PRIVACY POLICY

Adopted under the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

VERSION 2.0 · EFFECTIVE 29 AUGUST 2026

1. Introduction and Applicability

1.1 Green Aero Propulsion Private Limited, a company incorporated under the Companies Act, 2013 (CIN: U72100DL2023PTC419262), with its registered office at B1/H3, Mohan Cooperative, Mathura Road, Block B, Badarpur (South Delhi), New Delhi, Delhi, India, 110044 ("Company", "we", "us" or "our"), is committed to protecting the personal data of its website visitors, customers, vendors, business contacts, job applicants, employees and other individuals who interact with the Company ("Data Principals" or "you").

1.2 This Privacy Policy ("Policy") describes how the Company, acting as a Data Fiduciary, collects, uses, stores, shares and otherwise processes personal data. It is published under (a) the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), and (b) Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") framed under Section 43A of the Information Technology Act, 2000 ("IT Act"), for as long as those provisions remain in force.

1.3 This Policy applies to personal data processed through the Company's website, platforms, correspondence, recruitment and employment processes, and commercial dealings. It applies to personal data collected in digital form, and to personal data collected in non-digital form that is subsequently digitised.

2. Legal Framework and Transition

2.1 The DPDP Act and the DPDP Rules are being brought into force in phases. The Company will comply with each provision of the DPDP Act and the DPDP Rules from the date on which that provision takes effect, and has structured this Policy to meet the substantive obligations that apply under them.

2.2 Until Section 43A of the IT Act is omitted by Section 44(2) of the DPDP Act, the SPDI Rules continue to apply alongside the DPDP framework. During that period the Company will follow both, and where they differ the Company will apply the standard that is more protective of the Data Principal. The provisions of this Policy that refer specifically to the SPDI Rules will cease to apply, without further notice, when Section 43A and the SPDI Rules cease to have effect.

2.3 The Company will also continue to comply with other applicable laws that govern information it holds, including the CERT-In Directions of 28 April 2022 on cyber incident reporting.

3. Definitions

3.1 Terms used in this Policy such as “personal data”, “Data Fiduciary”, “Data Principal”, “Data Processor”, “processing”, “personal data breach” and “Board” have the meanings given in the DPDP Act and the DPDP Rules.

3.2 “Personal data” means any data about an individual who is identifiable by or in relation to such data.

3.3 “Sensitive Personal Data or Information” (“SPDI”) has the meaning given in Rule 3 of the SPDI Rules and includes passwords; financial information such as bank account, card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information. Information that is freely available in the public domain or furnished under the Right to Information Act, 2005 is not SPDI. The DPDP Act does not create a separate category of sensitive personal data, and the Company applies the safeguards in this Policy to all personal data.

4. Personal Data We Process

4.1 The Company processes the following categories of personal data, limited to what is necessary for the purposes stated in Section 5:

- Identity and contact data: name, designation, employer, postal address, email address and telephone number;
- Financial and tax data: bank account details, PAN and GST details and billing information of vendors, customers and employees, used for payments and statutory compliance;
- Recruitment and employment data: resumes, educational qualifications, employment history, background verification details and payroll information;
- Technical data: IP address, browser type, device identifiers, cookies and usage data from the Company’s website and IT systems;
- Security and access data: visitor, access-control and facility records for the Company’s premises; and
- Any other personal data you voluntarily submit through forms, correspondence, meetings or commercial dealings.

4.2 The Company does not seek to collect biometric, health or similar information except where it is needed for a specific, lawful purpose, such as statutory employee benefits or secure site access, and in that case only after notice to the Data Principal.

5. Notice, Purposes and Lawful Basis

5.1 The Company processes personal data only for a lawful purpose, either (a) with the consent of the Data Principal, or (b) for a “legitimate use” recognised in Section 7 of the DPDP Act.

5.2 When the Company asks for consent, it will give you a notice, in clear and plain language and independent of any other information, that describes (a) an itemised description of the personal data being processed, (b) the specific purpose and the goods, services or uses enabled by that processing, (c) how to withdraw consent and exercise your rights, and (d) how to make a complaint to the Data Protection Board of India (“Board”). The notice will also give the contact details of the person who can answer your questions, as set out in Section 14.

5.3 The purposes for which the Company processes personal data are:

- performing contracts and managing relationships with customers, vendors and business partners;
- processing employment applications and administering employment relationships;
- complying with law and regulation applicable to the Company's business, including tax, company law, export control (including SCOMET under the Foreign Trade (Development and Regulation) Act, 1992), aviation and defence-sector requirements, and lawful requests of courts and authorities;
- financial reporting, payments and statutory filings;
- communicating with you about our products, services and updates, where you have consented;
- operating, securing and improving our website, systems and premises, and preventing fraud and unauthorised access; and
- corporate transactions, investor and lender due diligence and reporting, on a need-to-know basis and subject to confidentiality.

