THINKSONO GUIDANCE

GDPR Compliance Statement

Document owner	Dignesh Shah [Data Protection Officer / Regulatory Lead]
Effective date	10 Sep 2026
Last reviewed	10 Sep 2026
Version	v1.0
Applies to	ThinkSono Guidance and associated ThinkSono services

1. Introduction

ThinkSono ("ThinkSono," "we," "us," or "our") is committed to protecting the privacy and security of personal data, including special category health data, processed in connection with ThinkSono Guidance and our related software and AI-assisted diagnostic support services (the "Services").

This Statement explains how we comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable, the EU General Data Protection Regulation (Regulation (EU) 2016/679) (together, "GDPR") in relation to personal data we process as a data controller and, where relevant, as a data processor acting on behalf of healthcare provider customers.

This Statement is intended for customers, healthcare partners, and other stakeholders who wish to understand our approach to data protection. It supplements, and does not replace, our full Privacy Policy and any Data Processing Agreement (DPA) entered into with individual customers.

2. Scope and Roles

Depending on the context in which personal data is processed, ThinkSono may act as either a data controller or a data processor:

- Data Controller: where ThinkSono determines the purposes and means of processing, such as for account administration, product improvement, and business operations.
- Data Processor: where ThinkSono processes patient data on behalf of a healthcare provider customer strictly in accordance with that customer's documented instructions, as set out in a Data Processing Agreement.

Where ThinkSono acts as a processor, the healthcare provider customer remains the data controller responsible for the underlying legal basis for processing patient data, and for informing patients accordingly.

3. Data Controller and Data Protection Officer

Legal entity	ThinkSono Ltd.
Company number	10470929

Registered office	33 Flowers Avenue, Ruislip, England, HA4 8GA
ICO registration (UK only)	ZB722842
Data Protection Officers	Dignesh Shah, Sven Mischkewitz
Data protection contact	dignesh@thinksono.com, sven@thinksono.com

4. Categories of Personal Data We Process

The personal data processed through the Services may include:

- Patient health data: ultrasound imaging data, AI-generated diagnostic outputs and annotations, and associated clinical metadata relevant to deep vein thrombosis (DVT) assessment.
- Healthcare professional account data: names, professional credentials, institutional affiliation, and login/usage data of clinicians and sonographers using the Services.
- Customer administration data: names, job titles, and contact details of individuals at healthcare provider organizations who administer or procure the Services.
- Technical and usage data: device identifiers, IP addresses, log files, and diagnostic/performance telemetry generated by use of the software.

Patient health data constitutes “special category data” under Article 9 GDPR and is subject to enhanced protections as described in this Statement.

5. Legal Basis for Processing

Where ThinkSono acts as a data controller, we rely on one or more of the following legal bases, as applicable to the specific processing activity:

- Performance of a contract (Art. 6(1)(b)) — to provide the Services to our customers.
- Legal obligation (Art. 6(1)(c)) — to comply with medical device regulatory, quality, and vigilance obligations, including UK MDR, EU MDR, and FDA requirements.
- Legitimate interests (Art. 6(1)(f)) — for product improvement, security monitoring, and fraud prevention, balanced against data subjects' rights.
- Consent (Art. 6(1)(a)) — where required for specific processing activities, such as marketing communications.

Where special category health data is processed, we additionally rely on Article 9(2)(h) GDPR (provision of health or social care/medicine) or Article 9(2)(i) (public health), or explicit consent where required, consistent with the arrangements set out in the applicable Data Processing Agreement with the healthcare provider customer.

6. Purposes of Processing

- Providing AI-assisted ultrasound image analysis and diagnostic support (ThinkSono Guidance).
- Maintaining, securing, and improving the safety, accuracy, and performance of our software, including algorithm validation and retraining under our Predetermined Change Control Plan (PCCP).

