

Our Privacy Statement

Introduction

This Privacy Policy sets out how we handle your personal information in accordance with the General Data Protection Regulations (GDPR), effective from 25th May 2018.

These regulations increase the accountability of organisations such as The Mindfull Practice™ who handle personal data professionally and transparently. Individuals are granted specific rights regarding their personal information, and how it is collected, stored, used, shared and protected. You can read more about the GDPR requirements on the [Information Commissioner's Office](#) website.

We've tried to make this policy as transparent and understandable as possible. If you are not sure about any part of it, think that something in this policy is wrong or missing, or have any questions regarding your personal data, please contact us.

Definitions

'Client' refers to any person or company who uses our services.

'E-Subscriber' refers to anyone who received emails from us or subscribes to our newsletter.

'Our services' refers to the therapy, treatments, assessments, consultation, coaching and training we provide.

'Visitor' refers to any person who visits our website or social media profiles for information purposes

'We' or 'us' refers to The Mindfull Practice™ everyone who is involved in running the business.

'Website' refers to the website of the The Mindfull Practice™ which is the www.TheMindfullPractice.com

What personal data do we collect from you?

We collect personal data directly from you before becoming a client, whilst you are a client and after leaving treatment. Once you become a client, we will collect information relating to your treatment, including medical history, assessments, consultations, case notes and reports. We may collect personal data in hard copy form, usually during a treatment session. We hold paper copies of files in a locked filing cabinet. We also hold information

on digital format and that is securely protected on our system. We are required by our governing body, GHR, to keep clinical information and not to destroy it. After you have been discharged, we would archive the information for a period of 3 years.

We also collect personal data 'automatically'. This happens when you navigate our website, engage with our emails or social media. The information can be from conversations you have with us, emails you send to us or other information/documents you give to us. The information we collect depend on who you are

If you are a potential client or third party provider, we will store contact information, including your name, email address and telephone numbers.

If you are a website visitor, your information may be collected by our third party providers, including IP addresses, location (by country), browser type and other web analytics data.

Why we collect this data

We collect your data to ensure that we have all the information we need to contact you and take the best care of you. We also collect data that is within our legitimate interest so that we can run our business more effectively. We analyse what clients and visitors want from our services so that we can improve the services we provide and inform you of these changes. It is our duty to safeguard your information and our business, so we verify identities and prevent unauthorised access to our website and services, monitor visitor traffic to our site and secure our site against malicious human and automated visitors. Personal information collected for our legitimate interests includes:

- Operating and protecting our website
- Providing you with services described on the website.
- Carrying out technical analysis to determine how to improve our website and the services we provide or resolve any technical problems.
- Monitoring activity on our sites to identify potentially fraudulent activity and prevent spam and 'hacking'
- To ensure compliance with our website's Terms of Use.
- Managing our relationship with you, e.g. by responding to your comments or queries submitted to us on our website or asking for your feedback.
- Managing our legal and operational affairs (including, managing risks relating to content and fraud matters).
- Improving our products and services.
- Providing general administrative and performance functions and activities.
- Providing clients with important information about changes to products and services e.g. forthcoming holiday dates and emergency contact procedures, changes to website requirements, regulations or 'best practice' guidance.
- We may be required by law to collect personal information when responding to requests by government, a court of law or a regulatory or other legal investigation.

Who has access to your personal data?

We do not sell your personal information to third party companies. We may need to transfer your personal data to companies we appoint to host our services or provide services (which include processing personal data.) Sometimes actual or potential business partners may need access to personal data to evaluate or carry out a business relationship or to conclude a transaction with us. There may be certain circumstances in which we need to disclose your personal information, for example:

- To regulators and government authorities in connection with our compliance procedures and obligations.
- A purchaser or prospective purchaser of all or part of our assets or our business, and their professional advisers, in connection with the purchase.
- A third party, to respond to requests relating to a criminal investigation or alleged or suspected illegal activity.
- A third party, to address financial or reputational risks and we need to enforce or defend our rights
- A rights holder in relation to an allegation of intellectual property infringement or any other infringement.
- Where we are authorised or required by law to do so.

