

## Privacy Policy — India

### Digital Personal Data Protection Act, 2023 (DPDP Act) and DPDP Rules, 2025

#### Version 1.1 — September 2026 · Applies to Data Principals in India

This Privacy Policy applies to persons in India (“**you**”, “**Data Principal**”) who use our websites, our online store and our software products, including [www.mejuvante.ai](https://www.mejuvante.ai), [store.mejuvante.ai](https://store.mejuvante.ai) (the “**Store**”), [www.mejuvante.co.in](https://www.mejuvante.co.in) and the software-as-a-service products offered through them (together, the “**Services**”).

It explains, in plain language, which personal data we process, for which purposes, on which lawful basis, how long we keep it, with whom we share it, and how you can exercise your rights and raise a grievance. It has been drafted to meet the requirements of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, and — for the period until those provisions become fully enforceable — the Information Technology Act, 2000 (Section 43A) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“**SPDI Rules**”).

### 1. Who we are (Data Fiduciary)

The **Data Fiduciary** — the entity that determines the purpose and means of processing your personal data — is:

#### Mejuvante Private Limited

CIN: U74999KA2022PTC159102 · GSTIN: 29AAPCM5684G1ZR

Registered office: Flat No 133, Wing 1, 3rd Floor, Uber Verdant, Sarjapur Main Road, Doddakanehalli, Bangalore, Karnataka 560035, India

Office: 301/302, 3rd Floor, Saket Callipolis, Sarjapur – Marathahalli Road, Doddakannelli, Bengaluru, Karnataka 560035, India

Directors: Ankita Rishabh, Timo Traurig

Telephone: +91 98113 04887

E-mail: [work@mejuvante.co.in](mailto:work@mejuvante.co.in)

Mejuvante Private Limited concludes the contracts with customers in India, issues the invoices for Indian customers and is therefore the Data Fiduciary for the personal data of Data Principals in India.

**Group company and platform operator.** Mejuvante Private Limited is a member of the Mejuvante group. The websites and the technical platform of the Store are operated by our parent company, **Mejuvante GmbH**, Robert-Bosch-Str. 4b, 35440 Linden, Germany, which processes personal data on our behalf and under our instructions as a **Data Processor** (see Section 7). Where Mejuvante GmbH itself offers goods or services to persons in India, the DPDP Act also applies to it (Section 3(b) DPDP Act) and this Policy applies in the same way.

**Grievance Officer and data protection contact** — see Section 13.

## 2. Legal framework and effective dates

- **DPDP Act, 2023 and DPDP Rules, 2025.** The Rules were notified on 13 November 2025. Provisions concerning the Data Protection Board of India took effect immediately. The framework for Consent Managers takes effect on 13 November 2026. The substantive obligations relating to notice, consent, Data Principal rights, security safeguards, breach notification and children's data take effect on **13 May 2027**. We have chosen to apply these standards to your personal data **already now**.
- **IT Act, 2000 and SPDI Rules, 2011.** Until repealed by the DPDP Act, these rules continue to apply to “sensitive personal data or information”. This Policy also serves as the privacy policy required under Rule 4 of the SPDI Rules and designates the Grievance Officer required under Rule 5(9).
- **Other laws.** Where applicable, we also comply with the Consumer Protection (E-Commerce) Rules, 2020 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

## 3. Key terms

- **Personal data:** any data about an individual who is identifiable by or in relation to such data.
- **Processing:** any operation performed on digital personal data, including collection, recording, storage, use, sharing, disclosure and erasure.
- **Data Principal:** the individual to whom the personal data relates (for a child: including the parent or lawful guardian; for a person with a disability: including the lawful guardian).
- **Data Fiduciary:** the person who determines the purpose and means of processing.
- **Data Processor:** a person who processes personal data on behalf of a Data Fiduciary.
- **Consent Manager:** a registered entity through which you may give, manage, review and withdraw consent (available from 13 November 2026).
- **Board:** the Data Protection Board of India.

