

Privacy Policy

Drivn Transition Private Limited

Privacy Policy

1. Introduction & Purpose

Drivn Transition Private Limited ("**Drivn**", "**we**", "**our**", or "**us**") is committed to protecting the privacy and security of personal data of all individuals who interact with us, including customers, employees, contractors, vendors, and website visitors (collectively, "**Data Principals**").

This Privacy Policy ("Policy") explains how Drivn, acting as a Data Fiduciary under the Digital Personal Data Protection Act, 2023 ("DPDP Act"), collects, uses, stores, shares, and protects your personal data. It also describes your rights as a Data Principal and how you may exercise them.

This Policy is issued in compliance with the following legislation:

- **Information Technology Act, 2000** ("IT Act") and the rules framed thereunder;
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** ("SPDI Rules");
- **Digital Personal Data Protection Act, 2023** ("DPDP Act"); and
- **Digital Personal Data Protection Rules, 2025** ("DPDP Rules")

By accessing our website (www.drivn.co.in), using our services, or providing us with your personal data, you acknowledge that you have read and understood this Policy.

2. Key Definitions

Term	Definition
Data Principal	The individual to whom personal data relates. In the context of employment, the employee is the Data Principal in respect of their employment-related personal data.
Data Fiduciary	A person or entity that alone or in conjunction with others determines the purpose and means of processing personal data. Drivn Transition Private Limited is the Data Fiduciary for personal data collected through its website, services, and operations.
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary pursuant to a contract.
Personal Data	Any data about an individual who is identifiable by or in relation to such data. Includes name, identification number, email address, location data, and online identifiers.
Sensitive Personal Data or Information (SPDI)	Under SPDI Rules 2011: passwords; financial information (bank account, credit/debit card, payment instrument details); physical, physiological and mental health conditions; sexual orientation; medical records and history; biometric information. Such data will be treated with heightened protection under this Policy.

Processing	Any automated operation performed on personal data, including collection, recording, organisation, storage, adaptation, use, disclosure, transmission, erasure or destruction.
Consent	A free, specific, informed, unconditional and unambiguous expression of agreement by a Data Principal through a clear affirmative action to the processing of their personal data for a specified purpose.
Personal Data Breach	Any unauthorised processing, loss, destruction, alteration, disclosure or access to personal data that may adversely affect a Data Principal.
Purpose Limitation	The principle that personal data may only be collected for a specific, clear, and lawful purpose and must not be processed in a manner incompatible with that purpose.

3. Scope and Applicability

This Policy applies to:

- All individuals who access or use the Drivn website, platform, or services;
- Customers or prospective customers
- Employees, contractors, consultants, and other individuals whose personal data is processed by Drivn in the course of its business;
- Vendors, suppliers, and business partners of Drivn; and
- Any other individual whose personal data Drivn processes in connection with its operations.

Third-Party Websites: This Policy does not apply to third-party websites linked from our website or services. Drivn has no control over such websites and is not responsible for their privacy practices. We encourage Data Principals to review the privacy policies of any third-party websites they visit.

4. Categories of Personal Data Collected

Identity and KYC Information

- Government-issued identification numbers
- KYC documentation as required for regulatory and contractual compliance;

Financial Information (SPDI)

- Bank account details
- Income details, credit scores, and financial statements for leasing assessments;
- GST and tax-related information.

Employment and Professional Information (Employee Data)

- Employee identification number, employment terms, and compensation details;
- Performance records, attendance, and leave records;
- Emergency contact details and nominee information.

Technical and Usage Data

- IP address, device identifiers, browser type, and operating system;
- Log data, cookies, and session information when you visit our website;
- Usage patterns, pages visited, and interactions with our digital services.

Health Information (SPDI, where applicable)

- Health or medical information submitted in connection with employee welfare or insurance claims, processed only with explicit consent.

