# Remote–I

## Privacy Policy (Full)

**Document Type:** Policy

**Version:** 1.0 **Effective Date:** 12 December 2025

**Owner:** Remote-I Ltd – Technical Lead

**Classification:** Internal / Customer Assurance

**Review Cycle:** Annual, and after major storage/schema change or incident

**Organisation:** Remote-I Ltd
**Company Number:** 15293974
**Registered Office:** 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB
**Compliance Contact:** compliance@remote-i.com
**Data Protection Lead:** Remote-I Ltd – Data Protection Lead

## 1.1 Who we are

### 1.2 Scope

This Privacy Policy covers:

- visitors to our website;
- users who create accounts and use the Platform (including hospital users, administrators, and radiographers);
- individuals whose personal data may be included in Customer Data uploaded or entered by Customer users (for example workforce compliance documentation).

This Privacy Policy does **not** apply to third-party websites or services linked from our website or Platform.

### 1.3 Roles under data protection law

Depending on the context, Remote-I may act as:

- **Controller**: for personal data we process to operate our business and manage accounts, security, and billing (e.g., administrative contact details; security logs used for fraud prevention and system protection).
- **Processor**: for personal data processed on behalf of a hospital or imaging organisation (the "Customer") as part of the Platform's workforce governance, compliance and job workflow functions ("Customer Data").

Where we act as a Processor, processing is governed by our **Data Processing Agreement (DPA)** with the Customer.

---

### 1.4 What personal data we collect

#### A) Website visitors

We may collect:

- device and technical data (IP address, browser type, OS, device identifiers);
- usage data (pages viewed, time on pages, clickstream);
- cookie and similar tracking data (see Cookies section).

#### B) Platform account and identity data

We may collect:

- name, email address, phone number (where used);
- organisation and role (hospital, radiographer, admin);
- authentication data (login events, MFA status, verification status);
- account preferences and settings.

#### C) Workforce and compliance data (Platform content)

Depending on Customer configuration and user role, the Platform may process:

- professional profile data (registration identifiers, specialties, qualifications);
- compliance documents and metadata (e.g., right-to-work evidence, DBS evidence, insurance evidence, training evidence, expiry dates);

- availability and scheduling data;
- job lifecycle and workflow data (job creation, assignment, acceptance, completion, handover, associated notes);
- SOP acknowledgements and sign-off records;
- incidents, reflections, and governance notes entered into the system;
- communications content (job chat messages, and notification records where enabled).

### D) Audit and security logs

We may process:

- audit logs of key platform actions (who did what and when);
- device and security telemetry (IP address, timestamps, session identifiers);
- system error logs and operational logs (designed to avoid logging sensitive message content unnecessarily).

### E) Support and communications

We may collect:

- support requests and content;
- email communications;
- call notes (if applicable).

## Special category data and patient data

Remote-I is designed primarily for **workforce operations and governance**, and it is **not intended** for storage of patient-identifiable clinical data. Customers should configure and train users to avoid entering unnecessary patient identifiers.
However, free-text fields (e.g., incidents or notes) may incidentally include sensitive information. Where that occurs, we rely on strict access controls, audit logging, and minimisation practices.

---

## 1.5 Lawful bases for processing

We rely on the following lawful bases under UK GDPR/GDPR, depending on context:

1. **Contract** (Article 6(1)(b))
   To provide the Platform and services you request (account creation, authentication, job workflows, compliance functions).
2. **Legitimate interests** (Article 6(1)(f))
   To secure and improve the Platform, prevent fraud, maintain logs for security, and to support operations and governance. We balance these interests against your rights.
3. **Legal obligation** (Article 6(1)(c))
   Where we must comply with applicable laws (e.g., tax, corporate record-keeping, lawful requests).
4. **Consent** (Article 6(1)(a))
   Where required (e.g., certain cookie categories; marketing preferences). You can withdraw consent at any time.

Where special category data is processed (Article 9), the primary responsibility for lawful basis typically sits with the Customer as Controller, supported by the DPA and Customer governance arrangements.

