ZYGO

A Product of Adyanaavya Technology Services Private Limited

Privacy Policy

Effective Date: May 15, 2026 | Version 2.0

Applicable Law: DPDP Act 2023 | IT Act 2000 | IT (Intermediary Guidelines) Rules 2021 | SPDI Rules 2011

This Privacy Policy ("Policy") describes how Adyanaavya Technology Services Private Limited ("Company", "We", "Us", or "Our"), the owner and operator of the Zygo platform ("Platform"), collects, uses, processes, stores, shares, and protects the personal data of individuals ("Users", "You", or "Your") who access or use the Platform.

This Policy is incorporated by reference into the Zygo Terms and Conditions of Use and forms an integral part of the agreement between the Company and each User. By registering on or using the Platform, You consent to the practices described in this Policy.

This Policy applies to all Users of the Platform, including Riders and Commute Partners, and covers all personal data collected through the Platform's mobile application, website (gowithzygo.com), and associated services.

DATA MINIMISATION PRINCIPLE: The Company collects only such personal data as is reasonably necessary for the purposes described in this Policy. Users are not required to provide personal data beyond what is essential for the specific Platform feature or service they wish to access.

1. Applicable Legal Framework

This Policy is framed in compliance with the following legislation and rules, as amended from time to time:

- Digital Personal Data Protection Act, 2023 ("DPDP Act") — the primary legislation governing personal data processing in India, establishing obligations for Data Fiduciaries and rights for Data Principals.
- Information Technology Act, 2000 ("IT Act") — governing electronic records, digital transactions, cybersecurity offences, and intermediary liability.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") — governing the collection, use, storage, transfer, and disclosure of sensitive personal data or information.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Guidelines") — governing the obligations of intermediaries including grievance redressal, content moderation, and law enforcement cooperation.
- Information Technology (Amendment) Act, 2008 — provisions relating to data protection obligations of body corporates.

In this Policy, the Company acts as a Data Fiduciary within the meaning of the DPDP Act, as it determines the purpose and means of processing personal data collected through the Platform.

2. Key Definitions

For the purposes of this Policy, the following terms carry the meanings set out below:

- "Personal Data" means any data about an individual who is identifiable by or in relation to such data, as defined under the DPDP Act.
- "Sensitive Personal Data or Information (SPDI)" means personal data as specified under Rule 3 of the SPDI Rules, including passwords, financial information, health data, biometric data, and any other information collected, received, possessed, stored, dealt, or handled by the Company.
- "Data Fiduciary" means the Company, which determines the purpose and means of processing personal data.
- "Data Principal" means the User whose personal data is being processed.
- "Data Processor" means any person who processes personal data on behalf of the Company pursuant to a contract.
- "Consent" means a free, specific, informed, unconditional, and unambiguous indication of the Data Principal's agreement to processing of their personal data, given by a clear affirmative action.
- "Processing" means any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, transmission, or deletion.
- "Grievance Officer" means the officer designated by the Company to address User grievances under the IT Act, Intermediary Guidelines, and DPDP Act.

---

3. Categories of Personal Data Collected

The Company collects the following categories of personal data from Users, strictly for the purposes of operating and improving the Platform:

3.1 Identity and Contact Data

- Full legal name
- Mobile phone number
- Work email address
- Name and address of employer or organisation
- Profile photograph (optional)

3.2 Verification Data

- Driving Licence number and document image (Commute Partners only)
- Vehicle Registration Certificate (RC) number and document image (Commute Partners only)
- Company or institution identity verification details

3.3 Location and Commute Data

- Home area or residential locality (neighbourhood level only — precise home address is not collected)
- Office or workplace location
- Preferred commute route, timing, and corridor
- Real-time location data during active commutes — where the User has explicitly enabled this feature and only for the duration of the active commute session. Real-time location is shared only with matched Commute Group participants within

the same active session and is not stored beyond the commute session or used for any other purpose.

