

Auftragsverarbeitungsvertrag

Data Processing Agreement (DPA)

Version 2.0 · Zuletzt aktualisiert: Oktober 2026

Gemäß **Artikel 28 der Datenschutz-Grundverordnung (DSGVO)**. Dieser Auftragsverarbeitungsvertrag („AVV“) ist Bestandteil der Nutzungsbedingungen zwischen der **Kodex-Compliance UG (haftungsbeschränkt)** („Auftragsverarbeiter“, „wir“) und der Organisation, die den Dienst nutzt („Verantwortlicher“, „Sie“).

1. Vertragsparteien, Geltungsbereich und Form

Auftragsverarbeiter ist die Kodex-Compliance UG (haftungsbeschränkt), Lindenstraße 29c, 12555 Berlin, eingetragen beim Amtsgericht Charlottenburg (Berlin) unter HRB 289793, vertreten durch den Geschäftsführer Jeremiah Matador.

Dieser AVV gilt, soweit wir bei der Erbringung des Dienstes personenbezogene Daten in Ihrem Auftrag verarbeiten. Sie nehmen ihn zusammen mit den Nutzungsbedingungen an, wenn Sie Ihr Konto anlegen. Nach Art. 28 Abs. 9 DSGVO kann dieser Vertrag in einem elektronischen Format geschlossen werden. Sie können jede Fassung jederzeit als PDF herunterladen, und auf Anfrage senden wir Ihnen ein gegengezeichnetes Exemplar.

Soweit wir selbst über Zwecke und Mittel der Verarbeitung entscheiden, etwa bei Ihren Benutzerkonten, der Abrechnung, Sicherheitsprotokollen und unseren eigenen gesetzlichen Pflichten, sind wir Verantwortlicher. Für diese Verarbeitung gilt unsere Datenschutzerklärung, nicht dieser AVV.

Widersprechen sich dieser AVV und die Nutzungsbedingungen beim Schutz personenbezogener Daten, hat dieser AVV Vorrang.

2. Gegenstand und Dauer

Wir verarbeiten personenbezogene Daten in Ihrem Auftrag, um Leistungen der Compliance-Bewertung, der Dokumentenverwaltung und der KI-gestützten Compliance-Analyse zu erbringen. Die Verarbeitung dauert, solange Sie den Dienst nutzen, und endet mit der Löschung nach Abschnitt 14.

3. Art und Zweck der Verarbeitung

- Speicherung und Analyse der von Ihnen hochgeladenen Compliance-Nachweise und Dokumente
- KI-gestützte Bewertung von Compliance-Kontrollen anhand regulatorischer Rahmenwerke
- Erstellung von Compliance-Berichten, Richtlinien und Risikobewertungen
- Auslesen von Einstellungen, Benutzerlisten und Berechtigungen aus Systemen, die Sie verbinden (Integrationen), nur lesend und nur für die von Ihnen gestarteten Prüfungen
- Prüfung Ihrer öffentlichen Website auf ihre Rechtstexte (Website-Prüfung), sofern Sie diese nicht deaktiviert haben
- Transkription von Beispielen von Sprachassistenten, die Sie hochladen, soweit Sie diese Funktion nutzen
- Verwaltung der Benutzerkonten und Zugriffe Ihres Teams im Dienst

4. Arten personenbezogener Daten

- Kontaktdaten (Namen, E-Mail-Adressen, Funktionen)
- Beschäftigungsdaten, die in hochgeladenen Compliance-Nachweisen enthalten sind
- Benutzer-, Rollen- und Berechtigungsdaten aus Systemen, die Sie verbinden
- IT-Sicherheitsdaten (Zugriffsprotokolle, Systemkonfigurationen)
- Sprachaufnahmen und Transkripte, soweit Sie Beispiele von Sprachassistenten hochladen
- Sonstige personenbezogene Daten in Dokumenten, die Sie hochladen

Bitte laden Sie besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) nur hoch, soweit Ihre Compliance-Arbeit dies erfordert.

5. Kategorien betroffener Personen

- Ihre Beschäftigten und Auftragnehmer
- Ihre Kunden, soweit sie in hochgeladenen Nachweisen vorkommen
- Ihre Partner, Zulieferer und Dienstleister
- Nutzer der Systeme, die Sie verbinden

6. Ihre Weisungen

Wir verarbeiten personenbezogene Daten nur auf Ihre dokumentierte Weisung. Ihre Weisungen sind dieser AVV, die Nutzungsbedingungen, die Einstellungen, die Sie im Dienst wählen, sowie weitere Weisungen, die Sie uns in Textform erteilen. Eine E-Mail genügt.

