DATA PROCESSING AGREEMENT

Under Article 28 of the UK General Data Protection Regulation
and the EU General Data Protection Regulation

Between

The Controller (Data Controller)

and

Therasee (Data Processor)

Last updated: 4 November 2026

1. Definitions and Interpretation

1.1 In this Agreement, unless the context requires otherwise, the following terms shall have the meanings set out below:

“Agreement” means this Data Processing Agreement, including any schedules and annexes attached to it.

“Controller” means the sole practitioner, partnership, company, charity, or other organisation that holds an account with Therasee and determines the purposes and means of the processing of personal data of its clients and other data subjects under this Agreement.

“Clinical Executor” means a person named by the Controller in a clinical will set up in the Services to act for the Controller if the Controller dies or cannot continue to practise.

“Data Subject” means an identified or identifiable natural person whose personal data is processed under this Agreement.

“EEA” means the European Economic Area.

“Personal Data” means any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Services, as further described in Schedule 1.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

“Processing” (and related terms such as Process and Processed) means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

“Processor” means Therasee, the entity that processes Personal Data on behalf of the Controller in connection with the Services.

“Services” means the practice management platform and related services provided by Therasee to the Controller, as described in clause 2.

“Special Category Data” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, data concerning health, or data concerning a natural person’s sex life or sexual orientation, as defined in Article 9 of UK GDPR and Article 9 of EU GDPR.

“Sub-processor” means any third party appointed by the Processor (or by any Sub-processor of the Processor) to process Personal Data on behalf of the Controller in connection with this Agreement.

“Supervisory Authority” means the Information Commissioner’s Office (ICO) or any successor body responsible for the supervision of data protection matters in the United Kingdom, and where applicable, any competent data protection supervisory authority in the European Union established pursuant to Article 51 of EU GDPR.

“UK GDPR” means the UK General Data Protection Regulation, being the retained EU law version of the General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (as amended), together with the Data Protection Act 2018.

Confidential

“EU GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as applicable to the processing of personal data within the European Union.

“Applicable Data Protection Law” means UK GDPR, EU GDPR, and any other applicable data protection legislation in force from time to time in the United Kingdom and the European Union, including the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003.

1.2 Words in the singular include the plural and vice versa. A reference to a statute or statutory provision includes any subordinate legislation made under it and any modification or re-enactment of it.

2. Scope and Purpose of Processing

2.1 This Agreement sets out the terms on which the Processor shall process Personal Data on behalf of the Controller in connection with the provision of the Services.

2.2 The Processor provides a practice management platform designed for mental health practitioners, including therapists, counsellors and psychologists. The Services include:

- Storage and management of client records, including clinical and demographic information.
- Session scheduling and calendar management.
- Secure messaging between the Controller and their clients.
- Automated appointment reminders and service notifications sent by email and SMS.
- Form creation, storage, and completion, including AI-assisted form generation and document-to-form conversion.
- Billing and payment processing through integrated payment providers.
- Video session facilitation through integrated video conferencing.
- Clinical will: recording the Controller’s nominated Clinical Executors and instructions, and giving those Clinical Executors access to the Controller’s records if the Controller cannot continue to practise.
- Optional integrations with third-party calendars (such as Google Calendar and Microsoft Outlook), video meeting services (such as Zoom and Google Meet) and other services at the Controller’s discretion. Where calendar or video meeting integration is used, only minimal data is shared, including appointment times and client initials only.

2.3 The nature, purpose, duration, types of Personal Data, and categories of Data Subjects are further described in Schedule 1.

2.4 The Processor shall process Personal Data only for the purposes of providing the Services to the Controller and as set out in this Agreement. The Processor shall not process Personal Data for any other purpose unless required to do so by applicable law, in which case the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such notification. In particular, the Processor shall not use Personal Data to test or develop the Services, and shall not use it to train any artificial intelligence model.

2.5 For the avoidance of doubt, this Agreement applies only to Personal Data that the Processor processes on behalf of the Controller in connection with the Services. Therasee acts as an independent controller in respect of certain limited personal data relating to the Controller, including account and billing information, support correspondence, and product usage analytics. Such processing is described

in the Therasee Privacy Policy and is not governed by this Agreement.