---

## 1.6 How we use personal data

We use personal data to:

- provide and administer the Platform (accounts, authentication, workflows);
- verify accounts (email verification, MFA setup, and security checks);
- enable governance functions (audit logs, SOP acknowledgements, reporting);
- send notifications (email/SMS) where enabled by the Customer;
- provide customer support and respond to requests;
- monitor and protect Platform security (intrusion prevention, fraud detection);
- maintain platform performance and reliability (error monitoring, diagnostics); • comply with legal obligations and enforce terms.

---

## 1.7 Sharing and disclosure

**We may share personal data with:**

### A) Customers (hospital organisations)

Where a Customer administers the Platform, Customer administrators may view and manage certain user information and compliance data in line with their role and governance model.

### B) Service providers (subprocessors)

We use service providers to deliver infrastructure and communications services (e.g., hosting, email delivery, SMS gateway). These providers are bound by confidentiality and data protection obligations, and (where applicable) are listed in the DPA Annex on subprocessors.

### C) Professional advisers

Legal, accounting, insurance, and professional advisers (under confidentiality).

### D) Authorities

If required by law, regulation, or to protect rights and safety.

### E) Corporate transactions

If we undergo a merger, acquisition, or asset sale, data may be transferred subject to appropriate safeguards.

---

## 1.8 International transfers

If personal data is transferred outside the UK/EEA, we implement appropriate safeguards, such as:

- adequacy decisions where applicable;
- UK IDTA or the UK Addendum to EU SCCs;
- EU SCCs for EU data, where applicable;

- additional technical and organisational safeguards.

Details are provided in the DPA where Remote-I acts as Processor.

---

## 1.9 Data retention

We retain personal data only as long as necessary:

- **Account data:** retained for the duration of the account and subscription, and for a reasonable period after closure for security, dispute handling and legal compliance.
- **Audit logs:** retained in accordance with Customer configuration and governance needs, typically **12 months** unless otherwise agreed (or longer where required for investigations).
- **Support records:** typically retained up to **24 months** to improve service quality and evidence support outcomes.
- **Backups:** retained for a defined operational period (e.g., **30 days**), after which they are rotated and deleted in line with the Backup Policy.
- **Billing and finance:** retained as required by law.

Customers may also configure retention for certain fields or modules, subject to Platform capability and contract terms.

---

## 1.10 Security measures

We implement security measures designed to protect confidentiality, integrity, and availability of personal data, including (as appropriate):

- role-based access control (RBAC) and least-privilege access;
- multi-factor authentication (MFA) support;
- encryption in transit (TLS);
- secure configuration management (secrets stored outside public web roots where applicable);
- audit logging and monitoring;
- backup and restore procedures;
- vulnerability and patch management processes;
- supplier and subprocessor controls.

A fuller description of TOMs appears in the DPA Annex B.

---

## 1.11 Your rights

Depending on your location, you may have rights including:

- access to your personal data;
- correction of inaccurate data;
- deletion (where applicable);
- restriction of processing;
- data portability;
- objection to processing (especially where we rely on legitimate interests);
- withdrawal of consent (where processing is based on consent).

Where Remote-I acts as Processor, we may refer your request to the Customer as Controller, or assist the Customer in responding under the DPA.

---

## 1.12 How to contact us and complain

For privacy requests or questions, contact: **compliance@remote-i.com**.

If you are in the UK, you may complain to the **Information Commissioner's Office (ICO)**. If you are in the EEA, you may complain to your local supervisory authority.

---

## 1.13 Cookies and tracking

We use cookies and similar technologies to:

- operate the website and Platform;
- maintain secure sessions;
- measure and improve performance and usability;
- (where enabled) analytics and marketing.

Where required, we will request consent for non-essential cookies. You can manage cookie preferences via your browser settings and any cookie banner controls.

---

## 1.14 Children

The Platform is not intended for children, and we do not knowingly collect personal data from children.

---

## 1.15 Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in law, technology, or our practices. We will post updates on our website and/or notify Customers where material changes occur.