

Data Protection Policy and Privacy Notice

Document control

ITEM	DETAIL
Organisation	InnoRail, Company No. 17055194, registered in England and Wales
Registered office	71 to 75 Shelton Street, London, WC2H 9JQ
Operating office	Electric Works, 3 Concourse Way, Sheffield, S1 2BJ
Policy owner	Tim Jones, Chief Technology Officer and Data Manager
Version	1.0
Approved	Tim Jones, Chief Technology Officer, July 2026
Next review	July 2027, or sooner after a significant change in law or in how we process data
ICO registration	ZB502494, held by our sister company InnoRail

1. Purpose and scope

InnoRail ("InnoRail International", "we", "us") processes personal data lawfully, fairly and securely, in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This document is both our data protection policy and our privacy notice.

It applies to all personal data we handle, in any format, and to everyone who works for or with us: directors, employees, contractors, associates and delivery partners.

2. Who we are and our role

InnoRail International is a UK rail industry consultancy that also provides software services to train operators and other rail organisations. We act in 2 roles:

ROLE	WHEN	WHAT IT MEANS
Controller	Running our own business: staff, recruitment, client and supplier contacts, website enquiries, marketing	We decide why and how the data is used, and we are responsible to you for it
Processor or sub-processor	Delivering consultancy or software services where a customer's personal data is involved	We act only on the customer's documented instructions under a written data processing agreement. The customer is the controller

Our software services are designed so that they do not need personal data to work. Where a service does involve personal data, such as the names and work email addresses of a customer's own admin users, we handle it as the customer's processor under this policy and the contract.

3. Data protection principles

We follow the 7 UK GDPR principles in everything we do with personal data:

- **Lawfulness, fairness and transparency:** we have a lawful basis for every use and tell people what we do.

- **Purpose limitation:** we use data only for the purposes we collected it for.
- **Data minimisation:** we collect only what we need. Our products are designed not to require personal data.
- **Accuracy:** we keep data accurate and correct it promptly when told.
- **Storage limitation:** we keep data no longer than needed (section 5).
- **Integrity and confidentiality:** we protect data with appropriate security (section 7).
- **Accountability:** we keep records of processing and can show how we comply.

4. Lawful bases

When we act as controller, we rely on these lawful bases:

- **Contract:** to enter into and perform contracts with clients, suppliers, staff and contractors.
- **Legal obligation:** for example tax, employment, right to work and company law records.
- **Legitimate interests:** to run and develop our business, manage client relationships and keep our systems secure, where this does not override your rights.
- **Consent:** for optional marketing emails and non-essential website cookies. You can withdraw consent at any time.

We do not use personal data for automated decision-making or profiling that has legal or similarly significant effects on individuals.

5. Personal data we process as controller

WHO	DATA	WHY	HOW LONG WE KEEP IT
Client and supplier contacts	Name, job title, organisation, work email and phone	Managing contracts, projects and relationships	Length of the relationship plus 6 years
Staff, contractors and associates	Contact and identity details, right to work checks, contract, pay and bank details, CVs, training records	Employment and engagement, payroll, legal duties, putting forward CVs in bids with the person's agreement	Length of employment or engagement plus 6 years
Job applicants	CV, contact details, interview notes	Recruitment	6 months after the role is filled, unless the applicant agrees to us keeping it longer
Website visitors and enquirers	Contact form details; cookie and analytics data	Answering enquiries; running and improving our website	Enquiries: 2 years. Analytics: as set out in our cookie notice
Marketing contacts	Name, work email, organisation	Sending updates that people have opted into	Until they unsubscribe
Users of our software services	Admin users' names, work emails, sign-in and activity logs	Providing secure access and support (as processor for the customer)	As agreed with the customer in the contract

At the end of a retention period we securely delete or anonymise the data.

6. Processing on behalf of customers

When we process personal data for a customer, we:

- act only on the customer's documented instructions, set out in a data processing agreement that meets UK GDPR Article 28;
- make sure everyone with access is bound by confidentiality;
- apply the security measures in section 7;
- use sub-processors only with the customer's authorisation, under terms that give equal protection, and tell the customer in advance of any change;

- help the customer respond to individuals' rights requests, carry out data protection impact assessments and meet its security and breach duties;
- notify the customer of any personal data breach without undue delay, and in any case within 24 hours of becoming aware;
- delete or return all personal data at the end of the contract, as the customer chooses, unless the law requires us to keep it;
- make available the information needed to show compliance, and allow audits.

