POLICY DOCUMENT

Privacy Policy

Remote-I Platform and Website

DOCUMENT TYPE	Policy
VERSION	1.1 (rev. 2)
EFFECTIVE DATE	7 May 2026
OWNER	Remote-I Ltd — Data Protection Lead
CLASSIFICATION	Public (replaces v1.0 internal)
REVIEW CYCLE	Annual, and after material processing change

ORGANISATION

Remote-I Ltd

Company No: 15293974
Registered Office: 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB

Privacy contact: compliance@remote-i.com
Operational support: support@remote-i.com

LAST UPDATED: 7 MAY 2026 · REV. 2 — RETENTION TABLE ALIGNED WITH DATA RETENTION POLICY V1.1

LEGAL ENTITY	Remote-I Ltd
REGISTERED OFFICE	45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB
COMPANY NUMBER	15293974
PRIVACY CONTACT	compliance@remote-i.com
OPERATIONAL SUPPORT	support@remote-i.com

> *This Privacy Policy explains how Remote-I Ltd ("Remote-I", "we", "us", "our") collects, uses, stores, and shares personal data when you use our web-based platform and related services. It is written for transparency under the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), and the UK Data Protection Act 2018.*

1. Scope of this Policy

This Policy applies to:

- **Radiographers** and other individual professionals using Remote-I;
- **Hospital and diagnostic centre users** using Remote-I on behalf of their organisation;
- **Visitors** to our website at remote-i.com.

This Policy does not describe how hospitals process patient data within their own RIS, PACS, or HIS systems. For such processing, the hospital remains the data controller and its own privacy notices apply.

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

2. Our roles under data protection law

Remote-I acts in two distinct roles depending on context:

Controller — when we process personal data for our own purposes, including:

- Operating our business (administrative contacts, billing)
- Securing the platform (security event logs, fraud prevention)
- Maintaining our website (analytics in aggregate)

Processor — when we process personal data on behalf of a hospital or imaging organisation (the "Customer"). This applies to the workforce, compliance, and governance data the Customer enters into the platform. In these cases, the Customer is the Controller, and our processing is governed by a separate **Data Processing Agreement (DPA)**.

For account credentials and authentication data of individual users (radiographers, hospital staff), Remote-I acts as Controller for the security and integrity of the account itself, while the operational data created through that account belongs to the Customer's processing context.

3. Personal data we collect

Account and contact data

- Name, email address, telephone number (where provided)
- Hashed password
- Role (radiographer, hospital user, administrator)
- Organisation details (hospital or diagnostic centre name, department, address)

Professional profile data (radiographers)

- Professional registration body and number (e.g., HCPC)
- Qualifications and years of experience
- Modalities, areas of expertise, preferred locations
- Availability and scheduling preferences
- Uploaded CV, profile picture, references, and feedback

Compliance documentation

- Right-to-work documentation
- Proof of indemnity insurance
- DBS or criminal record check confirmations
- Training certificates with expiry dates

Platform usage data

- Jobs created, accepted, declined, started, and completed
- Job-related messages and handover notes
- Standard Operating Procedure (SOP) acknowledgements (who, when, version)
- Incident reports and reflections
- Audit logs of platform actions

Technical and security data

- IP address, browser type and version, device information
- Authentication events (login attempts, MFA enrolment, password resets)
- Session identifiers
- Security event logs (e.g., suspected unauthorised access)

Communications and support data

- Support requests and email correspondence
- Notification delivery records (email, SMS attempts)

Special category and patient data — important note

> IMPORTANT
>
> The platform is designed primarily for **workforce operations and governance**, and is **not intended for storage of patient-identifiable clinical data**. Customers should configure access and train users to avoid entering unnecessary patient identifiers, particularly in free-text fields such as incident reports or notes.
>
> If special category data (e.g., health information, biometric identifiers) is incidentally entered, Remote-I relies on access controls, audit logging, and data minimisation as protective measures. Lawful basis for any such processing rests with the Customer as Controller.

