DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) forms part of the agreements between Fareclock, LLC (“Fareclock,” “Processor,” “we,” “us,” or “our”) and the entity or individual purchasing or using the Fareclock Services (“Customer,” “Controller,” “you,” or “your”). This DPA sets forth the parties’ respective rights and obligations with respect to the Processing of Personal Data and is intended to ensure compliance with applicable Data Protection Laws, including, but not limited to, the EU and UK General Data Protection Regulation (GDPR) and the EU-U.S. Data Privacy Framework (EU-U.S. DPF).

In the event of any conflict between the provisions of this Data Processing Addendum (“DPA”) and the Terms of Service agreed to by the user upon registration, the provisions of this DPA shall prevail solely with respect to the Processing of Personal Data.

1. DEFINITIONS AND ROLES

“Customer” means the Personal Information Controller (PIC), i.e., the organization or entity that determines the purposes and means of processing personal data through the Fareclock platform.

“Fareclock” means (1) the Personal Information Processor (PIP), responsible for processing personal data on behalf of the Customer, managing the service relationship, and acting as the primary point of contact for the Customer, and (2) the software application provided to the Customer, through which personal data is collected, processed, and managed in accordance with this DPA.

“Personal Data” means any information relating to an identified or identifiable individual processed by Fareclock on behalf of the Customer.

“Subprocessor” means any third-party service provider engaged by Fareclock to process personal data on behalf of the Customer, including cloud hosting, email delivery, analytics, or other support services.

“Super Administrator" means the user account with the highest-level access in Fareclock, having full control over system settings, user management, permissions, reporting, and configuration.

“Administrator” means a user account in Fareclock authorized to manage users, assign roles, access reports, and configure system settings, subject to the permissions granted by the Super Administrator.

“Services” means any work, support, or activities performed by Fareclock, including but not limited to the Purpose of Data Collection that is stated in Section 2.

2. **INFORMATION COLLECTION, USE, AND RESPONSIBILITIES**

2.1. Purpose of Data Collection. Fareclock collects and processes personal data solely to provide, operate, and improve its services, and to comply with legal obligations. The data is used for the following purposes:

- Delivering time and attendance, scheduling, payroll, and HR software services
- Verifying employee identity during clock-in or -out
- Managing user accounts and providing Customer support, service notifications, and updates
- Monitoring system performance, preventing fraud, and ensuring security
- Performing billing, invoicing, and other financial operations
- Ensuring compliance with applicable laws and regulations

We do not use personal data for purposes materially different from or incompatible with these without providing notice and, where required, obtaining consent.

2.2. Data Collected. Fareclock collects and processes identity and contact information (such as names, email addresses, employee identifiers, and login credentials); employment and workforce data (including roles, departments, work locations, shift schedules, time and attendance records, payroll-related data, and manager-employee hierarchy information); biometric data (if face recognition is enabled, encrypted facial photos are stored and accessible only by authorized administrators and are used solely for employee identity verification during clock-in); device, usage, and log data (including IP addresses, device details, application usage logs, and support communications); geolocation data (recorded only when a user clocks in or out via the Fareclock mobile app, if the live location tracking feature is enabled it will record for the entire shift

between the time a worker clocks in and clocks out, stored securely, and accessible only by authorized organization administrators); and Customer administrative data (such as billing information, subscription records, and communications with Customer administrators), strictly for the purpose of delivering and supporting the Fareclock service.

2.3. Account Setup and Management. Administrators are responsible for adding and removing their own users, assigning roles and permissions, and defining login requirements, including multi-factor authentication (MFA), permitted email domains, and supported login providers (e.g., Google). Each user is responsible for managing their own password, which must meet strong password requirements, and for enabling MFA. Customers do not contact Fareclock to create or manage administrator accounts.

