Vertrags ist.

Auftragnehmer (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO) ist die eigenapp UG (haftungsbeschränkt), Mühlenstraße 8 A, 14167 Berlin, eingetragen im Handelsregister des Amtsgerichts Charlottenburg unter HRB 213261 B, vertreten durch den Geschäftsführer Jan Michael Gerstein. Datenschutzkontakt: gerstein@eigenapp.ai.

§ 1 Gegenstand, Dauer und Hauptvertrag

(1) Der Auftragnehmer stellt dem Auftraggeber die Software eigenapp Fibu als Dienst über das Internet bereit (Finanzbuchhaltung mit Buchungsjournal, Belegarchiv, Bankabruf, Auswertungen und Exporte), soweit vereinbart auch das Belegportal (Hochladen von Belegen und Übergabe an die Buchhaltung). Dabei verarbeitet er personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers (Auftragsdaten). Gegenstand, Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Hauptvertrag ist die Vereinbarung der Parteien über die Nutzung von eigenapp Fibu in ihrer jeweils geltenden Form, auch wenn die Nutzung unentgeltlich oder zur Erprobung erfolgt. Dieser Vertrag geht in allen Fragen des Datenschutzes dem Hauptvertrag und allgemeinen Geschäftsbedingungen vor.

(3) Dieser Vertrag gilt, solange der Auftragnehmer Auftragsdaten verarbeitet, mindestens für die Laufzeit des Hauptvertrags. Er endet nicht vor Abschluss der Rückgabe und Löschung nach § 12.

§ 2 Weisungen

(1) Der Auftragnehmer verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf die Übermittlung in ein Drittland oder an eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Die Weisungen sind abschließend in diesem Vertrag und im Hauptvertrag festgelegt. Als Weisung gelten außerdem alle Einstellungen und Handlungen, die Nutzer des Auftraggebers in eigenapp Fibu vornehmen (zum Beispiel einen Bankzugang hinterlegen, einen Abruf auslösen, Belege hochladen, Exporte erzeugen, Zugänge vergeben). Weitere Weisungen erteilt der Auftraggeber in Textform an den Datenschutzkontakt des Auftragnehmers; mündliche Weisungen bestätigt er unverzüglich in Textform.

(3) Weisungsberechtigt sind die gesetzlichen Vertreter des Auftraggebers und Nutzer mit Inhaberzugang für die Gesellschaft. Weisungsempfänger ist der Geschäftsführer des Auftragnehmers.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich zur Erfüllung des Hauptvertrags und nicht für eigene Zwecke. Er verwendet sie insbesondere nicht für Werbung, nicht für Profile und nicht zum Training von Modellen der künstlichen Intelligenz. Er setzt keine Dienste der künstlichen Intelligenz Dritter zur Verarbeitung von Auftragsdaten ein, es sei denn, der Auftraggeber weist dies ausdrücklich und gesondert an.

(2) Der Auftragnehmer gewährleistet, dass sich alle Personen, die Auftragsdaten verarbeiten dürfen, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29 DSGVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus. Zugang erhalten nur Personen, die ihn für ihre Aufgabe benötigen.

(3) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Er darf sie an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt; wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber mit.

(4) Auftragsdaten werden in Rechenzentren in der Europäischen Union gespeichert. Ein Zugriff aus einem Drittland ist nur nach § 7 zulässig.

(5) Der Auftragnehmer leistet keine Hilfe in Steuersachen. Kontierung, Buchungsentscheidungen, Abschlüsse, Steuererklärungen und die Erfüllung der Buchführungs- und Aufbewahrungspflichten verantwortet der Auftraggeber; eigenapp Fibu stellt dafür die technischen Mittel bereit.

(6) Der Auftragnehmer hat keinen Datenschutzbeauftragten benannt, weil die Voraussetzungen von Art. 37 DSGVO und § 38 BDSG nicht vorliegen. Ansprechpartner ist der Geschäftsführer unter dem Datenschutzkontakt. Benennt er künftig einen Datenschutzbeauftragten, teilt er dessen Kontaktdaten mit.

(7) Der Auftragnehmer führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten, die er im Auftrag durchführt (Art. 30 Abs. 2 DSGVO), und arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen (Art. 31 DSGVO).