3.4 Platform Usage Data

- Commute history and group membership records
- Ratings and reviews submitted or received — visible to matched Commute Group participants and prospective group members for safety and trust purposes; historical ratings persist on the User's profile and are not automatically deleted upon group changes
- In-app communications and chat logs
- Device identifiers, operating system, and app version
- IP address and access timestamps
- Crash logs and diagnostic data

3.5 Financial Data

The Company does not collect, store, or process any payment card details, bank account information, or UPI credentials. All cost-share transactions occur directly between Users outside the Platform. Any future payment processing, if introduced, will be handled by a separately notified, PCI-DSS compliant third-party payment processor.

3.6 Sensitive Personal Data or Information (SPDI)

Verification documents (Driving Licence, Vehicle RC) are treated as Sensitive Personal Data under Rule 3 of the SPDI Rules. These are collected only with explicit consent, stored with enhanced security controls, accessed only by authorised trust and safety personnel, and retained only for as long as necessary for verification purposes.

3.7 What the Company Does NOT Collect

The Company expressly does not collect or process the following: (a) precise home address or GPS coordinates of a User's place of residence; (b) biometric data including fingerprints, facial geometry, iris scans, or voice prints; (c) financial account or payment instrument details; (d) health or medical data. The Company does not use facial recognition, biometric authentication, or automated biometric profiling technologies in connection with the Platform or the processing of verification documents.

3.8 User Responsibility for Voluntarily Shared Information

Users are responsible for ensuring that personal information they voluntarily share with other Users during in-Platform commute coordination — including through chat, profile descriptions, or direct communication — is appropriate, accurate, and lawful. The Company is not responsible for personal data that Users choose to disclose directly to other Users beyond the data shared through the Platform's structured profile and matching features.

---

4. Purpose and Legal Basis for Processing

The Company processes personal data only for specified, explicit, and legitimate purposes. The following table sets out each processing purpose and its legal basis:

4.1 Consent-Based Processing (Section 6, DPDP Act)

- User registration and account creation
- Professional identity and employment verification
- Commute Partner vehicle and licence verification
- Matching Users into Commute Groups based on route and timing
- Sending Platform notifications, updates, and service communications

- Real-time location sharing during commutes (where opted into)
- Collection and display of User ratings and reviews

4.2 Legitimate Use and Contractual Necessity

- Enforcing the Terms and Conditions of Use
- Investigating and responding to safety complaints and User reports
- Fraud detection, prevention, and account security
- Maintaining platform integrity and preventing misuse

4.3 Legal Obligation (Section 7, DPDP Act / IT Act 2000)

- Compliance with lawful orders from courts, law enforcement agencies, and regulatory authorities
- Retention of records as required under Applicable Law
- Responding to valid legal process including summons, warrants, and statutory notices

4.4 Legitimate Interest

- Improving Platform features, matching algorithms, and User experience based on anonymised usage analytics
- Conducting internal research and platform performance analysis
- Maintaining system logs for security and audit purposes
- Processing personal data where reasonably necessary to investigate safety incidents, fraud, harassment, abuse, or violations of Platform policies, including reviewing reported communications and commute records

The Company does not process personal data for purposes incompatible with those listed above without obtaining fresh consent from the Data Principal.

4.5 AUTOMATED SYSTEMS AND AI DISCLOSURE: The Platform may use automated systems, machine learning algorithms, and AI-assisted tools to improve commute matching accuracy, detect fraudulent or abusive account activity, monitor Platform safety, and analyse usage patterns for service improvement. Such systems process User data as described in this Policy. Where automated processing results in a significant decision affecting a User (such as account suspension or matching exclusion), Users have the right to request human review as described in Clause 8.6. The Company will update this Policy to reflect any material change in the nature or scope of automated processing as the Platform develops.

---

5. Consent — Collection, Withdrawal, and Management

5.1 COLLECTION OF CONSENT: Consent is obtained at the point of registration through a clear, affirmative action — specifically, the User's confirmation of registration after being presented with this Policy and the Terms and Conditions. Consent is not bundled with unrelated terms and is not a condition of any service where processing is not necessary for that service.

5.2 GRANULAR CONSENT: Where processing activities extend beyond the minimum required for platform operation (such as real-time location tracking during commutes, or optional profile enrichment), the Company seeks separate, specific consent at the point of enabling each such feature.

