

Auftragsverarbeitungsvertrag

Fassung 2026-09-24 · gültig ab 24.09.2026

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 der Datenschutz-Grundverordnung (DSGVO)

zwischen dem Kunden von zettl, der den Betrieb in zettl führt (im Folgenden „Verantwortlicher“),

und der Develogix Agency e.U., Johannes-Filzer-Straße 46, 5020 Salzburg, Österreich, FN 594182 y (im Folgenden „Auftragsverarbeiter“).

Dieser Vertrag wird elektronisch geschlossen, indem der Verantwortliche ihm in zettl zustimmt (Art. 28 Abs. 9 DSGVO). Name und Anschrift des Verantwortlichen ergeben sich aus den Betriebsdaten in zettl; Version und Zeitpunkt der Zustimmung sind in zettl unter „Einstellungen · Verträge“ einsehbar und dort als PDF abrufbar.

§ 1 Gegenstand und Dauer

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die Registrierkasse zettl nach den [Allgemeinen Geschäftsbedingungen](#) (Hauptvertrag) bereit. Dabei verarbeitet er personenbezogene Daten, für die der Verantwortliche verantwortlich ist.

1.2 Dieser Vertrag gilt für die Dauer des Hauptvertrags, einschließlich der Testphase, und darüber hinaus, solange der Auftragsverarbeiter Daten des Verantwortlichen verarbeitet – insbesondere während der gesetzlichen Aufbewahrung nach § 7.

§ 2 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich, um die Leistungen des Hauptvertrags zu erbringen: Erfassen, Speichern, Signieren, Anzeigen, Drucken, Versenden und Exportieren von Belegen und Aufzeichnungen der Registrierkasse; Führen von Kundenstamm, Gutscheinen, Kassabuch und Abschlüssen; Verwaltung der Mitarbeiterkonten und Geräte; Versand digitaler Belege; Datensicherung, Fehlerbehebung und Support. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

§ 3 Art der Daten und betroffene Personen

3.1 **Kundschaft des Verantwortlichen:** Name bzw. Firma, Kundennummer, UID-Nummer, Anschrift, E-Mail-Adresse, Telefonnummer, Geburtstag und Notizen, soweit erfasst; Kaufdaten und Belege (Positionen, Beträge, Rabatte, Zahlart, Zeitpunkt, Kasse, Belegnummer, Signatur); E-Mail-Adresse für digitale Belege; Rechnungsempfänger; Gutscheine und Guthaben; Referenzen von Kartenzahlungen (ohne vollständige Kartennummer).

3.2 **Mitarbeiterinnen und Mitarbeiter des Verantwortlichen:** Name, E-Mail-Adresse, Profilbild, Rolle und Berechtigungen, Kassen-PIN (nur als Hash), Zuordnung als Bedienerin oder Bediener zu Belegen, Stornos, Kassabuch-Einträgen und Abschlüssen, Unterschriften bei Kassenzahlung und Entnahmen, zugeordnete Geräte, Anmelde- und Protokolldaten.

3.3 **Weitere Personen**, soweit ihre Daten in Belegen, Notizen oder hochgeladenen Fremdbelegen enthalten sind.

3.4 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung; der Verantwortliche erfasst solche Daten nicht in Freitextfeldern.

§ 4 Pflichten des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen (§ 5), es sei denn, er ist durch Unionsrecht oder österreichisches Recht zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese Verpflichtung vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

4.2 Er gewährleistet, dass sich alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (§ 6 Datenschutzgesetz).

4.3 Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in **Anlage 1** beschrieben sind. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

4.4 Er unterstützt den Verantwortlichen nach § 8 und § 9 bei der Erfüllung der Betroffenenrechte und der Pflichten nach Art. 32 bis 36 DSGVO.