§ 4 Unterstützung bei Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten (Art. 28 Abs. 3 Satz 2 lit. e DSGVO). Auskunft und Datenübertragbarkeit sind über die Ansichten und Exporte von eigenapp Fibu möglich; wo das nicht genügt, hilft der Auftragnehmer auf Anforderung.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst, außer der Auftraggeber weist ihn dazu an.

(3) Berichtigung und Löschung von Buchungen und Belegen erfolgen nach den Grundsätzen ordnungsmäßiger Buchführung: Buchungen werden storniert und neu gebucht, nicht überschrieben; Daten mit Aufbewahrungspflicht des Auftraggebers werden gesperrt statt gelöscht (Art. 17 Abs. 3 lit. b, Art. 18 DSGVO). Die rechtliche Prüfung, ob eine Pflicht zur Löschung besteht, obliegt dem Auftraggeber.

§ 5 Unterstützung bei Sicherheit, Datenpannen und Folgenabschätzung

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(2) Wird dem Auftragnehmer eine Verletzung des Schutzes von Auftragsdaten bekannt, meldet er sie dem Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, in Textform an die hinterlegten Inhaberzugänge. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung mit Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, Kontakt für weitere Informationen, wahrscheinliche Folgen und ergriffene oder vorgeschlagene Maßnahmen. Fehlende Angaben reicht er unverzüglich nach. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen bleiben Sache des Auftraggebers.

(3) Der Auftragnehmer ergreift unverzüglich die Maßnahmen, die nötig sind, um die Verletzung zu beheben, die Daten zu sichern und mögliche nachteilige Folgen zu mindern, und dokumentiert Verlauf und Maßnahmen.

(4) Für eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation der Aufsichtsbehörde stellt der Auftragnehmer die Informationen bereit, die ihm zur Verarbeitung vorliegen, insbesondere diese Anlagen.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Bei Vertragsschluss sind die in Anlage 3 genannten Unterauftragsverarbeiter genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform (E-Mail an die Inhaberzugänge und Hinweis in eigenapp Fibu) mit Name, Anschrift, Tätigkeit und Ort der Verarbeitung. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform Einspruch erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Hilft der Auftragnehmer dem Einspruch nicht ab, kann der Auftraggeber den Hauptvertrag und diesen Vertrag ohne Frist kündigen; bis zur Kündigung wird der neue Unterauftragsverarbeiter für die Daten des Auftraggebers nicht eingesetzt, soweit das technisch möglich ist. Muss ein Unterauftragsverarbeiter wegen einer akuten Sicherheits- oder Verfügbarkeitsstörung kurzfristig ersetzt werden, informiert der Auftragnehmer unverzüglich; das Einspruchsrecht bleibt unberührt.

(3) Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 Satz 1 DSGVO). Er wählt Unterauftragsverarbeiter sorgfältig aus und überprüft sie regelmäßig. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Pflichten (Art. 28 Abs. 4 Satz 2 DSGVO).

(4) Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Leistungen, die der Auftragnehmer als reine Nebenleistung in Anspruch nimmt (zum Beispiel Telekommunikation, Post, Reinigung) sowie die Bank des Auftraggebers, deren Schnittstelle eigenapp Fibu mit den Zugangsdaten und auf Weisung des Auftraggebers abfragt. Für das Verhältnis zu seiner Bank ist allein der Auftraggeber verantwortlich.

§ 7 Übermittlung in Drittländer

(1) Eine Übermittlung von Auftragsdaten in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, einschließlich eines Zugriffs von dort, erfolgt nur, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Grundlage ist ein Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO, insbesondere das EU-US Data Privacy Framework für zertifizierte Empfänger) oder, wo ein solcher nicht greift, die Standardvertragsklauseln der Kommission nach dem Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO) mit ergänzenden Maßnahmen, soweit diese erforderlich sind. Die Grundlage je Unterauftragsverarbeiter steht in Anlage 3.

(2) Fällt ein Angemessenheitsbeschluss weg, stellt der Auftragnehmer die betroffenen Übermittlungen unverzüglich auf Standardvertragsklauseln um oder beendet sie und informiert den Auftraggeber. Auf Anforderung legt er dem Auftraggeber seine Bewertung der Übermittlungsrisiken vor.