5.4 Where the Company processes personal data for a legitimate use, such as a purpose for which you voluntarily provided your data and did not indicate that you do not consent to its use, employment purposes or safeguarding the Company from loss or liability, compliance with law or a court order, or responding to a medical emergency, it will do so without a separate request for consent, and only to the extent needed for that use.

5.5 The Company will not process personal data for a purpose other than the one notified to you without obtaining fresh consent or relying on another lawful basis.

6. Consent and Withdrawal

6.1 Consent given to the Company will be free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the personal data necessary for the stated purpose.

6.2 Wherever the Company collects personal data through a form, such as a website enquiry or contact form, a sign-up or registration form, a job application form, or a vendor or customer onboarding form, consent will be obtained through a tick box that you must select yourself. The box will not be pre-ticked, and the form will display or link to the notice described in Section 5.2 beside it. The Company will not collect or submit your personal data through the form until you have ticked the box.

6.3 Where personal data is collected in some other way, such as on paper, by email or in person, the Company will obtain your consent in writing or by electronic means, including by a confirming email, before it processes the data. For as long as the SPDI Rules apply, the Company will do the same before collecting SPDI.

6.4 The Company will keep a record of the consent you give, including the date and time, the purpose and the version of the notice shown, so that it can demonstrate that consent was obtained.

6.5 You may withdraw consent at any time. The Company will make withdrawal as easy as giving consent, by writing to the contact point in Section 14. You will bear the consequences of withdrawal, including that we may be unable to continue providing the related goods or services. Withdrawal does not affect the lawfulness of processing done before it.

6.6 On withdrawal, the Company will stop processing your personal data, and will cause its Data Processors to stop, within a reasonable time, unless processing is required or permitted by law or is a legitimate use.

7. Children's Personal Data

7.1 The Company's website and services are not directed at children (individuals under 18 years of age). The Company does not knowingly process the personal data of a child, or of a person with a disability who has a lawful guardian, without first obtaining verifiable consent of the parent or lawful guardian.

7.2 The Company does not undertake tracking or behavioural monitoring of children, or targeted advertising directed at children. If you believe a child has provided personal data to the Company, please contact us at the details in Section 14 and we will take appropriate steps.

8. Disclosure and Sharing

8.1 The Company may share personal data with the following, to the extent necessary for the purposes in Section 5:

- Data Processors engaged by the Company, such as payroll, IT, cloud hosting, communications and recruitment service providers, under a valid contract that requires them to apply safeguards equivalent to those in this Policy and to process the data only on the Company's instructions;
- affiliates and business partners, on a need-to-know basis;
- professional advisers, auditors, lenders, and current or prospective investors and their advisers, subject to confidentiality;
- courts, government and regulatory authorities, and law enforcement agencies, where required by law, including for the prevention, detection or investigation of offences and cyber incidents.

8.2 The Company remains responsible for personal data processed by a Data Processor on its behalf. A recipient that obtains SPDI from the Company may not disclose it further, as required by Rule 6 of the SPDI Rules.

8.3 The Company does not sell or rent personal data.

9. Transfer of Personal Data Outside India

9.1 The Company may process personal data outside India, including through cloud service providers or group and investor entities abroad. Under Section 16 of the DPDP Act, transfers are permitted except to countries or territories the Central Government restricts by notification, and the Company will comply with any such restriction and with any sector-specific law that requires data to remain in India.

9.2 For as long as the SPDI Rules apply, the Company will transfer SPDI only to a person that ensures the same level of data protection that the SPDI Rules require, and only where the transfer is necessary to perform a lawful contract or you have consented.

10. Security Safeguards and Breach Notification

10.1 The Company maintains reasonable security safeguards to protect personal data in its possession or under its control, including data held by Data Processors, and to prevent personal data breaches. These are consistent with Rule 6 of the DPDP Rules and Rule 8 of the SPDI Rules, and include:

- documented information security policies and procedures covering managerial, technical, operational and physical controls;
- encryption, obfuscation, masking or tokenisation of personal data where appropriate;

- access controls that limit access to authorised personnel on a need-to-know basis, including to computer resources used to process personal data;
- logging, monitoring and review of access to personal data to detect and investigate unauthorised access, with logs and related personal data retained for at least one year, or longer if law requires;
- data backups and measures to maintain continued processing if confidentiality, integrity or availability is compromised;
- contractual security obligations for Data Processors;
- confidentiality undertakings and periodic training for personnel handling personal data; and
- periodic review and audit of controls, and an incident response procedure.

10.2 If a personal data breach occurs, the Company will, as required by the DPDP Act and Rule 7 of the DPDP Rules, inform each affected Data Principal without delay, in a concise and clear manner, of the nature, extent, timing and likely impact of the breach, the steps taken to mitigate risk, safety measures you may take, and a contact point for queries. The Company will also inform the Board without delay and provide detailed information within seventy-two (72) hours, or any longer period the Board permits. Where applicable, the Company will also report the incident to CERT-In within the period it prescribes.

10.3 When called upon by a competent authority, the Company will be able to demonstrate that it has implemented security measures in accordance with its documented information security programme.