## 4. Personal data we process (itemised)

We process only the personal data that is necessary for the specified purpose. Depending on how you use the Services, this may include:

| Category                            | Examples                                                                                                               | Source                 |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>Identity and contact data</b>    | Name, e-mail address, telephone number, postal address, company and job title (business users)                         | You                    |
| <b>Account data</b>                 | User name, password (stored only as a cryptographic hash), account settings, language, subscription plan, licence keys | You / generated by us  |
| <b>Transaction and billing data</b> | Products purchased, order number, invoice details, billing address, payment                                            | You / payment provider |

| Category                                  | Examples                                                                                                                                                                             | Source        |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                                           | status, GSTIN (business customers), transaction ID.<br><b>We do not store full card numbers;</b> payments are processed by our payment service providers.                            |               |
| <b>Usage and technical data</b>           | IP address, date and time of access, browser type and version, operating system, device identifiers, pages visited, referrer, error logs, feature usage within our software products | Automatically |
| <b>Communication data</b>                 | Content of e-mails, contact-form and chat messages, support tickets, meeting bookings                                                                                                | You           |
| <b>Marketing data</b>                     | Newsletter subscription status, consent records, communication preferences                                                                                                           | You           |
| <b>Recruitment data</b>                   | Application documents, CV, qualifications, correspondence (only if you apply to us)                                                                                                  | You           |
| <b>Content you upload to our products</b> | Documents, data sets, prompts and outputs you process with our AI products                                                                                                           | You           |

We do not intentionally collect **sensitive personal data or information** within the meaning of the SPDI Rules (such as financial information beyond what payment providers process, health information, biometric data or sexual orientation). Please do not upload such data to our products unless a written data processing agreement with us expressly provides for it.

## 5. Purposes of processing and the Services they enable (itemised)

| Purpose                                                                                                | Services / goods enabled                 | Lawful basis                                                                                                 |
|--------------------------------------------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Creating and administering your account; providing the Store and our SaaS products; licence management | Store, MeJuVerse products, customer area | Consent for the specified purpose (Sec. 6) / voluntarily provided data for the specified purpose (Sec. 7(a)) |
| Processing orders, payments, invoices, refunds and subscription renewals                               | Store checkout, billing                  | Sec. 7(a); compliance with law (Sec. 7(c))                                                                   |
| Providing customer support and responding to enquiries                                                 | Contact form, chat, e-mail, booked calls | Sec. 7(a)                                                                                                    |
| Ensuring security, preventing                                                                          | All Services                             | Sec. 7(a); compliance with law                                                                               |

| Purpose                                                                        | Services / goods enabled | Lawful basis                                                   |
|--------------------------------------------------------------------------------|--------------------------|----------------------------------------------------------------|
| fraud and abuse, maintaining server logs                                       |                          |                                                                |
| Sending product information and newsletters                                    | Marketing e-mails        | <b>Consent</b> (Sec. 6) — withdrawable at any time             |
| Website analytics and performance measurement                                  | Websites, Store          | <b>Consent</b> (Sec. 6) — withdrawable at any time             |
| Embedding third-party content (e.g. maps, videos)                              | Websites                 | <b>Consent</b> (Sec. 6) — loaded only after you click “accept” |
| Handling job applications                                                      | Careers pages            | Sec. 7(a); employment purposes (Sec. 7(i))                     |
| Complying with legal obligations (tax, accounting, court or regulatory orders) | All Services             | Sec. 7(c)                                                      |
| Establishing, exercising or defending legal claims                             | —                        | Sec. 7(c)/(d)                                                  |

**Important:** Unlike EU law, the DPDP Act does not recognise a general “legitimate interest” basis. Any processing that is not necessary for the service you have requested or required by law — in particular analytics, marketing and third-party embeds — is carried out **only with your consent**.

## 6. Consent

**6.1 Standard of consent.** Where we rely on your consent, it is free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the personal data necessary for the specified purpose. We do not use pre-ticked boxes.

**6.2 Notice.** Before or at the time we request your consent, we provide you with a standalone notice in clear and plain language containing (a) an itemised description of the personal data, (b) the specified purpose and the goods or services enabled, (c) how you can withdraw consent, (d) how you can exercise your rights, and (e) how you can make a complaint to the Board. The notice is available in English and, at your option, in any language specified in the Eighth Schedule to the Constitution of India (please contact us). A model notice is attached as **Annex A**.

**6.3 Withdrawal.** You may withdraw consent at any time, as easily as you gave it — via the “Privacy settings” link in your account, the cookie banner, the unsubscribe link in each marketing e-mail, or by e-mail to the Grievance Officer. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. After withdrawal, we cease the processing concerned within a reasonable time and erase the data unless retention is required by law. Where the processing was necessary to provide a Service, you may no longer be able to use that Service.

**6.4 Consent Manager.** From 13 November 2026, you may also give, manage and withdraw consent through a Consent Manager registered with the Board, where we support such an integration.