5. Purposes of Processing and Lawful Bases

Lawful Basis	Purpose	Categories of Data
Contractual Necessity	Providing EV leasing and financing services; executing and performing lease agreements; processing payments and invoices; KYC verification and credit assessment; delivery of contracted services.	Identification, KYC, financial information
Legal Obligation	Compliance with applicable laws including tax, anti-money laundering, and regulatory reporting obligations; responding to lawful requests from government authorities.	All categories as required by law
Employment	Processing employee personal data for HR administration, payroll, performance management, benefits, and emergency response.	Employee data, health information (with consent)
Safety & Security	Monitoring system access, detecting fraud and cybersecurity incidents, protecting the security of Drivn's systems, users, and assets.	Technical data, access logs
Research & Analytics	Aggregated, anonymised analysis of service usage to improve product offerings, operations, and user experience.	Anonymised technical and usage data

6. Notice to Data Principals

Drivn shall provide a clear, accessible, and standalone notice to Data Principals before or at the time of collecting personal data. Such notice shall:

1. Be written in plain language that is easy to understand;
2. Describe, in itemised form, the specific personal data that will be collected;
3. State the specific purpose for which each category of data is being collected and processed;
4. Provide a link or mechanism through which the Data Principal may: (a) withdraw consent at any time; (b) exercise their rights under the DPDP Act; or (c) raise a complaint or grievance; and
5. Be provided separately from any other information or terms and conditions.

Drivn shall not collect personal data that has not been specified in the notice, and shall not process personal data for a purpose other than that specified in the notice, without providing a fresh notice and obtaining fresh consent where required.

7. Consent

Where Drivn relies on consent as the lawful basis for processing personal data, such consent must be:

- Free – given voluntarily, without coercion or undue influence;
- Specific – given for a clearly defined purpose;
- Informed – given after the Data Principal has been provided a complete and clear notice;
- Unconditional – not bundled with acceptance of other terms as a condition of service (unless processing is necessary for the service); and
- Based on a clear affirmative action

A Data Principal has the right to withdraw consent at any time. The withdrawal of consent:

- Shall be as easy to effect as the giving of consent;
- May be communicated through the mechanisms described in the notice;
- Shall not affect the lawfulness of processing carried out prior to withdrawal; and
- May require Drivn to cease providing certain services that depend on the processing of such data.

Processing of SPDI (as defined under the SPDI Rules 2011) shall require explicit written consent of the Data Principal, which shall clearly describe the information being collected and the purpose of collection. Consent for SPDI shall not be presumed.

8. How We Collect Personal Data

Drivn collects personal data through the following mechanisms:

- **Directly from you:** When you register on our website, submit an enquiry, enter into commercial discussions or contractual arrangements, or contact us.
- **Through our digital platforms:** Drivn's website is built and hosted on Wix. When you visit www.drivn.co.in, Wix may place cookies on your device to support basic website functionality and to collect anonymous usage data such as page views and traffic patterns. Drivn does not operate any independent tracking or advertising cookies. For details on how Wix collects and uses cookies, please refer to the [Wix Privacy Policy](#).
- **From third parties:** Credit bureaus, KYC verification agencies, public registries, and financial institutions, where you have authorised such sharing or where Drivn is legally permitted to obtain such data.
- **From employers or fleet operators:** In respect of employees whose data is provided by their employer.

9. Storage and Disclosure of Data

Drivn keeps personal data in electronic records maintained on secure servers, which may include cloud-based infrastructure operated by third-party providers.

When we share your data

We may share personal data in the following circumstances:

Service providers and partners: We work with third parties who support our operations; including KYC verification platforms, credit bureaus, payment processors, cloud infrastructure providers, legal and accounting advisors, and fleet telematics providers. These parties receive only the data necessary for the service they provide and are bound by contractual obligations to protect it.

Vehicle and fleet operations: As part of our EV leasing service, we track vehicle location and usage data to ensure safety, manage the fleet, and assist in emergencies, theft, or accident recovery. This information may be shared with insurance companies, roadside assistance providers, law enforcement, or courts where required in connection with an incident, claim, or investigation.

Financial and regulatory bodies: We may share data with banks, NBFCs, the Reserve Bank of India, the Ministry of Corporate Affairs, income tax authorities, or other regulators where required by applicable law or as part of our regulatory reporting obligations.

Legal proceedings: We may disclose personal data to courts, tribunals, law enforcement agencies, or government authorities where legally required, or where necessary to establish, exercise, or defend legal rights.

