Privacy Notice

[Organisation Legal Name] (operating as “[Trade / Brand Name]”)

How we collect, use, protect and govern personal data under India's Digital Personal Data Protection framework.

Version	Effective / updated	Legal framework
[X.X]	[DD Month YYYY]	DPDP Act, 2023 + DPDP Rules, 2025

Publication status

This is [Organisation]'s publication-ready Privacy Notice. It is drafted to align the organisation's stated privacy practices with the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules), taking account of their notified phased commencement dates.

Important

A Privacy Notice describes the organisation's privacy practices; it does not by itself establish compliance with every operational, technical, contractual or governance obligation under the DPDP framework. [Organisation] must maintain the corresponding controls, records, contracts and processes in practice.

How to use this template

Replace every bracketed placeholder with your own details, delete any processing activity that does not apply to you, and add any that is missing. Have the completed notice reviewed by your legal counsel before publication.

[Organisation] is based in [City, State], India. This notice applies to personal data processed through the [Organisation] website, [Primary Assessment / Diagnostic Service], [Higher Service Tiers] qualification journeys, assessments, consulting services, enquiries, partner referrals and related digital services.

Contents

01 Who we are

[Organisation Legal Name] ("[Organisation]", "we", "us" or "our"), operating under the trade name "[Trade / Brand Name]", is the Data Fiduciary for personal data for which [Organisation] determines the purpose and means of processing, subject to the scope and applicability of the DPDP Act.

Location: [City, State], India

Privacy & grievance contact: [Name / Designation of Grievance Officer]

Email: [privacy@organisation.example]

Telephone: [+91 XXXXX XXXXX]

Where [Organisation] processes personal data solely on behalf of a customer under the customer's documented instructions, [Organisation] may act as a Data Processor for that processing. The applicable customer contract and processor terms will then also govern that processing.

02 Notice at a glance

This notice is intended to be understandable independently of other information. Where [Organisation] requests consent for processing, the associated consent notice will identify the personal data requested and the specific purpose or purposes for which it is needed.

You can use the contact details in Section 13 to withdraw consent, exercise applicable rights, ask questions about processing, or raise a grievance. The current official information page of the Data Protection Board of India is maintained by the Ministry of Electronics and Information Technology.

Official Board information: https://www.meity.gov.in/data-protection-board-of-india

03 Personal data we collect

We seek to collect only personal data reasonably necessary for the relevant service or purpose. The categories below are representative and may vary depending on how you interact with [Organisation].

Processing activity	Itemised personal data	How obtained
[Primary Assessment / Diagnostic Service]	Name; work email; phone number; organisation/company name; industry; city/state; assessment responses; readiness score/results; recommendations and related business-contact information.	Directly from you or an authorised representative
[Higher Service Tiers] qualification	Name and business contact details; organisation profile; qualification responses; assessment/scorecard information; service-tier qualification information and related notes.	Directly from you or an authorised representative
Payments	Payment status; transaction reference; billing information where required. Card/UPI credentials are handled by the payment provider and are not intentionally stored by [Organisation].	Payment provider / you
Enquiries	Name; email; phone; message content; correspondence and support information.	Directly from you
Partner / referrals	Partner name and contact details; client contact name, business email/phone, organisation details, referral information and notes.	Partner or you

Processing activity	Itemised personal data	How obtained
Updates / newsletter	Name and email address; subscription preferences.	Directly from you
Website / technical data	IP address; browser/device information; pages visited; referring page; cookie or similar identifiers; technical logs and usage information, subject to applicable law and settings.	Automatically

04 Purposes and uses

- Provide and administer [Primary Assessment / Diagnostic Service], scorecards, reports and assessment services.
- Qualify an organisation for [Higher Service Tiers] and provide appropriate next steps.
- Communicate about assessments, services, support, transactions, enquiries and customer relationships.
- Process payments and maintain transaction records through payment service providers.
- Administer partner or referral arrangements.
- Send newsletters, compliance updates or service information where you have opted in or where otherwise permitted by law.
- Secure, troubleshoot, monitor and improve our website, applications and services.
- Meet legal, regulatory, accounting and contractual obligations and respond to lawful requests.

Where consent is required, we will not use consented personal data for a purpose materially different from the specified purpose without an applicable lawful basis or further notice/consent where required.

