

LEGAL

Technical & organisational measures

LAST UPDATED · 14 OCT 2026

Radiant Science UG acts as a processor, and in some engagements as a sub-processor, for healthcare providers. This document describes the technical and organisational measures we apply under Article 32 of the UK GDPR and EU GDPR, and serves as the description required by Annex II of the Standard Contractual Clauses.

It describes our measures at the level of the control, not the product. Further security documentation is available to controllers on request under the heading [Further information](#) below.

Data Hosting & Location

- Patient audio, transcripts and call records are processed and stored in the United Kingdom or the European Economic Area.
- The platform — databases, object storage, caches, secrets, message queues and application hosting — runs in Microsoft Azure's UK South region.
- Transfers from the United Kingdom to the EEA rely on the adequacy decision made under Article 45 of the UK GDPR.
- A limited set of business systems used to run the company, rather than to deliver the service, are operated by providers whose processing takes place outside the UK and EEA. These are named in our [subprocessors list](#) with the transfer mechanism relied on for each. They do not receive patient audio, transcripts or call records.
- Where personal data is transferred outside the UK or EEA, we rely on an appropriate transfer mechanism such as an adequacy decision, Standard Contractual Clauses, or the UK International Data Transfer Addendum, supported by a transfer risk assessment.

Encryption and Pseudonymisation

- Data in transit is encrypted using TLS 1.2 or higher.

- Data at rest on durable storage — databases, object storage and backups — is encrypted using AES-256.
- Encryption keys, application secrets and certificates are held in a managed key management service with restricted access, soft delete and purge protection.
- At the end of a call's retention period the recording is deleted, and the transcript and call record are anonymised so that they can no longer be linked to an individual. The identifiable originals are then deleted.

Access Control

- Access to personal data is restricted to authorised personnel and granted only for a documented business purpose.
- Multi-factor authentication is required for administrative and remote access to systems holding personal data.
- Access to production systems, which are segregated from day-to-day working environments, requires an additional hardware-backed authentication factor and is limited to a small number of named individuals recorded in our access register.
- Administrative tasks use accounts separate from routine work, and privileged access is granted as a time-bound elevation scoped to the task rather than as standing permission.
- Accounts are individually named. Credentials are never shared between users.
- New accounts are created with minimal rights under a dual-approval process and require multi-factor authentication before any access is granted.
- Access rights are reviewed periodically and at least annually, on any role change, and immediately when a person leaves or the business need ends.

Customer Access to the Service

- Access to the dashboard requires multi-factor authentication.
- Where a password is used, a minimum length is enforced with no maximum, and common or breached passwords are blocked.
- Repeated failed authentication attempts are throttled or locked out.
- Each clinic's data is segregated, and access is scoped to the organisation the user belongs to.

Leavers and Credential Handling

- When a person leaves, we disable their identity and accounts at or before their confirmed leaving time, revoke active sessions, tokens, certificates, authentication factors and recovery methods, remove role memberships, and recover or remotely restrict company devices.

- Credentials and keys the person could reach are rotated where exposure is possible.
- Completion is recorded and independently checked against the access register.
- Where a credential is known or suspected to be compromised, we disable the account, revoke sessions and recovery tokens, rotate affected secrets, review the relevant audit logs to establish cause and extent, and restore access only after containment and verification.

Endpoint and Network Security

- Organisational data is accessed only from company-provided, centrally managed devices. Personal and unmanaged devices are not used.
- Managed devices enforce disk encryption, screen lock with a biometric or passphrase, host firewall, malware protection with automatic updates and malicious-site blocking, and disabled automatic execution of downloaded files.
- Remote access to organisational data over networks we do not control is made through an authenticated, encrypted channel, which is mandatory on work devices.
- Production services require authentication and authorisation on every request, and are reachable only through managed service endpoints with access-control rules applied. Inbound exposure requires a documented business need, named approval and periodic review. Webhook endpoints validate provider signatures or tokens.
- Processing takes place in certified third-party data centres operated by our cloud provider. Radiant operates no server rooms or physical processing locations of its own, and personal data is not held on removable media.

Patching and Software Management

- Only vendor-supported operating systems and software receiving regular security updates are used.
- Security updates are applied on a risk-prioritised basis, with high-risk and critical vulnerabilities prioritised for prompt remediation. Automatic updates are enabled where the platform supports them.
- Application dependencies are monitored and updated through automated dependency scanning.
- Underlying platform and server operating systems are maintained by our cloud provider under its managed service model.

Testing and Evaluation of Measures

- Application dependencies are scanned automatically and vulnerabilities are triaged on a risk-prioritised basis.
- Infrastructure changes are peer-reviewed before deployment.

- The effectiveness of these measures is reviewed at least annually and on any material change to the service.

Infrastructure Management

- All cloud infrastructure is defined and deployed as code, so every configuration change is version-controlled, peer-reviewed and auditable.
- Production and non-production environments are separated. Non-production environments do not contain patient data.
- Cloud resources are removed or disabled when their business purpose ends.

