Data Retention Policy

Introduction

This data retention policy sets out the obligations of The Menopause Club ("us/we/our") and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control.

This policy applies to our entire organisation including our officers, employees, agents and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

We are registered under the Information Commissioner's Office under registration number TBC.

Objectives

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a 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.

This Policy sets out the procedures that are to be followed when dealing with personal data and how we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

With this in mind, this policy should be read in conjunction with our other policies which are relevant such as our data protection policy and IT security policy.

Security and Storage

All data and records are stored securely to avoid misuse or loss. We will process all personal data we hold in accordance with our IT Security Policy [**OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data].

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

Examples of our storage facilities are as follows:

All online password protected using LastPass to ensure password security

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the [COMPANY'S] central computer system instead of individual PCs.

Retention Policy

Data retention is defined as the retention of data for a specific period of time and for back up purposes.

We shall not keep any personal data longer than necessary, but acknowledge that this will be dependent on the different types of documents and data that we have responsibility for.

As such, our general data retention period shall be for a period of 5 years. Our specific data retention periods are set out below

Type of data	**Type of data subject**	**Type of processing**	**Purpose of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**	**Data accuracy and minimisation review date**
Customers	Email, contact details, address	Online through mailchimp, memberpress and paypal	Marketing, sales, information	3rd party GDPR compliant companies i.e. mailchimp and paypal	5 years	Annually
Business contacts	Email, Contact details	Email and social media	Networking and information	Linked on, Facebook, Twitter	5 years	Annually
Employees	n/a					
Contractors	Email, Contact details Payment details	Email, password protected laptop	Doing business/Buying	Bank for online payments	5 years	Annually
Potential employees	n/a/					

From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of our retention periods, we shall delete confidential or sensitive records categorised as requiring high protection and very high protection, and we shall either delete or anonymise less important documents.

Our Managing Director is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.