**6.5 Children and persons with disabilities.** Our Services are directed at adults and businesses. We do not knowingly process the personal data of children (persons under 18 years) without the verifiable consent of a parent or lawful guardian, and we do not undertake tracking, behavioural

monitoring or targeted advertising directed at children. If you believe a child has provided personal data to us, please contact the Grievance Officer and we will erase it. The same applies to persons with disabilities who have a lawful guardian.

## 7. Sharing of personal data and Data Processors

We do not sell personal data. We share it only as follows:

**7.1 Data Processors acting on our instructions**, bound by written contracts with confidentiality and security obligations:

| Category                               | Processor                                                                            | Location                                                | Purpose                                                                     |
|----------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------|
| Group platform operator                | MeJuvante GmbH (parent company)                                                      | Germany                                                 | Operation of websites, Store platform and SaaS infrastructure on our behalf |
| Web hosting                            | 1&1 IONOS / 1&1 Telecommunication SE                                                 | Germany                                                 | Hosting of websites                                                         |
| Online store platform                  | [CONFIRM: Shopify International Ltd. / other]                                        | [CONFIRM: EU/Ireland; global infrastructure]            | Store, checkout, order management                                           |
| Payment processing (India, INR)        | PayU Payments Private Limited — hosted checkout; card data never reaches our servers | India                                                   | Payment authorisation and settlement for Indian customers                   |
| Cloud infrastructure for SaaS products | Amazon Web Services; Microsoft Azure                                                 | [CONFIRM regions, e.g. EU (Frankfurt) / India (Mumbai)] | Running our software products                                               |
| E-mail and communication tools         | [CONFIRM]                                                                            | [CONFIRM]                                               | Transactional and marketing e-mail, chat, support                           |
| Web analytics                          | Google (Google Analytics) — <b>only with your consent</b>                            | USA/EU                                                  | Statistical analysis of website use                                         |
| Maps and video embeds                  | Google Maps, YouTube — <b>only with your consent</b>                                 | USA/EU                                                  | Display of maps and videos                                                  |

**7.2 Group companies.** MeJuvante Private Limited and MeJuvante GmbH share personal data with each other where necessary to deliver the Services or provide support, under the inter-company service agreement and a data processing agreement.

**7.3 Marketplaces.** If you purchase our products through AWS Marketplace or the Microsoft Store, the respective marketplace operator processes your data under its own privacy terms; we receive only the data necessary to provision and support the product.

**7.4 Legal disclosures.** We may disclose personal data where required by law, court order or a lawful request of a competent authority, or to protect our rights, property or safety.

**7.5 Business transfers.** In the event of a merger, acquisition or restructuring, personal data may be transferred to the successor entity, which will remain bound by this Policy.

---

## 8. Transfer of personal data outside India

The platform of our Store and many of our Data Processors — including our parent company MeJuvante GmbH — are located in Germany and the European Union, and some in other countries. Your personal data will therefore be transferred outside India. Under Section 16 of the DPDP Act, such transfers are permitted except to countries or territories restricted by the Central Government of India. We will comply with any such restriction and with any conditions the Central Government imposes. Within the European Union, your data enjoys the protection of the General Data Protection Regulation (GDPR). We ensure by contract that all Data Processors protect your data to the standard required by Indian law.

---

## 9. Security safeguards

We implement reasonable security safeguards to prevent personal data breaches, in line with Section 8(5) DPDP Act, the DPDP Rules and the “reasonable security practices” standard of the SPDI Rules, including:

- encryption of data in transit (TLS) and at rest;
- role-based access control, multi-factor authentication for administrative access, and the principle of least privilege;
- logging and monitoring of access to personal data, with logs retained for at least one year where required;
- regular backups, tested restoration procedures and business-continuity measures;
- contractual security obligations imposed on every Data Processor;
- staff confidentiality obligations and training.

Please note that the transmission of information over the internet can never be guaranteed to be completely secure.

---

## 10. Personal data breaches

If a personal data breach occurs, we will (a) notify the **Data Protection Board of India** without delay, followed by a detailed report within the period prescribed by the DPDP Rules (currently 72 hours, extendable on request), and (b) notify **you** without delay, in plain language, describing the nature, extent, timing and location of the breach, its likely consequences, the measures we have taken or propose to take to mitigate the risk, the safety measures you may take to protect your interests, and the contact details of a person who can answer your questions.

