

Starcore — Privacy Policy

Data Fiduciary: Zerotime Solutions LLP **Service:** Starcore Workforce Management System ("Starcore", the "Service") **Last updated:** 24 June 2026

1. Introduction & Scope

1.1 This Privacy Policy explains how **Zerotime Solutions LLP** ("we", "us", "our"), the operator of Starcore, collects, uses, shares, and protects personal data, and the rights available to you under the **Digital Personal Data Protection Act, 2023** and the **Digital Personal Data Protection Rules, 2025** (together, the "**DPDP Law**"), along with the Information Technology Act, 2000 and rules made under it.

1.2 **What this policy covers (important).** This policy applies to personal data **for which we act as the Data Fiduciary** — i.e., data we collect and control in running our business, including: - people who visit our websites (starcore.live, starcore.space) and marketing pages; - people who sign up for, administer, or pay for a Starcore account; and - people who contact our support or sales teams.

1.3 **What this policy does NOT cover.** When a customer organisation uses Starcore to manage its own workforce, the employee/worker personal data it processes through the Service (such as attendance, punch in/out, break, and location data) is controlled by **that customer**, who is the Data Fiduciary for it. For such data, **we act only as the Data Processor** on the customer's instructions. Our handling of that data is governed by our **Data Processing Agreement (DPA)** at <https://starcore.live/dpa>, not by this policy. If you are an employee of a Starcore customer and have questions about your data, please contact your employer.

2. Definitions

- **Personal Data** — any data about an individual who is identifiable by or in relation to such data.
 - **Data Principal** — the individual to whom the personal data relates.
 - **Data Fiduciary** — the person who determines the purpose and means of processing personal data.
 - **Data Processor** — a person who processes personal data on behalf of a Data Fiduciary.
 - **Processing** — any operation performed on personal data (collection, storage, use, sharing, deletion, etc.).
-

3. Personal Data We Collect

We collect the following categories of personal data when we act as Data Fiduciary:

3.1 Account & identity data — name, work email, phone number, company name, job role, and login credentials of the person who registers, administers, or is invited to manage a Starcore account.

3.2 Billing & payment data — billing name, business address, GSTIN, invoice history, and transaction references. Card and bank payment details are collected and processed directly by our payment gateway (Razorpay); **we do not store full card numbers or banking credentials** on our systems.

3.3 Usage, device & analytics data — IP address, browser and device type, pages and features used, clicks, session activity, and similar product-usage events captured through our analytics provider and cookies (see Clause 6).

3.4 Communications & support data — messages, queries, and attachments you send us via email, support tickets, or chat, and our responses.

3.5 Marketing data — your preferences and interactions where you subscribe to updates or engage with our marketing communications.

We collect data directly from you, automatically as you use the Service, and occasionally from your colleagues who invite you to an account.

4. How We Use Personal Data & Our Legal Basis

We process personal data for the following purposes, relying on either your **consent** or a **legitimate use** permitted under the DPDP Law (such as performing our contract with you or a purpose for which you voluntarily provided the data):

Purpose	Basis
Creating and administering your account	Performance of contract / legitimate use
Providing, maintaining, and securing the Service	Performance of contract
Billing, invoicing, and tax compliance	Legal obligation / contract
Responding to support and queries	Legitimate use
Product analytics and improving the Service	Consent (where required)
Sending service and security notices	Performance of contract
Sending marketing communications	Consent (withdrawable anytime)
Detecting fraud, abuse, and meeting legal obligations	Legal obligation / legitimate use

We will not use your personal data for a new, incompatible purpose without informing you and, where required, obtaining your consent.

5. Consent

5.1 Where we rely on consent, it will be free, specific, informed, unconditional, and unambiguous, given through a clear affirmative action.

5.2 You may **withdraw consent at any time**, as easily as you gave it, by using the controls in your account, the unsubscribe link in our emails, or by contacting our Grievance Officer (Clause 12). Withdrawal does not affect processing already carried out, and some processing necessary to provide the Service or meet legal duties may continue on another lawful basis.

6. Cookies & Analytics

6.1 We use cookies and similar technologies (local storage, identifiers) to keep you logged in, remember preferences, secure the Service, and understand how the Service is used. For full details of the cookies we use and how to manage them, see our **Cookie Policy** at <https://starcore.live/cookies>.

6.2 **Product analytics.** We use **PostHog** (EU Cloud) as our third-party product-analytics provider to collect usage and event data that helps us improve Starcore. PostHog processes this data on infrastructure located in the **European Union** (see Clause 8). We configure it to limit the personal data collected and, where supported, to anonymise IP addresses.