3. Obligations of the Controller

3.1 The Controller warrants and represents that:

- It has a lawful basis under Applicable Data Protection Law for the processing of Personal Data and Special Category Data, including an appropriate Article 9 condition for the processing of health and mental health data.
- It has provided appropriate privacy notices to Data Subjects informing them of the processing of their data by the Processor and any Sub-processors.
- It shall comply with its obligations under Applicable Data Protection Law in respect of the Personal Data processed under this Agreement.
- It shall ensure that any instructions it gives to the Processor in respect of the processing of Personal Data comply with Applicable Data Protection Law.
- Where it uses AI-assisted features, it is recommended as a matter of best practice to use blank or template versions of documents when uploading for conversion, in accordance with the principle of data minimisation. The Processor has measures in place to mask client data variables and to ensure that data processed by the AI service is not retained beyond the individual request.

4. Obligations of the Processor

Processing Instructions

4.1 The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by Applicable Data Protection Law. The Processor shall promptly inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes Applicable Data Protection Law.

Clinical Executors

4.1A Where the Controller sets up a clinical will in the Services, the Controller instructs the Processor to give each Clinical Executor named in it access to the areas of the Services the Controller has chosen. This covers access started by the Controller and access released by the Processor's support team where the Controller cannot act, after the checks described to the Controller in the Services. This instruction continues to apply if the Controller dies or loses capacity, until the access is ended. The Controller is responsible for having a lawful basis for this disclosure, for making sure each Clinical Executor it names is bound by a duty of confidentiality, and for telling its clients, in its own privacy notice, that a named Clinical Executor may contact them and see their records if the Controller cannot continue to practise.

Confidentiality

4.2 The Processor shall ensure that all persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This obligation shall continue after the termination of this Agreement and any individual's engagement with the Processor.

Security Measures

4.3 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation,

and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. These measures shall include, as appropriate and as further described in Schedule 2:

- Encryption of Personal Data in transit and at rest.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Access controls and authentication mechanisms to ensure that Personal Data is accessible only to authorised personnel.
- Audit logging of access to and modifications of Personal Data.

4.4 In assessing the appropriate level of security, the Processor shall take account of the risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, and shall have particular regard to the sensitive nature of health and mental health data processed in connection with the Services.

Sub-processors

4.5 The Controller hereby provides general written authorisation for the Processor to engage Sub-processors for the processing of Personal Data in connection with the Services, subject to the conditions set out in this clause.

4.6 The Processor shall maintain a list of Sub-processors engaged in connection with the Services, as set out in Schedule 3. The Processor shall make this list available to the Controller upon request and shall keep it up to date.

4.7 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller the opportunity to object to such changes before the change takes effect. The Processor shall provide at least 30 days' notice before engaging any new Sub-processor or making any change that materially alters the location of, or the level of protection applied to, Personal Data. Where the Processor reallocates processing activities between Sub-processors already listed in Schedule 3, without materially changing the location of or level of protection applied to Personal Data, it may do so on shorter notice, and shall update Schedule 3 and notify the Controller accordingly. If the Controller objects to any change on reasonable grounds relating to data protection, the parties shall discuss the matter in good faith. If the parties cannot resolve the objection, the Controller may terminate this Agreement on written notice.

4.8 Where the Processor engages a Sub-processor, the Processor shall impose on the Sub-processor, by way of a contract or other legal act, the same data protection obligations as are set out in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The Processor shall remain fully liable to the Controller for the performance of any Sub-processor's obligations.

Data Subject Rights

4.9 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under Chapter III

of UK GDPR and Chapter III of EU GDPR, including rights of access, rectification, erasure, restriction, data portability, and the right to object.

4.10 The Processor shall promptly notify the Controller if it receives a request from a Data Subject in respect of their Personal Data. The Processor shall not respond to such a request itself unless authorised to do so by the Controller or required by applicable law.

Data Protection Impact Assessments

4.11 The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments (DPIAs) and, where necessary, prior consultations with the Supervisory Authority, in each case solely in relation to the processing of Personal Data under this Agreement and taking into account the nature of the processing and the information available to the Processor.

