

Data Processing Agreement

Auftragsverarbeitungsvertrag (AVV)

Version 2.0 · Last updated: October 2026

Pursuant to **Article 28 of the General Data Protection Regulation (GDPR)**. This Data Processing Agreement ("DPA") forms part of the Terms of Service between **Kodex-Compliance UG (haftungsbeschränkt)** ("Processor", "we") and the organisation using the Service ("Controller", "you").

1. Parties, Scope and Form

The Processor is Kodex-Compliance UG (haftungsbeschränkt), Lindenstraße 29c, 12555 Berlin, Germany, registered at the Amtsgericht Charlottenburg (Berlin) under HRB 289793, represented by its managing director Jeremiah Matador.

This DPA applies whenever we process personal data on your behalf while providing the Service. You accept it together with the Terms of Service when you create your account. Art. 28(9) GDPR allows this agreement to be concluded in electronic form. You can download each version as a PDF at any time, and we send you a countersigned copy on request.

Where we decide ourselves why and how personal data is processed, for example for your user accounts, billing, security logs and our own legal obligations, we act as a controller. Our Privacy Policy applies to that processing, not this DPA.

If this DPA and the Terms of Service conflict on the protection of personal data, this DPA prevails.

2. Subject Matter and Duration

We process personal data on your behalf to provide compliance assessment, document management and AI-assisted compliance analysis. Processing lasts for as long as you use the Service and ends with the deletion described in section 14.

3. Nature and Purpose of Processing

- Storing and analysing the compliance evidence and documents you upload
- AI-assisted evaluation of compliance controls against regulatory frameworks
- Generating compliance reports, policies and risk assessments
- Reading settings, user lists and permissions from systems you connect (integrations), read-only and only for the checks you run
- Checking your public website for its legal pages (website check), unless you have switched it off
- Transcribing voice agent samples you upload, where you use that feature
- Managing the user accounts and access of your team in the Service

4. Types of Personal Data

- Contact details (names, email addresses, job titles)
- Employment information contained in uploaded compliance evidence
- User, role and permission data from systems you connect
- IT security data (access logs, system configurations)
- Voice recordings and transcripts, where you upload voice agent samples
- Any other personal data contained in documents you upload

Please upload special categories of personal data (Art. 9 GDPR) only where your compliance work requires it.

5. Categories of Data Subjects

- Your employees and contractors
- Your customers, where they appear in uploaded evidence
- Your partners, suppliers and vendors
- Users of the systems you connect

6. Your Instructions

We process personal data only on your documented instructions. Your instructions are this DPA, the Terms of Service, the settings you choose in the Service and any further instructions you give us in writing. Email is enough.

We also process personal data where EU or German law requires us to. In that case we tell you before we do, unless that law forbids it.

If we believe an instruction breaks data protection law, we tell you immediately. We may pause that instruction until you confirm or change it.

7. Our Obligations

We:

- (a) make sure everyone who can access your personal data is bound to confidentiality
- (b) protect your personal data with the technical and organisational measures in section 11 (Art. 32 GDPR)
- (c) use sub-processors only as described in section 9
- (d) help you answer requests from data subjects (Art. 12 to 23 GDPR). The Service lets you find, export, correct and delete data yourself. If a data subject contacts us directly, we pass the request on to you without undue delay and do not answer it ourselves unless you ask us to
- (e) help you meet your obligations under Art. 32 to 36 GDPR (security, breach notifications, data protection impact assessments and prior consultation) with the information available to us
- (f) keep a record of the processing we carry out for you (Art. 30(2) GDPR)
- (g) tell you without undue delay if we can no longer meet our obligations under this DPA
- (h) make available the information you need to show compliance with Art. 28 GDPR, and allow audits as described in section 13

We are not currently required to appoint a data protection officer. You can reach us on all data protection matters at contact@kodex-compliance.com.

8. Your Obligations

You are responsible for the lawfulness of the processing you instruct, including having a legal basis for the data you upload or connect, and for informing the data subjects concerned. Tell us without undue delay if you find errors or irregularities in our processing.

9. Sub-Processors

You give us general authorisation to engage sub-processors. We currently use the following:

Sub-Processor	Purpose	Location	Safeguards
Supabase Pte. Ltd.	Database, authentication, file storage	EU	EU region; EU Standard Contractual Clauses for support access from outside the EEA
Amazon Web Services EMEA SARL (Amazon Bedrock, Anthropic Claude models)	AI inference for compliance evaluation	EU (Frankfurt, eu-central-1; EU inference profiles stay within the EU)	EU entity; EU region
Stripe Payments Europe, Limited	Payment processing	EU (Ireland)	EU entity; EU Standard Contractual Clauses for transfers within the Stripe group
Upstash, Inc.	Redis caching, rate limiting, background job coordination	EU (Frankfurt)	EU region; EU Standard Contractual Clauses for access from the US
Render Services, Inc.	Application hosting and deployment	EU (Frankfurt)	EU region; EU Standard Contractual Clauses for access from the US
Resend, Inc.	Transactional email delivery	EU	EU region; EU Standard Contractual Clauses for access from the US
Functional Software, Inc. (Sentry)	Error monitoring	EU (Frankfurt ingest)	EU region; EU Standard Contractual Clauses for access from the US
Cloudflare, Inc.	Domain, network security, traffic delivery	Global network	EU Standard Contractual Clauses

We tell you about any intended addition or replacement of a sub-processor at least 30 days before it takes effect, by email to the owners and admins of your organisation and by updating this page.

