POLICY

Data Processing Agreement

Article 28 UK GDPR / GDPR — with Annexes A–D

DOCUMENT TYPE	Policy
VERSION	1.0 · Effective 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

LEGAL ENTITY	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

> This Data Processing Agreement ("DPA") forms part of the contract between Remote-I Ltd ("Processor") and the Customer ("Controller") where Remote-I processes Personal Data on behalf of the Customer in connection with the Platform.

2.1 Parties

Controller: The Customer identified in the Order Form (hospital / imaging organisation).

Processor: Remote-I Ltd, Company No. 15293974, 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB.

2.2 Definitions

Terms such as **Personal Data**, **Processing**, **Controller**, **Processor**, **Data Subject**, **Personal Data Breach** have the meanings in UK GDPR / GDPR.

"Restricted Transfer" means a transfer of Personal Data to a country outside the UK/EEA that is not covered by an adequacy decision and requires appropriate safeguards.

"Subprocessor" means any third party appointed by Processor to process Personal Data on behalf of Controller.

2.3 Subject matter, duration, nature and purpose

The subject matter, duration, nature and purpose of processing are described in **Annex A**.

3. Processor Obligations (Article 28)

3.1 Instructions

Processor shall process Personal Data only on documented instructions from Controller, including as set out in the contract, this DPA, and Controller's lawful configuration and use of the Platform.

If Processor believes an instruction infringes applicable law, Processor will inform Controller, unless prohibited by law.

3.2 Confidentiality

Processor ensures that persons authorised to process Personal Data are subject to confidentiality obligations (contractual or statutory) and receive appropriate security awareness.

3.3 Security (Article 32)

Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to risk, as set out in **Annex B (TOMs)**.

3.4 Subprocessing (Article 28(2) and 28(4))

Processor may engage Subprocessors in accordance with **Annex C**.

Processor shall:

- impose data protection obligations on Subprocessors that are no less protective than this DPA;
- remain responsible for Subprocessors' performance;
- provide notice to Controller of changes to Subprocessors, and allow Controller a reasonable opportunity to object on legitimate grounds.

3.5 Assistance to Controller

Processor shall provide reasonable assistance to Controller with:

- responding to Data Subject requests (access, deletion, etc.), taking into account the nature of processing;
- DPIAs and prior consultations where required;
- security and breach information required for Controller's compliance.

3.6 Personal Data Breach Notification

Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed on Controller's behalf, providing:

- the nature of the breach;
- categories and approximate number of affected data subjects (where known);
- likely consequences;
- measures taken or proposed to address the breach.

Processor will cooperate with Controller's investigation and regulatory reporting obligations.

3.7 Deletion or return of Personal Data (Article 28(3)(g))

At termination of the Services, Processor shall (at Controller's choice and as technically feasible):

- return Controller Personal Data; and/or
- delete Controller Personal Data,

subject to legal retention requirements and backup rotation cycles. Backup deletion occurs as backups expire under the retention schedule (e.g., 30 days), unless a longer retention is legally required.

3.8 Audits and information (Article 28(3)(h))

Processor shall make available to Controller information reasonably necessary to demonstrate compliance with this DPA and Article 28 obligations, and allow audits:

- on reasonable notice;
- during normal business hours;
- subject to confidentiality and security restrictions;
- limited to Processor systems relevant to the Services.

Where Controller requests on-site audits, Processor may propose reasonable alternatives (e.g., independent reports, security questionnaires, remote evidence) to minimise risk to other customers and platform integrity.

4. Controller Obligations

Controller shall:

- ensure it has lawful basis for processing and providing Personal Data to Processor;
- provide appropriate notices to Data Subjects;
- ensure its instructions are lawful;
- configure access controls appropriately;

- ensure Authorised Users follow least privilege and do not upload unnecessary patient identifiers;
- handle DSARs and regulatory engagement, with Processor assistance as described above.

5. International Transfers

5.1 Transfer mechanisms

Where processing involves Restricted Transfers, Processor shall ensure appropriate safeguards are implemented as described in **Annex D**, including:

- UK IDTA or UK Addendum to EU SCCs;
- EU SCCs where applicable;
- additional safeguards (encryption, minimisation, access restrictions).

5.2 Transfer risk assessment

Processor will support Controller's transfer risk assessment where required, by providing reasonable information on data location, subprocessors, and security controls.

6. Liability

Liability allocation and caps are governed by the main agreement / Order Form, except where prohibited by applicable law.

7. Order of precedence

> **If there is conflict between this DPA and the Terms, this DPA prevails for data protection matters.**

ANNEX A

Details of Processing

Article 28(3)

A1. Subject matter

Provision of the Remote-I Platform for workforce operations, compliance management, SOP acknowledgement, job lifecycle workflows, audit logging, and related support services.

A2. Duration

For the duration of the Services under the Order Form, plus post-termination retention as required for legal obligations and backup rotation.

A3. Nature of processing

Collection, recording, organisation, structuring, storage, consultation, use, disclosure by transmission, alignment / combination (where configured), restriction, and deletion.