Personal Data Breaches

4.12 The Processor shall notify the Controller without undue delay, and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Personal Data processed under this Agreement. Such notification shall:

- Describe the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned.
- Communicate the name and contact details of the Processor's data protection point of contact.
- Describe the likely consequences of the Personal Data Breach.
- Describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.13 The Processor shall co-operate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of each Personal Data Breach.

Deletion and Return of Data

4.14 On termination of this Agreement, or at the Controller's written request, the Processor shall, at the choice of the Controller, delete or return all Personal Data to the Controller and delete existing copies, unless applicable law requires storage of the Personal Data. The Processor shall provide the Controller with a reasonable period following termination to export their data from the platform before deletion occurs, in accordance with the timescales set out in Schedule 4.

4.15 Where the Controller requests deletion, the Processor shall confirm in writing that all Personal Data has been deleted, except where retention is required by applicable law.

Compliance and Cooperation

4.16 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of UK GDPR and Article 28 of EU GDPR and this Agreement, and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

4.17 The Processor shall immediately inform the Controller if, in its opinion, an instruction from the Controller infringes Applicable Data Protection Law.

5. International Transfers of Personal Data

5.1 The Processor shall not transfer Personal Data to any country outside the United Kingdom or the European Economic Area without appropriate safeguards being in place in accordance with Chapter V of UK GDPR and Chapter V of EU GDPR, as applicable.

5.2 Personal Data is stored and processed within the United Kingdom, including the Processor's own infrastructure and AI-assisted processing. Where a Sub-processor processes Personal Data outside the UK, the following safeguards apply:

Transfers to the European Union

5.3 Certain Sub-processors listed in Schedule 3 may process Personal Data in the European Union, for example Jitsi as a Service where it is used for a video session, and certain processing by Stripe. The EU has been recognised as providing an adequate level of data protection under the UK's Data Protection (Adequacy) (EU and EEA EFTA States) Regulations. Accordingly, transfers of Personal Data from the UK to the EU do not require additional transfer mechanisms such as Standard Contractual Clauses.

5.3A Where Personal Data is processed within the European Union, such processing is subject to EU GDPR. The Processor ensures that its Sub-processors operating within the EU comply with EU GDPR, including through each Sub-processor's data processing terms, such as the Google Cloud Data Processing Addendum (CDPA), which addresses obligations under both UK GDPR and EU GDPR.

Transfers to Other Jurisdictions

5.4 Where Sub-processors process Personal Data outside the UK and the EEA, the Processor shall ensure that appropriate transfer mechanisms are in place, including Standard Contractual Clauses approved by the ICO (International Data Transfer Agreement or Addendum to the EU SCCs) or the European Commission, or reliance on an adequacy decision by the Secretary of State or the European Commission, as applicable.

5.5 Details of the locations and transfer mechanisms for each Sub-processor are set out in Schedule 3.

6. Audit Rights

6.1 The Controller shall have the right to audit and inspect the Processor's compliance with this Agreement and Applicable Data Protection Law. The Controller may exercise this right directly or through a mandated third-party auditor, provided that such auditor is bound by appropriate confidentiality obligations.

6.2 The Controller shall give the Processor at least 30 days' written notice of any audit or inspection, unless an audit is required due to a Personal Data Breach or a request from the Supervisory Authority, in which case reasonable notice shall be given.

6.3 Audits shall be conducted during normal business hours and shall not unreasonably interfere with the Processor's business operations. The Controller shall bear its own costs in connection with any audit.

6.4 The Processor shall co-operate fully with any audit or inspection and shall provide the Controller with access to relevant records, systems, and personnel as reasonably required.

6.5 Where the Processor engages an independent third party to conduct security audits or certifications (such as SOC 2 or ISO 27001), the Processor may make the results of such audits available to the Controller in lieu of a direct audit, provided the Controller considers the scope and results sufficient for its purposes.

Confidential

7. Liability and Indemnification

7.1 Each party shall be liable for damage caused by processing that infringes Applicable Data Protection Law in accordance with Article 82 of UK GDPR and Article 82 of EU GDPR, as applicable.