§ 8 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer und trägt dazu bei (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

(2) Als Nachweis dienen zunächst diese Anlagen, die Verfahrensdokumentation, Prüfprotokolle sowie Nachweise und Zertifikate der Unterauftragsverarbeiter. Inspektionen vor Ort meldet der Auftraggeber mit angemessener Frist, in der Regel zwei Wochen, an; sie finden während der üblichen Geschäftszeiten und ohne Störung des Betriebs statt und dürfen die Daten anderer Kunden sowie Geschäftsgeheimnisse nicht offenlegen. Prüfungen durch eine Aufsichtsbehörde bleiben unberührt.

(3) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen nach Anlage 2 regelmäßig, mindestens einmal im Jahr und nach wesentlichen Änderungen, und dokumentiert das Ergebnis.

§ 9 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er stellt sicher, dass er die Daten, die er in eigenapp Fibu verarbeitet oder abrufen lässt, verarbeiten darf.
- (2) Der Auftraggeber vergibt Zugänge nur an Personen, die sie benötigen, hält die Liste seiner Zugänge aktuell und sorgt dafür, dass Zugangsdaten und zweite Faktoren geschützt sind. Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
- (3) Für die Aufbewahrung nach § 147 AO und § 257 HGB bleibt der Auftraggeber verantwortlich. Vor dem Ende des Vertrags sichert er die Daten, die er aufbewahren muss, durch die Exporte nach § 12.

§ 10 Haftung

- (1) Für Schäden betroffener Personen gilt Art. 82 DSGVO; die Haftung gegenüber betroffenen Personen kann durch diesen Vertrag nicht beschränkt werden.
- (2) Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags. Fehlen solche Regeln, gelten die gesetzlichen Vorschriften. Eine Beschränkung gilt nicht für Vorsatz und grobe Fahrlässigkeit, für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit und nicht für die Verletzung wesentlicher Vertragspflichten im Rahmen des vorhersehbaren, vertragstypischen Schadens. Die Verteilung im Innenverhältnis richtet sich im Übrigen nach Art. 82 Abs. 5 DSGVO.

§ 11 Berufsgeheimnisträger

Erklärt der Auftraggeber beim Abschluss, dass er Berufsgeheimnisträger ist (insbesondere Steuerberater, Rechtsanwalt, Wirtschaftsprüfer oder vereidigter Buchprüfer) oder dass Auftragsdaten fremde Geheimnisse im Sinne von § 203 StGB enthalten, gilt zusätzlich die Vereinbarung in Anlage 4.

§ 12 Beendigung, Rückgabe und Löschung

- (1) Nach Ende der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle Auftragsdaten oder gibt sie zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 Satz 2 lit. g DSGVO).
- (2) Zur Rückgabe stehen dem Auftraggeber jederzeit und unentgeltlich die Exporte von eigenapp Fibu in gängigen, maschinenlesbaren Formaten zur Verfügung: Buchungsjournal mit Hash-Kette, DATEV-Buchungsstapel, Datenträgerüberlassung nach GoBD (Z3), Summen- und Saldenliste, Kontenblätter, Belege als unveränderte Originaldateien mit Prüfsumme sowie Kontoumsätze. Nach Ende des Hauptvertrags gilt eine Übergangsfrist von 30 Tagen, in der eigenapp Fibu unverändert nutzbar bleibt, und danach ein Abrufzeitraum von mindestens 30 weiteren Tagen, in dem alle Exporte abrufbar bleiben. Der Auftraggeber kann die Übergangsfrist einmal verlängern. Die Regeln der Verordnung (EU) 2023/2854 (Datenverordnung) zum Wechsel des Anbieters bleiben unberührt.
- (3) Nach Ablauf des Abrufzeitraums löscht der Auftragnehmer die Auftragsdaten einschließlich der Belegdateien innerhalb von 30 Tagen und bestätigt die Löschung in Textform. Kopien in Datensicherungen werden mit dem Ablauf der Sicherungsfrist gelöscht und bis dahin nicht mehr verwendet. Weist der Auftraggeber in Textform an, die Daten für die Dauer seiner Aufbewahrungsfristen weiter vorzuhalten, ist dafür eine gesonderte Vereinbarung zu treffen; bis dahin werden die Daten gesperrt aufbewahrt.
- (4) Unterlagen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen (insbesondere dieser Vertrag mit Abschlussnachweis und Zugriffsprotokolle), darf der Auftragnehmer entsprechend den gesetzlichen Fristen aufbewahren.