Subprocessor Management

- All subprocessors are listed at www.radiantscience.io/subprocessors, with the purpose of processing and the processing region for each.
- Each subprocessor is bound by a written agreement imposing obligations equivalent to those we owe our customers, including the obligation to assist the controller.
- Before a subprocessor may process patient or other customer personal data, we confirm its data processing agreement, transfer mechanism, processing location, retention settings and training settings.
- Each subprocessor is configured to the shortest data retention it offers for the services we use, and is contractually prohibited from using customer personal data to train or improve its models. We keep a record of these settings for each provider.
- We notify customers of additions to and replacements of subprocessors in advance of the change taking effect.

Data Minimisation and Retention

- We collect and process only the data needed to handle the call and produce the call record for the clinic.
- Call content — the recording, transcript, call record, details collected, messages and forms sent because of the call, and internal session data — is kept for the duration of the service by default. A clinic may instead choose a shorter retention period of 30, 90, 180 or 365 days after each call ends. One period applies to all content of a call.
- At the end of a call's retention period, an automated job deletes the recording, anonymises the transcript and call record, and deletes the identifiable originals. Call content cannot be retrieved after that point.

- A clinic may request deletion of an individual call. The call is withheld from the clinic's users at once and its content is permanently deleted within 30 days.
- Patient records and caller phone numbers are kept for the duration of the service, unless deleted earlier on the clinic's instruction. Data subject erasure requests are completed within 14 days.
- On termination, a clinic may request an export of its data within the period set out in our Terms of Service. The export is prepared when the service ends and remains available until deletion. All remaining personal data is securely deleted within 30 days of the end of the service, and we confirm the deletion in writing within 52 days.
- Database backups are retained on a rolling 7-day cycle within the United Kingdom, and storage-level recovery copies of recordings for at most 7 days, so data deleted under the rules above can persist in a copy for up to 7 further days before ageing out.
- Operational logs and application telemetry are designed to exclude call content.
- Audit records of access and system events contain no call content and are kept as our own security and accountability records.
- Incident records and personal data breach documentation are kept for 6 years after the incident is closed.

Model Training

Radiant does not use customer personal data, including patient audio, transcripts or call records, to train, fine-tune or otherwise improve any model, and our subprocessors are contractually prohibited from doing so. Anonymised call records, which can no longer be linked to an individual, are used only to evaluate and maintain the quality of the service. Agent development and testing use synthetic callers, with test scenarios that may be derived from anonymised call records.

Security Monitoring & Incident Response

- Infrastructure is continuously monitored, with alerting configured for anomalous and suspicious activity.
- Audit logs are reviewed periodically.
- We maintain a documented breach response process. Data controllers are notified without undue delay and no later than 48 hours after we become aware of a personal data breach, with the information needed to meet their own notification obligations, and are updated as further information becomes available. The controller informs affected patients and the supervisory authority where required.

Audit Logging

Access to personal data and significant system events are logged. Logs are centrally aggregated and access-controlled. Audit records hold who did what and when, without call content.

Staff Awareness and Confidentiality

- Staff review our security and data protection policies at induction and complete training covering safe credential handling.
- Confidentiality undertakings are required at onboarding, and personnel process personal data only on documented instructions.
- Access is limited to job function and business need.

Business Continuity and Recovery

- Encrypted backups are taken regularly and stored in the United Kingdom.
- Object storage is geo-redundant within the United Kingdom.
- Restore procedures are tested periodically.

Data Subject Rights

We support the Controller in fulfilling data subject rights under UK GDPR, including access, correction, and deletion. Erasure requests are forwarded to the Controller, who may object within 7 days, and are completed within 14 days. Anonymised records are outside the scope of these requests because they can no longer be linked to an individual.

No Automated Decision Making

Radiant Science does not perform any automated decision-making producing legal or similarly significant effects. Our AI-assisted systems support administrative workflows, such as processing voice input, structuring clinical notes, or assisting with communication. These tools do not make clinical decisions or offer diagnostic conclusions. All outputs are intended to assist healthcare professionals and are subject to review by authorised users.

Certifications and Assurance

- We are registered with the Information Commissioner's Office under reference number ZB842255.
- We hold Cyber Essentials certification for Radiant Science UG. Our current certificate and its scope are available on request.
- We have completed the NHS Data Security and Protection Toolkit self-assessment. Our published status is available through the Toolkit's organisation search.

Further information

Further security documentation — including certification evidence, penetration test summaries, our information security policy set, and completed security questionnaires — is made available to controllers on written request under Article 28(3)(h) UK GDPR, subject to a non-disclosure agreement, normally within ten business days. Requests should be sent to support@radiantscience.io.

We may update these measures from time to time to reflect changes in technology and practice, provided that any update does not materially decrease the overall level of security of the service. Material changes are notified to customers.

Information Governance Contact

For privacy or data protection inquiries, contact our Data Protection Officer:

Felix Geilert Email: info@radiantscience.io