## 11. Retention and erasure

We erase personal data — and cause our Data Processors to erase it — as soon as it is reasonable to assume that the specified purpose is no longer being served, or when you withdraw consent, unless retention is required by law. Indicatively:

| Data                                   | Retention                                                                                                                                                          |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server log files                       | 3 months, then erased or anonymised                                                                                                                                |
| Account data                           | For the life of the account, then erased within 30 days of closure (subject to legal retention below)                                                              |
| Transaction, invoicing and tax records | As required by applicable tax and commercial law — up to 10 years under German law (HGB/AO) and up to 8 years under Indian company and tax law [LAWYER TO CONFIRM] |
| Consent records                        | For the duration of the processing plus the applicable limitation period, as evidence of consent                                                                   |
| Marketing data                         | Until you withdraw consent or unsubscribe                                                                                                                          |
| Support communications                 | Up to 3 years after the enquiry is closed                                                                                                                          |
| Recruitment data                       | 6 months after the end of the application process, unless you consent to longer retention in a talent pool                                                         |
| Product content you upload             | For the duration of your subscription; erased or returned within 30 days after termination unless agreed otherwise                                                 |

Where the DPDP Rules require it, we retain personal data and associated traffic data for one year after the date on which erasure would otherwise occur, solely for the limited purposes permitted by law, and erase it thereafter. If you have not approached us for the performance of the specified purpose or exercised your rights for the period specified in the DPDP Rules, we will notify you at least 48 hours before erasing your personal data.

## 12. Your rights as a Data Principal

Under Sections 11 to 14 of the DPDP Act you have the right to:

1. **Access** — obtain a summary of the personal data we process about you and the processing activities, and the identities of all Data Fiduciaries and Data Processors with whom we have shared it (and a description of the data shared).
2. **Correction, completion and updating** — have inaccurate or misleading data corrected, incomplete data completed and data updated.
3. **Erasure** — have your personal data erased, unless retention is necessary for the specified purpose or required by law.

4. **Grievance redressal** — a readily available means to raise a grievance (Section 13).
5. **Nominate** — nominate another individual who may exercise your rights in the event of your death or incapacity.
6. **Withdraw consent** at any time (Section 6.3).

Under the SPDI Rules you additionally have the right to review the information you have provided and to have it corrected.

**How to exercise your rights.** Send a request to the Grievance Officer (Section 13) or use the privacy settings in your account. Please state the right you wish to exercise and provide enough information to verify your identity; we may ask for additional verification to protect your data. We respond **free of charge** and **within 30 days** of receipt (in any event within the maximum period prescribed by the DPDP Rules, which is 90 days). If we cannot comply with a request, we will tell you why.

**Duties of Data Principals.** When exercising your rights you must comply with applicable law, not impersonate another person, not suppress material information, not register a false or frivolous grievance, and only furnish information that is verifiably authentic (Section 15 DPDP Act).

---

## 13. Grievance Officer and grievance redressal

In accordance with Section 8(9) and (10) DPDP Act, Rule 5(9) SPDI Rules and Rule 3(2) of the IT Rules, 2021, we have appointed the following Grievance Officer, who is also the person able to answer your questions about the processing of your personal data:

### Grievance Officer

Name: **Ankita Rishabh**

Designation: Director, Mejuvante Private Limited

E-mail: [work@mejuvante.co.in](mailto:work@mejuvante.co.in)

Postal address: Mejuvante Private Limited, 301/302, 3rd Floor, Saket Callipolis, Sarjapur – Marathahalli Road, Doddakannelli, Bengaluru, Karnataka 560035, India

Telephone: +91 98113 04887

For persons in the European Union, our Data Protection Officer under the GDPR can be reached at [evelyn.schiener@mejuvante.com](mailto:evelyn.schiener@mejuvante.com).

**Timelines.** We acknowledge every grievance within **48 hours** and aim to resolve it within **30 days** of receipt; in all cases we respond within the maximum period prescribed by the DPDP Rules (90 days).

**Data Protection Board of India.** If you are not satisfied with our response, or if we do not respond within the prescribed period, you have the right to make a complaint to the Data Protection Board of India in the manner prescribed by the DPDP Rules ([PLACEHOLDER: Board website / complaint portal URL once published]).

---

## 14. Cookies and similar technologies

We use strictly necessary cookies (e.g. session, shopping cart, security, consent storage) which are required to operate the Services and do not require consent. All other cookies and similar technologies — analytics, embedded maps and videos, marketing — are set **only after you have given consent** through our consent banner, where you can also change or withdraw your choice at any time. Embedded YouTube videos and Google Maps are loaded only after you actively click on the placeholder (“two-click solution”). Details of the individual cookies, their providers and storage periods are listed in the consent banner.

