Effective 25 October 2026 · Last updated 21 October 2026

Data processing agreement

This Data Processing Agreement ("DPA") is part of the Friday Terms of Service ("Terms") between **Liftu Technology Private Limited (operating as Kodiva.ai)** ("Kodiva", the **Processor**) and the customer that holds the Friday workspace ("Customer", the **Data Fiduciary / Controller**). It applies automatically when the Customer accepts the Terms. It needs no separate signature. A signed copy is available on request.

If this DPA and the Terms conflict on data protection, this DPA wins. If this DPA and the Standard Contractual Clauses conflict, the Clauses win.

1. Definitions

- **Data Protection Law:** India's Digital Personal Data Protection Act, 2023 and its Rules ("DPDP"); the EU General Data Protection Regulation 2016/679 ("GDPR"); the UK GDPR and Data Protection Act 2018; and any other data protection law that applies to the Customer Personal Data.
- **Customer Personal Data:** personal data about candidates, client contacts, the Customer's users and other individuals that the Customer or its agents put into Friday.
- **Data Principal / Data Subject:** the individual the data is about.
- **Personal Data Breach:** a breach of security that leads to accidental or unlawful destruction, loss, change, unauthorised disclosure of, or access to, Customer Personal Data.
- **Sub-processor:** a third party that Kodiva engages to process Customer Personal Data.
- **Standard Contractual Clauses (SCCs):** the clauses approved by European Commission Decision (EU) 2021/914.

2. Roles and instructions

2.1 The Customer is the data fiduciary (DPDP) and controller (GDPR) of Customer Personal Data. Kodiva is its processor.

2.2 Kodiva processes Customer Personal Data only on the Customer's documented instructions. These instructions are the Terms, this DPA, and what the Customer and its users or agents do in Friday (for example adding a candidate, sending an email or submitting a CV to a client).

2.3 If Kodiva believes an instruction breaks Data Protection Law, it will tell the Customer and may refuse to act on it.

2.4 The Customer is responsible for:

- having a lawful basis, and where needed consent, for the data it puts into Friday;
- giving candidates and contacts the notices the law requires;
- the accuracy of the data;
- the actions its agents take in Friday. An agent acts with its owner's permissions.

2.5 Kodiva will not sell Customer Personal Data, use it for its own purposes, or use it to train AI models.

3. Confidentiality

Everyone at Kodiva who can access Customer Personal Data is bound by confidentiality. Staff open a workspace only to provide support, and only with the workspace owner's approval, which shows in the app while access is on. The exception is access needed to keep the service secure or to meet a legal obligation.

4. Security

Kodiva maintains the technical and organisational measures in **Annex 2**. These measures are designed to protect Customer Personal Data against breaches and to be suitable for the risk. Kodiva may update them, as long as the overall level of protection does not go down.

5. Sub-processors

5.1 The Customer authorises Kodiva to use the sub-processors listed on the Security page at friday.kodiva.ai/homepage/security#sub-processors (see Annex 3).

5.2 Kodiva will give at least **30 days' notice** before adding or replacing a sub-processor, by email to workspace owners and on the Security page. The Customer can object on reasonable data protection grounds within that time. If the parties can't resolve the objection, the Customer may end the affected service and receive a pro-rata refund of prepaid fees.

5.3 Kodiva puts data protection terms in writing with each sub-processor that are no less protective than this DPA. It stays responsible to the Customer for each sub-processor's work.

6. Helping with individuals' rights

Kodiva gives the Customer tools in Friday to find, export, correct and erase a person's data, record consent and withdrawals, and mark someone as "do not contact". If a request comes straight to Kodiva, it will pass it to the Customer without undue delay and won't respond itself unless the Customer asks. Kodiva will reasonably help the Customer with further requests.

7. Personal data breaches

7.1 Kodiva will notify the Customer **without undue delay, and in any case within 48 hours** of becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 The notice will describe, as far as Kodiva then knows:

- what happened and when;
- the categories and approximate number of people and records affected;
- likely consequences;
- the steps taken to contain it;
- a contact person.

Kodiva will send updates as it learns more.

7.3 This lets the Customer meet its own duties to inform the Data Protection Board of India and affected Data Principals (including the detailed report the DPDP Rules require within 72 hours), or a GDPR supervisory authority within 72 hours. Kodiva's notice is not an admission of fault.

