Remote–I

Data Protection Impact Assessment (DPIA) – Full

Document Type: Assessment

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

Owner: Remote-I Ltd – Data Protection Lead

Classification: Internal / Customer Assurance

Review Cycle: Annual and after material processing change

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. DPIA Overview

This Data Protection Impact Assessment (DPIA) evaluates privacy risks arising from operation of the Remote-I Platform and the processing of Personal Data in workforce governance workflows.

It is intended to support UK GDPR/GDPR accountability and procurement due diligence, and should be reviewed by each Customer (Controller) deployment.

2. Roles and Context

Controller (typically): the Customer (hospital/imaging organisation) for Customer Data processed in the Platform.

Processor: Remote-I Ltd for Customer Data under the Data Processing Agreement (DPA).

Remote-I is Controller for its own business administration data and certain security logs processed for legitimate interests (security and fraud prevention).

3. Description of Processing

The Platform processes workforce and operational data to:

- manage user identities and role access;
- create/manage jobs and lifecycle events;
- store compliance documents and expiry metadata;
- publish SOPs and capture acknowledgements/signatures;
- record incidents and reflections;
- maintain audit trails;
- send notifications (email/SMS) where enabled;
- maintain backups and restore capability.

The Platform is not intended to store patient-identifiable clinical data; Customers must minimise patient identifiers in free-text fields.

4. Data Categories and Data Subjects

Data subjects:

- Customer staff (administrators, managers);
- Radiographers and workforce members;
- (Not intended) patients—unless the Customer enters identifiers.

Personal data categories may include identity/contact data, professional credentials, compliance documentation, job records, SOP sign-offs, incidents/reflections, and audit/security logs.

5. Necessity and Proportionality

Necessity: Processing supports workforce governance, compliance assurance, and auditable job workflows.

Proportionality: Data minimisation is emphasised, with RBAC, audit logging, and retention controls to reduce risk exposure.

6. Data Flow (Narrative)

1) Customer admin creates jobs and SOP libraries.
2) Radiographers maintain profile and compliance documentation.
3) SOPs are accessed and signed; sign-offs are stored with timestamp and version.
4) Incidents are reported and stored with audit evidence.
5) Notifications are sent via configured channels.
6) Logs and audit events are stored for investigations and governance.
7) Automated backups run and are retained for defined periods.

7. Key Risks (Summary)

• Unauthorised access to compliance documents or workforce records;
• Over-collection or excessive retention;
• Accidental disclosure via exports/misconfigured access;
• Loss of availability due to outages/corruption;
• Credential compromise;
• International transfer risks via subprocessors.

8. Controls and Mitigations

Mitigations include RBAC, MFA for privileged roles, secure secret handling, audit logging/monitoring, incident response procedures, supplier governance and DPA controls, backup/restore and DR runbooks, retention schedule, change management, and patch management.

9. DPIA Risk Assessment Table

The table below summarises key risks, inherent risk, controls, and residual risk using a 1–5 likelihood/impact scoring model.

Risk ID	Risk	Inherent (L×I)	Key Controls	Residual
D-01	Unauthorised access via credential compromise	20	MFA; monitoring; least privilege; incident response	8
D-02	Misconfigured roles allow over-broad access	12	RBAC; access reviews; change control; audit logs	6
D-03	Incidental patient identifiers in free-text	15	Minimisation guidance; training; auditing; retention controls	9
D-04	Data loss due to corruption or deletion	10	Daily backups; restore tests; DRP	5
D-05	International transfer risk via providers	8	DPA; SCC/IDTA; supplier due diligence; minimisation	4
D-06	Excessive retention beyond necessity	8	Retention policy; periodic review; deletion controls	4
D-07	Disclosure via exports shared improperly	8	Role restrictions; audit logs; governance procedures	4

D-08	Service outage disrupts governance access	12	BCP/DRP; backups; supplier escalation	6

10. Consultation and Sign-off

Customer (Controller) should review and sign this DPIA per deployment (particularly if adding integrations or processing additional data categories).

Sign-off fields:

• Customer IG/Privacy Lead: _____ Date: _____

• Remote-I Data Protection Lead: _____ Date: _____

11. Residual Risk Decision

Residual risks are considered acceptable for pilot and early production deployments provided Customers enforce minimisation of patient identifiers, least privilege access, and agreed retention settings, and follow incident escalation procedures for suspected compromise.

12. Review Schedule

This DPIA is reviewed annually and after material changes to processing or platform architecture, and following major incidents or near misses.