CUSTOMER CONTRACT

Data Processing Agreement

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

DOCUMENT TYPE	Contract (Customer Agreement)
VERSION	1.1 · Effective 7 May 2026
SUPERSEDES	v1.0 · 12 December 2025
OWNER	Remote-I Ltd — Data Protection Lead
CLASSIFICATION	Customer-facing (subject to mutual NDA)
REVIEW CYCLE	Annual, after material processing change, or following relevant regulatory updates

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
Data Protection Lead: Remote-I Ltd — Data Protection Lead

V1.1 · EFFECTIVE 7 MAY 2026 · SUPERSEDES V1.0 (12 DECEMBER 2025)

> *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.*

1. Introduction

1.1 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.

1.2 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.

1.3 Subject matter, duration, nature and purpose

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

2. Processor Obligations (Article 28)

2.1 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.

2.2 Confidentiality

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

2.3 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).

2.4 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.

2.5 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.

2.6 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.

2.7 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 (30 days), unless a longer retention is legally required.

Detailed retention periods for Personal Data within the Platform are described in Processor's **Data Retention and Disposal Policy**, available to Controller on request, and summarised in the Processor's **Privacy Policy** at remote-i.com/privacy.

2.8 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.

3. 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.

4. International Transfers

4.1 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).

4.2 Transfer risk assessment

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

5. Liability

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

6. Order of precedence

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

7. Document Changelog

Version	Date	Changes
1.1	7 May 2026	Annex C revised to name specific Subprocessors (GoDaddy, ClickSend, Google, LinkedIn) with location, role, and transfer mechanism, replacing the v1.0 generic-category table. Cover page metadata corrected (document type changed to Contract; classification changed to Customer-facing; owner changed to Data Protection Lead). Contact field expanded to distinguish privacy and operational contacts. Section 2.7 updated to reference Data Retention and Disposal Policy and Privacy Policy. Aligned with Privacy Policy v1.1 (web-published 7 May 2026). No changes to substantive Article 28 obligations.
1.0	12 December 2025	Initial version. Article 28 framework established with Annexes A–D.

Changes pending in future revisions

The following items are scheduled for inclusion in future DPA revisions:

- **Annex B (Technical and Organisational Measures):** Will be reviewed and aligned with platform implementation status during the planned compliance review.
- **Section 2.8 (Audit rights):** Will be revisited if Customer profile shifts toward NHS DSPT-required deployments.

These pending updates will be communicated to Controllers under contract through the variation process.

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 in accordance with the Data Retention and Disposal Policy;
- 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 (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

Named providers, locations, and change process — Revised v1.1

Processor maintains a current list of Subprocessors used to deliver the Platform. Customers receive notice of material changes and may object on legitimate grounds within 10 business days, in accordance with the Subprocessor change process below.

Current Subprocessors

#	Subprocessor	Role	Data processed	Location	Transfer mechanism
1	**GoDaddy.com LLC**	Hosting infrastructure (compute, storage, daily backups)	All Customer Data (databases, file uploads, application logs, backups)	France (EU) — Strasbourg data centre	UK adequacy regulations / EU GDPR
2	**GoDaddy.com LLC** (mail relay)	Transactional email delivery	Email recipient address; subject and body of verification, notification, and workflow emails	France (EU)	UK adequacy regulations / EU GDPR
3	**ClickSend Pty Ltd**	SMS notification delivery (where enabled by Customer)	Recipient mobile number; SMS body content (notification text only)	Australia	UK IDTA / EU SCCs (2021 modules)
4	**Google LLC** (Google Analytics 4)	Aggregate website usage analytics (marketing website only — no Platform data)	Anonymised IP, browser type, device type, page-view events on remote-i.com	United States	UK Addendum to EU SCCs / EU SCCs
5	**Google LLC** (reCAPTCHA)	Bot and abuse protection on contact forms	IP address, browser fingerprinting signals on form submission	United States	UK Addendum to EU SCCs / EU SCCs
6	**LinkedIn Corporation**	Marketing campaign measurement (with consent)	Campaign engagement signals on remote-i.com (consent-gated)	United States / Ireland	UK Addendum to EU SCCs / EU SCCs

Notes on the subprocessor list

Customer Data scope — Only Subprocessors #1, #2, and #3 process Customer Data as defined in this DPA. Subprocessors #4, #5, and #6 are limited to the public marketing website (remote-i.com) and do not have access to Platform data, accounts, or Customer Data.

Customer-configurable — SMS notifications (Subprocessor #3) are enabled per-Customer. A Customer that does not enable SMS notifications has no Personal Data flow to ClickSend.

Mail relay disclosure — The current production setup uses GoDaddy's outbound mail relay as part of the hosting service. Processor reserves the right to migrate to a dedicated transactional email subprocessor under the change process below; Customers will receive notice.

Geographic preference — For NHS or UK public sector deployments, Processor will prioritise UK or EEA-located subprocessors where alternatives exist. Specific Order Form addenda may further restrict subprocessor choice.

Subprocessor change process

Processor will:

1. Provide written notice to Controller of any addition, replacement, or material change of Subprocessor at least **10 business days** before the change takes effect.
2. Notify via the email address designated by Controller for compliance matters, or via the Platform admin notification channel where configured.
3. Provide reasonable information to support Controller's transfer risk assessment, including the new Subprocessor's identity, location, role, and applicable transfer mechanism.

Controller may **object on legitimate grounds** within the 10-business-day notice period. If Processor and Controller cannot resolve the objection within a further 10 business days, Controller may terminate the affected Services as provided in the main agreement, with pro-rata refund of pre-paid fees for the unused period.

For routine maintenance changes that do not affect Subprocessor identity or data location, no notice is required.

Subprocessor due diligence

Before engaging or replacing a Subprocessor, Processor performs due diligence proportionate to the Subprocessor's data access scope, which may include:

- review of the Subprocessor's published security documentation and certifications (e.g., ISO 27001, SOC 2, Cyber Essentials);
- review of data location and applicable transfer mechanisms;
- contractual review for confidentiality, breach notification, and onward subprocessing obligations;
- where available, review of independent assurance reports.

Due diligence evidence is retained by Processor and may be made available to Controller on reasonable request, subject to confidentiality obligations.

Onward subprocessing

Subprocessors may engage their own sub-subprocessors. Where this occurs:

- the Subprocessor remains responsible to Processor for the acts and omissions of its sub-subprocessors;
- contractual obligations no less protective than this DPA flow down to sub-subprocessors;
- Processor will, on Controller's reasonable request, identify named sub-subprocessors of Tier 1 Subprocessors (those processing Customer Data) where the information is available.

Subprocessor offboarding

When a Subprocessor relationship ends:

- Processor revokes Subprocessor access to systems and credentials;
- Processor obtains written confirmation from the Subprocessor that Customer Data has been deleted or returned in accordance with the underlying contract;
- where deletion is delayed by backup rotation or legal holds, Processor documents the delay and confirms eventual deletion;
- Processor provides Controller with a written summary on request.

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 v1.1. For questions, contact compliance@remote-i.com.

REMOTE-I LTD · COMPANY NO. 15293974 · COMPLIANCE@REMOTE-I.COM