4.5 Er führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

4.6 Die Verarbeitung findet in der Europäischen Union statt. Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

4.7 Betriebsüberwachung. Für die Überwachung des technischen Betriebs setzt der Auftragsverarbeiter Laravel Nightwatch ein (Anlage 2). Dabei gilt:

- Verarbeitet werden **technische Kennzahlen**: aufgerufene Adresse, Dauer, Statuscode, Fehlermeldung mit Aufrufliste, Name und Dauer von Hintergrundaufgaben und Datenbankabfragen.
- Dabei können die **Kennung der angemeldeten Person und IP-Adressen** aus Fehlermeldungen übertragen werden. Das sind die einzigen personenbezogenen Daten, die dorthin gelangen können.
- **Nicht übertragen** werden Inhalte aus der Kasse: Belegzeilen, Beträge, Kunden- und Mitarbeiterdaten, PINs sowie Zugangsdaten zum Signatordienst, zu SumUp oder zu FinanzOnline. Anfrage- und Formularinhalte sowie Quelltextauszüge sind in der Einstellung abgeschaltet, Mail- und Benachrichtigungsereignisse werden gefiltert.
- Verarbeitet wird in der **EU-Region** des Dienstes.
- Anbieter ist die **Laravel Holdings, Inc.** mit Sitz in den Vereinigten Staaten. Auch bei Verarbeitung in der EU-Region ist damit ein Zugriff aus einem Drittland nicht auszuschließen. Die Übermittlung stützt sich auf den Angemessenheitsbeschluss zum EU-US Data Privacy Framework (Art. 45 DSGVO), soweit der Anbieter danach zertifiziert ist, ergänzend auf die Standardvertragsklauseln der Europäischen Kommission (Art. 46 Abs. 2 lit. c DSGVO).
- Der Auftragsverarbeiter kann die Betriebsüberwachung **jederzeit abschalten**, ohne dass zettl dadurch eingeschränkt wird. Widerspricht der Verantwortliche nach § 6.2, wird sie für seinen Betrieb abgeschaltet.

§ 5 Weisungen

5.1 Die Weisungen des Verantwortlichen ergeben sich aus dem Hauptvertrag, diesem Vertrag und der Nutzung der Funktionen und Einstellungen von zettl (etwa Anlegen, Ändern, Exportieren oder Anonymisieren von Daten). Weitere Weisungen erteilt der Verantwortliche per E-Mail an support@mail.zettl.io oder über <https://zettl.io/support>.

5.2 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich und darf die Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

5.3 Belege, Stornos, Kassabuch-Einträge und Abschlüsse sind nach der RKSv unveränderbar. Weisungen, diese Aufzeichnungen zu ändern oder vor Ablauf der Aufbewahrungsfrist zu löschen, kann der Auftragsverarbeiter nicht ausführen.

§ 6 Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter stehen in **Anlage 2**; die jeweils aktuelle Liste ist unter [Unterauftragsverarbeiter](#) abrufbar.

6.2 Über eine beabsichtigte Hinzuziehung oder Ersetzung informiert der Auftragsverarbeiter den Verantwortlichen mindestens **vier Wochen** vorher per E-Mail und in zettl. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen widersprechen. Können sich die Parteien nicht einigen, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

6.3 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen. Er haftet gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.

6.4 Keine Unterauftragsverarbeitung im Sinn dieses Vertrags sind Leistungen, die der Verantwortliche selbst bei Dritten beauftragt – insbesondere die Kartenzahlung über SumUp –, sowie Nebenleistungen wie Telekommunikation oder Postdienste. Die Abrechnung des Abos über Stripe und Runple betrifft nur Daten des Verantwortlichen selbst, nicht die Daten nach § 3.

§ 7 Löschung und Rückgabe

7.1 Der Verantwortliche kann seine Daten während der Vertragslaufzeit jederzeit exportieren und Daten seiner Kundschaft berichtigen, löschen oder anonymisieren, soweit keine Aufbewahrungspflicht entgegensteht.

7.2 Nach Ende des Hauptvertrags bleibt der Zugang im Nur-Lesen-Modus bestehen, damit der Verantwortliche seine Daten exportieren kann. Belege, Kassabuch, Abschlüsse und Datenerfassungsprotokolle unterliegen einer Aufbewahrungspflicht von **sieben Jahren** (§ 132 BAO); der Auftragsverarbeiter bewahrt sie in dieser Zeit im Auftrag des Verantwortlichen auf und löscht sie danach. Personenbezogene Daten der Kundschaft, die nicht Teil dieser Aufzeichnungen sind, werden nach Vertragsende gelöscht oder anonymisiert; beantragt der Verantwortliche die Löschung seines Betriebs, geschieht das mit der Durchführung des Antrags.