7.2 The Processor shall indemnify and hold harmless the Controller against all claims, actions, third-party claims, losses, damages, and expenses incurred by the Controller that arise out of or are related to the Processor's breach of this Agreement or its obligations under Applicable Data Protection Law, to the extent that the Processor is at fault.

7.3 The Controller shall indemnify and hold harmless the Processor against all claims, actions, third-party claims, losses, damages, and expenses incurred by the Processor that arise out of or are related to the Controller's breach of this Agreement, its instructions to the Processor, or its obligations under Applicable Data Protection Law, to the extent that the Controller is at fault.

7.4 Nothing in this Agreement shall limit or exclude either party's liability for fraud, death, or personal injury caused by negligence, or any other liability that cannot be limited or excluded by applicable law.

7.5 Subject to clause 7.4, the total aggregate liability of either party under or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by the Controller to the Processor under the applicable service agreement in the 12-month period immediately preceding the event giving rise to the claim.

8. Term and Termination

8.1 This Agreement is incorporated into the Therasee Terms of Service and shall come into effect on the date the Controller first uses the Services. It shall continue in force for as long as the Processor processes Personal Data on behalf of the Controller.

8.2 Subject to clause 8.5, this Agreement shall automatically terminate when the Controller's use of the Services ends and all Personal Data has been deleted or returned in accordance with clause 4.14.

8.3 Either party may terminate this Agreement immediately by written notice if the other party commits a material breach of this Agreement and, where such breach is capable of remedy, fails to remedy it within 30 days of receiving written notice of the breach.

8.4 Clauses 4.2 (Confidentiality), 4.14 and 4.15 (Deletion and Return of Data), 6 (Audit Rights), 7 (Liability and Indemnification), and 9 (General Provisions) shall survive termination of this Agreement.

8.5 Where access has been given to a Clinical Executor under clause 4.1A, this Agreement stays in force, and the Processor will not close or delete the account, for 90 days from the date that access is given. The Processor will extend this by a further 90 days if asked. Deletion under Schedule 4 starts once the access ends.

9. General Provisions

9.1 This Agreement, together with the schedules annexed to it, forms part of the Therasee Terms of Service and constitutes the entire agreement between the parties with respect to the processing of Personal Data, superseding all prior agreements, representations, and understandings on that subject. In the event of any conflict or inconsistency between this Agreement and the Terms of Service in relation to the processing of Personal Data, this Agreement shall prevail.

Confidential

9.2 This Agreement may be amended by written agreement signed by both parties, or by the Processor in accordance with the following:

(a) Material changes. Where the Processor makes a change to this Agreement that materially reduces the protections afforded to the Controller or its data subjects, or that materially expands the scope or purposes of processing, the Processor shall give the Controller at least 30 days' notice before the change takes effect. Where the Controller objects on reasonable grounds relating to data protection, the parties shall discuss the matter in good faith, and if the objection cannot be resolved, the Controller may terminate this Agreement on written notice.

(b) Non-material changes. Other changes, including clarifications, corrections, updates to contact details, additions to the technical and organisational measures, and changes that do not reduce the protections afforded to the Controller or its data subjects, may be made by the Processor and shall take effect upon publication of the updated Agreement.

(c) Changes required by law, for security, or for continuity of service. Where a change is required in order to comply with Applicable Data Protection Law, a binding direction of a Supervisory Authority or other competent authority, to address a security risk, or to maintain or restore the reliability, availability, or continuity of the Services, the Processor may make the change with immediate effect or on shorter notice as the circumstances require, provided that such change does not materially reduce the protections afforded to the Controller or its data subjects or move Personal Data outside the United Kingdom or the European Economic Area. The Processor shall notify the Controller as soon as reasonably practicable.

9.3 If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

9.4 This Agreement shall be governed by and construed in accordance with the laws of England and Wales. The parties submit to the exclusive jurisdiction of the courts of England and Wales.

9.5 Notices under this Agreement shall be sent to the contact details provided by each party. Notices to the Processor shall be sent to privacy@therasee.com or to Therasee Ltd, 1 St. Andrews Road, Studio 8, Montpelier, Bristol, BS6 5EH.

