

WHITE PLACARD MOBILITY PRIVATE LIMITED

PRIVACY POLICY

White Placard Mobility Private Limited (hereinafter referred to as “*We*”, “*Us*”, “*Our*”) owns and manages the website www.whiteplacardmobility.com and its other digital platforms and applications (“**Website**” and/or “**Apps**”). This Privacy Policy (“**privacy policy**”) explains how we may collect, use, store, disclose or otherwise process your personal data when using our websites or through any other means that we may employ to process your personal data. This policy also describes the rights you have with respect to your personal data.

We are committed to providing the highest level of protection regarding the processing of their employees, vendors’ and clients’/customers’ personal data based on applicable data protection laws and regulations. This privacy policy applies to all current and former users (collectively “**you**” or “**your**”) accessing or using our website or otherwise engaging with us through email or other means. By accessing or using our website or by otherwise giving us your information, you confirm that you have read and understood and agreed to the practices outlined in this privacy policy.

1. DEFINITIONS

- 1.1 **“Company”** means *white placard mobility private limited*, acting as a data fiduciary within the meaning of applicable data protection laws.
- 1.2 **“Platform”** means the digital ecosystem operated by the company, including mobile applications, websites, driver interfaces, dashboards, Api’s, telematics systems, and associated infrastructure through which services are provided.
- 1.3 **“Services”** means mobility, transportation, logistics, or allied services facilitated through the platform.
- 1.4 **“User”** means any individual or entity accessing or using the platform, including passengers, drivers, and visitors.
- 1.5 **“Driver”** includes independent contractor drivers, fleet drivers, and any individual operating a vehicle registered on the platform.
- 1.6 **“Device”** means any internet-enabled device used to access the platform, including mobile phones, tablets, or computers, and includes associated identifiers such as IP address, device ID, and operating system details.
- 1.7 **“Personal data”** means any data about an identifiable individual, including but not limited to name, contact details, identification numbers, location data, and online identifiers.

- 1.8 **“Sensitive personal data”** includes financial information, government identification numbers, biometric data, precise location data, and any other category notified under applicable law.
- 1.9 **“Processing”** means any operation performed on personal data, including collection, recording, organization, storage, adaptation, retrieval, use, disclosure, sharing, transfer, or deletion.
- 1.10 **“Data principal”** shall have the meaning assigned under the digital personal data protection act, 2023, and refers to the individual to whom the personal data relates.
- 1.11 **“Consent”** means a free, specific, informed, unconditional, and unambiguous indication of the data principal’s agreement to the processing of personal data.
- 1.12 **“Hybrid onboarding”** means a process involving digital submission of information and physical or in-office verification of documents.
- 1.13 **“Location data”** means real-time or historical geographical information collected via GPS, IP address, or other tracking technologies.
- 1.14 **“Breach”** means any unauthorized access, acquisition, disclosure, alteration, loss, or destruction of personal data compromising its confidentiality, integrity, or availability.

1.15 **“Third party”** means any entity other than the company or the data principal, including vendors, service providers, and partners, who process personal data either:
(a) on behalf of the company (data processors), or
(b) independently as separate data fiduciaries.

1.16 **“Account”** means a registered profile created by a user to access and use the platform.

2. INTRODUCTION

White Placard Mobility Private Limited (hereinafter referred to as the **“Company”**), acting in the capacity of a Data Fiduciary, operates a hybrid mobility service platform comprising company-managed vehicles as well as independent driver-partners.

This Privacy Policy (**“Policy”**) Sets out the manner in which personal data is collected, recorded, processed, stored, used, disclosed, transferred, and otherwise handled by the company in connection with its platform and services, in compliance with applicable laws, including the digital personal data protection act, 2023.

By accessing or using the platform, or by otherwise providing personal data to the company, the user (including passengers, drivers, and partners) expressly acknowledges, understands, and consents to the practices described herein. This policy shall constitute a legally binding agreement between the user and the company with respect to data protection and privacy.

3. INFORMATION COLLECTED

White Placard Mobility Private Limited (the “**Company**”) collects and processes personal data of users, including but not limited to identity particulars, contact information, real-time and historical location data, ride and transaction records, in-app and customer support communications, and payment-related information processed through razorpay or other authorized payment intermediaries.

