Temico Motor India – Privacy Notice

Effective Date: December 2025

1. Introduction

Temico Motor India ("Temico," "we," "our," or "us") is committed to protecting the privacy and personal data of our customers, employees, vendors, suppliers, and other stakeholders. This Privacy Notice explains how we collect, use, store, share, and protect personal data in compliance with the Digital Personal Data Protection Act, 2023 (DPDPA) and its Rules. We respect your privacy and aim to ensure transparency in how your personal data is processed.

2. Scope

This Privacy Notice applies to:

- All personal data collected by Temico Motor India, whether online, offline, or via connected vehicles.
- All individuals whose personal data we process, including customers, employees, vendors, suppliers, and other third parties.
- All processing activities conducted by Temico and third-party service providers on our behalf.

3. Data We Collect

A. Customers / Vehicle Users:

- Identifiers: Name, contact details, email, phone number, address
- Identification Documents: Aadhaar, PAN, driving license
- Payment Information: Card details, bank account for transactions
- Purchase and service history, warranty details
- Marketing & Communication Preferences

B. Employees:

- Identifiers: Name, contact details, photograph
- Employment-related data: PAN, Aadhaar, bank account, payroll, leave records, performance reviews
- Health & Medical Data: Health insurance, medical records, emergency contacts
- Background checks and references

C. Vendors / Suppliers:

- Company details, primary contacts
- Contractual information, tax and compliance documents
- Banking and payment information
- Vendor performance and history

D. Website and Digital Services:

- IP addresses, device information, browser type
- Cookies, analytics, usage data
- Communication history with support or marketing channels

4. Legal Basis for Processing

We process personal data based on the following lawful grounds under DPDPA:

- Consent of the data principal
- Performance of a contract or pre-contractual obligations
- Compliance with statutory/legal obligations
- Protection of legitimate interests of Temico or its stakeholders
- Any other lawful basis as required under DPDPA

5. How We Use Personal Data

We may use personal data for the following purposes:

- Vehicle sales, servicing, maintenance, and warranty support
- Employee administration, payroll, benefits, and HR management
- Vendor and supplier management, contract performance, and payments
- Marketing, promotions, and customer engagement (with consent)
- Compliance with legal and regulatory obligations
- Product development, analytics, and improving connected vehicle services
- Fraud detection, risk assessment, and security management
- Responding to inquiries, complaints, or legal requests

6. Data Sharing and Disclosure

We may share personal data with:

- **Third-party service providers**: For IT services, cloud hosting, analytics, marketing, payment processing, and connected vehicle services, under data processing agreements ensuring DPDPA compliance.
- **Regulatory authorities / law enforcement**: When required by law or in response to lawful requests.
- **Affiliates or partners**: For joint services or operations, with strict data protection measures.
- **Auditors or consultants**: For audit, compliance, or risk assessment purposes.

We do **not sell personal data** to third parties.

7. Data Retention

Personal data is retained only as long as necessary for the purposes it was collected or as required by law. Retention periods may include:

- **Customer data:** Up to 5 years post relationship unless consent or law requires longer retention
- **Employee data:** Up to 7 years post-employment (statutory compliance)
- **Vendor / supplier data:** 7 years after contract completion
- **Connected vehicle data:** Processed for service improvement, warranty, and analytics purposes; anonymized when possible

Data no longer required will be securely deleted or anonymized.

8. Data Security

We implement robust technical and organizational measures to protect personal data:

- Encryption in transit and at rest
- Secure servers and firewalls
- Access control and role-based permissions
- Regular security audits and vulnerability assessments
- Employee training and confidentiality agreements

Connected vehicle data is processed with additional security controls, including secure telematics protocols, monitoring, and anonymization where feasible.

9. Cross-Border Data Transfers

- Personal data may be transferred outside India with adequate protection or standard contractual safeguards.
- Data principals will be informed of transfers, purpose, and measures taken to protect data.
- Transfers are conducted in compliance with DPDPA Rules.

10. Third-Party Processing

- Vendors or service providers processing personal data on our behalf must enter Data Processing Agreements (DPAs).
- Vendors are required to implement appropriate security measures and comply with DPDPA.
- Periodic audits and assessments ensure vendor compliance.

11. Data Subject Rights

Data principals have the following rights:

1. Right to confirmation and access of personal data
2. Right to correction of inaccurate data
3. Right to erasure/blocking of unlawful or unnecessary data

4. Right to withdraw consent at any time
5. Right to data portability, where applicable
6. Right to object to processing for certain purposes
7. Right to grievance redressal

Exercise of Rights:

Requests can be submitted via (Customer-care@temico.co.in). Temico will respond within the timelines prescribed under DPDPA.

12. Cookies and Tracking Technologies

Our websites and apps may use cookies and similar technologies to:

- Improve user experience
- Track analytics and site performance
- Personalize content and offers

Users can manage cookie preferences through their browser settings.