If we are required to disclose your personal information at any time, you would be informed of this, unless our legal or other obligation prevented us from disclosing this to you.

Security and Safeguards

The safeguards we have put in place to ensure that our contractors and other third parties keep your personal data secure and confidential and use it only as authorised by us are as follows:

- We require all third parties to whom we disclose personal data to enter into a contract with us that includes confidentiality obligations
- We carry out such due diligence as is reasonably necessary in relation to the technical and organisation measures used by our suppliers to ensure that personal data is processed securely
- We take all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach.
- Our service provider, affiliates and storage providers may store and process your personal data centres located in the USA, Europe, Israel, (or other jurisdictions, as necessary for the proper delivery of their Services and/or as may be required by law). The third-party storage providers are contractually committed to keep your data protected and secure, in accordance with industry standards and regardless of any lesser legal requirements which may apply in their jurisdiction. Should your personal data be transferred anywhere outside of Europe, our service provider, their affiliates and their third-party storage providers are contractually committed to make sure that (i) there is a level of protection deemed adequate by the European Commission or (ii) that the relevant Standard Contractual Clauses are in place.

- Our service provider and their affiliates participate in, and has certified its compliance with, the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework and have Privacy Shield Certification. Our service provider is based in Israel which is considered by the European Commission to offer an adequate level of protection for the Personal Information of EU Member State residents. Among other things, they will ensure that there is the adequate level of protection or that relevant Standard Contractual Clauses are in place for the international transfer of our EU users' data. Our third-party provider has implemented security measures designed to protect the personal information you share with us, including physical, electronic and procedural measures. Among other things, they offer HTTPS secure access to most areas of our website services; the transmission of sensitive payment information (such as a credit card number) through designated purchase forms is protected by an industry standard SSL/TLS encrypted connection; and they regularly maintain a PCI DSS (Payment Card Industry Data Security Standards) certification.

How long do we hold your data?

If you are our client, we hold client personal information whilst we are providing our treatment services to you. When you are no longer a client, we will still need to keep your information for three years (or as long as we need to, to comply with our legal obligations.) longer want us to use your personal information, you can tell us to erase it. However, we will still have to keep information from deleted accounts (in a static, archived form) to comply with the law, prevent fraud, collect fees, resolve disputes, troubleshoot problems, assist with investigations, enforce the terms of use and take other actions permitted by law.

If you are an e-subscriber, we will keep your required personal details whilst you are actively engaged with our e-service. If you no longer want us to use your personal information, please tell us to erase it. Emails and related personal details may be retained for up to one year.

If you are a visitor, we will keep your required personal details whilst you are actively engaged with our e-service. If you no longer want us to use your personal information, please tell us to erase it. Emails and related personal details may be retained for up to one year.

Identity of the data controller

The Mindfull Practice™ is responsible for deciding how personal data is processed and for what purpose. The person responsible for this is the Data Protection Officer, who can be contacted by writing to hello@TheMindfullPractice.com or The Mindfull Practice,™ Top Floor, 40-42 High Street, Old Town, Poole, BH15 1BT.

Your rights

You have the right to request copies of the personal information that we hold. However, this will incur an administrative charge and we will also need you to provide us with appropriate identification before we comply with this request. If you believe there are errors in the personal information we hold, you can ask us to delete or revise the information. You can also ask us to delete the personal information, we hold. However, we may have to retain core information to comply with our legal responsibilities. If you no longer want to receive our emails, please use

the 'unsubscribe' button at the bottom contained in the emails or by contacting us at hello@TheMindfullPractice.com

If you are not happy about the way in which we use your personal information you have the right to complain to the Information Commissioner whose details can be found at www.ico.gov.uk

Changes to this Privacy Policy

This Privacy Statement came into form in February 2023 and will be updated from time to time.

Contact us

If you have any questions about anything in this Privacy Statement, please contact us at hello@themindfullpractice.com