7.3 Datensicherungen werden im Rahmen ihres regulären Zyklus überschrieben; bis dahin bleiben sie durch die Maßnahmen nach Anlage 1 geschützt.

§ 8 Unterstützung bei Betroffenenrechten

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO). zettl bietet dafür Funktionen zum Anzeigen, Berichten, Exportieren und Anonymisieren von Kundendaten.

8.2 Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst, außer auf Weisung.

§ 9 Datenschutzverletzungen und weitere Unterstützung

9.1 Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO), die dessen Daten betrifft, unverzüglich, nach Möglichkeit innerhalb von 48 Stunden nach Bekanntwerden, per E-Mail an die hinterlegte Adresse des Betriebs. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben werden nachgereicht.

9.2 Er ergreift unverzüglich Maßnahmen, um die Verletzung zu beheben und nachteilige Folgen zu mindern, und unterstützt den Verantwortlichen bei dessen Meldepflichten gegenüber der Datenschutzbehörde und den betroffenen Personen.

9.3 Er unterstützt den Verantwortlichen im erforderlichen Umfang bei einer Datenschutz-Folgenabschätzung und einer vorherigen Konsultation der Aufsichtsbehörde (Art. 35 und 36 DSGVO).

§ 10 Nachweise und Kontrollen

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung.

10.2 Der Verantwortliche kann die Einhaltung selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren. Kontrollen vor Ort sind mindestens vier Wochen im Voraus anzukündigen, finden zu üblichen Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig stören; die Rechte anderer Kunden und die Sicherheit der Systeme bleiben gewahrt. Rechenzentren von Unterauftragsverarbeitern werden über deren Nachweise (etwa Zertifizierungen) geprüft.

§ 11 Supportzugriff

Mitarbeiterinnen und Mitarbeiter des Auftragsverarbeiters greifen auf die Daten des Verantwortlichen nur zu, soweit das für den Betrieb, die Fehlerbehebung oder eine vom Verantwortlichen erbetene Hilfestellung nötig ist. Ein Zugriff auf das Konto des Betriebs („als Inhaber anmelden“) wird sichtbar gekennzeichnet und mit Person und Zeitpunkt protokolliert; Abo-Änderungen sind dabei ausgeschlossen.

§ 12 Haftung und Schlussbestimmungen

12.1 Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln des Hauptvertrags.

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

12.3 Änderungen dieses Vertrags werden wie Änderungen der AGB mitgeteilt (Punkt 14 der AGB); der Inhaber des Betriebs bestätigt eine neue Fassung in zettl.

12.4 Es gilt österreichisches Recht. Gerichtsstand ist das für Salzburg sachlich zuständige Gericht.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Hosting in der EU:** Server, Datenbank und Datensicherungen liegen in Rechenzentren der Hetzner Online GmbH in der Europäischen Union; physische Zutrittskontrolle durch den Rechenzentrumsbetreiber.
- **Verschlüsselte Übertragung:** alle Verbindungen zu zettl, zur Tablet-App und zu Unterauftragsverarbeitern über TLS; Anmeldung nur über HTTPS mit sicheren Cookies.
- **Verschlüsselung sensibler Felder:** Zugangsdaten zu FinanzOnline, Schlüssel und Tokens für fiskaly und SumUp sowie Push-Tokens der Geräte werden verschlüsselt in der Datenbank gespeichert. Passwörter und Kassen-PINs werden nur als Hash gespeichert.
- **Mandantentrennung:** Jeder Datensatz ist einem Betrieb zugeordnet; jede Abfrage ist technisch auf den Betrieb beschränkt, der sich aus der Adresse ({betrieb}.zettl.io) bzw. dem App-Zugang ergibt. Die Trennung wird durch automatisierte Tests geprüft.
- **Rollen und Rechte:** feste Rollen (Inhaber, Leitung, Kasse, Buchhaltung) mit abgestuften Rechten; heikle Kassenvorgänge (etwa Stornos, Rabatte über der Schwelle) verlangen eine PIN-Freigabe.

- **Zwei-Faktor-Authentifizierung** (TOTP) für alle Konten verfügbar; Begrenzung von Anmeldeversuchen und Registrierungen.
- **Private Dateiablage:** Belege, Exporte und Fremdbelege liegen in einem nicht öffentlichen Speicher; Downloads laufen über zeitlich begrenzte Links.
- **Administrativer Zugriff** nur für berechtigte Personen von Develogix, auf Wunsch zusätzlich auf freigegebene IP-Adressen beschränkt.