- Complying with medical device vigilance, quality management system (QMSR/ISO 13485), and post-market surveillance obligations.
- Managing customer accounts, billing, and support.
- Ensuring the security and integrity of our systems, including detection and prevention of unauthorized access.

7. Your Rights as a Data Subject

Subject to applicable exemptions, individuals whose personal data we process have the right to:

- Access a copy of their personal data (Art. 15).
- Request rectification of inaccurate or incomplete data (Art. 16).
- Request erasure of their data in certain circumstances (Art. 17).
- Request restriction of processing (Art. 18).
- Request data portability (Art. 20).
- Object to processing based on legitimate interests (Art. 21).
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects, without appropriate human oversight (Art. 22).

Because ThinkSono Guidance provides AI-assisted analysis intended to support, not replace, clinical judgment, a qualified healthcare professional must review all diagnostically significant outputs before any decision affecting patient care.

Where ThinkSono acts as a data processor for patient data, requests to exercise these rights should generally be directed to the relevant healthcare provider (data controller) first. We will support our customers in fulfilling such requests as required under the applicable Data Processing Agreement.

8. International Data Transfers

We primarily process and store personal data electronically within the United Kingdom and/or the European Economic Area.

- Where we transfer personal data outside the UK/EEA, we ensure an adequate level of protection through appropriate safeguards.

Details of specific international transfers and the safeguards applied are available on request from our data protection contact.

9. Data Retention

- We retain patient health data for the period specified in the applicable customer Data Processing Agreement and in accordance with applicable clinical record-keeping and medical device regulatory requirements, currently: [retention period, e.g., 15 years from last processing activity].
- We retain account and administrative data for the duration of the customer relationship plus 15 years to meet legal, accounting, and regulatory obligations.

Data is securely deleted or anonymized once it is no longer required for the purposes for which it was collected, unless a longer retention period is required by law.

10. Security Measures

We implement technical and organizational measures appropriate to the risk, including:

- Encryption of personal data in transit and at rest.
- Role-based access controls and authentication requirements for all systems processing personal data.
- Secure software development practices aligned with our FDA, EU and UK MHRA cybersecurity obligations, including secure product development lifecycle controls.
- Regular security testing, vulnerability management, and a Coordinated Vulnerability Disclosure process.
- Staff training on data protection and information security obligations.

11. Data Sharing and Sub-processors

We do not sell personal data. We may share personal data with:

- Sub-processors engaged to support the Services (e.g., cloud hosting providers), each bound by a written data processing agreement imposing GDPR-equivalent obligations.
- Regulatory authorities, where required to comply with medical device vigilance or legal obligations.
- Professional advisers, where necessary for the establishment, exercise, or defence of legal claims.

12. Personal Data Breach Notification

In the event of a personal data breach affecting personal data for which ThinkSono is the controller, we will notify the relevant supervisory authority without undue delay and, where required, within 72 hours of becoming aware of the breach, and will inform affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

Where ThinkSono acts as a processor, we will notify the relevant healthcare provider customer without undue delay upon becoming aware of a personal data breach, to enable the customer to meet its own notification obligations as data controller.

13. Your Right to Complain

If you have concerns about how we process your personal data, we encourage you to contact us first using the details in Section 3 so we can try to resolve the matter directly.

You also have the right to lodge a complaint with a supervisory authority. In the United Kingdom, this is the Information Commissioner's Office (ICO), ico.org.uk. If you are located in the European Economic Area, you may lodge a complaint with your local data protection supervisory authority.

14. Updates to This Statement

We may update this Statement from time to time to reflect changes in our practices, technology, legal requirements, or other factors. The “Last reviewed” date at the top of this document indicates when it was last updated. We will communicate material changes to customers in accordance with the terms of their agreement with ThinkSono.

15. Contact Us

For questions about this Statement or our data protection practices, please contact:

Email	dignesh@thinksono.com
Postal address	33 Flowers Avenue, Ruislip, England, HA4 8GA