6.3 **Your choices.** Non-essential (analytics/performance) cookies are used only where permitted by your cookie settings. You can manage preferences through our cookie banner or your browser settings. Disabling non-essential cookies will not affect core functionality.

7. How We Share Personal Data

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

7.2 **Sub-processors / service providers** who help us run the Service, under contracts requiring appropriate security and confidentiality: - **Payment processing** — Razorpay (and bank transfer facilitation); - **Product analytics** — PostHog (EU Cloud); - **Hosting & infrastructure** — Amazon Web Services (AWS), Asia Pacific (Mumbai) region; - **Email** — our transactional email service provider, Amazon SES (AWS, Mumbai region, India), for account, security, and billing emails. A CRM provider may be added in future and will be added to this list.

7.3 **Legal & safety disclosures** — where required by law, court order, or to protect rights, safety, and the integrity of the Service.

7.4 **Business transfers** — in connection with a merger, acquisition, or sale of assets, subject to this policy.

8. Cross-Border Transfers

8.1 Core Customer Data is hosted in India (AWS Asia Pacific, Mumbai region). However, certain service providers — in particular our product-analytics provider, **PostHog (EU Cloud)** — process limited personal data on servers **outside India**, in the **European Union**.

8.2 We undertake such transfers in accordance with **Section 16 of the DPDP Act**, which permits transfer of personal data outside India except to territories restricted by the Central Government. We will not transfer personal data to any country so restricted.

8.3 Where possible, we prefer providers and configurations that keep data within India or within a region offering equivalent protection.

9. Data Retention

9.1 We retain personal data only as long as necessary for the purposes above or as required by law:

- **Account data** — for the life of your account, then deleted or anonymised within 90 days of account closure, subject to the export window in our Terms.
- **Billing, invoice & tax records** — retained for the period required under applicable tax, GST, and company law (which may be up to **8 years**).
- **Support communications** — up to 3 years.
- **Analytics data** — up to 24 months, in aggregated or pseudonymised form where feasible.
- **Marketing data** — until you withdraw consent or unsubscribe.

9.2 When the retention period ends, we securely delete or irreversibly anonymise the data.

10. Security Safeguards

We implement reasonable technical and organisational measures designed to protect personal data, including access controls, encryption in transit, secured infrastructure, logging, and staff confidentiality obligations, consistent with Section 8(5) of the DPDP Act. No system is perfectly secure, but we work to protect your data and to detect and respond to incidents.

11. Your Rights as a Data Principal

Subject to the DPDP Law, you have the right to:

- **Access** — request a summary of the personal data we process about you and the processing activities;
- **Correction & updating** — request correction of inaccurate or incomplete data;
- **Erasure** — request deletion of your personal data where it is no longer needed and retention is not legally required;
- **Withdraw consent** — at any time, as described in Clause 5;
- **Grievance redressal** — have your complaint addressed by us (Clause 12);
- **Nominate** — nominate another individual to exercise your rights in the event of death or incapacity.

To exercise any right, contact our Grievance Officer (Clause 12). We may need to verify your identity before acting. We will respond within the timelines required by law.

If you are not satisfied with our response, you may make a complaint to the **Data Protection Board of India**.

12. Grievance Officer & Contact

For any privacy questions, requests, or complaints:

Grievance Officer: Jaydeep Bhavsar **Email:** grievance@starcore.space **Company:** Zerotime Solutions LLP
Registered office: 232, Iscon Emporio, Besides Star Bazaar, Near Jodhpur Cross Road, Satellite,
Ahmedabad, Gujarat 380015, India **General queries:** hello@starcore.live | **Support:**
support@starcore.space

We aim to acknowledge grievances within **7 (seven) days** and resolve them within the timelines prescribed under the DPDP Law.

13. Children's Data

The Service is intended for business use by individuals aged 18 and above and is not directed at children. We do not knowingly collect personal data of children (individuals under 18) as Data Fiduciary through our signup channels. Where a customer uses Starcore to manage workers, the customer is responsible for ensuring it has any consents required under law, including for any worker who is a minor; such processing is governed by the DPA.

14. Personal Data Breach

In the event of a personal data breach, we will take prompt remedial action and will notify the Data Protection Board of India and affected Data Principals where and as required under the DPDP Law.

15. Changes to this Policy

We may update this Privacy Policy from time to time. We will post the updated version with a revised "Last updated" date and, for material changes, provide reasonable notice (e.g., by email or in-app). Your continued use of the Service after changes take effect constitutes acceptance.