

FONPAI Driver Application Privacy Policy (Revised)

Last Updated: September 01, 2026 Effective: August 21, 2026

This Privacy Policy (hereinafter referred to as "this Policy") applies to the SoFast Driver application (Package Name: com.sftc.mtms.sea, hereinafter referred to as "SoFast Driver" or "this App"), which is developed by Beijing Shunda Peer Technology Co., Ltd. (北京顺达同行科技有限公司, Address: 14F, Tower A, Building 1, No. 10 Xueqing Road, Haidian District, Beijing, 100083, China) and operated by PT FONPAI LOGISTICS INDONESIA (a limited liability company established under the laws of Indonesia, hereinafter referred to as "we" or "FONPAI"). This App is published on Google Play under the developer account of Beijing Shunda Peer Technology Co., Ltd. We understand the importance of personal information to you and are committed to protecting the security and privacy of your personal data in accordance with Law No. 27 of 2022 of the Republic of Indonesia concerning Personal Data Protection (UU PDP) and its implementing regulations.

Important Notice: PT FONPAI LOGISTICS INDONESIA is a subsidiary controlled by SF Holding Co., Ltd. and forms part of SF Group. To provide continuous and stable services and support the unified operations of SF Group, your personal information will be stored centrally on servers in Singapore; Singapore is a data storage location outside Indonesia, and the transfer of data from Indonesia to Singapore constitutes a cross-border data transfer. Please read Section 7 of this Policy and confirm that you acknowledge and agree.

1. Our Basic Rules for Processing Your Personal Information

Important definitions in this Policy are based on the relevant definitions in Law No. 27 of 2022 of the Republic of Indonesia concerning Personal Data Protection (UU PDP).

Personal Information and Specific Personal Data: Personal Information: any information relating to an identified or identifiable natural person. Specific Personal Data: data that may pose greater risks to the data subject in the event of a breach, including biometric information, health data, personal financial information, criminal records, etc. In this Policy, **Specific Personal Data will be presented in bold.**

2. How We Collect and Use Your Personal Information

We will collect and process your personal information in accordance with the principles of lawfulness, fairness, and necessity to provide relevant products and services. As products and services are iterated, expanded, and improved, the types of personal information we collect and use may change; if so, we will explain in detail through updates to this Policy and through in-product pop-ups or pages, and will seek your consent. The categories of personal information to be collected and processed for different purposes are as follows:

Table 1 Collection and Use of Information

(1) Account Registration — Basic Profile

Purpose: Register account

Legal Basis: Necessary for contract

Personal Info: Personal phone number

Specific Data: Phone number

(2) Complete Info — Identity/Basic Profile

Purpose: Complete account info

Legal Basis: Consent given

Personal Info: Name, address, bank account

Specific Data: KTP info, driver's license, vehicle registration, insurance policy, bank account

(3) Identity Verification — Biometric

Purpose: Facial recognition verification

Legal Basis: Written/explicit consent

Personal Info: —

Specific Data: Facial feature recognition info

(4) Message Notification — Device Info

Purpose: Service message push

Legal Basis: Necessary for contract

Personal Info: Device identifiers (Android ID, IMEI, IMSI, ICCID, MAC address, SIM serial, device serial, installed apps, IDFA, IDFA)

(5) Identification Analysis — Identity/Basic Profile

Purpose: Identification analysis

Legal Basis: Consent given

Personal Info: Name, phone, address, operation logs, device ID, model, OS version, installed apps, carrier, device name

Specific Data: KTP info, driver's license, vehicle registration, lat/lon coordinates

(6) Anomaly Report / Feedback — Basic Profile

Purpose: Issue feedback

Legal Basis: Necessary for contract

Personal Info: Name, address, personal phone

Specific Data: Phone number, lat/lon coordinates

Note: The "Specific Data" column is filled only when Specific Personal Data (e.g. biometric information) is involved; device identifiers (Android ID, IMEI, IMSI, ICCID, etc.) are not classified as Specific Personal Data in this Policy.

Table 2 Device Permission Information

(1) Geolocation

Scenario, Purpose & Reason: Enter app or use navigation; background location for driver tracking and delivery monitoring.

Personal Info Item: Location Info

(2) Camera

Scenario, Purpose & Reason: Facial recognition.

Personal Info Item: Biometric Data

(3) Album/Gallery

Scenario, Purpose & Reason: Upload vehicle / vehicle-document / identity-document info.

Personal Info Item: Identity Info

(4) Bluetooth

Scenario, Purpose & Reason: Geofencing and location tracking.

Personal Info Item: Location Info

(5) Auto-Start

Scenario, Purpose & Reason: Facilitate timely message delivery in background.