5.3 RIGHT TO WITHDRAW CONSENT: Data Principals may withdraw consent for any processing activity at any time by: (a) adjusting in-app privacy settings for optional features; or (b) submitting a written withdrawal request to privacy@gowithzygo.com. Withdrawal of consent shall not affect the lawfulness of processing carried out prior to withdrawal. Where consent withdrawal makes continued Platform use impossible (such as withdrawal of consent to identity verification), the Company reserves the right to suspend or terminate the User's account.

5.4 CONSENT FOR MINORS: The Platform is not intended for use by individuals below eighteen (18) years of age. The Company does not knowingly collect personal data of minors. If the Company becomes aware that a minor has registered on the Platform, the account shall be immediately suspended and associated data deleted.

---

6. Disclosure and Sharing of Personal Data

6.1 The Company does not sell, rent, trade, or otherwise transfer User personal data to third parties for commercial purposes.

6.2 Personal data may be shared in the following limited circumstances:

6.1 Within the Platform — Between Users

To facilitate Commute Group formation and coordination, the following limited profile information is visible to other matched Users within the same Commute Group: first name, employer name, commute corridor, profile photograph (if uploaded), and User rating. Verification document details are never shared with other Users.

6.2 With Data Processors

The Company engages trusted third-party service providers (Data Processors) who process data on the Company's behalf under written data processing agreements that impose confidentiality and security obligations at least equivalent to those under this Policy. Categories of processors currently engaged or likely to be engaged as the Platform scales include:

- Cloud infrastructure and hosting providers (such as Amazon Web Services or equivalent)
- Mobile analytics and crash reporting services (such as Firebase Crashlytics, Sentry, or equivalent)
- User behaviour and product analytics platforms (such as Mixpanel, Amplitude, or equivalent)
- Communication and notification services (such as Twilio, Firebase Cloud Messaging, or equivalent)
- Identity and document verification services

The Company will update this section to name specific processors as they are engaged. Users may request the current list of active Data Processors by contacting privacy@gowithzygo.com.

6.3 With Law Enforcement and Regulatory Authorities

The Company shall disclose personal data to law enforcement agencies, courts, regulatory bodies, and government authorities when required to do so by: (a) a valid court order or judicial process; (b) a statutory obligation under the IT Act, DPDP Act, or any other Applicable Law; (c) a direction from a competent government authority. The Company shall endeavour to notify the relevant User of such disclosure where permitted by law.

6.4 In Connection with Corporate Transactions

In the event of a merger, acquisition, restructuring, or sale of all or a substantial portion of the Company's assets, User personal data may be transferred to the acquirer, subject to equivalent data protection obligations. Users shall be notified of any such transfer in advance.

6.5 With Explicit User Consent

Personal data may be shared with any third party where the User has provided specific, informed, and prior consent to such sharing.

---

7. Data Storage, Security, Retention, and Cross-Border Transfers

7.1 STORAGE LOCATION: All personal data collected through the Platform is endeavoured to be stored on servers located within the territory of India, in compliance with applicable data localisation requirements under the DPDP Act and any sectoral regulations.

7.2 SECURITY MEASURES: The Company endeavours to implement industry-standard security practices and procedures that are reasonable and appropriate for a platform at its current stage of operation, as required under Rule 8 of the SPDI Rules and Section 8(4) of the DPDP Act. Security measures the Company aims to implement and maintain include, but are not limited to:

- Encryption of personal data in transit using industry-standard protocols (TLS 1.2 or above)
- Encryption of sensitive personal data at rest where technically feasible
- Role-based access controls limiting data access to authorised personnel on a need-to-know basis
- Security reviews and vulnerability assessments conducted periodically as the Platform scales
- Access controls for administrative systems handling personal data
- Secure deletion protocols for data no longer required to be retained
- Incident response procedures for detecting, reporting, and remedying personal data breaches

7.3 LIMITATION: No method of electronic transmission or storage is completely secure. The Company does not warrant or represent that its security measures are impenetrable or equivalent to enterprise-grade security frameworks. Users acknowledge this inherent limitation and use the Platform at their own risk in this regard.

7.4 DATA BREACH NOTIFICATION: In the event of a personal data breach that is likely to result in risk to the rights of Data Principals, the Company shall notify the Data Protection Board of India as required under the DPDP Act, and shall notify affected Users through registered contact details without undue delay.