3. DISCLOSURE OF PERSONAL DATA TO SUBPROCESSORS OR THIRD PARTIES

3.1. Subprocessors. Customer acknowledges and agrees that Fareclock may engage third-party subprocessors to assist with service delivery, including SMS/voice/email communication (i.e. Twilio), customer support, cloud hosting, data security and monitoring, analytics, and billing or payments (i.e. Stripe). These providers may have access to certain personal data, such as names and email addresses, but this information is never further shared outside their service scope.

Fareclock maintains a list of its current subprocessors ("Subprocessor List"), including the name and purpose of each subprocessor, which is available on the Fareclock Subprocessor page.

3.2. Subprocessor Updates and Notice. Fareclock may update its Subprocessor List from time to time. Fareclock will provide Customers with a notice of any new subprocessor(s) or replacement subprocessor(s) prior to authorizing such subprocessors to process Personal Data. Notice may be provided by updating the Subprocessor List page and/or by email or in-product notification.

3.3. Customer Objection Rights. If a Customer reasonably objects to a new or replacement subprocessor on grounds relating to data protection, they will have thirty (30) days from the date of notice to object to the new or replacement subprocessor.

Customers may provide Fareclock with a written notice of objection within the timeframe,

including the grounds for the objection. Upon receiving a valid objection, Fareclock will use commercially reasonable efforts to address the objection. If Fareclock determines that it cannot reasonably accommodate the objection, Customer may, as its sole and exclusive remedy, cancel their affected Services upon written notice.

3.4. Fareclock will ensure that all subprocessors are bound by written terms that provide a level of data protection no less protective than this DPA. Fareclock remains responsible for its compliance with this DPA and for the performance of its subprocessors' obligations to the extent required under applicable Data Protection Laws.

4. CONFIDENTIALITY

Fareclock agrees to keep in strict confidence and not to disclose to any party any and all information relating to the businesses, operations, financial transactions, procedures or other practices of the Customer and those of its customers, its subsidiaries, affiliates, directors, officers or employees, which we or any of our personnel may acquire, except those which are generally known or available to the public.

5. DATA SECURITY AND STORAGE

Fareclock operates on the Google Cloud Platform, which provides a secure-by-design infrastructure and adheres to industry-leading compliance standards, including ISO/IEC, SOC, PCI DSS, FedRAMP, GDPR, and HIPAA.

All customer data is encrypted in transit and at rest, with access restricted to authorized personnel only. Data is continuously replicated across a minimum of three data centers to ensure availability and resilience.

Google Cloud's enterprise privacy commitments and transparency measures further protect customer data and support compliance with applicable data protection regulations.

6. SECURITY MEASURES

Fareclock implements reasonable and appropriate administrative, technical, and physical safeguards to protect personal data against loss, misuse, unauthorized access, disclosure, alteration, or destruction. Measures include:

Role-Based Access Control (RBAC). Granular permission levels for super administrators, administrators, managers, supervisors, and employees. Users only access information relevant to their role, reducing unauthorized exposure.

Multi-Factor Authentication (MFA) & Admin Security. Two-step verification for admins. Supports configurable password requirements and authentication settings.

Biometric Verification. Face recognition with liveliness and anti-fraud safeguards to prevent impersonation or "buddy punching." Advanced detection for spoofing attempts (e.g., photos, videos). Face reference models retained for up to one year, with options for manual deletion.

GPS & Geolocation Controls. Location captured only at clock-in/out (when enabled). No continuous background location tracking, unless enabled. Employers can enforce location availability and block fake or disabled location services.

Audit Logs & Activity Monitoring. Comprehensive logs of access events, administrative updates, and suspicious activity. Supports reports for audits, login attempts, and system changes.

Device Security. Optional device binding to prevent unauthorized device use. Protections against rooted devices, tampering, and airplane mode misuse.

Fraud & Abuse Prevention. Detection of fake locations or timestamps. Alerts for mismatched facial verification and unusual device or login activity. Security notifications sent for account changes or suspicious events.

