Data Protection Policy

Version: December 20, 2022

I. **Introduction**

The Mental Health Hub (mHub), takes its responsibilities regarding the management of the requirements of relevant data protection legislation, including the EU General Data Protection Regulation (GDPR), very seriously. This policy sets out how mHub manages those responsibilities.
mHub obtains, uses, stores and otherwise processes personal data relating to potential staff and clients, current staff and clients, former staff and clients, current and former contractors, website users and contacts, collectively referred to in this policy as "data subjects". When processing personal data, mHub is obliged to fulfil individuals' reasonable expectations of privacy by complying with relevant data protection legislation.

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and mHub's expectations for all those who process personal data on its behalf;
2. comply with the relevant data protection legislation and with good practice;
3. protect mHub's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights; and
4. protect mHub from risks of personal data breaches and other breaches of data protection legislation.

The main terms used are explained in the glossary at the end of this policy (Appendix 2).

II. Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff at mHub's offices processing personal data on mHub's behalf are sent a copy of this policy and must read it. A failure to comply with this policy may result in disciplinary action.

All mHub's managers are responsible for ensuring that the staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance. mHub's most senior staff member responsible for data protection – our "Data Protection Officer" – is our Executive Director, Dr Michael Grosspietsch, who can be reached at michael@mental-health-hub.org.

III. Personal data protection principles

When you process personal data, you should be guided by the principles listed below, which are derived from the GDPR. We are responsible for these principles and must be able to demonstrate compliance with them. Further details on how to achieve these principles can be found in Appendix 1 below.

1. Lawfulness, fairness and transparency: Data needs to be processed lawfully, fairly and in a transparent manner.
2. Purpose limitation: Data needs to be collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. Data minimization: Data needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accuracy: Data needs to be accurate and where necessary kept up to date.
5. Storage limitation: The keeping of data in a form which permits identification of data subjects needs to be limited to what is necessary for the purposes for which the personal data is processed.
6. Security, integrity and confidentiality: Data needs to be processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage.

IV. Data subjects' rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. Where the legal basis of our processing is consent by the data subject, to withdraw that consent at any time.
2. To ask for access to the personal data that we hold.
3. To prevent our use of the personal data for direct marketing purposes.
4. To object to our processing of personal data in limited circumstances.
5. To ask us to erase personal data without delay:

   a) if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
   b) if the only legal basis of processing is consent of the data subject and that consent has been withdrawn and there is no other legal basis on which we can process that personal data;
   c) if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
   d) if the data subject has objected to our processing for direct marketing purposes; or
   e) if the processing is unlawful.

6. To ask us to rectify inaccurate data or to complete incomplete data.
7. To restrict processing in specific circumstances, e.g. where there is a complaint about accuracy.
8. To ask us for a copy of the safeguards under which personal data is transferred from one country to another.
9. To prevent processing that is likely to cause damage or distress to the data subject or anyone else.
10. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
11. To make a complaint to the relevant supervisory authority.
12. To receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Legitimate data subject access requests must be complied with, usually within one month of receipt. You must immediately forward any data subject access request you receive to the Data Processor. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

V. Accountability

mHub must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. We are responsible for the data protection principles and must be able to demonstrate compliance with them.

We must therefore apply adequate resources and controls to ensure and to document compliance including the integration of data protection into our policies and procedures, the training of staff on compliance with relevant data protection legislation, and the regular testing and conducting of periodic reviews to assess compliance.

VI. Responsibilities

1.mHub:
As the data controller, mHub is responsible for establishing policies and procedures in order to comply with relevant data protection legislation. Our Data Processor advises our staff of their obligations and generally monitors compliance with relevant data protection legislation.

2. Staff:
Staff who process personal data about clients, staff or other individuals must comply with the requirements of this policy. Staff must ensure that:

a) All personal data is kept securely.
b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.
c) Personal data is kept in accordance with mHub's data retention schedule (see Appendix 3 below).
d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Processor.
e) Any data protection breaches are swiftly brought to the attention of the Data Processor and that they support him in resolving breaches.
f) Where there is uncertainty around a data protection matter, advice is sought from the Data Processor.

Staff who are unsure about who are the authorized third parties to whom they can legitimately disclose personal data should seek advice from the Data Processor.

3. Third-party data processors
Where external companies are used to process personal data on behalf of mHub, responsibility for the security and appropriate use of that data remains with mHub.