In addition, the company collects and maintains driver-specific data, including driver verification and KYC documentation, driving license details, background verification records, vehicle registration and compliance documents, insurance particulars, and operational logs. The company may further collect safety-related data, including trip monitoring information, incident reports, emergency alerts, and behavioural analytics, for the purposes of user safety, fraud prevention, and regulatory compliance.

Such data may be collected directly from users, generated through use of the platform, or obtained from third-party verification agencies, payment processors, and service providers, and shall be processed strictly in accordance with applicable law and the terms of this policy.

4. MODE OF COLLECTION

- 4.1 Personal data is collected by the company through multiple touchpoints, including at the time of user registration, account creation, ride booking, and during driver onboarding processes, including hybrid onboarding involving both digital submission and physical verification.
- 4.2 The company further collects data through in-app interactions, including chat communications, feedback submissions, and customer support engagements, including call recordings for quality assurance, dispute resolution, and compliance purposes.
- 4.3 In addition, personal data is collected automatically through technological means, including continuous gps-based location tracking, device-level identifiers, and usage analytics during the course of use of the platform and services.
- 4.4 The company may also collect and process data through safety and surveillance mechanisms, including but not limited to SOS/emergency response systems, in-vehicle monitoring systems, and CCTV or video recording devices, whether currently deployed or implemented in the future, for purposes of ensuring user safety, fraud prevention, and operational integrity.

By accessing or using the platform, the user expressly consents to such collection, including continuous and automated data collection mechanisms, as may be reasonably required for the provision of services and compliance with applicable law.

5. PURPOSE OF PROCESSING

Personal data is processed by the company for legitimate business purposes connected with the provision, operation, and improvement of its platform and services, including but not limited to facilitating ride bookings, allocating drivers, enabling passenger-driver communication, managing trip execution, and maintaining customer support services.

Such processing further includes payment processing and reconciliation (through authorised intermediaries), fraud detection and prevention, risk assessment, safety monitoring, incident response, and enforcement of platform policies.

The company may also process personal data for internal analytics, service optimisation, research and development, quality control, and audit purposes, including the generation of aggregated or anonymised datasets.

In addition, personal data is processed to comply with applicable statutory, regulatory, and legal obligations, including disclosures to governmental authorities, law enforcement agencies, and judicial bodies as may be required.

Processing shall be undertaken on the basis of consent of the data principal, performance of contractual obligations, compliance with legal requirements, and such other lawful purposes as recognised under applicable law, including the digital personal data protection act, 2023.

6. LAWFUL BASIS OF PROCESSING

- 6.1 Processing of personal data by the company is undertaken on lawful grounds, including consent obtained from the data principal at the time of registration or use of the platform, and for the performance of contractual obligations necessary for the provision of transport and allied services.
- 6.2 Such processing is further carried out to comply with applicable legal and regulatory obligations, including disclosures mandated by law or competent authorities.
- 6.3 In addition, personal data may be processed for certain legitimate uses as recognised under applicable law, including but not limited to fraud detection and prevention, dispute resolution, enforcement of platform policies, network and information security, service optimisation, and ensuring operational safety.

6.4 Where permitted under law, certain processing activities may be undertaken on the basis of deemed consent, including where such processing is reasonably necessary for the provision of services, compliance with law, or in connection with public interest or emergency situations.

6.5 The data principal retains the right to withdraw consent; however, such withdrawal shall not affect the lawfulness of processing undertaken prior there to and may result in suspension or limitation of access to the platform and services.

7. RECIPIENTS OF DATA

7.1 Personal data may be shared by the company with authorised recipients strictly on a need-to-know basis and for purposes consistent with this policy, including:

- a) Internal personnel and authorised representatives of the company for operational, administrative, and support functions;
- b) Driver-partners and fleet operators, to the extent necessary for the provision and facilitation of services;
- c) Payment processing intermediaries, including razorpay, for transaction processing and reconciliation;

- d) Third-party service providers, including mapping and navigation service providers, cloud hosting vendors, communication service providers (including phone masking service providers, where deployed), analytics providers, and verification agencies;
- e) Insurance partners for underwriting, claims processing, and risk management purposes; and
- f) Governmental authorities, regulators, law enforcement agencies, or judicial bodies, where disclosure is required under applicable law or pursuant to lawful orders.