§ 13 Änderungen und Schlussbestimmungen

- (1) Änderungen dieses Vertrags erfolgen als neue Fassung mit neuer Versionsnummer. Der Auftragnehmer teilt sie dem Auftraggeber in Textform mit; die neue Fassung gilt erst, wenn der Auftraggeber sie abschließt. Bis dahin gilt die zuletzt abgeschlossene Fassung fort. Änderungen der Anlage 3 richten sich nach § 6.

(2) Dieser Vertrag wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO), indem eine vertretungsberechtigte Person des Auftraggebers ihn in eigenapp Fibu bestätigt. Der Abschlussnachweis hält Fassung, SHA-256-Prüfsumme dieses Vertragstexts, Gesellschaft, handelnde Person, Zeitpunkt, IP-Adresse und Browserkennung fest. Der Auftraggeber kann den Vertrag mit Abschlussnachweis jederzeit als PDF abrufen.

(3) Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die den Anforderungen von Art. 28 DSGVO entspricht.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Berlin, soweit der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Anlage 1 – Gegenstand, Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

Art und Zweck der Verarbeitung

- Speicherung und Bereitstellung des Buchungsjournals des Auftraggebers mit lückenloser Nummerierung, Hash-Kette, Storno statt Änderung und Festschreibung nach den GoBD.
- Übernahme von Buchungen aus Vorsystemen des Auftraggebers über die Programmierschnittstelle von eigenapp Fibu mit Prüfung jeder Buchung gegen ihre Prüfsumme.
- Belegarchiv: unveränderte Speicherung von Belegen im Originalformat mit SHA-256-Prüfsumme, Verknüpfung mit Buchungen und Bankbewegungen, Anzeige im Browser.
- Bankabruf: Abfrage von Konten, Salden, Umsätzen und angehängten Belegen bei der Bank des Auftraggebers über deren Schnittstelle mit den vom Auftraggeber hinterlegten Zugangsdaten, automatisch in regelmäßigen Abständen und auf Knopfdruck.
- Auswertungen und Exporte: Übersichten, offene Belege, Summen- und Saldenliste, Kontenblätter, DATEV-Buchungsstapel, Datenträgerüberlassung (Z3), Grundlagen für Umsatzsteuer-Voranmeldungen.
- Belegportal, soweit vereinbart: Hochladen von Belegen durch den Auftraggeber oder seine Buchhaltung, Ablage je Gesellschaft und Bereitstellung der Pakete für die Buchhaltung.
- Benutzerverwaltung für die Zugänge des Auftraggebers mit zweitem Faktor sowie Protokollierung von Anmeldungen, Zugriffen und Änderungen.
- Technische Benachrichtigungen per E-Mail (zum Beispiel Anmeldung, Einladung, Sicherheitsmeldungen).
- Datensicherung, Fehlerbehebung und Support auf Anforderung des Auftraggebers.

Art der personenbezogenen Daten

- Nutzer des Auftraggebers: Name, E-Mail-Adresse, Rolle, Kennungen der Anmeldefaktoren (keine Passwörter im Klartext), Anmelde- und Zugriffsprotokolle mit Zeitpunkt, IP-Adresse und Browserkennung.
- Geschäftspartner des Auftraggebers (Kunden, Lieferanten, Zahlungspartner, Behörden): Name oder Firma, Anschrift, Kontaktdaten, Steuer- und Registernummern, Bankverbindung (IBAN, BIC), Beträge, Rechnungs- und Vertragsinhalte, Verwendungszwecke.
- Beschäftigte, Gesellschafter und Organe des Auftraggebers, soweit sie in Belegen, Buchungen oder Bankumsätzen vorkommen: Name, Bankverbindung, Zahlungen, Reisekosten und vergleichbare Angaben.
- Inhalte von Belegen, die der Auftraggeber hochlädt oder abrufen lässt.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) und Daten über Straftaten (Art. 10 DSGVO) sind nicht Gegenstand der Verarbeitung. Sie können sich im Einzelfall aus Belegen ergeben (zum Beispiel Angaben zur Religionszugehörigkeit in Lohnunterlagen); sie werden dann wie alle Auftragsdaten geschützt.

