Mindmaps Wellbeing Ltd.
Data Protection Policy

Contents

Summary of Policy

This policy and other supporting policies, procedures and guidance evidence Mindmaps Wellbeing Ltd. commitment to protecting the rights and privacy of individuals (including students, staff and others) by safeguarding their personal data and ensuring that privacy is central to what we do.

Summary of significant changes since last version

This is a new policy, developed to ensure compliance with regard to the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 and related EU and national legislation protecting privacy rights. ("data protection law").

Scope

What this policy covers

As an organisation processing personal information, Mindmaps Wellbeing Ltd. is registered with the Information Commissioner's Office (ICO) as a "data controller" (Z8006960). This policy covers the processing of all personal information whose use is controlled by it.

Mindmaps Wellbeing also acts as a "data processor", processing personal data on behalf of other data controllers. When it does so, it acts on their instructions and on contractual obligations.

This policy applies to everyone working for or on behalf of Mindmaps Wellbeing who obtains, uses, accesses or stores personal data, regardless of their role, grade or type of contract. This includes, but is not limited to, agency staff, volunteers, visiting research and teaching staff and external committee members. It also applies to all students when processing personal data on behalf of the Mindmaps Wellbeing or as a requirement of their studies.

This policy applies regardless of where the personal data is held, including outside Mindmaps Wellbeing property and on personally owned equipment.

This policy applies to staff and others working for or on behalf of Mindmaps Wellbeing.

Introduction

The University is an organisation highly dependent on the processing of personal data to carry out its activities and it takes its responsibilities with regard to data protection law very seriously. Personal data is owned by data subjects and the Mindmaps Wellbeing will fully comply with data protection law in order to ensure their rights, informed by good data governance.

Policy

1. Purpose

1.1 This Policy evidences commitment by Mindmaps Wellbeing to ensuring that all those defined by the scope of this policy, process personal data in line with data protection law.

1.2. This Policy aims to

a. Ensure adherence to the data protection principles in all processing of personal data
b. Protect the rights of individual data subjects by applying the principles
c. Outline the roles and responsibilities of all users of personal data
d. Outline the potential consequences of non-compliance with this policy

2. Principles

Personal data will be:

2.1. processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")

2.2. collected and created for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation")

2.3. adequate, relevant and limited to what is necessary in relation to those purposes ("data minimisation")

2.4. accurate and, where necessary, kept up to date ("accuracy")

2.5 retained for no longer than is necessary ("storage limitation")

2.6 kept safe from unauthorised access, accidental loss or deliberate destruction ("integrity and confidentiality")

Mindmaps Wellbeing will ensure additional controls are in place for "special category" (sensitive) personal data.

Mindmaps Wellbeing will also ensure that it applies appropriate safeguards to protect the rights and freedoms of data subjects when archiving personal data in the public interest for research, statistical or historical purposes.

3. Data Subject Rights

Mindmaps Wellbeing will uphold individual data subject rights, specifically the right to:

3.1. obtain free of charge, confirmation as to whether personal data concerning them is being processed and, if it is, a copy of that personal data

3.2 have their personal data rectified and incomplete personal data completed

3.3 erasure when no longer required or to be forgotten, subject to legal obligations

3.4 object to and restrict further processing of their data until the accuracy of the data or use has been resolved

3.5 data portability where the personal data has been provided by consent or contract for automated processing and the data subject requests that a machine readable copy be sent to another data controller

3.6 not be subject to a decision based solely on automated decision making and processing

We will communicate these rights to data subjects through timely privacy notices.

4. Roles and Responsibilities

4.1 **All Users** of personal data must:

- complete relevant training to support compliance with this policy
- ensure that the personal data they hold in any format (for example: electronic, paper) is kept securely
- not disclose personal data in writing or orally, accidently or otherwise to un-authorised third parties
- keep personal data only for as long as required for purpose.
- regularly check that any personal information they have provided Mindmaps Wellbeing regarding their employment or studies is accurate and up to date
- raise any concerns with Mindmaps Wellbeing in respect of the processing of personal data
- report losses or un-authorised disclosures of personal data to the Information Rights Team
- co-operate fully with any investigation conducted by Mindmaps Wellbeing or the Information Commissioner's Office and implement any necessary improvements following a personal data breach
- support the completion of Subject Access Requests by providing information when requested

4.2 Mindmaps Wellbeing has a corporate responsibility as a data controller and when acting as a joint data controller or a data processor to:

- ensure there are appropriate technical and organisational measures are in place so that all processing of personal data is carried out in accordance with data protection law
- hold records evidencing its compliance
- co-operate with the UK supervisory authority, the Information Commissioner's Office, to uphold data subject rights

5. Non-compliance

5.1 All users of personal data are encouraged to seek advice and support as quickly as possible if there is a risk of personal data breach, a suspected breach, a near miss or an actual breach. The Personal Data Breach Procedure should be followed without delay. Our intention is to promote a culture of increased openness and improvement with regard to information security and data protection.

5.2 Any careless or deliberate infringement of this policy or data protection law by

users of personal data will be treated seriously by Mindmaps Wellbeing and may result in disciplinary action.

5.3 The responsibilities outlined in this policy do not waive personal liability for individual criminal offences resulting from the willful misuse of personal data under data protection law. These include:

- Unlawfully obtaining, disclosing or retaining personal data
- Re-identifying de-identified personal data without the authority of the data controller or processor
- Altering or deleting personal data to prevent disclosure in accordance with the rights of access to data subjects
- Impeding an officer of the Information Commissioner's Office in the course of their duty

6. Data handling process & Back-up

Once the register has been provided by the authority, we will register delegates to the course via the MHFA England website. The file with the information is also stored on our securely encrypted P-Cloud server & 4CRM systems. On the day of training a register is completed to confirm attendees, we will inform the client of those in attendance or those registered but not on the course by email. All data handled by Mindmaps Wellbeing is done so in accordance with our data protection policy. Any files with personal information shared between Mindmaps Wellbeing and the client will be password protected with a minimum of 8 characters, including a symbol, number, capital and lowercase letters to ensure its security. Upon course completion the only data retained will be attendee names and emails for continued use in the learning support hub and to inform of relevant refreshers when due. Data no longer required is deleted through the p-cloud encrypted shredding system. Data held for clinical support services is held for 6 years, this allows the individual to request a copy up to this time.
All our systems require two-factor authentication to access accounts such as emails, CRM and login's at administrator level.

6.1 Destroying data

Any data on paper is shredded and taken away by a secure collection for protected data. All electronic devices which hold data are virus protected, and biometric entry is required for entry. All our files are stored on the encrypted p-cloud. Servers are stored in a secure location in Switzerland for the p-cloud. Should Mindmaps Wellbeing have a data breach those effected will be notified immediately.
Disposal of any hard drive that contained data is disposed of securely ensuring all data is fully destroyed. All other electronical files are destroyed using the encrypted p-cloud shredder.

7. Training

Mindmaps Wellbeing will ensure any member of staff handling data have read and understood the data policy. We will ensure everyone is aware of their responsibility in guidance with the policy. Ensure all members of staff are aware of our password policy, how to spot and report suspected phishing, how we store data and to be aware of public Wi-Fi vulnerabilities.

Glossary of Terms

The following terms are defined within data protection law as follows:

1. ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

3. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

4. ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

5. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

6. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

7. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

8. ‘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

9. ‘Supervisory authority' means an independent public authority responsible for monitoring the application of GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union. In the United Kingdom this is the Information Commissioner’s Office

Useful Links

Information Commissioner's Office

General Data Protection Regulations (final legal text)

UK Data Protection Bill (UK Parliament website