7.2 All such disclosures shall be made subject to appropriate contractual, technical, and organizational safeguards, as may be applicable.

Notwithstanding anything contained herein, the company shall not be liable for any misuse, unauthorised access, or processing of personal data by third parties, once such data has been shared in accordance with this policy and applicable law.

8. COMMUNICATION AND PHONE MASKING

8.1 The platform enables in-app chat communication and centralized ride support call systems between users, driver-partners, and the company.

- 8.2 To enhance user privacy, the company may deploy phone number masking or proxy communication systems, whereby actual contact details of users are not disclosed during ride-related interactions.
- 8.3 The company may record, store, and analyse communication logs, including chat transcripts and call recordings, for purposes including but not limited to dispute resolution, incident investigation, fraud detection, safety monitoring, service quality improvement, and compliance with applicable law.
- 8.4 By accessing or using the platform, users expressly consent to such monitoring and recording of communications. Such records may be relied upon by the company as evidence in the event of disputes, claims, or legal proceedings.
- 8.5 Users acknowledge that communications conducted through the platform or company-facilitated systems are subject to monitoring and, to the extent permitted by law, may not carry an absolute expectation of privacy.
- 8.6 All communication records shall be retained for such duration as may be necessary for the purposes stated herein or as required under applicable law.

9. SAFETY AND MONITORING

- 9.1 The company may deploy and utilise safety and monitoring technologies, including but not limited to gps-based location tracking, telematics systems, panic/SOS response mechanisms, CCTV or in-vehicle video recording systems (whether currently implemented or introduced in the future), and route monitoring technologies, for purposes including passenger and driver safety, incident detection and investigation, fraud prevention, and operational oversight.
- 9.2 Such systems may involve continuous, real-time or periodic monitoring and recording of location data, vehicle movement, and in-vehicle activities, to the extent permitted under applicable law.
- 9.3 By accessing or using the platform, or by participating in services as a user or driver-partner, individuals expressly consent to such monitoring and data collection, including recording through CCTV or similar surveillance technologies.
- 9.4 Data collected through such systems may be stored, analysed, and relied upon by the company as evidence in connection with disputes, claims, regulatory proceedings, or legal enforcement actions.

- 9.5 Users and driver-partners acknowledge that, in vehicles operating on the platform and equipped with such systems, there may be a limited expectation of privacy to the extent of such monitoring, subject always to applicable legal safeguards.

10. DATA RETENTION

- 10.1 Personal data shall be retained by the company only for such period as is necessary to fulfil the purposes for which it was collected, including operational requirements, contractual performance, dispute resolution, and compliance with applicable legal and regulatory obligations, as further detailed in *annexure-b* of this policy.
- 10.2 Retention periods may vary depending on the nature, sensitivity, and purpose of the data, as well as applicable statutory requirements and limitation periods for legal claims.
- 10.3 Notwithstanding the foregoing, the company may retain personal data for longer durations where such retention is necessary for the establishment, exercise, or defence of legal claims, prevention of fraud, enforcement of contractual rights, or compliance with lawful orders of authorities.

- 10.4 Upon expiry of the applicable retention period, personal data may be deleted, anonymized, or irreversibly de-identified, at the discretion of the company, unless continued retention is required under applicable law.
- 10.5 The company reserves the right to retain and use anonymized or aggregated data for analytical, statistical, and business purposes without restriction.

11. RIGHTS OF DATA PRINCIPALS

- 11.1 Subject to applicable law, the data principal may exercise certain rights in relation to their personal data, including the right to seek access to, correction or updating of inaccurate or incomplete data, erasure of personal data, and withdrawal of consent previously granted.
- 11.2 All such requests shall be submitted through designated channels of the company and shall be processed only upon satisfactory verification of the identity and authority of the requesting individual, in accordance with applicable regulatory timelines and procedures.

