Starcore — Data Processing Agreement (DPA)

Between: (1) The Customer — the organisation that has agreed to the Starcore Terms of Service ("**Customer**" / "**Data Fiduciary**"); and **(2) Zerotime Solutions LLP**, LLPIN AAZ-2134, registered office at 232, Iscon Emporio, Besides Star Bazaar, Near Jodhpur Cross Road, Satellite, Ahmedabad, Gujarat 380015, India ("**Zerotime**" / "**Data Processor**", "we", "us").

Last updated: 24 June 2026

1. Background & Scope

1.1 This DPA governs the processing of personal data by Zerotime on behalf of the Customer in connection with the Customer's use of the Starcore Workforce Management System (the "**Service**").

1.2 Under the **Digital Personal Data Protection Act, 2023** and the **Digital Personal Data Protection Rules, 2025** (the "**DPDP Law**"): - the **Customer is the Data Fiduciary** — it determines the purposes and means of processing the personal data of its employees, workers, and Authorized Users; and - **Zerotime is the Data Processor** — it processes that personal data only on behalf of, and on the documented instructions of, the Customer.

1.3 This DPA is required to satisfy **Rule 6 of the DPDP Rules, 2025**, which obliges a Data Fiduciary to ensure reasonable security safeguards through a contract with its Data Processor. If there is a conflict between this DPA and the Agreement on data-protection matters, this DPA prevails.

1.4 Separately, Zerotime acts as a **Data Fiduciary** for the limited business data it controls (account, billing, support, and analytics data). That processing is governed by the **Starcore Privacy Policy** (https://starcore.live/privacy), not by this DPA.

2. Definitions

Terms used here have the meaning given in the DPDP Law. In particular: - **Personal Data** — any data about an identifiable individual. - **Data Principal** — the individual to whom personal data relates (here, primarily the Customer's employees, workers, and Authorized Users). - **Processing** — any operation performed on personal data. - **Personal Data Breach** — any unauthorised processing, or accidental disclosure, acquisition, sharing, alteration, loss, or destruction of, or loss of access to, personal data, that compromises its confidentiality, integrity, or availability. - **Sub-processor** — any third party engaged by Zerotime to process personal data under this DPA. - **Customer Personal Data** — personal data processed by Zerotime on the Customer's behalf via the Service, as described in **Annexure A**.

3. Roles & Processing Instructions

3.1 Zerotime will process Customer Personal Data **only on the documented instructions of the Customer**, including as set out in this DPA, the Agreement, and the Customer's use and configuration of the Service.

3.2 The Customer's instructions are reflected in **Annexure A** (Details of Processing). The Customer may give additional reasonable instructions consistent with the Agreement.

3.3 Zerotime will inform the Customer if, in its opinion, an instruction infringes the DPDP Law, unless legally prohibited from doing so.

3.4 Zerotime will not sell Customer Personal Data and will not use it for its own purposes, including advertising or building external profiles. Zerotime may generate aggregated, de-identified statistics that cannot reasonably identify any Data Principal or the Customer, solely to operate and improve the Service.

4. Customer (Data Fiduciary) Responsibilities

4.1 The Customer is responsible, as Data Fiduciary, for: - (a) providing all required **notices** to, and obtaining all required **consents** or establishing another lawful basis from, its employees/workers/Authorized Users for processing their personal data (including attendance, punch in/out, break, location, and any selfie/photo data) through the Service; - (b) the accuracy of the personal data it provides; and - (c) ensuring it has the right to transfer the personal data to Zerotime for processing under this DPA.

4.2 The Customer warrants that its instructions and the personal data it submits comply with applicable law.

5. Zerotime (Data Processor) Obligations

Zerotime will:

5.1 **Confidentiality** — ensure that personnel authorised to process Customer Personal Data are bound by confidentiality obligations and access data only on a need-to-know basis.

5.2 **Security** — implement and maintain the technical and organisational security measures set out in **Annexure B**, consistent with Section 8(5) of the DPDP Act and Rule 6 of the DPDP Rules.

5.3 **Assistance with Data Principal rights** — provide reasonable assistance (through appropriate technical and organisational measures, and the Service's self-service features where available) to help the Customer respond to Data Principal requests for access, correction, erasure, and similar rights.

5.4 **Assistance with compliance** — provide the Customer with reasonable information and assistance needed to demonstrate compliance, including in relation to security, breach handling, and any data-protection impact assessment the Customer undertakes.

5.5 **Breach notification** — notify the Customer of a Personal Data Breach affecting Customer Personal Data **without undue delay and in any event within 48 hours** of becoming aware of it, and provide available information to help the Customer meet its own notification obligations to the Data Protection Board of India and affected Data Principals (see Clause 8).

5.6 **Records** — maintain records of its processing sufficient to demonstrate compliance with this DPA.

6. Sub-processing

6.1 The Customer provides **general authorisation** for Zerotime to engage Sub-processors to process Customer Personal Data. The current Sub-processors are listed in **Annexure C**.

6.2 Zerotime will impose data-protection and security obligations on each Sub-processor that are no less protective than those in this DPA, and remains responsible to the Customer for each Sub-processor's performance.