Sub-processors and partners

ORGANISATION	PURPOSE	LOCATION
Amazon Web Services	Cloud hosting, storage, backups and security services for our software	United Kingdom (AWS UK region)
Microsoft (Microsoft 365)	Business email, documents and collaboration	[Location to be confirmed]

Rail industry data sources used by our software (for example Network Rail data through the Rail Data Marketplace) supply information to our services but do not receive personal data.

International transfers

We host and process data in the United Kingdom. We do not transfer personal data outside the UK unless there are appropriate safeguards: a UK adequacy regulation, or the UK International Data Transfer Agreement or Addendum, supported by a transfer risk assessment. For customer data, we transfer only with the customer's agreement.

7. Security of personal data

We protect personal data with technical and organisational measures suited to the risk:

- Cyber Essentials certification, held by our sister company InnoRail, covering firewalls, secure configuration, access control, malware protection and patch management;
- encryption at rest (AES-256) and in transit (TLS 1.2 or higher);
- named user accounts, multi-factor authentication and role based, least privilege access;
- logical separation of each customer's data within our software platforms;
- audit logging of access and changes;
- vulnerability management and patching under our Vulnerability Management Policy;
- encrypted, access restricted backups held in the UK;
- confidentiality terms in all staff, contractor and supplier agreements.

8. Personal data breaches

Anyone who suspects a personal data breach must report it to the Data Manager immediately. We then:

- contain the breach and limit its impact;
- assess the risk to the people affected;
- where we are processor, notify the customer (controller) without undue delay, and in any case within 24 hours of becoming aware;
- where we are controller, notify the Information Commissioner's Office within 72 hours if the breach is likely to result in a risk to people's rights and freedoms, and tell the affected people without undue delay if the risk is high;
- record every breach, whether reported or not, with the facts, effects and action taken;
- review the cause and put in place actions to prevent it happening again.

9. Your rights

You have the right to:

- be told how your data is used (this notice);
- get a copy of your personal data;
- have inaccurate data corrected;
- have your data deleted in some circumstances;
- restrict or object to our use of your data in some circumstances;
- have data you gave us transferred to another organisation (data portability);
- withdraw consent at any time, where we rely on consent.

To use any of these rights, contact us (section 12). We respond within 1 month, free of charge in most cases, and may ask you to confirm your identity first. Where we hold your data as a processor, we pass your request to the customer that controls it and help them respond.

10. Data protection by design

- We build data protection into our products and services from the start, and design our software so it does not need personal data to work.
- We carry out a data protection impact assessment (DPIA) before any processing likely to be high risk, and support customers with their own DPIAs.
- Where our products use artificial intelligence, they do not make decisions about individuals, and customer data is not used to train AI models.
- We keep a record of processing activities under UK GDPR Article 30.

11. Responsibilities and training

WHO	RESPONSIBILITY
Chief Technology Officer and Data Manager (Tim Jones)	Owns this policy, handles rights requests and breaches, keeps records, and is the contact for the ICO and customers
Staff, contractors and associates	Follow this policy, complete data protection training when they join and every year, and report any suspected breach straight away
Delivery partners and suppliers	Protect personal data under the data protection terms in their contracts

We have assessed that we are not required to appoint a statutory Data Protection Officer. The Data Manager carries out that role in practice. Breaking this policy may lead to disciplinary action or ending a contract.

12. Contact and complaints

For any question about this policy or your personal data, or to use your rights, contact our Data Manager:

- **Email:** privacy@innorail.co.uk
- **Post:** Data Manager, InnoRail, Electric Works, 3 Concourse Way, Sheffield, S1 2BJ

If you are unhappy with how we have handled your data, please tell us first so we can put it right. You also have the right to complain to the Information Commissioner's Office (ICO): ico.org.uk/make-a-complaint, or 0303 123 1113.

13. Review

We review this policy at least once a year, and sooner after a change in the law or in how we process personal data. The latest version is always published on our website.