05 Consent and legitimate uses

Where consent is the basis of processing, [Organisation] will seek consent that is free, specific, informed and unambiguous, with clear affirmative action, and limited to personal data necessary for the specified purpose. Consent withdrawal will be enabled with an ease comparable to giving consent.

The DPDP Act also recognises specified legitimate uses. Where [Organisation] processes personal data under a legitimate use or another lawful basis available under applicable law, we will identify that basis where required and apply the safeguards applicable to that processing.

If a partner provides personal data about an individual, the partner must have the authority or other lawful basis required to provide the information to [Organisation] for the stated purpose.

Consent Managers: Once the Consent Manager framework under the DPDP Rules becomes operative, Data Principals may also be able to give, manage or withdraw consent through a registered Consent Manager. [Organisation] will update this notice with the relevant interoperability details once that framework applies to our services.

06 Sharing and Data Processors

- Payment providers — for payment processing and transaction confirmation.
- Cloud, hosting, infrastructure and security providers — to operate, secure and maintain [Organisation] services.
- Email, communications and support providers — to send service communications and respond to requests.
- Professional advisers — legal, audit, accounting or compliance support where reasonably necessary.

- Partners / referring firms — where relevant to a referral or engagement and consistent with the stated purpose.
- Government, regulators or law enforcement — where disclosure is required or authorised by law.

[Organisation] will use Data Processors under appropriate contractual arrangements and will require appropriate security safeguards and processing only for authorised purposes.

[Organisation] does not sell personal data.

07 Cross-border processing

[Organisation] and its service providers may process personal data using infrastructure located outside India. Any such transfer will be subject to the DPDP Act, DPDP Rules and any restrictions or requirements issued by the Central Government that apply to making personal data available outside India.

Where a customer contract imposes additional location, residency or transfer requirements, those contractual requirements will also apply.

08 Retention and deletion

[Organisation] retains personal data only for as long as necessary for the specified purpose, to provide the relevant service, to establish or defend legal claims, to meet accounting or other legal requirements, or for another period permitted or required by applicable law.

We maintain retention schedules by processing activity and category. When personal data is no longer required, we securely delete, anonymise or otherwise dispose of it, subject to lawful retention requirements.

Where the DPDP Rules prescribe a specific erasure period for a specified class of Data Fiduciary or purpose, [Organisation] will apply that requirement when it becomes applicable to the relevant processing.

09 Security safeguards

[Organisation] implements reasonable technical and organisational safeguards appropriate to the nature and risks of the personal data processed. These may include:

- Encryption, masking, obfuscation or other appropriate protection of personal data where applicable.
- Access controls and authentication for relevant computer resources.
- Logging, monitoring and review to detect and investigate unauthorised access.
- Backups and resilience measures to support continued processing following loss or compromise.
- Security provisions in contracts with relevant Data Processors.
- Security, incident-response, vulnerability-management and secure-development practices appropriate to the service.

The DPDP Rules, 2025 specify minimum reasonable security safeguards, including measures relating to access control, logs/monitoring, backups, processor contracts and technical and organisational controls. The Rules also prescribe retention of relevant logs and personal data for at least one year for specified purposes, subject to applicable exceptions.

10 Personal data breach response

If [Organisation] becomes aware of a personal data breach, we will activate our incident-response process, assess the incident, contain and remediate it, document relevant facts and determine notification obligations.

When the applicable DPDP Rules require notification to affected Data Principals, [Organisation] will communicate the required information in a concise, clear and plain manner without delay. This includes, as applicable, the nature and extent of the breach, timing, likely consequences, mitigation measures, safety measures for the Data Principal and business contact information for questions.

Notification to the Data Protection Board follows a two-stage process under the applicable Rules:

- Initial intimation — without delay, informing the Board of the nature, extent, timing and likely impact of the breach as known at that stage.
- Detailed report — within 72 hours of becoming aware of the breach, or within a longer period permitted by the Board, providing an updated and more complete account of the breach, including remedial measures and other prescribed particulars.

[Organisation] will follow the applicable statutory procedure and timelines for both stages.

Customers under a contractual engagement may have additional incident-notification obligations that apply to [Organisation] as a Data Processor.

11 Children's data

[Organisation]'s services are intended primarily for businesses, professionals and organisations. We do not knowingly seek to process children's personal data for our ordinary business services.