Kategorien betroffener Personen

- Nutzer, Inhaber, Geschäftsführer und Beschäftigte des Auftraggebers
- Kunden, Lieferanten, Dienstleister und sonstige Geschäfts- und Zahlungspartner des Auftraggebers
- Gesellschafter und Ansprechpartner der Geschäftspartner

Ort der Verarbeitung

Datenbank, Belegarchiv und Serverfunktionen liegen in Rechenzentren in Frankfurt am Main (Deutschland), Hintergrundaufgaben laufen auf einem Server in Rotterdam (Niederlande). Einzelheiten und Drittlandbezüge stehen in Anlage 3.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Gliederung folgt Art. 32 Abs. 1 DSGVO und den Gewährleistungszielen des Standard-Datenschutzmodells der Datenschutzkonferenz. Die ausführliche Beschreibung mit Prüfstand steht unter <https://www.eigenapp.ai/rechtliches/tom>.

Vertraulichkeit

- Zutritt: kein eigenes Rechenzentrum; Datenbank, Speicher und Serverfunktionen laufen bei zertifizierten Anbietern (Anlage 3) in Frankfurt am Main. Der Server für Hintergrundaufgaben steht in nicht öffentlich zugänglichen Räumen in Rotterdam (Niederlande); seine Datenträger und die der Arbeitsrechner der Geschäftsführung sind verschlüsselt.
- Zugang: Anmeldung nur mit Passwort, Passkey oder Google-Konto und zusätzlich einem zweiten Faktor (Authenticator-App oder Sicherheitsschlüssel nach FIDO2); ohne zweiten Faktor (Stufe aal2) sind keine Buchhaltungsdaten lesbar.
- Zugriff: Mandantentrennung in der Datenbank durch Zeilenrechte (Row Level Security): ein Nutzer sieht nur Gesellschaften, deren Mitglied er ist, auch Administratoren haben keinen pauschalen Durchgriff. Buchhaltungsschemata sind über die öffentliche Daten-Schnittstelle nicht erreichbar; gelesen wird nur über geprüfte Datenbankfunktionen. Schlüssel mit Vollzugriff liegen nur auf dem Server, nie im Browser.
- Geheimnisse: Bankzugangsdaten liegen verschlüsselt im Tresor der Datenbank (Supabase Vault) und sind nur über eine protokollierte Serverfunktion lesbar. Schlüssel für die Programmierschnittstelle werden nur als SHA-256-Wert gespeichert.
- Trennung: Daten verschiedener Kunden liegen logisch getrennt; Test- und Produktivdaten sind getrennt gekennzeichnet; Kundendaten werden nicht in interne Wissens- oder Auswertungssysteme übernommen.
- Verschlüsselung: Übertragung ausschließlich über TLS (HTTPS mit HSTS); Speicherung bei den Anbietern verschlüsselt (AES-256 at rest).

Integrität

- Buchungen sind nur anhängbar: Ändern, Löschen und Leeren von Tabellen sind durch Rechte und Datenbanktrigger gesperrt, auch für Datenbankverwalter; Korrekturen nur als Storno und Neubuchung.
- Jede Buchung trägt eine SHA-256-Hash-Kette über ihren vollständigen Inhalt und den Vorgänger; die Kette wird bei jeder Übernahme und regelmäßig geprüft.
- Belege werden unverändert mit SHA-256-Prüfsumme gespeichert; die Prüfsumme wird bei jeder Auslieferung mitgegeben.
- Änderungs- und Zugriffsprotokolle (wer, wann, was) sind nur anhängbar.
- Eingaben werden serverseitig geprüft; Änderungen am Programm gelangen nur über die Versionsverwaltung und einen protokollierten Bereitstellungsweg mit automatischer Geheimnisprüfung in den Betrieb.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbank durch den Anbieter mit sieben Tagen Aufbewahrung; die Wiederherstellung wird mindestens einmal im Jahr getestet.
- Belegdateien liegen im redundanten Objektspeicher des Anbieters in Frankfurt am Main; neue Belege werden nie überschrieben (Ablage unter ihrer Prüfsumme).
- Serverfunktionen laufen auf einer skalierenden Plattform mit Schutz gegen Überlastungsangriffe.
- Abhängigkeiten und Plattform werden aktuell gehalten; Sicherheitsmeldungen werden ausgewertet.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Automatisierte Sicherheitsprüfung der Mandantentrennung, der Rechte und der Unveränderbarkeit vor jeder

Änderung an Zugriffsregeln.