Where a third-party data processor is used, a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data. We must always take reasonable steps that such security measures are in place. Where reasonably feasible, we also need to sign a data processing agreement with the third party, establishing what personal data will be processed and for what purpose.

4. Contractors, interns, short-term and voluntary staff:
mHub is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, interns, short-term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

a) Any personal data collected or processed in the course of work undertaken for mHub is kept securely and confidentially.

b) All personal data is returned to mHub on completion of the work, including any copies that may have been made. Alternatively, the data is securely destroyed and mHub receives notification in this regard from the contractor, intern, short-term or voluntary staff.

c) mHub receives prior notification of any disclosure of personal data to any other organization or any person who is not a direct employee of the contractor.

d) Any personal data made available by mhub, or collected in the course of the work, is neither stored nor processed unless official consent to do so has been received from mHub.

e) All practical and reasonable steps are taken to ensure that contractors, interns, short-term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

5. Clients:

Clients are responsible for familiarizing themselves with our data protection policy and privacy policy (for the clinic) provided when they enter into an agreement with mHub or seek therapy, and for ensuring that their personal data provided to mHub is accurate and up to date.

VII. Data subject access requests

Data subjects have the right to receive a copy of their personal data which is held by mHub. In addition, an individual is entitled to receive further information about our processing of their personal data in relation to the purposes, the categories of personal data being processed, recipients/categories of recipients, data retention schedules, information about their rights, the right to complain to a relevant supervisory authority, details of the relevant safeguards where personal data is transferred to another country, and any third-party source of the personal data.

You should not allow third parties to persuade you into disclosing personal data without proper authorization. For example, relatives of the clinic's patients do not have an automatic right to gain access to their relative's data.

You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact the Data Processor before any changes are made to personal data which is the subject of an access request.

VIII. Reporting a personal data breach

Relevant data protection legislation like the GDPR requires that we report any personal data breach to the relevant supervisory authority where there is a risk to the rights and freedoms of the data subject. Where the personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialize, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the relevant supervisory authority where we are legally required to do so. If you know or suspect that a personal data breach has occurred, you should immediately contact the Data Processor. You must retain all evidence relating to personal data breaches, particularly also to enable mHub to maintain a record of such breaches, as required by relevant data protection legislation like the GDPR.

IX. Limitations on the transfer of personal data

Relevant data protection legislation like the GDPR restricts data transfers to other countries in order to ensure that the level of data protection afforded to individuals is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

Due to the nature of our operations, data transfers between our headquarters and the other mHub companies are typically permissible if they take place in the usual course of our operations. In particular, we are allowed to transfer data abroad if the transfer is necessary for the performance of a contract between us and the data subject, or if the data subject has provided explicit consent to the proposed transfer after being informed of any potential risk. Additionally, we are allowed to transfer data abroad to protect the vital interests of the data subject where he/she is physically or legally incapable of giving consent. The latter case might apply to extreme emergencies with matters of life and death.

X. Record keeping

Relevant data protection legislation like the GDPR generally requires companies to keep accurate records of their data processing activities. This does not apply to companies with less than 250 employees like ours. Nevertheless, we desire to keep and maintain accurate records, particularly records of data subjects' consents for counselling sessions as well as relevant agreements with clients.

Furthermore, records of personal data breaches must also be kept, setting out the facts surrounding the breach, its effects and the remedial action taken.

XI. Training and audit

We are required to ensure that all staff undergo adequate training to enable them to comply with relevant data protection legislation. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data protection related training. You must also regularly review all the systems and processes under your control to ensure they comply with this policy.

XII. Data privacy by design and default

We are required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organizational measures (like pseudonymization) in an effective manner, to ensure compliance with data protection principles. mHub must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. You should ensure that you adhere to those measures.

As well as complying with company-wide practices designed to fulfil reasonable expectations of privacy, you should also ensure that your own data-handling practices default to privacy to minimize unwarranted intrusions in privacy e.g. by disseminating personal data to those who need to receive it to discharge their duties.