You may object within 14 days of our notice, on reasonable data protection grounds, by writing to contact@kodex-compliance.com. We will try to find a solution with you. If we cannot, you may terminate the affected part of the Service before the change takes effect, and we refund any fees you paid in advance for the period after termination.

If we must replace a sub-processor urgently to keep the Service secure or running, we may do so with shorter notice. We then tell you without undue delay and your right to object applies in the same way.

We bind every sub-processor by contract to data protection obligations that are at least as protective as this DPA (Art. 28(4) GDPR). We remain fully liable to you for our sub-processors.

10. International Data Transfers

We host the Service and your data in the European Union. Where a sub-processor, its group or its support staff can access personal data from outside the EEA, we transfer data only on the basis of Chapter V GDPR, mainly the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, Module 3) together with a transfer impact assessment.

Where a US sub-processor is certified under the EU-US Data Privacy Framework, that certification is an additional safeguard. We do not rely on it alone, so a change in its legal status does not leave a transfer without a basis.

11. Technical and Organisational Measures

We take the following measures:

- Encryption at rest (AES-256) and in transit (TLS 1.2 or higher)
- Separation of customers: every request is scoped to your organisation, and this is covered by automated tests
- Role-based access control in the Service following the principle of least privilege
- Access to production systems limited to the people who need it for their work
- Daily backups by our hosting provider
- Logging of security-relevant actions in an audit log
- Rate limiting and automated monitoring with error and incident detection
- Automated scanning for leaked secrets and vulnerable dependencies on every code change
- Confidentiality obligations for everyone with access to personal data

We review these measures at least once a year and whenever risks change. We may update them as technology develops, as long as the overall level of protection does not drop.

12. Personal Data Breaches

We notify you without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting your data. We notify the owners and admins of your organisation by email.

Our notice includes the information required by Art. 33(3) GDPR, as far as it is available. Where information is not yet available, we provide it in phases as soon as we have it. We help you notify the supervisory authority and the data subjects, and we document every breach.

13. Audits

On request we provide the information you need to check our compliance with this DPA, such as this DPA, our technical and organisational measures and information on our sub-processors. In most cases this answers the questions.

If it does not, you may audit us, or have an independent auditor bound to confidentiality audit us, once per calendar year, with at least 30 days' written notice, during normal business hours and without disrupting our operations. More frequent audits are possible after a personal data breach or where a supervisory authority requires them.

Each party bears its own costs of an audit. The rights of supervisory authorities remain unaffected.

14. Deletion and Return of Data

You can export your data from the Service at any time. When the Service ends, we keep your data for 30 days so you can export it, then we delete it. You can also delete your account and data yourself at any time in the settings. Backup copies are removed within 90 days.

We keep data longer only where EU or German law requires us to. On request we confirm the deletion in writing.

15. AI Processing

AI analysis runs on Amazon Bedrock in the EU (Frankfurt). Neither we nor our AI providers use your data to train or improve AI models.

We use your data only to provide the Service to you. We do not sell it, share it for advertising or combine it with other data for our own purposes.

16. Liability

Your rights and the rights of data subjects under Art. 82 GDPR are not limited by this DPA. Between you and us, the limitation of liability in the Terms of Service applies, and each party is responsible for its own share of any damage in line with Art. 82(2) and (5) GDPR.

17. UK, Swiss and US Data Protection Laws

United Kingdom. Where UK GDPR applies, this DPA applies to it in the same way. For transfers of UK personal data to sub-processors outside the UK and the EEA, the UK International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the ICO applies.

Switzerland. Where the Swiss Federal Act on Data Protection (FADP) applies, this DPA applies to it in the same way. For transfers of Swiss personal data, the EU Standard Contractual Clauses apply with the adjustments required by the Swiss Federal Data Protection and Information Commissioner (FDPIC): the FDPIC is the competent authority, the term “member state” includes Switzerland, and data subjects in Switzerland can bring claims there.

United States. Where you are a “business” under the California Consumer Privacy Act (CCPA) or a controller under a similar US state law, we act as your “service provider” or processor. We process personal information only for the purposes in section 3. We do not sell or share it, retain, use or disclose it outside our direct business relationship with you, or combine it with other personal information, except as those laws permit. We provide the same level of privacy protection the law requires of you, help you answer consumer requests, tell you if we can no longer meet these obligations, and let you take reasonable steps under section 13 to check our compliance and stop and fix any unauthorised use.

If the law of another country requires specific contract terms, such as the standard contractual clauses of Brazil’s data protection authority, we agree them with you on request.

18. Term and Changes

This DPA lasts as long as we process personal data on your behalf.

We tell you about material changes to this DPA at least 30 days before they take effect, by email and in the Service. You can object and terminate under the Terms of Service before they take effect. Changes required by law, or that do not reduce the protection of your data, may take effect sooner.

This is version 2.0. It applies to new customers from its publication and to existing customers 30 days after we notified them. Earlier versions are available on request.

19. Contact

For questions about this DPA or to request a countersigned copy, please contact: contact@kodex-compliance.com