- 11.3 The company reserves the right to refuse, restrict, or defer such requests, in whole or in part, where retention or continued processing of personal data is necessary for compliance with applicable law, fulfilment of contractual obligations, prevention of fraud, protection of legal rights, or for the establishment, exercise, or defence of legal claims.
- 11.4 Withdrawal of consent shall not affect the lawfulness of processing undertaken prior to such withdrawal and may result in suspension, restriction, or termination of access to the platform or services to the extent such processing is essential for their provision.
- 11.5 Requests that are manifestly unfounded, excessive, or repetitive may be declined or subject to reasonable administrative conditions, as permitted under applicable law, including the digital personal data protection act, 2023.

12. SECURITY MEASURES

- 12.1 The company implements appropriate technical and organisational measures to safeguard personal data against unauthorised access, disclosure, alteration, loss, or destruction. Such measures include, but are not limited to, encryption of data in transit and at rest, secure storage systems, access control mechanisms based on role and necessity, network security protocols, periodic vulnerability assessments and audits, and documented incident response and recovery procedures.
- 12.2 The company endeavours to align its security practices with commercially reasonable industry standards and applicable legal requirements.
- 12.3 Notwithstanding the foregoing, no method of transmission over the internet or method of electronic storage is completely secure. Accordingly, the company does not guarantee absolute security of personal data and shall not be liable for any unauthorised access, loss, or misuse of data arising from factors beyond its reasonable control, including but not limited to acts of third parties, cyber-attacks, system failures, or force majeure events.

13. BUSINESS TRANSFER

- 13.1 In the event of any merger, acquisition, restructuring, amalgamation, assignment, or sale of all or substantially all of the company's assets or business, personal data may be transferred, assigned, or disclosed to the acquiring or successor entity as part of such transaction.
- 13.2 Any such transfer shall be subject to obligations of confidentiality and data protection standards no less stringent than those set out in this policy, and the successor entity shall be entitled to continue processing personal data in accordance with this policy and applicable law.
- 13.3 By using the platform or providing personal data, the user expressly consents to such transfer and continued processing by the successor entity.
- 13.4 The company shall not be liable for any acts or omissions of the successor entity occurring after the completion of such transaction, to the extent personal data has been transferred in compliance with this policy and applicable law.

14. THIRD-PARTY LINKS

- 14.1 The platform may contain links to, or enable access to, third-party websites, applications, or services that are not owned, operated, or controlled by the company.
- 14.2 The company does not exercise any control over, and is not responsible for the privacy of practices, data handling, content, or security of such third-party services. Any interaction, access, or transaction undertaken by the user with such third parties shall be at the user's own discretion and risk.
- 14.3 Users are advised to review the privacy policies and terms of use of such third-party services prior to providing any personal data or engaging with them.
- 14.4 The company shall not be liable for any loss, damage, unauthorised disclosure, or misuse of personal data arising out of or in connection with the user's interaction with any third-party services.

15. COOKIE POLICY REFERENCE

- 15.1 The platform uses cookies and similar tracking technologies, as further detailed in ***annexure-a*** of this policy, for purposes including maintaining session continuity, enabling core functionalities, enhancing user experience, analysing usage patterns, and improving overall service performance.
- 15.2 Such technologies may include first-party and third-party cookies, web beacons, pixels, sdks, and other tracking mechanisms that collect technical and usage-related information from the user's device.
- 15.3 By accessing or using the platform, the user consents to the use of such technologies in accordance with this policy. Where required under applicable law, such use shall be subject to appropriate consent mechanisms.
- 15.4 Users may control or disable cookies through their device or browser settings; however, such actions may impact the availability or functionality of certain features of the platform.
- 15.5 The company shall not be responsible for the use of cookies or similar technologies by third-party services integrated with or linked to the platform.

16. POLICY UPDATES

This policy may be revised, updated, or modified by the company from time to time to reflect changes in applicable law, regulatory requirements, business practices, or operational needs.

Any updated version of this policy shall be published on the platform or through other official communication channels of the company and shall become effective from the date of such publication, unless otherwise specified.

Continued access to or use of the platform after such updates shall constitute the user's deemed acceptance of the revised policy.

The company may, at its discretion, notify users of material changes; however, it shall not be under any obligation to provide prior or individual notice of such updates.

17. CONTACT INFORMATION

Grievance Officer: Grievance Department

Email: contact@whiteplacardmobility.com

Registered Office Address: 2nd floor, Flat No.: 2B, Sundram Enclave, Sarna Toli, Morabadi, Ranchi, Jharkhand 834008 India.