SCHEDULE 1

Details of Processing

Nature and Purpose of Processing

The Processor processes Personal Data for the purpose of providing a practice management platform to mental health practitioners. Processing activities include the storage, organisation, retrieval, and management of client records; facilitation of secure messaging and video sessions; scheduling; delivery of automated appointment reminders and service notifications by email and SMS; billing and payment processing; form creation and management (including AI-assisted form generation and document conversion); the clinical will, including recording the Controller's nominated Clinical Executors and giving them access where the Controller cannot continue to practise; and related administrative functions.

Duration of Processing

Processing shall continue for the duration of the Controller's use of the Services. On termination, data shall be retained in accordance with the Processor's retention policy and deleted in accordance with clause 4.14.

Confidential

Types of Personal Data

The following types of Personal Data may be processed:

- Full name and title.
- Contact details (email address, telephone number, postal address).
- Date of birth.
- Gender and pronouns.
- GP and referrer details (name, practice, contact information).
- Emergency contact details (name, relationship, telephone number).
- Medical and mental health information, including diagnoses, treatment history, medication, and presenting issues. This constitutes Special Category Data under Article 9 of UK GDPR and EU GDPR.
- Session notes and clinical records.
- Form responses and assessment results.
- Voice and audio data, where the practitioner or client uses speech-to-text features.
- Technical data, including IP address, device and browser information, and authentication and audit log records.
- Any personal data, including Special Category Data, contained in documents or files uploaded to the platform by the Controller or their clients.
- Billing information (name, address; payment card details are processed by Stripe and not stored by the Processor).
- Communication records (secure messages between practitioner and client, and email and SMS notifications sent to clients on the Controller's behalf).
- Scheduling information (appointment dates, times, and types).
- Clinical will details: the name, contact details (email address, mobile number, postal address) and relationship to the Controller of each Clinical Executor and of the person the Controller names to tell them; the Controller's professional body memberships and membership numbers, insurer and policy number; and the Controller's written instructions, including where records and access details are kept.
- Signatures of the Controller and of Clinical Executors, stored as images.
- Documents the Controller uploads with a clinical will, such as an existing will.
- Records of a Clinical Executor's access, including clients marked as contacted and a log of actions taken.

Categories of Data Subjects

The following categories of Data Subjects are affected by the processing:

- Clients and patients of the Controller.
- Emergency contacts nominated by clients.
- GPs, referrers, and other healthcare professionals associated with client care.
- Clinical Executors nominated by the Controller.
- The person the Controller names to tell a Clinical Executor.
- The Controller, as an individual, where a clinical will holds their own details.

Clients may include children and vulnerable adults. The Controller is responsible for ensuring that any additional safeguards or conditions required under Applicable Data Protection Law for the processing of such data are met.

SCHEDULE 2

Technical and Organisational Security Measures

The Processor implements the following technical and organisational measures to protect Personal Data:

Encryption

- All data in transit is encrypted using TLS 1.2 or higher.
- All data at rest is encrypted using AES-256 or equivalent industry-standard encryption.
- Database connections use encrypted channels.

Access Controls

- Role-based access controls ensure that practitioners can only access their own client data.
- Administrative access to production systems is restricted to authorised personnel and requires multi-factor authentication.
- Principle of least privilege is applied to all system access.

Authentication

- Secure password requirements are enforced for all user accounts.
- Two-factor sign-in using an authenticator app, with recovery codes, is available on every practitioner account, and we recommend all practitioners turn it on.
- Session management includes automatic timeout and secure token handling.

Infrastructure Security

- Application, API, identity and file storage services are hosted on Google Cloud in the United Kingdom (London). The primary database is hosted on Microsoft Azure in the United Kingdom (UK South). Both providers hold ISO 27001 and SOC 2 certification.
- Network security includes firewalls, intrusion detection, and DDoS protection.
- Regular vulnerability scanning and patching.

Audit and Monitoring

- Audit logging of access to and modifications of Personal Data.
- Monitoring of system health and security events.
- Regular security reviews and risk assessments.