XIII. Direct marketing

We are subject to certain rules and privacy laws when marketing to our prospective and current clients and any other potential user of our services. For example, a data subject's prior consent is required for electronic direct marketing, e.g. by email.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honored. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Appendix 1: Further details on achieving the personal data protection principles

Principle 1: Processing personal data lawfully, fairly and transparently
You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but to ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, mHub may only process personal data if the processing in question is based on one (or more) of the following legal bases:

1. The data subject has given his or her consent. This is typically the case for clients because they have provided consent when entering into the services agreement with mHub and when seeking therapy.
2. The processing is necessary for the performance of a contract with the data subject. This is typically the case for services that we provide for our clients since we process data solely for the successful delivery of our services and have a contract in place. Clients seeking counseling will sign a consent form.
3. To meet our legal compliance obligations.
4. To protect the data subject's vital interests (i.e. matters of life or death). This could apply to situations of extreme emergencies.

Consent requires genuine choice and genuine control. A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes or inactivity are therefore unlikely to be sufficient. If consent is given in a document that deals with other matters, you must ensure that the consent is separate and distinct from those other matters. Data subjects must be able to withdraw consent to processing easily at any time. Withdrawal of consent must be promptly honored. Consent may need to be renewed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the consent is historic. You will need to ensure that you have evidence of consent and you should keep a record of all consents obtained so that we can demonstrate compliance.

Special attention and care are required for the processing of sensitive personal data as this represents a greater intrusion into individual privacy. Among others, this can be data concerning health, relating to criminal convictions and offences, or revealing the racial or ethnic origin, political opinions, or religious or philosophical beliefs of a data subject. While other exceptional cases may exist where the processing of such sensitive personal data is required and permitted, as a general rule, we only process such sensitive personal data (generally the users of our clinical services) when the data subject has given explicit consent to do so, we have a consent form that allows such processing or, in the case of an extreme emergency, where it is a matter of life and death.

In addition to only processing personal data fairly and lawfully and for specified purposes, the processing needs to take place in full transparency. mHub is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate privacy policies, e.g. on our website, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever we collect personal data directly from data subjects, for example for the clinical services, at the time of collection we must provide the data subject with all the prescribed

information, which includes mHub's details, the purposes of processing, the legal basis of processing, where the legal basis is "legitimate interest" identify that particular interest (e.g. marketing), where the legal basis is "consent" mention the right to withdraw, and where the legal basis is "contractual necessity" explain the consequences for the data subject of not providing the data.

When personal data is collected indirectly, e.g. from a third party or publicly available source, you must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with relevant data protection legislation and on a basis which contemplates our proposed processing of that personal data.

Principle 2: Purpose limitation
Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes.

Principle 3: Data minimization
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed. You may only process personal data when performing your job duties requires it and you should not process personal data for any reason unrelated to your job duties. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymized in accordance with mHub's data retention schedule (see Appendix 3 below).

Principle 4: Accuracy
Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files. Incomplete records can lead to inaccurate conclusions being drawn. Where there is such a risk, you should ensure that relevant records are completed. You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record). Where a data subject has required his/her personal data to be rectified or erased, you should inform recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 5: Storage limitation
You must not keep personal data in a form that allows data subjects to be identified for longer than needed for the legitimate business purposes for which mHub collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymized. You will take all reasonable steps to destroy or erase from mHub's systems all personal data that we no longer require in accordance with mHub's data retention schedule (see Appendix 3 below).

Principle 6: Security, integrity and confidentiality
mHub is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorized or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymization where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorized to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorized access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organizational measures to comply with relevant data protection legislation and who agree to act only on mHub's instructions.

Appendix 2: Glossary of terms

- Consent: Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.
- Data subject: A living, identified or identifiable individual about whom we hold personal data.
- Personal data: Any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymized personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behavior.
- Personal data breach: Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.
- Processing: Any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.
- Pseudonymization: Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Appendix 3: Data retention schedule

Unless other (longer) data retention schedules are required by law in individual countries where mHub has an office, the following data retention schedule applies to all mHub and affiliate offices:

- Permanent: Articles of incorporation, corporate ownership and shareholding information, annual financial reports, tax returns, financial audits
- 10 years from the end of the current calendar year: All tax-related data. This includes, among others, corporate tax returns and supporting records (including all invoices and receipts etc), payroll tax records (including wages, pension payments, tax deposits, benefits etc), accounting services records (including financial statements, check registers, profit and loss statements, budgets, general ledgers, cash books etc), and operational records (including bank statements, credit card statements, canceled checks, cash receipts etc).
- 6 years from the end of the current calendar year: All other business-related data. This includes, among others, business licenses and permits, board meeting minutes, corporate and vendor contracts, insurance contracts and policies, employment and employee relations and contracts, payroll and social security services, client's records, clients' records, clients' assessments, and all general strategy, policy and procedure documentation.