Wir verarbeiten personenbezogene Daten außerdem, soweit das Recht der EU oder Deutschlands uns dazu verpflichtet. In diesem Fall teilen wir Ihnen dies vorher mit, sofern das betreffende Recht dies nicht verbietet.

Sind wir der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informieren wir Sie unverzüglich. Wir können die Ausführung dieser Weisung aussetzen, bis Sie sie bestätigen oder ändern.

7. Unsere Pflichten

Wir

- (a) verpflichten alle Personen, die auf Ihre personenbezogenen Daten zugreifen können, zur Vertraulichkeit
- (b) schützen Ihre personenbezogenen Daten mit den technischen und organisatorischen Maßnahmen nach Abschnitt 11 (Art. 32 DSGVO)
- (c) setzen Unterauftragsverarbeiter nur nach Abschnitt 9 ein
- (d) unterstützen Sie bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO). Im Dienst können Sie Daten selbst finden, exportieren, berichtigen und löschen. Wendet sich eine betroffene Person direkt an uns, leiten wir die Anfrage unverzüglich an Sie weiter und beantworten sie nicht selbst, es sei denn, Sie bitten uns darum
- (e) unterstützen Sie bei Ihren Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldungen von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherige Konsultation) mit den uns vorliegenden Informationen
- (f) führen ein Verzeichnis der Verarbeitungen, die wir für Sie durchführen (Art. 30 Abs. 2 DSGVO)
- (g) informieren Sie unverzüglich, wenn wir unsere Pflichten aus diesem AVV nicht mehr erfüllen können
- (h) stellen Ihnen die Informationen zur Verfügung, die Sie zum Nachweis der Einhaltung von Art. 28 DSGVO benötigen, und ermöglichen Überprüfungen nach Abschnitt 13

Wir sind derzeit nicht verpflichtet, einen Datenschutzbeauftragten zu benennen. In allen Datenschutzfragen erreichen Sie uns unter contact@kodex-compliance.com.

8. Ihre Pflichten

Sie sind für die Rechtmäßigkeit der von Ihnen veranlassten Verarbeitung verantwortlich, einschließlich einer Rechtsgrundlage für die Daten, die Sie hochladen oder verbinden, und für die Information der betroffenen Personen. Teilen Sie uns Fehler oder Unregelmäßigkeiten bei unserer Verarbeitung unverzüglich mit.

9. Unterauftragsverarbeiter

Sie erteilen uns die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Derzeit setzen wir die folgenden ein:

Unterauftragsverarbeiter	Zweck	Standort	Garantien
Supabase Pte. Ltd.	Datenbank, Authentifizierung, Dateispeicherung	EU	Region in der EU; EU-Standardvertragsklauseln für Supportzugriffe von außerhalb des EWR
Amazon Web Services EMEA SARL (Amazon Bedrock, Claude-Modelle von Anthropic)	KI-Inferenz für die Compliance-Bewertung	EU (Frankfurt, eu-central-1; EU-Inferenzprofile bleiben innerhalb der EU)	EU-Gesellschaft; Region in der EU
Stripe Payments Europe, Limited	Zahlungsabwicklung	EU (Irland)	EU-Gesellschaft; EU-Standardvertragsklauseln für Übermittlungen innerhalb der Stripe-Gruppe
Upstash, Inc.	Redis-Caching, Ratenbegrenzung, Koordination von Hintergrundaufgaben	EU (Frankfurt)	Region in der EU; EU-Standardvertragsklauseln für Zugriffe aus den USA
Render Services, Inc.	Anwendungshosting und Bereitstellung	EU (Frankfurt)	Region in der EU; EU-Standardvertragsklauseln für Zugriffe aus den USA
Resend, Inc.	Versand von Transaktions-E-Mails	EU	Region in der EU; EU-Standardvertragsklauseln für Zugriffe aus den USA

Functional Software, Inc. (Sentry)	Fehlerüberwachung	EU (Datenannahme Frankfurt)	Region in der EU; EU-Standardvertragsklauseln für Zugriffe aus den USA
Cloudflare, Inc.	Domain, Netzwerksicherheit, Auslieferung	Globales Netzwerk	EU-Standardvertragsklauseln

Über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informieren wir Sie mindestens 30 Tage, bevor sie wirksam wird, per E-Mail an die Inhaber und Administratoren Ihrer Organisation und durch Aktualisierung dieser Seite.

Sie können innerhalb von 14 Tagen nach unserer Mitteilung aus berechtigten datenschutzrechtlichen Gründen schriftlich an contact@kodex-compliance.com widersprechen. Wir bemühen uns um eine Lösung mit Ihnen. Gelingt das nicht, können Sie den betroffenen Teil des Dienstes vor Wirksamwerden der Änderung kündigen, und wir erstatten im Voraus gezahlte Entgelte für den Zeitraum nach der Kündigung.