- Jährliche Überprüfung dieser Maßnahmen und der Unterauftragsverarbeiter; Ergebnis wird dokumentiert.
- Datenschutzfreundliche Voreinstellungen: keine Analyse- oder Werbedienste in eigenapp Fibu, nur technisch notwendige Cookies.
- Vorgehen bei Datenpannen nach § 5 mit Meldung binnen 24 Stunden.

Anlage 3 – Unterauftragsverarbeiter

Genehmigt sind bei Vertragsschluss die folgenden Unterauftragsverarbeiter. Die Verträge mit den Infrastrukturdiensten (Nr. 2 bis 6) bestehen derzeit über die StromWert Erneuerbare Energien GmbH (Nr. 1).

1. StromWert Erneuerbare Energien GmbH

- Anschrift: Mühlenstraße 8a, 14167 Berlin, Deutschland
- Kontakt: gerstein@stromwert.gmbh
- Tätigkeit: Vertragspartnerin der unten genannten Infrastrukturdienste, deren Konten sie dem Auftragnehmer bereitstellt; Betrieb eines Servers in Rotterdam (Niederlande) für Hintergrundaufgaben (zum Beispiel Abruf und Prüfung von Belegen). Geschäftsführung in Personalunion mit dem Auftragnehmer.
- Ort der Verarbeitung: Deutschland (Sitz) und Niederlande (Server in Rotterdam)
- Einbindung: unmittelbar (Schwestergesellschaft im selben Unternehmensverbund)
- Drittland und Grundlage: keine

2. Supabase Pte. Ltd.

- Anschrift: 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513
- Kontakt: privacy@supabase.com
- Tätigkeit: Datenbank, Anmeldung und zweiter Faktor, verschlüsselter Tresor für Bankzugangsdaten, Belegspeicher, Datensicherung
- Ort der Verarbeitung: Frankfurt am Main (Rechenzentrum Amazon Web Services, Region eu-central-1)
- Einbindung: über StromWert Erneuerbare Energien GmbH
- Drittland und Grundlage: Speicherung nur in Frankfurt am Main; Zugriff des Anbieters für Betrieb und Support aus Drittländern möglich, Grundlage Standardvertragsklauseln (EU) 2021/914, Modul 3

3. Amazon Web Services, Inc.

- Anschrift: 410 Terry Avenue North, Seattle, WA 98109-5210, USA
- Kontakt: über Supabase
- Tätigkeit: Rechenzentrum, Server und Speicher für die Leistungen von Supabase
- Ort der Verarbeitung: Frankfurt am Main (Region eu-central-1)
- Einbindung: über Supabase Pte. Ltd.
- Drittland und Grundlage: Speicherung in Frankfurt am Main; EU-US Data Privacy Framework (Art. 45 DSGVO), hilfsweise Standardvertragsklauseln

4. Vercel Inc.

- Anschrift: 440 N Barranca Avenue #4133, Covina, CA 91723, USA
- Kontakt: privacy@vercel.com
- Tätigkeit: Betrieb der Anwendung (Serverfunktionen, Auslieferung, Zeitsteuerung des Bankabrufs), Verbindungsprotokolle
- Ort der Verarbeitung: Frankfurt am Main (Region fra1) und weltweites Auslieferungsnetz
- Einbindung: über StromWert Erneuerbare Energien GmbH
- Drittland und Grundlage: Serverfunktionen in Frankfurt am Main; Auslieferung über ein weltweites Netz und Zugriff aus den USA möglich, Grundlage EU-US Data Privacy Framework (Art. 45 DSGVO), hilfsweise Standardvertragsklauseln (EU) 2021/914, Modul 3

5. Plus Five Five, Inc. (Resend)

- Anschrift: 2261 Market Street #5039, San Francisco, CA 94114, USA
- Kontakt: privacy@resend.com
- Tätigkeit: Versand technischer E-Mails an Nutzer des Auftraggebers (Anmeldung, Einladung, Sicherheitsmeldungen) mit E-Mail-Adresse, Name und Inhalt
- Ort der Verarbeitung: Irland (Region eu-west-1) und USA
- Einbindung: über StromWert Erneuerbare Energien GmbH
- Drittland und Grundlage: Versand aus Irland; Konto- und Protokolldaten in den USA, Grundlage EU-US Data Privacy Framework (Art. 45 DSGVO), hilfsweise Standardvertragsklauseln (EU) 2021/914, Modul 3