7.5 CROSS-BORDER TRANSFERS: Where personal data is transferred outside the territory of India for processing by authorised third-party service providers or Data Processors — including cloud infrastructure or analytics services with servers in other jurisdictions — the Company shall ensure that such transfers are carried out in compliance with applicable provisions of the DPDP Act, applicable cross-border transfer regulations as notified by the Central Government, and appropriate contractual safeguards including data processing agreements imposing equivalent protection standards. The Company will update this Policy to reflect any material cross-border transfer arrangements as they are established.

7.6 RETENTION PERIODS: Personal data is retained only for as long as necessary for the purposes for which it was collected, or as required by Applicable Law. The following general retention periods apply:

- Active account data: retained for the duration of the User's account plus 12 months following account deletion
- Verification documents (DL, RC): retained for the duration of the Commute Partner's active status plus 6 months, or as required by law
- Commute history and group data: retained for 24 months from the date of each commute
- Safety complaint and incident records: retained for 5 years from the date of resolution, or as directed by law enforcement
- System logs and access records: retained for 180 days as required under the Intermediary Guidelines
- Legal hold data: retained for the duration of any ongoing legal proceeding or investigation

8. Rights of Data Principals

Under the DPDP Act and other Applicable Law, Users (as Data Principals) have the following rights with respect to their personal data. All requests should be submitted to privacy@gowithzygo.com and will be addressed within thirty (30) days of receipt, unless extended by law.

8.1 Right to Access and Information

Users have the right to: (a) obtain confirmation of whether the Company is processing their personal data; (b) receive a summary of the personal data being processed; and (c) receive information about the identity of all Data Processors and other persons with whom data has been shared.

8.2 Right to Correction and Erasure — Including Account Deletion

Users have the right to: (a) request correction of inaccurate or incomplete personal data at any time through in-app profile settings or by contacting privacy@gowithzygo.com; (b) request erasure of personal data where processing is no longer necessary, consent has been withdrawn, or processing was unlawful.

ACCOUNT DELETION PROCESS: Users may request permanent account deletion through the in-app settings menu under 'Account > Delete Account', or by submitting a written deletion request to privacy@gowithzygo.com with the subject line 'Account Deletion Request'. Upon receipt of a verified deletion request, the Company will: (i) deactivate the account within 48 hours; (ii) permanently delete personal data within 30 days, subject to retention obligations under Applicable Law; (iii) send a written confirmation to the User's registered email address upon completion of deletion. Certain data categories — including safety incident records, legal hold data, and system logs — may be retained beyond the deletion request for the periods specified in Clause 7.6, in compliance with Applicable Law.

8.3 Right to Grievance Redressal

Users have the right to have grievances regarding personal data processing addressed by the Company's Grievance Officer within the timeframes prescribed under the DPDP Act and Intermediary Guidelines. If unsatisfied with the Company's response, Users may escalate to the Data Protection Board of India upon its establishment.

8.4 Right to Nominate

Users may nominate another individual to exercise their data rights in the event of death or incapacity, as provided under the DPDP Act.

8.5 Right to Withdraw Consent

As described in Clause 5.3 above, Users may withdraw consent to specific processing activities at any time.

8.6 Right Against Automated Decision-Making

Where the Platform makes significant decisions about Users solely through automated means (such as commute matching or account suspension based on rating thresholds), Users have the right to request human review of such decisions by contacting support@gowithzygo.com.

---

9. Cookies, Device Data, and Tracking Technologies

9.1 The Platform's mobile application and website use cookies, device identifiers, and similar tracking technologies to: (a) maintain User session state and authentication; (b) remember User preferences and settings; (c) collect anonymised usage analytics to improve Platform performance; (d) detect and prevent fraudulent or abusive activity.

9.2 COOKIE CONSENT NOTICE: Users accessing the Platform via web browser (gowithzygo.com) will be presented with a cookie consent notice upon first visit. Essential cookies required for Platform functionality are enabled by default. Optional analytics and performance cookies are enabled only upon User consent through the cookie preference centre. Users may review and update their cookie preferences at any time through the website's privacy settings.