13. Data Breach Management

- Breaches must be reported immediately to the Data Protection Officer (DPO).
- Breaches are classified based on risk (High, Medium, Low).
- High-risk breaches are notified to the Data Protection Authority and affected individuals per DPDPA timelines.
- A detailed response plan includes containment, investigation, mitigation, and preventive actions.

14. Data Protection Impact Assessment (DPIA)

- DPIAs are conducted for high-risk processing activities, such as connected vehicle analytics, marketing profiling, or cross-border data transfers.
- Includes risk identification, mitigation measures, and DPO approval before processing.

15. Accountability & Compliance

- Temico maintains records of all processing activities.
- Regular internal audits and compliance checks are conducted.
- Non-compliance is escalated to Senior Management.

16. Employee & Vendor Awareness

- All employees handling personal data undergo mandatory training.
- Vendors are informed of their obligations under DPDP and contractual agreements.

- Awareness campaigns are conducted for new processes, regulations, and connected vehicle services.

17. Automated Decision-Making and Profiling

- Temico may use automated systems for vehicle diagnostics, predictive maintenance, or marketing analytics.
- Data principals will be informed if such processing produces legal or significant effects.
- Individuals have the right to request human intervention and to contest automated decisions where applicable.

18. Anonymization and Pseudonymization

- Where feasible, personal data is anonymized or pseudonymized for analytics, R&D, or connected vehicle data purposes.
- Anonymized data is not treated as personal data under DPDPA.

19. Data Transfer within Group Companies

- Personal data may be shared within Temico Motor India group companies for operational purposes.
- Such transfers comply with DPDPA requirements and are subject to internal data-sharing agreements.

20. Mobile Applications and Connected Vehicle Services

- Mobile apps and connected vehicle systems collect data only for functional purposes (e.g., navigation, performance monitoring, safety alerts).
- Users are informed of data collection via app privacy notices and consent mechanisms.
- Third-party app stores and service providers are bound by contractual DPDP-compliant agreements.

21. Marketing and Communications

- Marketing communications are sent only with the consent of the data principal.
- Data principals can opt-out or unsubscribe at any time.
- Preferences are respected across all channels (SMS, email, push notifications).

22. Children and Minors

- We do not knowingly collect personal data from individuals under 18 years of age.
- Parental consent is required where child data is processed.

23. Employee Monitoring and Compliance

- Employee data may be monitored for lawful purposes such as IT security, productivity, and compliance with company policies.
- Monitoring is proportionate, transparent, and limited to necessary data.

24. Third-party Integrations and APIs

- Third-party APIs integrated into our services are reviewed for privacy compliance.
- Personal data shared via APIs is minimized, encrypted, and logged for accountability.

25. Data Quality Management

- Data collected must be accurate, complete, and updated periodically.
- Processes are in place to correct or update inaccurate personal data on request.

26. Data Subject Consent Management

- Consent is obtained through clear and unambiguous mechanisms.
- A central repository maintains all consents and withdrawals for accountability.
- Consent renewal occurs periodically, especially for sensitive data.

27. Physical Security of Data

- Physical access to offices, servers, and storage rooms is restricted.
- Access logs are maintained, and security measures (guards, CCTV) are in place.

28. Incident Reporting and Whistleblowing

- Employees and vendors are encouraged to report privacy incidents via secure channels.
- Whistleblower protection policies apply to privacy-related reports.

29. Vendor and Third-party Risk Assessment

- Vendors are assessed for privacy and security risks before engagement.
- Risk assessments are updated annually or when processing scope changes.

30. International Data Transfer Impact Assessment

- Cross-border data transfers require a detailed assessment of legal, technical, and operational risks.
- Transfers are blocked if adequate safeguards cannot be implemented.

31. Retention Schedule Review

- Retention schedules are reviewed annually to ensure compliance with statutory and operational requirements.
- Automatic archival and deletion systems are implemented where feasible.

32. Privacy by Design and Default

- All new systems, processes, or products are assessed for privacy impact before deployment.
- Minimum personal data is collected by default, and security measures are integrated into system design.

33. Audit Trails and Logging

- Processing activities are logged to ensure accountability and traceability.
- Audit logs are retained securely and reviewed periodically for anomalies.

34. Grievance Redressal Mechanism

- Temico maintains a dedicated grievance redressal process.
- Complaints are acknowledged within 3 business days and resolved within DPDPA-prescribed timelines.
- Data principals may escalate unresolved complaints to the DPO or Senior Management.

35. Compliance with Other Laws

- Processing complies with applicable Indian laws, including the IT Act, Motor Vehicles Act, labor laws, and financial regulations.
- Any conflict between laws is reviewed by the Legal Department to ensure minimum compliance obligations are met.

36. Updates and Communication

- Any material changes to the Privacy Policy are communicated to data principals via email, website notifications, or app notifications.
- Minor operational updates may be applied without separate notice if they do not affect data principal rights.

40. Contact Information
Email: [Customer-care@temico.co.in]