---

## 15. Artificial-intelligence products and automated processing

Our software products use artificial-intelligence and machine-learning techniques to process the content you submit. We do not make decisions producing legal or similarly significant effects on you based solely on automated processing without human involvement, unless you have expressly consented or the decision is necessary to perform a contract with you. Content you upload to our products is processed only to provide the product to you, is not used to train models available to other customers without your express agreement, and is subject to the security safeguards in Section 9.

---

## 16. Business customers — where we act as Data Processor

Where an enterprise customer uses our SaaS products to process personal data of its own employees, customers or users, that customer is the Data Fiduciary and we act as its **Data Processor** under a written data processing agreement. This Policy does not apply to that processing; please refer to the privacy notice of the respective customer.

---

## 17. Social media and external links

We maintain profiles on LinkedIn, Xing and Kununu. If you interact with us there, the privacy policy of the respective platform applies. Our websites contain links to third-party websites, for whose content and privacy practices we are not responsible.

---

## 18. Changes to this Policy

We may update this Policy to reflect changes in law, technology or our Services. The current version is always available at [PLACEHOLDER: URL, e.g. <https://store.mejuvante.ai/privacy-india>]. Material changes will be notified to you by e-mail or by a prominent notice in the Services before they take effect. Where a change requires your consent, we will ask for it.

---

## 19. Language

This Policy is provided in English. On request, we will provide the consent notice in any language specified in the Eighth Schedule to the Constitution of India. In case of any inconsistency, the English version prevails.

---

## 20. Contact

Mejuvante Private Limited · 301/302, 3rd Floor, Saket Callipolis, Sarjapur – Marathahalli Road, Doddakannelli, Bengaluru, Karnataka 560035, India

E-mail: [work@mejuvante.co.in](mailto:work@mejuvante.co.in) · Telephone: +91 98113 04887

Grievance Officer: Ankita Rishabh (see Section 13)

## Annex A — Model consent notice (standalone, point-of-collection)

*To be displayed at the point where personal data is collected (e.g. account registration, checkout, newsletter sign-up, cookie banner). Must be presented independently of other information and require an affirmative action.*

### MeJuvante — Notice for processing your personal data

**Who:** Mejuvante Private Limited, Saket Callipolis, Sarjapur – Marathahalli Road, Bengaluru 560035, India (Data Fiduciary).

**Which personal data:** [itemise – e.g. name, e-mail address, company, billing address, order details, IP address].

**For which purpose and service:** [state the specified purpose and the goods/services enabled – e.g. "to create your account and provide the MeJuVerse subscription you have ordered"].

**Withdrawing consent:** You may withdraw your consent at any time, as easily as you gave it, at [link to privacy settings] or by e-mail to [work@mejuvante.co.in](mailto:work@mejuvante.co.in). Withdrawal does not affect processing already carried out.

**Your rights:** You may access, correct, update and erase your personal data, nominate a person to exercise your rights, and raise a grievance at [link]. We respond within 30 days.

**Complaints:** If your grievance is not resolved, you may complain to the Data Protection Board of India at [Board URL].

**Full details:** Privacy Policy — India at [URL]. Available in other Eighth Schedule languages on request.

☐ **I consent** to the processing of my personal data as described above.

---

## Annex B — Implementation checklist (internal; remove before publication)

1. ~~Designate and name the Grievance Officer~~ — DONE: Ankita Rishabh, Director; contact work@mejuvante.co.in.
2. ~~Decide the Data Fiduciary allocation~~ — DONE: Mejuvante Private Limited (bills Indian customers via PayU); GmbH = Data Processor/platform operator. Lawyer to confirm.
3. Confirm the remaining **Data Processor list** items (store platform, cloud regions, e-mail tools) and put signed processor contracts in place — PayU confirmed.
4. Implement the **standalone consent notice** (Annex A) at each collection point; keep consent logs (who, when, what, version).
5. Ensure the **consent banner** blocks analytics, maps and video embeds until consent (two-click solution).
6. Implement **rights-request workflow** (30-day SLA, identity verification, access summary incl. list of processors).
7. Implement **breach-response runbook** (Board notification + Data Principal notification templates, 72-hour clock).
8. Implement **retention schedule** (Section 11) technically; 48-hour pre-erasure notice for inactive accounts.
9. Check **GST/OIDAR** registration requirement for online services supplied to non-business customers in India (tax adviser).
10. Check whether the **Consumer Protection (E-Commerce) Rules, 2020** apply to the Store for Indian consumers (nodal contact person, 48-hour acknowledgement, one-month resolution) and align the India store GTC (23i).
11. Re-check the **DPDP Rules** and any Board guidance before **13 May 2027** (full enforceability) and on **13 November 2026** (Consent Managers).