

Data Processing Addendum

Gradii's standard Data Processing Addendum for customers, covering the DPDP Act 2023, the GDPR and UK GDPR, with the security measures and sub-processors in its annexes.

VERSION	EFFECTIVE	OWNER	REVIEW	CLASSIFICATION
1.0	9 October 2026	Founder	Annual	Public

This is Gradii's standard Data Processing Addendum ("DPA"). It forms part of the agreement between Gradii and the customer when it is referenced in, or signed alongside, an order form or the Gradii Terms of Service. To receive a countersigned copy, email team@gradii.ai with your company's legal name and address.

1. Parties and scope

1.1 This DPA is between **Manjari Technologies Private Limited**, a company incorporated in India with its office at 316, Neelkanth Corporate Park, Vidyavihar West, Mumbai, Maharashtra, India ("**Gradii**"), and the customer identified in the Agreement ("**Customer**").

1.2 It applies whenever Gradii processes Customer Personal Data while providing the Gradii platform and related services (the "**Services**") under the Agreement.

1.3 If this DPA conflicts with the Agreement, this DPA prevails on matters of data protection. If it conflicts with the Standard Contractual Clauses, the Clauses prevail.

2. Definitions

- "**Applicable Data Protection Law**" means the Digital Personal Data Protection Act, 2023 and the rules made under it ("**DPDP Act**"); the Information Technology Act, 2000 and its rules; and, where they apply, Regulation (EU) 2016/679 ("**GDPR**") and the UK GDPR with the Data Protection Act 2018.
- "**Customer Personal Data**" means personal data that Gradii processes for Customer under the Agreement, including data about candidates, Customer's users and Customer's contacts.
- "**Personal Data Breach**" means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. It includes a "personal data breach" as defined in the DPDP Act.
- "**Sub-processor**" means a third party that Gradii engages to process Customer Personal Data.

- "**Controller**", "**Processor**", "**Data Fiduciary**", "**Data Processor**", "**Data Principal**" and "**Data Subject**" have the meanings given in Applicable Data Protection Law.

3. Roles

3.1 For Customer Personal Data, Customer is the Data Fiduciary and Controller, and Gradii is the Data Processor and Processor.

3.2 Customer is responsible for having a lawful basis for the processing, including any consent, and for giving candidates the notices that Applicable Data Protection Law requires. Gradii provides in-product consent and notice flows to help with this.

3.3 **Annex I** describes the processing: its subject matter, duration, nature and purpose, and the types of data and Data Principals.

4. Gradii's obligations

Gradii will:

- (a) process Customer Personal Data only on Customer's documented instructions. The Agreement, this DPA and Customer's use and configuration of the Services are those instructions. Gradii will tell Customer if it believes an instruction breaks Applicable Data Protection Law;
- (b) not sell Customer Personal Data, not use it for its own purposes, and not use it to train or fine-tune foundation AI models;
- (c) ensure that everyone authorised to process Customer Personal Data is bound by confidentiality;
- (d) implement and maintain the technical and organisational measures in **Annex II**. Gradii may update those measures, provided the overall level of security does not decrease;
- (e) assist Customer, taking into account the nature of the processing, with responding to Data Principal requests, with security, breach notification, data protection impact assessments and prior consultation;
- (f) keep a record of the processing it carries out on Customer's behalf.

5. Sub-processors

5.1 Customer gives general authorisation for Gradii to engage Sub-processors. The Sub-processors in place on the date of this DPA are listed in **Annex III** and at gradii.ai/trust-vault.

5.2 Gradii will give at least **30 days'** notice of a new Sub-processor, by updating the list and emailing Customer's notified contact. Customer may object on reasonable data-protection grounds within that period. The parties will then discuss it in good faith. If they cannot resolve the objection, Customer may terminate the affected Services and receive a refund of prepaid fees for them.

5.3 Gradii will put a written agreement in place with each Sub-processor, with data-protection obligations no less protective than this DPA. Gradii remains responsible for its Sub-processors' performance.

6. Personal Data Breach

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

6.2 The notice will describe, as far as is then known: the nature of the breach; the categories and approximate number of Data Principals and records involved; the likely consequences; and the measures taken or proposed. Gradii will provide further information as it becomes available.

6.3 Gradii will take reasonable steps to contain and remedy the breach. It will cooperate with Customer to meet Customer's notification duties to the Data Protection Board of India, supervisory authorities and Data Principals. Gradii will separately meet its own reporting duties to CERT-In.

6.4 A notice under this section is not an admission of fault.

7. Data Principal requests

If Gradii receives a request from a Data Principal about Customer Personal Data, it will pass the request to Customer within **5 business days**, and will not respond to it directly except to say it has been passed on. Gradii will help Customer respond, including through the export and deletion functions in the Services.

8. Audits

8.1 Gradii will make available to Customer the information reasonably needed to show compliance with this DPA, including its Trust Vault documents and completed security questionnaires.

8.2 No more than once a year, or after a Personal Data Breach, or when a regulator requires it, Customer may audit Gradii's compliance with this DPA. The audit is carried out by Customer, or by an independent auditor bound by confidentiality, on 30 days' written notice, during business hours, and without access to other customers' data. Customer bears its own costs.

