Data Privacy Policy

How Karnot collects, uses, stores, transfers and disposes of personal data — the rights of data subjects, the safeguards in place, and the channels for exercising those rights.

Document ID	KES-POL-006
Version	1.0
Effective from	11 May 2026
Next review	11 May 2027 (Annual)
Approved by	Stuart Edmund Cox, Managing Director
Applies to	All personal data processed by Karnot — covering customers, prospects, employees, applicants, suppliers, investors, website visitors and any natural person whose data Karnot holds, irrespective of jurisdiction.

1. Karnot's commitment to privacy

Karnot Energy Solutions Inc. ("Karnot") respects the right to privacy of every individual whose personal data it processes. The Company collects only the personal data necessary to do business, uses that data only for the purposes for which it was collected (or compatible purposes lawfully disclosed), keeps it secure, and disposes of it when it is no longer needed.

This Policy is the **corporate operating standard** used for supplier audits, B2B accreditation and ESG questionnaires. The public-facing Privacy Notice for website visitors and customers — covering cookies, contact-form data and the exercise of individual rights in plain English — is published separately at karnot.com/privacy. Both documents share the same Data Protection Officer, the same named processors, and the same retention schedule.

This Policy explains how Karnot meets those commitments in practice, and how data subjects can exercise their statutory rights.

2. Legal framework

This Policy is designed to comply with:

- Republic Act No. 10173 — Data Privacy Act of 2012 (Philippines), and its Implementing Rules and Regulations, together with all relevant National Privacy Commission (NPC) Circulars and Advisory Opinions.
- Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR), where Karnot processes data of EU/EEA-based individuals or operates as a processor for EU-based controllers.
- UK GDPR and the Data Protection Act 2018 for UK-based individuals.
- Other applicable national data-protection laws of jurisdictions in which Karnot does business.

3. Definitions

Personal data means any information that identifies, or could reasonably be used to identify, a natural person — including name, address, email, phone number, employment details, government-issued identifiers, financial information, and online identifiers such as IP address and cookie IDs.

Sensitive personal data (RA 10173 §3(l)) includes data about race, ethnic origin, marital status, age, colour, religious, philosophical or political affiliations, health, education, genetic or sexual life, government-issued identifiers, and details of any offence.

Data subject is the natural person to whom the personal data refers.

Processing includes any operation performed on personal data — collection, recording, storage, retrieval, use, disclosure, alignment, restriction, erasure and destruction.

4. Categories of personal data Karnot processes

Karnot processes personal data in the following categories:

- **Employees and applicants** — name, contact details, government identifiers (TIN, SSS, PhilHealth, Pag-IBIG), CV/resume, payroll, performance, training records.
- **Customers and prospects** — contact name, business email and phone, company affiliation, role, project requirements, technical site data submitted through calculators and forms.
- **Suppliers and contractors** — business contact details and bank details necessary to engage and pay them.
- **Investors** — name, email, contact details, KYC data where required, investor classification, holdings.
- **Website visitors** — IP address, browser type, pages viewed, referrer, submitted form data; cookie identifiers used for essential and analytics purposes as set out in the cookie notice on karnot.com.

5. Lawful basis for processing

Karnot relies on one of the lawful bases listed in RA 10173 §12-13 (and, where relevant, GDPR Article 6) for each category of processing:

- **Consent** — for marketing communications, the investor hub, and optional analytics cookies.
- **Performance of a contract** — for processing required to deliver products, services, employment and payment obligations.
- **Legal obligation** — for tax, payroll, occupational safety, AML/KYC and other statutorily-required record keeping.
- **Legitimate interest** — for security logging, fraud prevention, B2B contact for existing customers and prospects, and improvement of the Karnot website and products. Where Karnot relies on legitimate interest, it documents the balancing test in writing.
- **Vital interest** — for emergency response involving an identified individual at a Karnot site.

6. Data subject rights

Every data subject has the following rights, exercisable free of charge except where requests are manifestly unfounded or excessive:

- **Right to be informed** — about the existence, nature and purpose of processing (this Policy and the privacy notice published at karnot.com/privacy).
- **Right of access** — to obtain a copy of personal data held about them.
- **Right to rectification** — to correct inaccurate or incomplete data.
- **Right to erasure** — to have data erased where no overriding legal basis or legitimate interest requires Karnot to retain it.
- **Right to object** — to processing based on legitimate interest, and to direct marketing in all cases.
- **Right to data portability** — to receive personal data in a structured, commonly-used and machine-readable format and to transmit it to another controller.
- **Right to damages** — under RA 10173 §16(f) for processing in violation of the Act.
- **Right to lodge a complaint** — with the National Privacy Commission (privacy.gov.ph) or the supervisory authority in the data subject's home jurisdiction.

To exercise any of these rights, contact the Karnot Data Protection Officer at info@karnot.com. Karnot will acknowledge requests within 5 working days and respond substantively within 30 days, in line with NPC Circular 16-01 and GDPR Article 12.

7. Data sharing and cross-border transfers

Karnot uses a limited number of trusted processors to operate its business. Where personal data is transferred outside the Philippines, Karnot relies on appropriate safeguards (standard contractual clauses, adequacy decisions where available, or the data subject's explicit consent). The current principal processors are:

- **Cloudflare, Inc.** — website hosting, content delivery, security and Worker logic; data processed in distributed global locations under Cloudflare's published data-protection terms.
- **Google LLC (Firebase / Firestore)** — Karnot CRM database and authentication; data hosted in regions to be confirmed for each environment; standard contractual clauses in place.
- **Sendinblue SA (Brevo)** — transactional and marketing email; EU-based processor; processing under its standard data-processor agreement.
- **Netlify, Inc.** — hosting of the Karnot CRM application.

8. Retention

Karnot retains personal data only for as long as it is needed for the purposes for which it was collected, and for any further period required by law. Specific retention periods include:

- Employee records — for the duration of employment plus the period required by Philippine labour, tax and SSS regulations (typically 10 years after separation).
- Customer engagement records — for the duration of the engagement plus 10 years, in line with BIR retention requirements for accounting books.
- Marketing contact records — until the contact unsubscribes, or 24 months after the last interaction, whichever is sooner.
- Investor records — for the duration of the holding plus 10 years.
- Website logs — 12 months.

9. Security measures

Karnot implements technical and organisational measures to protect personal data:

- Encryption in transit (TLS 1.2+) for all data flowing over public networks; encryption at rest for stored data in cloud processors.
- Role-based access control with the principle of least privilege; periodic access review.
- Multi-factor authentication on all administrative and email accounts.
- Code-level secrets stored as Cloudflare Worker secrets and Firebase configuration; never in repository or document.
- Documented incident-response procedure with mandatory 72-hour breach notification to the NPC and affected data subjects, in line with NPC Circular 16-03 (and GDPR Article 33 where applicable).

10. Data Protection Officer

Karnot has designated a Data Protection Officer under RA 10173 §11 and NPC Advisory 17-01. The current DPO is:

Stuart Edmund Cox — Managing Director and Data Protection Officer
Karnot Energy Solutions Inc.
info@karnot.com • +63 75 510 8922

All data-subject requests, breach notifications and privacy concerns should be directed to the above contact.

11. Review

This Policy is reviewed annually and on any material change to Karnot's processing activities, to the processors used, or to the legal framework. The current published version takes precedence over any earlier draft or copy.

APPROVAL

This policy is approved by the undersigned for and on behalf of Karnot Energy Solutions Inc., with effect from 11 May 2026, and will be reviewed not later than 11 May 2027.

Stuart Edmund Cox
Managing Director
Karnot Energy Solutions Inc.
Date: 11 May 2026