Business Continuity

- Regular automated backups of all data.
- Disaster recovery procedures to restore services in the event of an incident.
- Redundancy in critical infrastructure components.

Clinical Executor Access

- Clinical Executors sign in with their own account and never use the Controller’s sign-in details.

Confidential

- Before any client data opens, a one-time code is sent by text message to the mobile number named in the clinical will.
- Access is limited to the Controller's own clients and to the areas of the Services the Controller has chosen.
- Links in emails to Clinical Executors are private and stored only in hashed form. A link stops working 24 hours after the Clinical Executor accepts, or after 30 days if it is not answered.
- While a Clinical Executor has access, automated reminders, invoice reminders and new online bookings for the Controller are paused.
- Access can be ended at any time. Ending access removes the Clinical Executor's permissions and signs them out.
- Key actions by a Clinical Executor, including cancelled sessions, invoice changes and clients marked as contacted, are recorded in a log the Controller can view.

AI-Specific Measures

- AI-assisted form generation is optional and is used only where the Controller chooses to use it. AI processing (Google Cloud's Gemini Enterprise Agent Platform, formerly Vertex AI) occurs in the United Kingdom (London) under enterprise-tier agreements with contractual guarantees against data use for model training. Client data variables are masked before content is sent to Google Cloud.
- Data sent to AI services is processed transiently and is not retained by the AI service provider beyond the individual API call. No personally identifiable client information is exchanged with the AI service during the form building process.
- Speech-to-text processing (Microsoft Azure) is hosted in the UK with a strict no logging policy. No audio content is retained.
- All AI-generated content requires practitioner review and approval before being saved or used.

SCHEDULE 3

Approved Sub-processors

The following Sub-processors are authorised to process Personal Data on behalf of the Controller in connection with the Services:

Sub-processor	Purpose	Data Processed	Location / Transfer Mechanism
Microsoft Azure	Database hosting (Azure Cosmos DB)	All platform data held in the database, including client records, session data, messages, forms, and billing information	United Kingdom (UK South)
Microsoft Azure Communication Services (Email)	Transactional email delivery, including appointment reminders, booking confirmations, portal invitations, account notifications, and clinical will emails to Clinical Executors and the person named to tell them	Recipient name, email address, appointment details, practice name, and notification content	United Kingdom

Sub-processor	Purpose	Data Processed	Location / Transfer Mechanism
Microsoft Azure Communication Services (SMS)	SMS appointment reminders, service notifications, and one-time sign-in codes for Clinical Executors	Recipient mobile number, appointment details, practice name, notification content, and one-time sign-in codes. Delivery involves onward transmission via mobile network operators.	United Kingdom
Google Cloud	Core platform hosting: application, API and identity services, file storage, message queues and video session hosting	Platform data processed in the course of delivering the Services, including uploaded files and documents, exports and invoices, notification content in transit, and video session traffic	United Kingdom (London, europe-west2)
Google Cloud: Gemini Enterprise Agent Platform (formerly Vertex AI)	Optional. AI-assisted form generation and document conversion, used only where the Controller chooses to use the AI form assistant. No Personal Data is processed through this service in the ordinary use of the Services.	Form structure and variables only; client data variables are masked before processing, practitioner profile data may be included for personalisation, no data is retained beyond the individual request, and no data is used for AI model training.	United Kingdom (London, europe-west2). No logging or AI training.
Jitsi as a Service (JaaS), provided by 8x8	Video session facilitation (alternative video service, retained for use where required)	Video and audio session data between practitioner and client where a session is routed through this service	EU
Stripe	Payment processing	Practitioner and client billing information (name, address, payment details)	EU / US. SCCs in place for US transfers.
Microsoft Azure Speech-to-Text	Speech-to-text within the platform, including AI assistant voice input	Audio data from practitioner or client voice input	United Kingdom. No logging. No AI training.

Video sessions are, by default, delivered through video infrastructure that the Processor maintains and operates itself, hosted on Google Cloud in the United Kingdom. Sessions are encrypted in transit, are not recorded, and no session content is stored. Jitsi as a Service (JaaS) remains an approved Sub-processor and may be used as an alternative video service, for example during maintenance or to maintain continuity of service.