9. International transfers

9.1 Gradii stores Customer Personal Data in India. Sub-processors may process it in the locations listed in Annex III.

9.2 Where the GDPR applies to a transfer from Customer to Gradii, the **Standard Contractual Clauses** in the Annex to Commission Implementing Decision (EU) 2021/914, **Module Two (controller to processor)**, are incorporated by reference, with these options: Clause 7 (docking clause) applies; under Clause 9, option 2 (general authorisation) applies with the notice period in section 5.2; the optional wording in Clause 11 does not apply; under Clauses 17 and 18, the law and courts of Ireland apply. Annexes I to III of this DPA complete the Annexes to the Clauses.

9.3 Where the UK GDPR applies, the UK International Data Transfer Addendum to the EU SCCs (version B1.0) is incorporated, with the Clauses above as the "Approved EU SCCs".

9.4 Gradii will comply with any restriction on cross-border transfer that the Central Government of India notifies under section 16 of the DPDP Act.

10. Return and deletion

When the Agreement ends, Gradii will make Customer Personal Data available for export for **30 days**. It will then delete it from its live systems within a further **30 days**, unless the law requires it to be kept. Backups are overwritten in the ordinary course, within **35 days**. Gradii will confirm deletion in writing on request.

11. Liability

Each party's liability under this DPA is subject to the limits in the Agreement, except where Applicable Data Protection Law does not allow such a limit.

12. Term

This DPA lasts for as long as Gradii processes Customer Personal Data under the Agreement.

Annex I — Description of processing

Subject matter	Providing the Gradii AI hiring platform
Duration	The term of the Agreement plus the return and deletion period in section 10
Nature of processing	Collection, storage, structuring, analysis (including by AI models), transmission, verification against third-party sources, retrieval, and erasure
Purposes	Sourcing, screening, interviewing, assessing and verifying job candidates; scheduling and communicating with candidates; reporting to Customer; supporting and securing the Services
Data Principals	Job candidates and applicants; Customer's employees and users; referees and contacts that Customer provides
Categories of personal data	Identity and contact details; resume, employment and education history; job applications; interview responses (audio, video, text, code) and transcripts; scores and assessments; call recordings; messages; verification identifiers and documents (for example PAN, bank account, government-issued documents fetched through DigiLocker); device and IP data; account and usage data of Customer's users
Special or sensitive categories	Biometric data (face images and face embeddings for identity verification and interview integrity), only where Customer uses those features. Financial identifiers, only for background checks Customer orders.
Frequency	Continuous, for the term of the Agreement
Competent supervisory authority (GDPR)	As set out in Clause 13 of the SCCs, based on Customer's establishment or representative

Annex II — Technical and organisational measures

Area	Measures
Encryption	TLS 1.2+ in transit; HSTS; AES-256 at rest for the database, backups and file storage; AES-256-GCM application-level encryption of stored third-party OAuth tokens; bcrypt (cost 12) for passwords and API tokens
Data location	Primary database and file storage in India
Access control (customers)	SSO (Google, Microsoft Entra ID, Okta, SAML 2.0); TOTP two-factor authentication; role-based access; per-company tenant scoping; least-privilege just-in-time provisioning; brute-force rate limiting
Access control (Gradii)	Named-individual production access; SSH key-only, no password login; secrets kept out of source control; app runs as an unprivileged user blocked from the cloud metadata service; access reviewed quarterly
Network	Host firewall allowing only SSH, HTTP and HTTPS; managed database reachable only over TLS with credentials; cache protected by credentials, with TLS being enabled
Application security	Mandatory CI gate (type checking, lint, automated tests including security regression tests) before every production deploy; static analysis; security headers; signature verification of inbound webhooks; rate limiting of public endpoints
Logging and monitoring	Security audit log retained for 365 days; continuous component health monitoring and a public status page; logs retained to meet CERT-In requirements
Integrity	SHA-256 hashing of interview recording chunks; audit logs of DigiLocker and identity-verification requests
Availability and recovery	Managed database with daily backups and point-in-time recovery; release-directory deploys with fast rollback; documented business continuity and disaster recovery plan
Data minimisation and retention	Per-check data collection; scheduled deletion of OTPs, archived assistant conversations, API usage logs and audit logs; defined retention schedule for all other data
Incident response	Written incident response plan with severity levels, escalation, 48-hour customer notification and 6-hour CERT-In reporting
Vendors	Sub-processor due diligence and written terms before onboarding; annual review
People	Confidentiality obligations for all staff; security and privacy onboarding; access removed on the day someone leaves

Annex III — Sub-processors

The current list of Sub-processors, with purpose and location, is published at gradii.ai/trust-vault and in the Gradii Sub-processor List. It forms Annex III of this DPA.

Manjari Technologies Private Limited (“Gradii”) · 316, Neelkanth Corporate Park, Vidyavihar West, Mumbai, Maharashtra, India · gradii.ai/trust-vault

The current version of this document is published at gradii.ai/trust-vault. Printed or downloaded copies are uncontrolled.