Group companies and affiliates: We may share data within the Drivn group of companies for related operational purposes, to the extent permitted under applicable law.

Business transfers: In the event of a merger, acquisition, or restructuring, personal data may be transferred to the relevant acquiring or successor entity, subject to equivalent data protection obligations.

In all cases, we limit disclosure to what is strictly necessary for the purpose at hand.

Transfer of Personal Data Outside India

In some circumstances, the parties to whom we disclose personal information may operate outside India. Where this occurs, Drivn takes appropriate steps to ensure it remains protected, including through contractual obligations that require the recipient to maintain standards of security and confidentiality equivalent to those that apply under Indian law.

You should be aware that in some countries, local laws may require service providers to make personal data available to government or regulatory authorities. Where this is the case, we have no control over such disclosures, but we will always ensure the transfer itself was carried out responsibly and in compliance with applicable Indian data protection law.

10. Security Safeguards

Drivn implements reasonable technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, loss, or destruction. This includes anonymisation and masking

of sensitive financial and identity data, multi-factor authentication, role-based access controls, regular vulnerability assessments, and system activity logging. All employees and contractors with access to personal data are bound by confidentiality obligations and receive data protection training. Vendors who handle personal data on our behalf are required to hold appropriate certifications and meet security standards consistent with those we apply internally. We also carry out internal privacy assessments before deploying new systems that involve personal data processing.

No system of transmission or storage can guarantee absolute security. If a personal data breach occurs, we will act in accordance with the process described in Section 11.

11. Data Breach Notification

In the event of a personal data breach, Drivn will notify the Data Protection Board of India as required under applicable law, providing details of the nature of the breach, the data and individuals affected, and the steps taken to address it.

If the breach is likely to affect your rights or interests, we will notify you through your registered contact details without undue delay. That notification will describe what happened, what data was involved, what you should do to protect yourself, and who to contact at Drivn with questions.

12. Data Retention and Deletion

Drivn retains personal data only for as long as is necessary to fulfil the purpose for which it was collected, or as required under applicable law. Where retention periods are governed by a specific contract or statutory obligation, those terms apply. Once the relevant purpose has been served or the applicable period has expired, personal data is deleted or anonymised. Data will also be deleted earlier if you withdraw consent, exercise your right to erasure, or where there is no longer a lawful basis for continued processing. Where Drivn intends to delete your personal data, we will notify you in advance unless immediate deletion is required by law.

13. Rights of Data Principles

As a Data Principal, you have the following rights, which Drivn is committed to facilitating.

Right to access: You may request a summary of the personal data Drivn holds about you, the purposes for which it is being processed, and the parties with whom it has been shared.

Right to correction and erasure: You may ask Drivn to correct any inaccuracy or incompleteness in your personal data, or to erase data that is no longer necessary for the purpose for which it was collected, subject to any legal obligation to retain it. Drivn may verify your identity before acting on such a request.

Right to withdraw consent: Where processing is based on your consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

Right of nomination: You may nominate another individual to exercise your rights under this Policy in the event of your death or incapacity.

Right to grievance redressal: If you have a complaint about how Drivn has handled your personal data, you may raise it using the process set out in Section 14. If you are not satisfied with our response, you may escalate to the Data Protection Board of India.

14. Grievance Redressal

If you have a complaint or grievance in respect of how Drivn has processed your personal data, you may raise it by:

- **Email:** grievances@drivn.co.in

Drivn's grievance redressal process:

1. Your complaint will be acknowledged in writing within seven (7) business days of receipt;
2. Drivn will investigate the complaint and take remedial action as appropriate;
3. The complaint will be resolved within ninety (90) days of receipt, and
4. Drivn will communicate the outcome of the investigation and any action taken to you in writing.

Escalation to the Data Protection Board: If you are not satisfied with the resolution provided by Drivn, you may escalate your complaint to the Data Protection Board of India in accordance with applicable law.

15. Updates to this Policy

Drivn may update or amend this Policy from time to time to reflect changes in applicable law, our business operations, or data processing practices. Continued use of Drivn's services or website after the effective date of any update shall constitute acknowledgment of the revised Policy.