4. Lawful bases for processing

We rely on the following lawful bases under UK GDPR and EU GDPR:

Basis	Article	Examples
Contract performance	6(1)(b)	Operating accounts, providing platform access, fulfilling Order Form obligations
Legitimate interests	6(1)(f)	Securing the platform, preventing fraud, maintaining audit logs, supporting governance and reporting
Legal obligation	6(1)(c)	Tax records, statutory accounting, lawful regulatory requests
Consent	6(1)(a)	Non-essential cookies (analytics, marketing); marketing communications where applicable

Where special category data is processed (Article 9), the Customer as Controller is responsible for establishing the lawful basis. Remote-I supports this through its role-based access controls and the DPA.

5. How we use personal data

We use personal data to:

- Create and administer accounts, including authentication and MFA
- Verify user identity (email verification, security checks)
- Enable workforce governance (jobs, scheduling, SOP sign-off, audit trails)
- Send notifications via email or SMS where enabled
- Provide customer support and respond to requests
- Monitor and protect platform security (intrusion prevention, anomaly detection)
- Maintain platform performance and reliability (error monitoring, diagnostics)
- Comply with legal and regulatory obligations
- Enforce our Terms of Service and Acceptable Use Policy

We do not use personal data for general marketing without your consent. We do not sell personal data.

6. Sharing and disclosure of personal data

Customers (hospital organisations)

Customer administrators may view and manage user information and compliance data within their organisation, in line with their role and governance model.

Service providers (subprocessors)

We use third-party service providers under contractual confidentiality and data protection obligations. The current categories include:

Category	Provider	Location	Purpose
Hosting infrastructure	GoDaddy.com LLC	France (EU)	Web and database hosting
Email delivery	GoDaddy mail relay	France (EU)	Transactional email (verification, notifications)
SMS notifications	ClickSend Pty Ltd	Australia	SMS delivery (where enabled by Customer)
Website analytics	Google LLC (Google Analytics 4)	United States	Aggregate website usage statistics
Marketing analytics	LinkedIn Corporation	United States/ Ireland	Marketing campaign measurement (with consent)
Bot protection	Google LLC (reCAPTCHA)	United States	Spam and abuse prevention on contact forms

A current list of subprocessors is maintained and shared with Customers under the DPA. Customers receive notice of material changes and may object on legitimate grounds.

Other recipients

- **Professional advisers** (legal, accounting, insurance) under confidentiality
- **Authorities** where required by law, regulation, or to protect rights and safety
- **Successors** in the event of a merger, acquisition, or asset transfer, subject to appropriate safeguards

We do not sell personal data to any third party.

7. International transfers

Personal data is primarily stored on infrastructure located in **France (European Union)**. We do not routinely transfer Customer Data outside the UK or EEA for storage purposes.

Where transfers do occur — for example, the SMS subprocessor (ClickSend, Australia), or where Google services involve data residency in the United States — we implement appropriate safeguards, including:

- **UK adequacy regulations** where applicable

- The **UK International Data Transfer Agreement (IDTA)** or the UK Addendum to EU Standard Contractual Clauses
- **EU Standard Contractual Clauses (SCCs)** for EU personal data
- **Supplementary safeguards** including data minimisation, encryption in transit, and contractual access restrictions

Detailed transfer mechanisms for Customer Data are described in the DPA.

8. Data retention

We retain personal data only as long as necessary for the purposes for which it was collected, in accordance with our **Data Retention and Disposal Policy**. Baseline retention periods are summarised below; Customers may configure longer or shorter periods where the platform supports it.

Category	Baseline retention
Account and identity data	Active subscription term plus 12 months
Job lifecycle records	12–24 months (configurable)
SOP acknowledgements	7 years (clinical governance baseline)
Compliance documents — Right-to-Work	2 years post-engagement (UK Home Office statutory)
Compliance documents — DBS evidence	12 months post-engagement
Compliance documents — Training and insurance	6 years (clinical governance baseline)
Incident records and reflections	24 months
Audit and security logs	12 months (configurable up to 24 months for higher-assurance environments)
Notification delivery metadata	6–12 months
Backups	30 days (rotation cycle)
Support records	24 months
Billing and finance records	6 years (UK statutory requirement)

Retention may be extended for legal holds, active investigations, or where Customer governance requires longer periods.