9.3 Users may also configure their browser or device settings to restrict or disable certain tracking technologies. Disabling essential cookies may impair the functionality of the Platform.

9.4 The Company does not use tracking technologies for behavioural advertising, cross-site tracking, or selling User activity data to third-party advertisers.

9.5 Third-party analytics and crash reporting providers engaged by the Company may collect anonymised diagnostic data in accordance with their own privacy policies. The Company ensures that such providers operate under appropriate contractual data protection obligations. The current list of third-party technology providers is set out in Clause 6.2 above and will be updated as providers change.

---

10. Children's Privacy

10.1 The Platform is strictly intended for use by individuals aged eighteen (18) years and above. The Company does not knowingly collect, process, or store personal data of individuals below this age.

10.2 If a parent or guardian becomes aware that a minor has registered on the Platform or submitted personal data without appropriate consent, they should immediately contact privacy@gowithzygo.com. Upon verification, the Company will promptly delete the minor's data and suspend the associated account.

10.3 The Company does not process any data of children as defined under the DPDP Act without verifiable parental consent, and does not undertake behavioural tracking of children under any circumstances.

---

11. Intermediary Obligations and Compliance

11.1 The Company operates as an intermediary within the meaning of Section 2(1)(w) of the IT Act and complies with the due diligence obligations prescribed under the Intermediary Guidelines, including:

- Publishing this Privacy Policy and the Terms and Conditions of Use in a clear and accessible manner on the Platform
- Appointing a Grievance Officer resident in India, whose contact details are published below
- Acknowledging grievances within twenty-four (24) hours and resolving them within fifteen (15) days of receipt
- Maintaining system logs for a period of one hundred and eighty (180) days
- Cooperating with law enforcement agencies and government authorities in accordance with lawful orders
- Implementing reasonable security practices to protect User data

11.2 The Company shall update this Policy and associated compliance measures as required to reflect amendments to the Intermediary Guidelines, the DPDP Act, or any other Applicable Law.

---

12. Third-Party Links and Services

12.1 The Platform may contain links to third-party websites, services, or content that are not owned or controlled by the Company. This Policy does not apply to any third-party platforms, and the Company is not responsible for the privacy practices of such third parties.

12.2 Users are encouraged to review the privacy policies of any third-party services they access through or in connection with the Platform.

---

13. Changes to This Privacy Policy

13.1 The Company reserves the right to update or modify this Policy at any time to reflect changes in legal requirements, Platform features, or data processing practices.

13.2 Material changes to this Policy will be communicated to Users via registered email or prominent in-app notification at least fourteen (14) days prior to the effective date of such changes.

13.3 The current version and effective date of this Policy are displayed at the top of this document. Continued use of the Platform following the effective date of any amendment constitutes acceptance of the revised Policy.

13.4 The version history of this Policy shall be maintained and made available to Users upon request.

---

14. Grievance Officer and Contact Details

In accordance with the IT Act, the Intermediary Guidelines, and the DPDP Act, the Company has designated a Grievance Officer to address User concerns regarding data privacy and personal data processing. Users may contact the Grievance Officer for:

- Requests to access, correct, or delete personal data

- Withdrawal of consent for specific processing activities
- Complaints regarding unauthorised use or disclosure of personal data
- Any other grievance relating to the processing of personal data by the Company

Grievance Officer

Adyanaavya Technology Services Private Limited

(Owners and Operators of the Zygo Platform)

Email: info@gowithzygo.com

Legal: info@gowithzygo.com

Support: info@gowithzygo.com

Phone: +91 90085 18250

Address: Bengaluru, Karnataka, India

Response Timeline: Grievances will be acknowledged within twenty-four (24) hours and resolved within thirty (30) days of receipt, or within such shorter period as may be prescribed under Applicable Law.

Data Protection Board: Upon the operationalisation of the Data Protection Board of India under the DPDP Act, Users who are unsatisfied with the Company's response to a grievance shall have the right to escalate the matter to the Board.

This Privacy Policy is published in compliance with the requirements of the Information Technology Act, 2000; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; and the Digital Personal Data Protection Act, 2023.

Last Updated: May 15, 2026 | Version 2.0 |