Customer support is provided through Intercom, and anonymised product analytics are collected through Google Analytics on the practitioner application only. These services process limited practitioner data for which Therasee acts as an independent controller, as described in clause 2.5 and the Therasee Privacy Policy, and are therefore not listed as Sub-processors under this Agreement.

Optional third-party integrations. The Services offer optional integrations that the Controller may choose to enable, including synchronisation with the Controller's own Google Calendar or Microsoft Outlook (Microsoft 365) account, and creating video meetings in the Controller's own Zoom or Google Meet account. Where the Controller enables calendar synchronisation, limited scheduling data (appointment dates, times, session type, and client initials only, with no client names, email addresses, or other directly identifying information, together with the practice location or the video session link) is transmitted to the Controller's connected Google or Microsoft account when appointments are scheduled in the Services. For Zoom and Google Meet, the data transmitted is limited to the meeting title (the client's initials and the practitioner's name), date, start time, length, time zone, repeat pattern

and meeting settings such as a waiting room, with no client names, email addresses or other directly identifying information. Where two-way synchronisation is enabled, the Controller's calendar events are accessed through the Google Calendar API or the Microsoft Graph API and processed transiently to display the Controller's availability within the Services and to prevent double booking; such event data is not retained or stored by the Processor. All such processing is carried out via the Controller's own connected account, under the Controller's own relationship with Google, Microsoft or Zoom, and is governed by the Controller's agreement with that provider rather than by this Agreement. The Controller is responsible for its decision to enable any such integration and for ensuring an appropriate lawful basis for the sharing of data with the integrated service.

The Processor shall notify the Controller of any changes to this list in accordance with clause 4.7.

SCHEDULE 4

Data Retention and Deletion

4.1 The Processor shall retain Personal Data for the duration of the Controller's active use of the Services.

4.2 On termination of the Controller's account, the Processor shall:

- Provide the Controller with a period of 45 days to export their data from the platform, in accordance with the Terms of Service.
- Following the export period, delete all Personal Data associated with the Controller's account from active systems without undue delay.
- Remove Personal Data from backup systems within 45 days of deletion from active systems, as backups expire on a rolling cycle.

4.3 The Processor may retain limited data where required by applicable law (for example, financial records required for tax or accounting purposes), but only for so long as required by that law and only for the purpose specified by that law.

4.4 Where Personal Data is processed by Sub-processors, the Processor shall ensure that Sub-processors delete data in accordance with their respective data processing agreements and the timescales set out in this schedule.

4.5 Data processed by the AI form generation service (Google Cloud's Gemini Enterprise Agent Platform, formerly Vertex AI) is not retained by that service beyond the individual API call and is therefore not subject to a separate retention period. Audio data processed by Microsoft Azure Speech-to-Text is processed in memory only and is not retained. Email and SMS notification content processed by Microsoft Azure Communication Services is retained only for as long as necessary to deliver the message and maintain delivery records. Video session content is not recorded or stored by the Processor's video infrastructure or by Jitsi as a Service.

4.6 The log of what a Clinical Executor did in the Services is kept for 6 years after their access ends, even if the clinical will or the Controller's account is deleted sooner, so that the Controller, those acting for the Controller, and the Processor can show what was done and why. It is then deleted. The Controller instructs the Processor to keep it for this purpose.

SCHEDULE 5

Record of Processing Activities and Lawful Bases

This Schedule is maintained by the Processor in its capacity as processor, in support of the Controller's record-keeping under Article 30 of UK GDPR. It describes the categories of processing carried out on behalf of the Controller and, for each, the lawful basis on which the Controller's processing is commonly carried out.

Important: the lawful bases set out below are provided for the Controller's assistance and reflect the bases on which processing of this nature is typically carried out by mental health practitioners. They do not constitute legal advice. The Controller remains solely responsible, as data controller, for determining and documenting the appropriate lawful basis for its own processing under Article 6 and, for special category data, the appropriate condition under Article 9 of UK GDPR and the Data Protection Act 2018, and for confirming that the bases indicated apply to its particular practice. Where an indicated basis does not apply, the Controller is responsible for identifying the basis that does.