9. Your rights

Depending on your location and our role in processing your data, you have the following rights:

- **Access** — request a copy of personal data we hold about you
- **Rectification** — correct inaccurate or incomplete data
- **Erasure** — request deletion in certain circumstances ("right to be forgotten")
- **Restriction** — limit how we process your data

- **Portability** — receive your data in a structured, machine-readable format
- **Objection** — object to processing based on legitimate interests, including for marketing
- **Withdrawal of consent** — where processing is based on consent
- **Right to complain** — to a supervisory authority (see Section 12)

To exercise any of these rights, contact **compliance@remote-i.com**. We will respond within statutory timelines (one calendar month under UK GDPR, extendable in complex cases with notification).

Where Remote-I acts as Processor on behalf of a Customer, we may refer your request to the Customer as Controller, or assist the Customer in responding under the DPA. We will inform you if this is the case.

10. Security measures

We implement technical and organisational measures designed to protect the confidentiality, integrity, and availability of personal data, including:

- **Role-based access control (RBAC)** with least-privilege principles
- **Multi-factor authentication (MFA)** support for privileged accounts
- **Encryption in transit** using HTTPS/TLS for all platform connections
- **Secure secret management** with credentials stored outside the public web root
- **Audit logging** of authentication events, privilege changes, and key actions
- **Daily automated backups** with documented restore procedures
- **Vulnerability and patch management** for server and application components
- **Subprocessor due diligence** including contractual confidentiality obligations

A more detailed description of our technical and organisational measures appears in our DPA Annex B and our Information Security Policy. These documents are available to Customers under NDA.

No system is completely secure. We encourage users to set strong, unique passwords, enable MFA where available, and notify us promptly of any suspected compromise at compliance@remote-i.com.

11. Cookies and tracking

Our website uses cookies and similar technologies. When you first visit, we present a cookie consent banner with three options:

- **Accept all** — enables essential, analytics, and marketing cookies
- **Essential only** — limits to cookies strictly necessary for the platform to function
- **Manage** — choose specific categories

Cookie categories

Essential cookies are required for the platform to operate (session management, authentication, security). These do not require consent under PECR.

Analytics cookies — we use Google Analytics 4 (GA4) on our public marketing website to understand aggregate usage patterns (pages viewed, approximate location, device type, browser). GA4 is configured with privacy-minimising settings, including IP anonymisation and disabled advertising features.

Marketing cookies — we use LinkedIn cookies to measure the effectiveness of our marketing campaigns where you have consented. LinkedIn may process device and behavioural signals to assess campaign engagement.

Bot protection — our contact pages use Google reCAPTCHA, which may set cookies to assess whether form submissions are likely to be legitimate.

You may withdraw consent or change your cookie preferences at any time via the banner or your browser settings.

Cookies are not used to track individual users for clinical purposes or to process patient information.

12. How to contact us and complain

For privacy-related questions, data subject rights requests, or concerns:

- **Email:** compliance@remote-i.com
- **Post:** Remote-I Ltd, 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB

For general operational support: **support@remote-i.com**

If you are not satisfied with our response, you have the right to complain to a supervisory authority:

- **United Kingdom:** Information Commissioner's Office (ICO) — ico.org.uk
- **European Economic Area:** your local supervisory authority (list at edpb.europa.eu)

13. Children

The platform is intended for use by professional users in healthcare settings and is not directed at children. We do not knowingly collect personal data from children under 16. If we become aware that we have collected personal data from a child without verified parental consent, we will delete it.

14. Marketing communications

We may send marketing communications to business contacts where we have a lawful basis (typically legitimate interest for B2B contacts, or consent). You can unsubscribe at any time using the link in any marketing email or by contacting compliance@remote-i.com.

15. Automated decision-making

Remote-I does not use the platform to make automated decisions producing legal or similarly significant effects on individuals. Any automated processing (e.g., job matching, severity calculations) supports human decisions made by Customer administrators and radiographers.

16. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in law, technology, or our processing practices. Material changes will be notified via the platform or by email to Customers. The "Last updated" date at the top of this Policy reflects the most recent revision.

Previous versions are retained internally and available on request.