8. Help with compliance

Where the law requires it, Kodiva will reasonably help the Customer with data protection impact assessments and consultations with regulators, and as a Significant Data Fiduciary if the Customer is classified as one.

9. Audits

Kodiva will provide the information reasonably needed to show it complies with this DPA, including completed security questionnaires and, once available, third-party audit reports. If that is not enough, or a regulator requires it, the Customer may carry out an audit:

- at most once a year;
- with 30 days' written notice;
- during business hours;
- at its own cost;
- under confidentiality;
- without access to other customers' data.

10. International transfers

10.1 Customer Personal Data is hosted in **India** (AWS, Mumbai) by default. Hosting in the United States is available on the Organizations plan.

10.2 **EU data:** where Customer Personal Data subject to the GDPR is transferred to Kodiva or its sub-processors outside the EEA, the SCCs apply and are incorporated into this DPA:

- Module 2 (controller to processor), or Module 3 (processor to processor) where the Customer is itself a processor;
- Clause 7 (docking) applies;
- Clause 9 option 2 (general authorisation, 30 days' notice);
- Clause 11 optional wording does not apply;
- Clauses 17 and 18: the law and courts of Ireland;
- Annexes I and II are Annexes 1 and 2 of this DPA.

10.3 **UK data:** the UK International Data Transfer Addendum to the SCCs (version B1.0) applies. **Swiss data:** the SCCs apply with references read as references to the Swiss FADP and the FDPIC.

10.4 **Indian data:** Kodiva will not transfer Customer Personal Data to any country restricted by the Government of India under section 16 of the DPDP Act.

11. Return and deletion

When the Customer's workspace is closed, the Customer can export all its data for **30 days**. Kodiva then deletes Customer Personal Data from live systems within 30 days and from backups within 90 days, unless the law requires it to keep some. Minimal "do not contact" records are kept only if the Customer chooses to keep them, so that those people are not contacted again.

12. Liability and term

Each party's liability under this DPA is subject to the limits in the Terms, except where Data Protection Law does not allow such limits. This DPA lasts as long as Kodiva processes Customer Personal Data.

Annex 1 · Details of processing

- **Subject matter and purpose:** providing Friday, a recruitment workspace for agencies: storing and organising candidates, roles and clients; sending and receiving email; recording calls and notes; submitting candidates to clients; and running careers pages.
- **Duration:** the term of the Terms, plus the deletion periods in section 11.
- **Data Principals:**
  - candidates and applicants;

    - the Customer's client contacts and hiring managers;
    - referees;
    - the Customer's users.
- **Categories of data:**
    - identity and contact details;
    - CV and work history, education and skills;
    - current and expected pay, notice period, location and work preferences;
    - messages, call records and notes;
    - interview feedback, offers and joining details;
    - consent and do-not-contact records;
    - usage logs.
- **Sensitive data:** not required by Friday. The Customer should not add health, caste, religion, biometric or similar data unless the law allows it and it is necessary.
- **Frequency:** continuous, for as long as the Customer uses Friday.

Annex 2 · Security measures

- **Encryption:** TLS 1.2+ in transit, AES-256 at rest, and encrypted backups.
- **Tenant isolation:** each workspace is scoped on every request; there is no cross-workspace search, cache or index.
- **Access:**
    - single sign-on through our identity provider, and multi-factor authentication available;
    - role-based permissions;
    - agents act only with their owner's permissions;
    - staff access only with the workspace owner's approval, shown by a banner while it is on.
- **Logging:** every action is recorded with who (and which agent) did it, and security logs are kept for at least 1 year.
- **Infrastructure:** hosted on AWS in India; production access limited to named engineers; regular patching; dependency and vulnerability scanning.
- **Continuity:** daily backups with tested restores, and backups kept for at most 90 days.
- **People:** confidentiality agreements and security training for staff.
- **Incident response:** a documented process with a 48-hour customer notice target.
- **Disclosure:** security@friday.kodiva.ai; we reply within 2 working days.

Annex 3 · Sub-processors (21 Oct 2026)

Company	Purpose	Location
Amazon Web Services	Hosting, database, file storage	India (Mumbai)
Clerk	Sign-in and user accounts	United States
SendGrid (Twilio)	Sending email	United States
Nylas	Mailbox connection and reply sync	United States

The live list is on the Security page.