6.3 Zerotime will give the Customer **at least 30 days' notice** before adding or replacing a Sub-processor, with such notice given by email. If the Customer has a reasonable, data-protection-based objection, the parties will discuss it in good faith; if it cannot be resolved, the Customer may terminate the affected part of the Service as its sole remedy.

7. Cross-Border Transfers

7.1 Core Customer Personal Data is hosted in India (AWS Asia Pacific, Mumbai region). Certain Sub-processors — in particular the product-analytics provider **PostHog (EU Cloud)** — may process limited personal data in the **European Union**.

7.2 Any transfer of personal data outside India will be carried out in accordance with **Section 16 of the DPDP Act**, and Zerotime will not transfer personal data to any territory restricted by the Central Government.

8. Personal Data Breach

8.1 On becoming aware of a Personal Data Breach affecting Customer Personal Data, Zerotime will, within the timeline in Clause 5.5: (a) inform the Customer; (b) describe the nature of the breach and the data and Data Principals likely affected (to the extent known); (c) describe measures taken or proposed to address it; and (d) provide a contact point for more information.

8.2 Zerotime will take reasonable steps to mitigate and remediate the breach. The Customer, as Data Fiduciary, is responsible for any notifications it is required to make to the Data Protection Board of India and to affected Data Principals.

9. Audit

9.1 Zerotime will make available to the Customer information reasonably necessary to demonstrate compliance with this DPA.

9.2 The Customer may, on at least 30 days' written notice and no more than **once per 12 months** (unless required by a regulator or following a breach), audit Zerotime's compliance — either by reviewing Zerotime's security documentation or third-party audit reports/certifications (where available), or, where reasonably required, an on-site or remote inspection during business hours that does not compromise the security or confidentiality of other customers.

10. Return & Deletion of Data

10.1 On termination or expiry of the Agreement, the Customer may export Customer Personal Data within the export window stated in the Agreement (currently 30 days).

10.2 After that window, Zerotime will delete or irreversibly anonymise Customer Personal Data within 30 days, except to the extent retention is required by applicable law, in which case Zerotime will continue to protect it under this DPA.

10.3 On request, Zerotime will confirm deletion in writing.

11. Liability

11.1 Each party's liability under this DPA is subject to the limitations and exclusions in the Agreement. Nothing in this DPA limits any liability that cannot be limited under the DPDP Law or other applicable law.

12. Term, Governing Law & Jurisdiction

12.1 This DPA takes effect when the Customer accepts the Agreement and continues for as long as Zerotime processes Customer Personal Data.

12.2 This DPA is governed by the laws of India. The dispute-resolution, arbitration (seat: Ahmedabad, Gujarat), and jurisdiction provisions of the Agreement apply to this DPA.

Annexure A — Details of Processing

Subject matter: Provision of the Starcore Workforce Management System to the Customer.

Duration: For the term of the Agreement, plus any retention/deletion period in Clause 10.

Nature & purpose of processing: Hosting, recording, storing, displaying, and processing workforce data to enable attendance and time tracking, punch in/out and break management, scheduling, location verification, reporting, and related workforce-management functions configured by the Customer.

Categories of Data Principals: - The Customer's employees and workers (including deskless/field/multi-site staff); - The Customer's Authorized Users (administrators, managers, supervisors).

Categories of Customer Personal Data: - Identity & contact data — name, employee ID, email, phone, role/designation, site/location assignment; - Attendance & time data — punch in/out events, timestamps, break records, shift/schedule data, worked hours; - Location data — GPS/geolocation captured at punch (where the Customer enables location-based punch); - Image data — selfie/photo captured at punch (where the Customer enables photo-at-punch); - Account & access data — login credentials, access logs, device/IP information.

Special note: Zerotime is configured by default for **non-biometric** punch. Any biometric processing depends on Customer configuration and the Customer's lawful basis.

Annexure B — Technical & Organisational Security Measures

Zerotime maintains measures including:

1. **Access control** — role-based access, least-privilege, unique accounts, and multi-factor authentication for administrative access.
2. **Encryption** — encryption of personal data in transit (TLS) and at rest.
3. **Infrastructure security** — hosting on AWS (Mumbai region) with network controls, firewalls, and security-group restrictions.
4. **Logging & monitoring** — audit logging of key actions and monitoring for anomalous activity.
5. **Backups & resilience** — regular backups and recovery procedures.

6. **Vulnerability management** — patching and periodic security review of the application and dependencies.
7. **Personnel** — confidentiality obligations and security awareness for staff with data access.
8. **Incident response** — a defined process to detect, assess, and respond to Personal Data Breaches.
9. **Data minimisation & segregation** — collecting only data needed for the Service and logically separating customer data.
10. **Secure development** — secure coding practices and access controls over source and deployment.

Annexure C — Sub-processors

Sub-processor	Purpose	Location
Amazon Web Services (AWS)	Hosting & infrastructure	India (Mumbai region)
Razorpay	Payment processing	India
PostHog (EU Cloud)	Product analytics	European Union
Amazon SES (AWS)	Transactional email delivery	India (Mumbai region)