A4. Purpose(s)

To:

- create and manage user accounts and role permissions;
- enable job creation, assignment, acceptance, completion, and handover;
- manage radiographer availability and compliance documentation;
- publish SOPs and record acknowledgement / sign-off;
- record incidents and reflections;
- generate audit trails and governance reports;
- deliver notifications via email / SMS where enabled;
- provide support and maintain platform security.

A5. Categories of data subjects

- Customer employees, contractors and staff who use the Platform (hospital users, administrators);
- Radiographers using the Platform;
- Workforce participants recorded in the Platform for scheduling / compliance purposes;
- (Not intended) patients — unless Controller chooses to input patient identifiers.

A6. Categories of personal data

May include:

- identity and contact data (name, email, phone);
- professional data (registration identifiers, qualifications, specialties);
- compliance documentation and metadata (right-to-work evidence, DBS evidence, insurance evidence, training evidence, expiry dates);
- availability and schedule preferences;

- job lifecycle records and notes;
- SOP acknowledgements (who / when / version);
- incident records and reflections;
- communications content (job chat messages where enabled);
- audit logs (user actions, timestamps, IP addresses, session identifiers).

A7. Special category data

Not intended. However, special category data may appear incidentally in free-text incident / reflection fields or attachments if Controller permits. Controller is responsible for lawful basis and minimisation; Processor supports security controls.

A8. Frequency of processing

Continuous, as required by platform usage, with automated logging and backup processes.

ANNEX B

Technical and Organisational Measures

Article 32 — risk-based security programme

Processor maintains a risk-based security programme aligned with healthcare governance expectations, including:

B1. Governance and policies

- documented information security policy framework;
- access control policy and MFA requirements;
- incident response procedures;
- change management and secure deployment practices.

B2. Access control and authentication

- role-based access control (RBAC);
- least-privilege role assignment;
- MFA support for privileged accounts;
- account verification (e.g., email verification);
- session security controls (timeouts, secure cookies where applicable).

B3. Encryption

- encryption in transit (TLS / HTTPS);
- secure mail transport (TLS where configured);
- secrets stored outside public web root and protected by restrictive file permissions;
- encryption at rest for backups and uploads may be implemented via hosting controls and/or optional customer-specific arrangements (where applicable).

B4. Logging and monitoring

- audit logging for key actions (job lifecycle, SOP sign-off, admin actions);
- security event logging (authentication attempts, privilege changes);
- controlled retention of logs;
- avoidance of unnecessary logging of sensitive content (e.g., SMS body) where feasible.

B5. Resilience and backups

- automated scheduled backups of databases and uploaded files;
- defined retention and rotation (e.g., 30 days);
- restore procedures tested periodically;
- backups stored outside public web root with restricted permissions.

B6. Vulnerability management

- patch management for server and application components;
- remediation prioritisation for critical vulnerabilities;
- dependency review and updates for third-party libraries.

B7. Secure development and change control

- controlled change process for production updates;
- code review and testing practices proportionate to risk;
- separation of configuration from code.

B8. Supplier security

- Subprocessor due diligence proportionate to risk;
- contractual obligations for confidentiality and data protection;
- review of Subprocessor security statements where available.

B9. Physical and environmental security

- hosting provider physical security controls apply where the Platform is hosted;
- access to infrastructure limited to authorised personnel.

B10. Data minimisation and privacy by design

- system designed to minimise patient data processing;
- role and workflow design to support governance and accountability.

ANNEX C

Subprocessors

Current / typical categories and change process

Processor maintains a list of Subprocessors used to deliver the Platform. The exact providers may vary by environment and Order Form. Controller is provided notice of changes and may object on legitimate grounds.

Current / typical categories

#	Category	Purpose	Location
1	Hosting and infrastructure provider (compute, storage, backups)	Hosting the Platform and Customer Data	Depends on hosting region selected; UK / EU preferred for NHS contexts
2	Email delivery provider (SMTP relay / transactional email)	Sending verification, workflow notifications, and service emails	Customer may configure their own SMTP in some deployments
3	SMS gateway provider (e.g., ClickSend)	Sending SMS notifications where enabled	May involve international routing depending on recipient geography

Subprocessor change process

- Processor shall provide reasonable prior notice of additions / replacements;
- Controller may object within a reasonable period (e.g., 10 business days) on legitimate grounds;
- if objection cannot be resolved, Controller may terminate affected services as set out in the main agreement.

ANNEX D

International Transfers

Mechanisms, safeguards and documentation

Where Controller Data is transferred outside the UK / EEA:

D1. Legal mechanisms

Processor will implement one or more of:

- UK adequacy regulations (where applicable);
- UK IDTA;
- UK Addendum to EU SCCs;
- EU SCCs for EU Personal Data (if applicable).

D2. Supplementary safeguards

Depending on the transfer risk profile, supplementary safeguards may include:

- minimisation of data transferred;
- encryption in transit and (where feasible) at rest;
- strict access controls and logging;
- contractual commitments on government access requests;
- incident notification requirements.

D3. Transfer documentation

Processor will provide Controller reasonable information to support:

- Transfer Risk Assessments (TRAs);
- DPIAs where required;
- NHS DSP Toolkit evidence requests.

End of Data Processing Agreement. For questions, contact compliance@remote-i.com.