
PRIVACY & DATA

Privacy Notice

What data we collect, why, and your rights

EFFECTIVE
17 May 2026
Subject to yearly legal review

ISSUED BY
Mothermind Limited

This Privacy Notice explains how Mothermind Limited ("**Mothermind**", "**we**", "**our**", "**us**") handles personal data in connection with the Mothermind at Work service. It applies to employers, employees, and anyone else whose data we process through the platform.

This Notice is separate from the privacy policy for our consumer Mothermind service.

Who We Are

Mothermind Limited

Registered in England and Wales: Company No. [XXXXXXXX] Registered office: [ADDRESS] Data Protection contact: ****

We are registered with the Information Commissioner's Office (ICO): registration number [TBC].

1. Why You Should Read This

We've written this Notice in plain English. We explain:

- what personal data we collect, from whom, and why;
- the legal basis we rely on;
- who we share it with;
- how long we keep it;
- your rights and how to use them.

If anything isn't clear, email us at ****.

2. Personal Data We Process

From Employers

When an organisation subscribes to Mothermind at Work, we process:

- organisation name, billing address, company number;
- contact details for the lead administrator and billing contact;
- subscription tier, billing history, and payment data (handled by Stripe);
- a list of employees authorised to access the service (name, work email, optionally job title or department).

From Employees

When you access Mothermind at Work as an employee, we process:

- your name, work email, and any optional profile information you choose to add;
- session bookings: who you booked with, when, and attendance;
- session content and practitioner notes (held confidentially — see Section 4);
- communications with practitioners and support;
- engagement data such as which resources you access (in aggregate where possible).

Automatically

We collect limited technical data to keep the platform working:

- device and browser information;
- IP address;
- log and audit data;
- essential cookies (see our Cookie Policy at [\[URL\]](#)).

3. Why We Process This Data and Our Legal Basis

What we process	Why	Legal basis (UK GDPR)
Employer billing and account data	Manage the subscription, comply with tax law	Contract; Legal obligation
Employee access data	Authenticate and authorise access	Contract (with employer); Legitimate interests
Booking data	Schedule and deliver sessions	Contract; Legitimate interests
Session content and practitioner notes	Provide and record clinical/specialist support	Article 6(1)(f) Legitimate interests AND Article 9(2)(h) — provision of health/social care, with professional secrecy under DPA 2018 Schedule 1 Part 1
Safeguarding records	Protect people at risk	Article 6(1)(d) Vital interests / 6(1)(c) Legal obligation; Article 9(2)(b)/(c)
Aggregate analytics	Improve the service	Legitimate interests
Marketing emails (where you've opted in)	Send updates	Consent

We hold an Appropriate Policy Document covering our processing of special category (health) data, available on request.

4. Session Confidentiality

Sessions between an employee and a Mothermind practitioner are **confidential**.

- Employers cannot see what is discussed.
- Practitioners record notes in line with professional standards (e.g. NMC). These notes are held by Mothermind as an independent data controller.
- We will not disclose session content to your employer, family members, or anyone else without your consent.

Exceptions (where we may disclose without consent):

- safeguarding concerns (Care Act 2014; Working Together to Safeguard Children 2023);
- risk of serious harm to you or another person;
- legal requirement (court order, regulator);
- professional or clinical governance obligations.

Where we have to break confidentiality, we will tell you wherever it is safe and reasonable to do so.

5. Data Sharing

We share data only where necessary:

- **With your employer:** only aggregate engagement data. No identifiable session content.
- **With practitioners:** to deliver your session.
- **With trusted subprocessors:** see Section 6.
- **With regulators or authorities:** where legally required or for safeguarding.
- **In an emergency:** with emergency services where necessary to protect life.

We never sell your data.

6. Subprocessors (Who Helps Us Run the Service)

Provider	Purpose	Location
Supabase	Hosting, database, authentication	UK / EU
Stripe Payments UK Ltd	Payment processing	UK with US transfers
Calendly	Scheduling	US
[Email provider]	Transactional email	[TBC]

Provider	Purpose	Location
Lovable	Platform build and hosting	[TBC]

We use contractual safeguards (UK IDTA or SCCs with UK Addendum) for any transfers outside the UK. A current subprocessor list is at [URL].

7. How Long We Keep Data

Data	Retention period
Employer commercial records	Term + up to 6 years
Employee access/account records	Up to 12 months after termination
Session booking records	Up to 3 years
Practitioner clinical notes	Up to 8 years (25 years for maternity-related records)
Safeguarding records	Up to 25 years
Marketing data (where consented)	Until you withdraw consent

Retention reflects professional, regulatory, and legal requirements including NMC Record Keeping Guidance and the NHS Records Management Code of Practice (2021).

8. Your Rights Under UK GDPR

You have the right to:

- **Access** the personal data we hold about you;
- **Correct** inaccurate or incomplete data;
- **Delete** your data ("right to be forgotten") — subject to legal/professional retention obligations;
- **Restrict** processing in certain circumstances;
- **Portability** — receive your data in a portable format where applicable;
- **Object** to processing based on legitimate interests or for direct marketing;
- **Withdraw consent** where we rely on consent;
- **Lodge a complaint** with the Information Commissioner's Office (ICO): ico.org.uk.

To exercise any right, email ****. We respond within 30 days, sometimes extended where requests are complex.

Some rights may be limited where data is held for clinical record-keeping, safeguarding, or legal reasons — we'll explain this if it applies to your request.

9. Security

We use technical and organisational measures to protect your data, including:

- encryption in transit and at rest;
- access controls and authentication;
- audit logging;
- regular security review;
- staff confidentiality training;
- vendor due diligence for subprocessors.

If a personal data breach occurs that is likely to result in a risk to your rights, we will tell you and notify the ICO within 72 hours.

10. Cookies

We use essential cookies to keep the platform working. We use optional cookies (such as analytics) only with your consent. See our **Cookie Policy** at [URL].

11. Children

Mothermind at Work is for adults aged 18 and over. We do not knowingly collect data from anyone under 18 through this service.

12. International Users

Mothermind at Work is operated from the UK and intended for UK-based employers and their employees. If you access the service from outside the UK, you do so on your own initiative and are responsible for compliance with local law.

13. Changes to This Notice

We may update this Notice. Material changes will be notified by email or platform message. The "Last updated" date at the top reflects the current version.

14. Contact

Mothermind Limited

[Registered Address] Data Protection: **** General: **** Complaints: ****

Information Commissioner's Office (ICO):

ico.org.uk | 0303 123 1113

Version 1.0. Subject to legal review.