Müssen wir einen Unterauftragsverarbeiter dringend ersetzen, um die Sicherheit oder den Betrieb des Dienstes zu gewährleisten, können wir dies mit kürzerer Frist tun. Wir informieren Sie dann unverzüglich, und Ihr Widerspruchsrecht gilt entsprechend.

Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die mindestens so schützend sind wie dieser AVV (Art. 28 Abs. 4 DSGVO). Für unsere Unterauftragsverarbeiter haften wir Ihnen gegenüber in vollem Umfang.

10. Internationale Datenübermittlungen

Wir betreiben den Dienst und speichern Ihre Daten in der Europäischen Union. Soweit ein Unterauftragsverarbeiter, seine Unternehmensgruppe oder sein Supportpersonal von außerhalb des EWR auf personenbezogene Daten zugreifen kann, übermitteln wir Daten nur auf Grundlage von Kapitel V DSGVO, vor allem der EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914 der Kommission, Modul 3) zusammen mit einer Transfer-Folgenabschätzung.

Ist ein US-Unterauftragsverarbeiter nach dem EU-US Data Privacy Framework zertifiziert, ist diese Zertifizierung eine zusätzliche Garantie. Wir stützen uns nicht allein darauf, sodass eine Änderung ihres rechtlichen Status keine Übermittlung ohne Grundlage lässt.

11. Technische und organisatorische Maßnahmen

Wir treffen die folgenden Maßnahmen:

- Verschlüsselung im Ruhezustand (AES-256) und bei der Übertragung (TLS 1.2 oder höher)
- Trennung der Kunden: Jede Anfrage ist auf Ihre Organisation beschränkt, was durch automatisierte Tests abgesichert ist
- Rollenbasierte Zugriffskontrolle im Dienst nach dem Prinzip der geringsten Rechte
- Zugang zu Produktivsystemen nur für Personen, die ihn für ihre Arbeit benötigen
- Tägliche Sicherungen durch unseren Hosting-Anbieter
- Protokollierung sicherheitsrelevanter Aktionen in einem Audit-Log
- Ratenbegrenzung und automatisierte Überwachung mit Fehler- und Vorfallerkennung
- Automatisierte Prüfung auf offengelegte Geheimnisse und Schwachstellen in Abhängigkeiten bei jeder Codeänderung
- Vertraulichkeitsverpflichtungen für alle Personen mit Zugriff auf personenbezogene Daten

Wir überprüfen diese Maßnahmen mindestens einmal jährlich und immer dann, wenn sich Risiken ändern. Wir können sie dem technischen Fortschritt anpassen, solange das Schutzniveau insgesamt nicht sinkt.

12. Verletzungen des Schutzes personenbezogener Daten

Wir benachrichtigen Sie unverzüglich, in jedem Fall innerhalb von 48 Stunden, nachdem uns eine Verletzung des Schutzes Ihrer personenbezogenen Daten bekannt geworden ist. Die Benachrichtigung geht per E-Mail an die Inhaber und Administratoren Ihrer Organisation.

Unsere Meldung enthält die nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen, soweit sie vorliegen. Fehlende Informationen reichen wir schrittweise nach, sobald wir sie haben. Wir unterstützen Sie bei der Meldung an die Aufsichtsbehörde und der Benachrichtigung der betroffenen Personen und dokumentieren jede Verletzung.

13. Überprüfungen

Auf Anfrage stellen wir Ihnen die Informationen zur Verfügung, die Sie zur Prüfung der Einhaltung dieses AVV benötigen, etwa diesen AVV, unsere technischen und organisatorischen Maßnahmen und Angaben zu unseren Unterauftragsverarbeitern. Meist sind Ihre Fragen damit beantwortet.

Ist das nicht der Fall, können Sie uns einmal pro Kalenderjahr selbst überprüfen oder durch einen zur Vertraulichkeit verpflichteten unabhängigen Prüfer überprüfen lassen, mit einer Vorankündigung von mindestens 30 Tagen in Textform, während der üblichen Geschäftszeiten und ohne Störung unseres Betriebs. Häufigere Überprüfungen sind nach einer Verletzung des Schutzes personenbezogener Daten oder auf Verlangen einer Aufsichtsbehörde möglich.

Jede Partei trägt ihre eigenen Kosten einer Überprüfung. Die Rechte der Aufsichtsbehörden bleiben unberührt.