Integrität

- **Protokollierung:** Anmeldungen, Rechteänderungen und fachlich wichtige Vorgänge werden in einem Änderungsprotokoll mit Person, Zeitpunkt, IP-Adresse und Browserkennung festgehalten; das Protokoll ist in der Datenbank gegen Ändern und Löschen gesperrt.
- **Unveränderbare Aufzeichnungen:** Belege, Stornos, Kassabuch, Abschlüsse und Zustimmungsnachweise sind append-only; die Datenbank verhindert Änderungen und Löschungen per Trigger. Korrekturen entstehen als neue Datensätze.
- **Signatur und Verkettung** der Belege nach RKSv über die fiskaly GmbH; zettl prüft Kette und Vollständigkeit des Datenerfassungsprotokolls.
- **Supportzugriff** („als Inhaber anmelden“) nur über den Administrationsbereich, sichtbar gekennzeichnet und protokolliert, ohne Abo-Änderungen.

Verfügbarkeit und Belastbarkeit

- **Regelmäßige Datensicherungen** der Datenbank und der Dateiablage; Versionierung der Dateiablage.
- **Ausfallkonzept** für die Signatur nach RKSv (Kennzeichnung, Nachsignatur, Nacherfassung von Papierbelegen).
- **Überwachung** von Warteschlangen, Signaturdienst und Kartenzahlungen; Wiederholung fehlgeschlagener Vorgänge ohne Doppelbuchungen (Idempotenz).

Verfahren zur regelmäßigen Überprüfung

- Automatisierte Tests für Mandantentrennung, Rechte und unveränderbare Aufzeichnungen bei jeder Änderung der Software.
- Zweite Prüfung von Änderungen an sicherheits- und geldrelevanten Funktionen vor der Auslieferung.
- Regelmäßige Aktualisierung von Betriebssystem, Laufzeitumgebung und Bibliotheken.
- Datenschutzfreundliche Voreinstellungen: keine Tracking-Cookies, keine Werbung, nur notwendige Daten.

Anlage 2 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Sitz / Verarbeitungsort
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Hosting: Server, Datenbank, Datensicherungen, Objektspeicher (Beleg-PDFs, Exporte, Bilder); Support-System (support.develogix.at), Anhänge von Support-Anfragen	Deutschland; Rechenzentren in der EU
Ploi	Verwaltung und Bereitstellung der Server	Niederlande (Nijkerk); Verarbeitung in den Niederlanden
fiskaly GmbH, Wien	Signatur der Belegdaten nach RKSv, Registrierung in FinanzOnline, Datenerfassungsprotokoll	Österreich
Lettermint B.V., Willemsvaart 16 B, 8019 AB Zwolle, Niederlande (KvK 99337711)	Versand digitaler Belege und weiterer E-Mails, Antworten auf Support-Anfragen	Niederlande; Verarbeitung ausschließlich in der EU
Laravel Holdings, Inc. (Laravel Nightwatch)	Überwachung des technischen Betriebs (Dauer und Fehler von Anfragen, Abfragen, Hintergrundaufgaben); keine Übertragung von Anfrage- oder Formularinhalten	EU-Region; Rechenzentren in der EU

Unterauftragsverarbeiter	Leistung	Sitz / Verarbeitungsort
Anthropic Ireland, Limited, Dublin, Irland	KI-gestützte Auswertung von Support-Anfragen der Betriebe (Zusammenfassung, Einordnung, Antwortvorschlag); nur was der Betrieb selbst in die Anfrage schreibt, keine automatische Übertragung von Belegzeilen, Beträgen oder Kassendaten; E-Mail-Adressen werden vorher unkenntlich gemacht, Antworten verschickt immer ein Mensch	Irland; teilweise USA durch Anthropic, PBC als Unterauftragsverarbeiter – EU-Standardvertragsklauseln (Modul 2/3) gemäß DPA vom 24.02.2025; Liste: https://www.anthropic.com/subprocessors

Die jeweils aktuelle Liste steht unter [Unterauftragsverarbeiter](#).