Personal Info Item: Message Notification

(6) Storage Permission

Scenario, Purpose & Reason: Save camera capture results.

Personal Info Item: Image Info

(7) Clipboard

Scenario, Purpose & Reason: Copy Task ID for issue feedback.

Personal Info Item: Text Info

(8) Phone Status & ID

Scenario, Purpose & Reason: User behavior tracking data analysis.

Personal Info Item: Device Info

3. Storage of Personal Information

We will store your Personal Information within Indonesia and for the period necessary to fulfill the purposes described in this Policy, in accordance with UU PDP and applicable laws.

Storage Location: To provide continuous and stable services and support the unified operations of SF Group, your Personal Information will be stored centrally on servers in Singapore, and Singapore is the primary data storage location.

Retention Period: We retain Personal Information only for the shortest period necessary to fulfill the purposes described in this Policy. Account and identity information is retained for the life of the account and deleted after a statutory period following account deactivation; biometric information is retained for a statutory period after verification and then deleted or anonymized; logs and device information are retained for 12 (twelve) months. Where laws or regulatory requirements provide otherwise, such provisions shall prevail.

Security Safeguards: We implement reasonable technical and managerial measures to protect the security of Personal Information and prevent unauthorized access, disclosure, alteration, or destruction. In the event of a security incident such as a personal information breach, we will promptly notify you and the relevant regulatory authority in accordance with the law.

4. Your Rights

You are entitled to the data subject rights provided under UU PDP, including the right to access, correct, and delete Personal Information, withdraw consent, deactivate your account, and file a complaint regarding data processing.

You may exercise the above rights through the contact details set out in Section 9 of this Policy.

Response Timeframe: We will respond to your request within 3 x 24 hours (72 hours) of receipt.

Withdrawal of Consent: You may withdraw your consent through the application settings or by contacting us; such withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

Account Deactivation: You may apply to deactivate your account via “Me – Account Settings – Deactivate Account”.

5. Children’s Personal Information

Our products and services are primarily intended for adults. If you are a child under 17 (seventeen) years of age, please use our services under the guidance of and with the consent of a parent or guardian. We will not knowingly collect personal information from children under 17 without parental/guardian consent.

6. Protection of Personal Information

We have established an information security management system and implement technical measures such as encryption, access control, and security auditing to protect Personal Information, and provide regular security training to employees and partners.

7. Data Storage Location and Cross-Border Data Transfer

Data Storage Location — Singapore: To provide continuous and stable services and support the unified operations of SF Group, your Personal Information will be stored centrally on servers in Singapore, and Singapore is the primary data storage location.

Cross-Border Data Transfer: By using this Application, you understand and agree that your personal information will be transferred from Indonesia to Singapore for storage and processing, which constitutes a cross-border data transfer. Upon arrival in Singapore, **no further transfer to any other jurisdiction will occur.** For necessary internal group operations (including SF Group), technical support, or data analysis, your personal information may be remotely accessed and processed from the Singapore server by SF Group affiliates or authorized service providers in the course of performing their duties; however, all such activities are conducted within Singapore and **do not involve any further cross-border transfer.** By using this Application, you understand and agree to the above data flow arrangement.

Safeguards: In accordance with UU PDP, we implement legally binding and adequate safeguards (such as Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC)) to ensure that Personal Information stored in Singapore receives a level of protection equivalent to that applicable in Indonesia.

8. Policy Updates

We may update this Policy from time to time. If an update involves material changes (e.g., significant changes to the purposes of processing, categories of Specific Personal Data, or third-party disclosures), we will notify you through in-app pop-ups and, where necessary, re-obtain your consent.

If no material changes are involved, the updated Policy will be published within the Application and take effect from the date of publication.

9. Contact Us

If you have any questions, comments, or requests regarding this Policy or the processing of Personal Information, please contact us via:

- **DPO Email**

dpo@fonpai.co.id; zhangjiajia@sf-express.com (group domain)

- **Company Address**

PT FONPAI LOGISTICS INDONESIA, Republic of Indonesia

- **Developer Address**

Beijing Shunda Peer Technology Co., Ltd.

14F, Tower A, Building 1, No. 10 Xueqing Road, Haidian District, Beijing, 100083, China (CN)

- **Data Storage Location**

Singapore (primary data storage location)

Note: The DPO email uses the @sf-express.com group domain because PT FONPAI is a subsidiary of SF Group (SF Holding Co., Ltd.), facilitating unified group-level data protection management.

This Policy is governed by the laws of Indonesia. Any dispute arising from this Policy shall be settled through friendly negotiation; if no settlement is reached, either party may file a lawsuit with a competent court in Jakarta, Indonesia.