
LEGAL — DATA PROCESSING

Data Processing Agreement

How we handle data on your behalf, in line with UK GDPR

EFFECTIVE
17 May 2026
Subject to yearly legal review

ISSUED BY
Mothermind Limited

This Data Processing Addendum ("**DPA**") forms part of the Employer Terms of Service between the Employer and Mothermind Limited (the "**Agreement**") and governs the processing of personal data in connection with the Mothermind at Work services.

In the event of any conflict between the Agreement and this DPA in relation to data protection, this DPA prevails.

1. Definitions

Terms used in this DPA have the meanings given in the UK GDPR and Data Protection Act 2018. Key terms:

- "**UK GDPR**" means Regulation (EU) 2016/679 as retained in UK law.
- "**Personal Data**", "**Data Subject**", "**Processing**", "**Data Controller**", "**Data Processor**" — as defined in UK GDPR.
- "**Special Category Data**" — as defined in Article 9 UK GDPR.

2. Roles of the Parties

2.1 Employer as Data Controller

The Employer is the Data Controller for:

- employee names and work email addresses;
- job titles, departments, and eligibility information;
- workforce access permissions and authorisation data.

The Employer warrants that it has a lawful basis under Article 6 UK GDPR (and, where applicable, Article 9) for sharing this data with Mothermind and that employees have been informed of the processing through an appropriate privacy notice.

2.2 Mothermind as Data Processor

Mothermind acts as Data Processor on the Employer's behalf when processing the data described in 2.1 for the purposes of:

- account provisioning and identity verification;
- access management and authorisation;
- aggregated usage reporting to the Employer;
- platform administration and support.

2.3 Mothermind as Independent Data Controller

Mothermind acts as an independent Data Controller (and not Processor) for:

- confidential support session records and recordings;
- practitioner clinical and support notes;
- safeguarding records and reports;
- clinical governance and audit records;
- complaints records;
- direct communications between practitioners and employees;
- any data generated through the practitioner-employee relationship.

The Employer has no access to and no controller responsibility for this data.

3. Processor Obligations (in respect of Employer-Controlled Data)

When acting as Data Processor, Mothermind shall:

3.1 Process Personal Data only on documented instructions from the Employer (the Agreement being the primary instruction);

3.2 Ensure persons authorised to process the data are subject to confidentiality obligations;

3.3 Implement appropriate technical and organisational security measures (see Section 5);

3.4 Engage subprocessors only in accordance with Section 4;

3.5 Assist the Employer (at the Employer's cost where the assistance is unreasonably extensive) in:

- (a) responding to Data Subject rights requests;
- (b) demonstrating compliance with UK GDPR Articles 32-36;
- (c) conducting Data Protection Impact Assessments where required;

3.6 Notify the Employer without undue delay (and no later than 72 hours) on becoming aware of a personal data breach affecting Employer-controlled data;

3.7 At the Employer's choice, delete or return Employer-controlled Personal Data at the end of the Services, subject to retention required by law or governance obligation;

3.8 Make available information necessary to demonstrate compliance with Processor obligations and allow reasonable audits (see Section 7).

4. Subprocessors

4.1 The Employer provides general authorisation for Mothermind to engage subprocessors, subject to the conditions below.

4.2 Current subprocessors:

Subprocessor	Purpose	Location	Transfer Mechanism
Supabase	Hosting, database, authentication	UK / EU	Within UK / EU adequacy
Stripe Payments UK Ltd	Payment processing	UK with US transfer	UK IDTA / SCCs + UK Addendum
Calendly LLC	Scheduling and booking	US	UK IDTA / SCCs + UK Addendum + Transfer Risk Assessment
[Email service provider]	Transactional email	[TBC]	[TBC]
Lovable	Platform hosting and build	[TBC]	[TBC]

4.3 Mothermind will:

- (a) impose data protection terms on each subprocessor materially equivalent to those in this DPA;
- (b) remain liable for the acts and omissions of subprocessors as if they were its own;
- (c) notify the Employer at least 30 days in advance of any new or replacement subprocessor handling Employer-controlled data, where reasonably practicable;
- (d) allow the Employer to object to a new subprocessor on reasonable data protection grounds within 30 days. If unresolved, the Employer may terminate the affected Services without penalty.

5. Security

5.1 Mothermind implements technical and organisational measures appropriate to the risk, including:

- encryption in transit (TLS) and at rest;
- role-based access controls and authentication;
- row-level security separating customer data;
- regular security review and patching;
- staff training on data protection and confidentiality;
- audit logging of access to sensitive data;
- secure backup and recovery;
- vendor security due diligence for subprocessors.

5.2 Mothermind reviews its security measures regularly and may update them provided the level of protection is not reduced.

6. International Transfers

6.1 Where Personal Data is transferred outside the UK, Mothermind shall implement an approved transfer mechanism under UK GDPR, including:

- the UK International Data Transfer Agreement (IDTA);
- the EU Standard Contractual Clauses with the UK Addendum;
- relevant adequacy decisions where applicable.

6.2 Mothermind will conduct Transfer Risk Assessments for transfers to countries without an adequacy decision, where required.

7. Audit

7.1 The Employer may, no more than once per 12 months and on reasonable notice (minimum 30 days), request reasonable information to verify Mothermind's compliance with this DPA.

7.2 Mothermind will first provide written information, attestations, and any available third-party audit reports or certifications. On-site audits will only be required where written information is insufficient.

7.3 The Employer shall bear its own audit costs. Mothermind's reasonable time costs may be charged.

7.4 Audits must not unreasonably interfere with Mothermind's operations or the confidentiality of other customers.

8. Data Subject Rights

8.1 Mothermind shall reasonably assist the Employer in responding to Data Subject requests in respect of Employer-controlled data.

8.2 Employees may exercise rights in respect of Mothermind-controlled data (including session records) by contacting Mothermind directly at ****.

8.3 Some rights may be subject to limitations under UK GDPR Article 23, the Data Protection Act 2018, professional secrecy obligations, or safeguarding considerations.

9. Retention and Deletion

9.1 Retention periods are set out in Section 14 of the Employer Terms of Service.

9.2 On request following termination, Mothermind will provide the Employer with:

- (a) an export of Employer-controlled data in a commonly used format, within 30 days; and
- (b) written confirmation of deletion of Employer-controlled data following the agreed retention period.

9.3 Mothermind-controlled data (including practitioner notes and governance records) is retained in accordance with professional and legal obligations regardless of the Employer's termination.

10. Liability

The liability provisions of the Agreement (Section 12 of the Employer Terms of Service) apply to this DPA.

11. Conflict and Term

11.1 In the event of conflict between this DPA and any other part of the Agreement on data protection matters, this DPA prevails.

11.2 This DPA continues for the duration of the Agreement and survives termination to the extent necessary to perform retention, deletion, and audit obligations.

12. Governing Law

This DPA is governed by the laws of England and Wales, with exclusive jurisdiction of the courts of England and Wales.

This DPA is version 1.0 and subject to legal review. Final version effective from [DATE].