Where processing of a child's personal data is applicable, [Organisation] will apply the DPDP Act and DPDP Rules requirements relating to verifiable parental consent and restrictions on tracking, behavioural monitoring and targeted advertising, as applicable.

12 Your Data Principal rights

- Access / information — request information and a summary of personal data and processing, as provided by applicable law.
- Correction / updating — request correction of inaccurate or misleading personal data and completion of incomplete personal data.
- Erasure — request erasure where the DPDP Act or other applicable law requires or permits it.
- Grievance redressal — raise a grievance regarding [Organisation]'s processing of your personal data.
- Nomination — nominate another individual to exercise your rights in accordance with the DPDP Act.
- Withdrawal of consent — where consent is the basis of processing, withdraw consent at any time with comparable ease to giving it.

Rights are subject to the applicable provisions, commencement dates, conditions and lawful exceptions under the DPDP Act and Rules.

13 How to exercise rights and withdraw consent

[Organisation] prominently publishes the means for exercising Data Principal rights through this Privacy Notice and its website. You may submit a request by email to [privacy@organisation.example] or by using the privacy/contact mechanism made available on the [Organisation] website.

Suggested subject lines include: DPDP – Access Request, DPDP – Correction Request, DPDP – Erasure Request, DPDP – Withdraw Consent or DPDP – Grievance.

Please provide the email address, mobile number, assessment/reference number or other identifier reasonably required to identify the relevant Data Principal and processing activity. [Organisation] may verify

identity or authority before acting on a request.

Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal. Where another lawful basis permits continued processing or retention, [Organisation] may continue that limited processing.

The DPDP Rules require Data Fiduciaries to publish a grievance-response period of not more than 90 days. [Organisation]'s operational target is to acknowledge requests promptly and endeavour to resolve grievances within [30] days, subject to the complexity of the matter and any applicable statutory requirement.

For questions about processing, the business contact is: [Name / Designation of Grievance Officer] — [privacy@organisation.example] — [+91 XXXXX XXXXX].

14 Grievance redressal

Grievance Officer / authorised privacy contact: [Name / Designation of Grievance Officer], [Organisation Legal Name]

Email: [privacy@organisation.example]

Phone: [+91 XXXXX XXXXX]

Location: [City, State], India

A grievance should identify the relevant service or interaction and describe the concern. We may request reasonable information to verify identity and investigate the matter. [Organisation] will maintain records of grievances and actions taken as appropriate.

Our stated target is to resolve grievances within [30] days, subject to the nature and complexity of the matter and the maximum period applicable under the DPDP framework.

15 Data Protection Board of India

The Data Protection Board of India (DPBI) was established by the Central Government under Section 18 of the DPDP Act with effect from 13 November 2025. It is the statutory authority responsible for functions assigned to it under the Act, including inquiries into specified non-compliance and personal data breaches.

If you remain dissatisfied after using [Organisation]'s grievance mechanism, you may make a complaint to the Board in accordance with the procedure made available by the Board and applicable law.

Official Board information: https://www.meity.gov.in/data-protection-board-of-india

[Organisation] will update this section if the Board publishes or changes its official complaint-filing mechanism.

16 Changes to this notice

[Organisation] may update this Privacy Notice when our services, processing activities, technology, contractual arrangements or legal requirements change. The version number and “Last updated” date will be updated when material changes are made.

Where applicable law requires notice, communication or fresh consent for a material change in processing, [Organisation] will provide the required notice or obtain the required consent before applying the changed processing.

Privacy & grievance contact

[privacy@organisation.example] • [+91 XXXXX XXXXX]

[Organisation Legal Name] (operating as “[Trade / Brand Name]”) • [City, State], India

Regulatory timing note — [DD Month YYYY]: The Government's 13 November 2025 commencement notification phases the DPDP Act. The core substantive provisions in Sections 3–17 and related provisions are scheduled to commence 18 months after publication, i.e. 13 May 2027; Rule 4 commences one year after publication, while Rules 3 and 5–16, 22 and 23 commence 18 months after publication. This notice is drafted to prepare for the notified requirements while applying the provisions that are currently in force. (Notification and Official Gazette publication dates should be reconfirmed against the primary Gazette copy before this figure is treated as final, as some trackers record a one-day gap between the two.)

This document is a generic, reusable privacy notice template. Replace all bracketed placeholders with your organisation's details and have the completed notice reviewed by your legal counsel before adoption as your final legal policy.