14. Löschung und Rückgabe der Daten

Sie können Ihre Daten jederzeit aus dem Dienst exportieren. Nach Beendigung des Dienstes bewahren wir Ihre Daten 30 Tage auf, damit Sie sie exportieren können, und löschen sie danach. Sie können Ihr Konto und Ihre Daten außerdem jederzeit selbst in den Einstellungen löschen. Sicherungskopien werden innerhalb von 90 Tagen entfernt.

Länger bewahren wir Daten nur auf, soweit das Recht der EU oder Deutschlands dies vorschreibt. Auf Anfrage bestätigen wir die Löschung in Textform.

15. KI-Verarbeitung

Die KI-Analyse läuft auf Amazon Bedrock in der EU (Frankfurt). Weder wir noch unsere KI-Anbieter verwenden Ihre Daten, um KI-Modelle zu trainieren oder zu verbessern.

Wir verwenden Ihre Daten nur, um Ihnen den Dienst zu erbringen. Wir verkaufen sie nicht, geben sie nicht für Werbung weiter und führen sie nicht für eigene Zwecke mit anderen Daten zusammen.

16. Haftung

Ihre Rechte und die Rechte betroffener Personen nach Art. 82 DSGVO werden durch diesen AVV nicht eingeschränkt. Im Verhältnis zwischen Ihnen und uns gilt die Haftungsbeschränkung der Nutzungsbedingungen, und jede Partei trägt ihren eigenen Anteil an einem Schaden entsprechend Art. 82 Abs. 2 und 5 DSGVO.

17. Datenschutzrecht des Vereinigten Königreichs, der Schweiz und der USA

Vereinigtes Königreich. Soweit die UK GDPR anwendbar ist, gilt dieser AVV für sie entsprechend. Für Übermittlungen personenbezogener Daten aus dem Vereinigten Königreich an Unterauftragsverarbeiter außerhalb des Vereinigten Königreichs und des EWR gilt das von der ICO herausgegebene UK International Data Transfer Addendum zu den EU-Standardvertragsklauseln.

Schweiz. Soweit das Schweizer Bundesgesetz über den Datenschutz (DSG) anwendbar ist, gilt dieser AVV für es entsprechend. Für Übermittlungen personenbezogener Daten aus der Schweiz gelten die EU-Standardvertragsklauseln mit den vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) verlangten Anpassungen: Zuständige Behörde ist der EDÖB, der Begriff „Mitgliedstaat“ umfasst die Schweiz, und betroffene Personen in der Schweiz können ihre Ansprüche dort geltend machen.

Vereinigte Staaten. Sind Sie ein „business“ im Sinne des California Consumer Privacy Act (CCPA) oder Verantwortlicher nach einem vergleichbaren Gesetz eines US-Bundesstaates, handeln wir als Ihr „service provider“ bzw. Auftragsverarbeiter. Wir verarbeiten personenbezogene Informationen nur für die Zwecke nach Abschnitt 3. Wir verkaufen sie nicht und geben sie nicht weiter, bewahren sie nicht außerhalb unserer unmittelbaren Geschäftsbeziehung mit Ihnen auf, verwenden oder offenbaren sie dort nicht und führen sie nicht mit anderen personenbezogenen Informationen zusammen, soweit diese Gesetze es nicht erlauben. Wir bieten das gesetzlich von Ihnen verlangte Datenschutzniveau, unterstützen Sie bei Anfragen von Verbrauchern, teilen Ihnen mit, wenn wir diese Pflichten nicht mehr erfüllen können, und ermöglichen Ihnen nach Abschnitt 13 angemessene Schritte, um unsere Einhaltung zu prüfen und unbefugte Nutzung zu unterbinden und zu beheben.

Verlangt das Recht eines anderen Landes bestimmte Vertragsklauseln, etwa die Standardvertragsklauseln der brasilianischen Datenschutzbehörde, vereinbaren wir diese auf Anfrage mit Ihnen.

18. Laufzeit und Änderungen

Dieser AVV gilt, solange wir personenbezogene Daten in Ihrem Auftrag verarbeiten.

Über wesentliche Änderungen dieses AVV informieren wir Sie mindestens 30 Tage vor ihrem Wirksamwerden per E-Mail und im Dienst. Sie können vor ihrem Wirksamwerden widersprechen und nach den Nutzungsbedingungen kündigen. Gesetzlich erforderliche Änderungen oder Änderungen, die den Schutz Ihrer Daten nicht verringern, können früher wirksam werden.

Dies ist Version 2.0. Sie gilt für neue Kunden ab ihrer Veröffentlichung und für bestehende Kunden 30 Tage nach unserer Mitteilung. Frühere Fassungen erhalten Sie auf Anfrage.

19. Kontakt

Bei Fragen zu diesem AVV oder für ein gegengezeichnetes Exemplar wenden Sie sich bitte an: contact@kodex-compliance.com