11. Retention and Erasure

11.1 The Company retains personal data only for as long as the purpose for which it was collected is being served, or as needed to comply with applicable law, including tax, company, labour and accounting requirements, to establish or defend legal claims, or to comply with contractual obligations.

11.2 When you withdraw consent or the purpose is no longer being served, and retention is not required by law, the Company will erase the personal data and ask its Data Processors to do the same. Personal data that must be retained for a legal requirement will be kept securely and used only for that purpose.

12. Your Rights as a Data Principal

12.1 You have the right to:

- access a summary of the personal data we hold about you and who we have shared it with;
- correct, complete or update your personal data, and ask us to erase it when it is no longer needed, unless the law requires us to keep it;
- have any grievance about your personal data addressed; and
- nominate another person to exercise these rights if you die or become incapacitated.

12.2 To exercise any of these rights, write to the Grievance Officer at the details in Section 14. We may ask for details to verify your identity. We will respond within the time set by the DPDP Rules, which is currently up to ninety (90) days for grievances.

12.3 While the SPDI Rules apply, you may also review the information you gave us and have anything inaccurate corrected. We are not responsible for the accuracy of information supplied by you or anyone else.

13. Your Duties as a Data Principal

In line with Section 15 of the DPDP Act, you must comply with applicable law when exercising your rights, must not impersonate another person or suppress material information when providing personal data, must not register a false or frivolous grievance or complaint, and must furnish only verifiably authentic information when exercising the right to correction or erasure. A breach of these duties may attract a penalty under the DPDP Act.

14. Grievance Redressal and Contact

14.1 The Company has designated the following Grievance Officer, who is also the contact point to answer questions about the processing of your personal data and to receive requests under Section 12. The Grievance Officer addresses grievances in accordance with Section 13 of the DPDP Act and Rule 5(9) of the SPDI Rules.

GRIEVANCE OFFICER	Farhan Pathan, Chief Operating Officer
ADDRESS	B1/H3, Mohan Cooperative, Mathura Road, Block B, Badarpur (South Delhi), New Delhi, Delhi, India, 110044
EMAIL	farhan.pathan@greenaero.in
PHONE	+91 8128563469

14.2 The Company will acknowledge a grievance promptly and resolve it within one (1) month while the SPDI Rules apply, and thereafter within the period prescribed under the DPDP Rules, which is currently ninety (90) days.

14.3 If you are not satisfied with the Company's response, or have received none within the prescribed period, you may make a complaint to the Data Protection Board of India once it is operational for that purpose. Under the DPDP Act, you should first have exhausted the Company's grievance redressal process.

15. Cookies and Website Usage Data

The Company's website may use cookies and similar technologies to operate the site and analyse traffic. Where cookies or similar technologies process personal data for a purpose that requires consent, the Company will seek that consent through a notice or banner. You can refuse cookies through your browser settings, although some features of the website may not function.

16. Third-Party Links

The Company's website may link to third-party websites. This Policy does not apply to those sites, and the Company is not responsible for their privacy practices. Please read the privacy policy of any site you visit.

17. Changes to this Policy

The Company may update this Policy to reflect changes in law, including further notifications under the DPDP Act and DPDP Rules, or in its practices. The revised Policy will be posted on the website with an updated effective date. Where a change affects the notice you were given for a consent-based purpose, the Company will seek fresh consent as required by law.

18. Governing Law and Jurisdiction

This Policy is governed by the laws of India, including the DPDP Act, the DPDP Rules and the IT Act and the rules under it. Subject to the jurisdiction of the Board and any appellate tribunal under the DPDP Act, the courts at New Delhi have exclusive jurisdiction over disputes arising out of this Policy.

Annexure: Compliance map

REQUIREMENT	SOURCE	POLICY SECTION
Publish privacy policy on website	SPDI Rule 4	Published at www.greenaero.in
Notice: itemised data, purpose, rights, Board complaint	DPDP Act s.5; DPDP Rules r.3	5.2
Free, specific, informed consent; easy withdrawal	DPDP Act s.6; SPDI Rule 5	6
Legitimate uses without consent	DPDP Act s.7	5.4
Children: verifiable parental consent	DPDP Act s.9	7
Disclosure and onward sharing; processors	DPDP Act s.8(2); SPDI Rule 6	8
Cross-border transfer	DPDP Act s.16; SPDI Rule 7	9
Security safeguards	DPDP Act s.8(5); DPDP Rules r.6; SPDI Rule 8	10.1, 10.3
Breach intimation to Board and Data Principals	DPDP Act s.8(6); DPDP Rules r.7	10.2
Retention and erasure	DPDP Act s.8(7); DPDP Rules r.8	11
Rights of access, correction, erasure, grievance, nomination	DPDP Act ss.11–14; DPDP Rules r.14	12
Duties of Data Principals	DPDP Act s.15	13
Grievance Officer and published contact	DPDP Act s.13; DPDP Rules r.9; SPDI Rule 5(9)	14