7. PERSONAL DATA BREACH NOTIFICATION

If Fareclock confirms that a personal data breach has occurred and is likely to result in a risk to user privacy or security, then it is our responsibility to promptly notify the affected Customer after confirming that a personal data breach has occurred.

8. DATA INTEGRITY, RETENTION, AND DELETION

We limit the collection and processing of personal data only to what is relevant for its intended purpose. We take reasonable steps to ensure that personal data is accurate, complete, and current.

Cancellation or closure of account will be effective at the end of your current billing cycle (month or year). The Customer may download all reports and data before the account is closed. After closure or when a contract or subscription ends, all associated data and content is permanently deleted after 30 days, unless otherwise required by law, and cannot be recovered. Customers may also permanently delete individual user data at any time. System backups are maintained for a fixed period and automatically purged thereafter.

Fareclock retains Customer billing history and account owner email registration data only for legal obligation and legitimate business purposes.

9. DATA SUBJECT RIGHTS

Individuals whose personal data we process have the following rights:

Right to Confirmation. Request confirmation if Fareclock holds their personal data.

Right of Access. Request access to their personal data.

Right to Rectification. Request correction of inaccurate or incomplete personal data.

Right to Erasure. Request deletion of personal data, subject to legal or contractual retention obligations.

Right to Object. Object to the processing of personal data for certain purposes, such as marketing communications, where applicable.

Right to Data Portability. Request a copy of personal data in a structured, commonly used, and machine-readable format, where feasible.

If a user's personal identifiable information (such as zip code, phone, email, or postal address) changes, or if a user is no longer affiliated with the Customer, the Customer may request to correct, update, delete, or deactivate the user's information by submitting a request to the contact information below.

10. DATA TRANSFER MECHANISM

EU-U.S. Data Privacy Framework. Fareclock LLC. represents and warrants that it is self-certified under the EU-U.S. Data Privacy Framework (EU-U.S. DPF), as administered by the U.S. Department of Commerce, and maintains ongoing compliance with the General Data Protection Regulation (GDPR).

Fareclock shall maintain its certification and comply with the DPF Principles for as long as it handles Personal Data protected by such frameworks. In the event that Fareclock determines it can no longer meet its obligation to provide the same level of protection as is required by the DPF Principles, it shall notify the Customer immediately and take reasonable and appropriate steps to stop and remediate unauthorized processing.

11. REGULAR PENETRATION TESTING AND SECURITY AUDITS

Fareclock engages with external security specialists to conduct regular penetration tests and security audits of the system. These assessments enforce continued security of the application by identifying vulnerabilities and ensure remediation measures are implemented on an ongoing basis.

12. TERM, TERMINATION, AND SURVIVAL

This Data Processing Addendum (DPA) remains in effect for the duration of the underlying Service between the parties. Upon termination or expiration of the Services, all obligations regarding the confidentiality, security, and proper deletion or return of personal data shall survive. These obligations continue to apply until all personal data has been securely deleted or returned in accordance with the terms of this DPA and applicable data protection laws.

13. REQUIRED DISCLOSURES

Fareclock may disclose personal data when required to comply with applicable laws or lawful requests from public authorities, including for national security or law enforcement purposes. Such disclosures will only be limited strictly to the personal data necessary to fulfill the legal obligation.

14. CHANGES TO THIS DPA

Fareclock may update this Data Processing Addendum from time to time to reflect changes in legal requirements, business practices, or services. Any updates will be properly communicated to its Customers.

15. CONTACT INFORMATION

If you have questions, concerns, or requests regarding this Data Processing Addendum (DPA) Addendum, please contact:

Fareclock, LLC.
privacy@fareclock.com

If you would like to sign and execute a copy of this DPA, you may do so by downloading this DPA, signing it, and returning it to Fareclock at privacy@fareclock.com. We will countersign and send back to you a copy for your records.

CUSTOMER ACCOUNT: _____

Name of signatory: _____

Work email address: _____

Designation/ Title: _____

Date: _____