Processing activity	Purpose	Common Article 6 basis	Article 9 condition (special category)
Client records	Maintaining identity, contact and demographic records to deliver the Controller's services	Art 6(1)(b) performance of a contract; or Art 6(1)(f) legitimate interests	Not applicable unless health data is included, in which case as for clinical notes below
Clinical and session notes	Documenting assessment and treatment to support continuity and quality of care	Art 6(1)(b); or Art 6(1)(c) where the Controller is under a statutory duty to keep records	Art 9(2)(h) health or social care, with the condition in DPA 2018, Schedule 1, Part 1, paragraph 2; or Art 9(2)(a) explicit consent
Forms and assessment responses	Collecting and storing form and assessment data used in care	Art 6(1)(b)	Art 9(2)(h) with DPA 2018 Sch 1 Pt 1 para 2; or Art 9(2)(a) explicit consent, where health data is included
Appointment scheduling	Booking and managing appointments between the Controller and their clients	Art 6(1)(b)	Art 9(2)(h) where health data is incidentally revealed
Secure messaging and notifications	Communication between the Controller and their clients, and delivery of reminders and notifications	Art 6(1)(b)	Art 9(2)(h) where messages contain health data
Billing and payments	Processing payment for the Controller's services	Art 6(1)(b); and Art 6(1)(c) for statutory financial record-keeping	Not applicable
Clinical will and continuity of care	Making sure clients are told and cared for if the Controller dies or cannot practise, as required by professional bodies such as the BACP	Art 6(1)(f) legitimate interests	Art 9(2)(h) with DPA 2018 Sch 1 Pt 1 para 2, where Clinical Executors see health data

The recipients of the above data are the Controller (as data controller), the Processor (as data processor), and the Sub-processors listed in Schedule 3. Retention is as set out in Schedule 4. Security measures are as set out in Schedule 2.

SCHEDULE 6

United Kingdom Specific Provisions

This Schedule applies where the Controller is established in the United Kingdom and supplements, and does not replace, the obligations set out in the main body of this Agreement.

1. Applicable legislation

The following apply to processing under this Agreement where the Controller is established in the United Kingdom:

Legislation	Relevance
UK GDPR	The retained EU law version of the GDPR as it forms part of UK domestic law under the European Union (Withdrawal) Act 2018, as amended
Data Protection Act 2018	Supplements UK GDPR. Schedule 1, Part 1, paragraph 2 provides the condition for processing special category health data for health or social care purposes
Privacy and Electronic Communications Regulations 2003 (PECR)	Applies to electronic communications, including email and SMS notifications and any marketing communications

2. Lawful basis for special category health data

Where the Controller processes health data (special category data under Article 9 of UK GDPR) in connection with the provision of its services, the condition commonly relied upon is the Data Protection Act 2018, Schedule 1, Part 1, paragraph 2 (health or social care purposes), in conjunction with Article 9(2)(h) of UK GDPR. Where the Controller instead relies on explicit consent, it is responsible for obtaining that consent in accordance with Articles 7 and 9(2)(a) of UK GDPR. The Controller is responsible for confirming which condition applies to its practice.

3. Supervisory authority

The competent supervisory authority for the processing of personal data in the United Kingdom is the Information Commissioner's Office (ICO), ico.org.uk.

4. International data transfers and adequacy

Personal Data is stored and processed in the United Kingdom, including AI-assisted form generation. Limited processing by certain Sub-processors may take place in the European Union, as set out in Schedule 3, which is permitted on the basis of the UK's adequacy regulations for the EU and EEA. Both parties acknowledge that the UK's adequacy regulations for the EU, and the European Union's adequacy decision in respect of the United Kingdom, are subject to periodic review and may be amended or revoked. The Processor shall notify the Controller promptly of any material change that affects the lawfulness of data transfers under this Agreement.

Processor Contact Details

Therasee

1 St. Andrews Road, Studio 8, Montpelier, Bristol, BS6 5EH

Email: privacy@therasee.com

ICO Registration Reference: ZB610705

4 November 2026: wording clarified and backup deletion period shortened. No reduction in protections.