6. Google Cloud EMEA Limited (Google Workspace)

- Anschrift: 70 Sir John Rogerson's Quay, Dublin 2, Irland
- Kontakt: über support.google.com/a/contact/googlecloud_dpr
- Tätigkeit: E-Mail-Postfächer für die Kommunikation mit dem Auftraggeber, nur soweit er Auftragsdaten per E-Mail sendet (zum Beispiel im Support)
- Ort der Verarbeitung: Europäische Union und USA
- Einbindung: über StromWert Erneuerbare Energien GmbH
- Drittland und Grundlage: Zugriff aus den USA möglich, Grundlage EU-US Data Privacy Framework (Google LLC), hilfsweise Standardvertragsklauseln

Keine Unterauftragsverarbeiter sind die Bank des Auftraggebers, deren Schnittstelle eigenapp Fibu auf seine Weisung abfragt (derzeit Qonto SA, Paris), und Anbieter, an die der Auftraggeber selbst Exporte weitergibt (zum Beispiel seine Steuerkanzlei).

Anlage 4 – Zusatzvereinbarung für Berufsgeheimnisträger (§ 62a StBerG, § 43e BRAO, § 203 StGB)

Diese Anlage gilt, wenn der Auftraggeber beim Abschluss erklärt hat, Berufsgeheimnisträger zu sein oder fremde Geheimnisse im Sinne von § 203 StGB verarbeiten zu lassen. Sie wird in Textform geschlossen (§ 62a Abs. 3 Satz 1 StBerG, § 43e Abs. 3 Satz 1 BRAO).

(1) Verschwiegenheit: Der Auftragnehmer verpflichtet sich, über alle fremden Geheimnisse, die ihm bei der Leistung bekannt werden, Verschwiegenheit zu wahren. Diese Pflicht gilt zeitlich unbegrenzt.

(2) Belehrung: Der Auftragnehmer ist darüber belehrt, dass er als mitwirkende Person nach § 203 Abs. 4 Satz 1 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird, wenn er ein fremdes Geheimnis unbefugt offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt geworden ist, und dass nach § 203 Abs. 4 Satz 2 StGB ebenso bestraft wird, wer nicht dafür Sorge getragen hat, dass eine von ihm herangezogene weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde. Handelt er gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, beträgt die Strafe nach § 203 Abs. 6 StGB Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe; nach § 204 StGB ist auch das unbefugte Verwerten eines fremden Geheimnisses strafbar.

(3) Erforderlichkeit: Der Auftragnehmer verschafft sich Kenntnis von fremden Geheimnissen nur, soweit das zur Erfüllung des Vertrags erforderlich ist (§ 62a Abs. 3 Satz 2 Nr. 2 StBerG).

(4) Weitere Personen: Der Auftragnehmer darf die in Anlage 3 genannten Unterauftragsverarbeiter und eigene Beschäftigte heranziehen. Er verpflichtet sie vor ihrem Einsatz in Textform zur Verschwiegenheit, soweit sie nicht bereits gesetzlich zur Verschwiegenheit verpflichtet sind, und belehrt sie über die Strafbarkeit (§ 62a Abs. 3 Satz 2 Nr. 3 StBerG).

(5) Ausland: Auftragsdaten werden in der Europäischen Union gespeichert. Soweit nach Anlage 3 ein Zugriff aus einem Drittland möglich ist, prüft der Auftraggeber, ob der dortige Geheimnisschutz dem Schutz im Inland vergleichbar ist (§ 62a Abs. 4 StBerG); der Auftragnehmer stellt ihm dafür die Angaben aus Anlage 3 zur Verfügung.

(6) Beendigung: Der Auftraggeber kann den Vertrag ohne Frist beenden, wenn die Einhaltung dieser Anlage nicht gewährleistet ist (§ 62a Abs. 2 Satz 2 StBerG).

(7) Einwilligung der Mandanten: Dient die Leistung unmittelbar einem einzelnen Mandat, holt der Auftraggeber die nach § 62a Abs. 5 StBerG oder § 43e Abs. 5 BRAO erforderliche Einwilligung seines Mandanten ein.