# GDPR PRIVACY NOTICE FOR CLIENTS

This notice describes what personal data we collect from you and how we store and process it as part of the services provided by the Microbiome Group practice. In the course of our practice we will collect, process and store personal data as a data controller.

We would like to reassure you that we adhere to all laws and procedures relating to the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 or other applicable data privacy legislation and will only use your personal data to provide you with the specific service or services you explicitly agree to. We are registered with the Information Commissioner's Office (ICO): registration reference ZB152859.

## A. YOUR RIGHTS

(a) the right to access: You may request a copy of your clinical file for free at any time by emailing us. Your records are identifiable, retrievable and intelligible as per GDPR requirements. We will comply within 30 days.

(b) the right to rectification: You may update any of the information we hold for you at any time. We will amend them immediately.

(c) the right to erasure: You may request that we erase your data. We will comply within 30 days unless we cannot for legal reasons.

(d) the right to restrict processing: You may request that we restrict how we process your data. We will comply within 30 days unless we cannot for legal reasons.

(e) the right to object to processing: You may object to us processing your data. We will comply within 30 days unless we cannot for legal reasons.

(f) the right to data portability: Your data is retrievable and may be able to be moved if necessary.

(g) the right to complain to a supervisory authority: If you believe we have contravened the GDPR, you may contact the ICO.

(h) the right to withdraw consent: You may withdraw your consent for us to hold your information. We will comply immediately unless we cannot for legal reasons.

(i) the right to request information about the existence of automated decision-making, including profiling.

(j) the right to be notified if your personal data is rectified or erased, or processing is restricted, in accordance with the above.

## B. DATA COLLECTION, PROCESSING & LEGAL BASIS

Below we have set out the categories of personal data and sensitive personal data (such as your microbiome data or medical history) we collect and how we process the data:

(a) we will hold your contact information such as name, email address, telephone number, home address, as well as your emergency contact's details where relevant, ("Contact Information") which we will use to provide our services and communicate either with you or your emergency contact in a secure manner;

(b) as a client, we will hold your biopsychosocial history and risk assessment data, other relevant medical history and ongoing information about your treatment and condition ("Medical Information") which we will use in order to provide our services to you;

(c) we may process certain financial information of yours, such as debit or credit card details, in order for us to receive payment in exchange for providing our services to you ("Financial Information");

(d) if you visit our website, we will hold "Cookie Information". A cookie is a small text file which asks permission to be placed on your computer's hard drive or mobile device. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. We use Cookie Information to analyse and improve our services or in order to customise the website according to your personal interests;

(e) a record of any correspondence or communication between you and us ("Communication Information") which we will use to provide our services and communicate with you;

(f) we may hold certain information about you in order to provide information about our services. This may include names, email addresses and other information ("Marketing Information") which with your additional consent we may use to market and promote our services.

We will process the Contact Information on the basis that you have consented to it (for one or more specific purposes), where the processing is necessary for us to comply with our obligations under a contract with you (for instance for the provision of our services to you as a client) or for our legitimate interests in providing services to you as a client or potential client. A legitimate interest in this context means a valid interest we have, or a third party has, in processing your personal data which is not overridden by your interests in data privacy and security.

We will process Medical Information on the basis that you have consented to it, where it is necessary for us to comply with our obligations under a contract with you or where it is necessary for the protection of your (or another person's) vital interests.

We will process Financial Information on the basis of our legitimate interests (in providing services to you) or as necessary for the performance of a contract with you.

Cookie Information will be processed on the basis you have consented to it or in the case of strictly necessary cookies, on the basis of our legitimate interests (in providing services to you).

Communication Information will be processed on the basis of our legitimate interests (in providing our services to you).

Marketing Information will be processed on the basis of our legitimate interests (in providing services to you) or on the basis that you have consented to it.

In addition to the above, all information may also be processed on the basis that it is necessary to comply with a legal obligation to which we are subject.

Generally, we will collect information directly from you. If for any reason, we obtain your personal data from any other third party your privacy rights under this notice are not affected and you are still able to exercise the rights contained within this notice.

You do not have to supply any personal data to us however in practice we would be unable to provide our services to you without personal data (for instance we will need contact information in order to communicate with you). You may withdraw our authority to process your personal data (or request that we restrict our processing) at any time but there are circumstances in which we may need to continue to process personal data (please see below).

## C. DISCLOSURE, DATA STORAGE & RETENTION

### Who has access to your personal data?

We do not disclose any information you provide to any third parties other than as follows:

(a) We may consult with other professionals involved in your treatment only with your explicit signed consent.

(b) If we believe you or another person is at risk of being harmed e.g. if we are concerned that you are in serious danger of attempting or completing suicide, in imminent danger or temporarily unable to take responsibility for your actions, we would advise the relevant emergency authorities and/or your doctor and/or your nominated emergency contact. Any decision to break confidentiality would not be taken lightly. We will usually consult with a colleague, the clinical supervisor and where possible, advise you as well. You have an ethical and legal right to know the importance of and/or see what is being said about you if you wish and we will make every effort to include you in the process except in circumstances where it would harm you or others to inform you (e.g. child protection situations, mental incapacity, terrorism).

(c) We may discuss our work in a general way with the clinical supervisor/mentor and supervision group in order to maintain high standards of practice. We will never use names or personally identifiable details.

(d) We participate in forums, listservs, relevant online groups and other opportunities to collaborate and consult with other professionals in order to further our training and skill set. We do not share names or identifying details.

(e) Your name may be contained in financial records and our online diary. It is possible that third parties may have access to those records, for example, an accountant, tax adviser, legal adviser or administrative assistant. We maintain agreements with these third parties to treat your data in compliance with UK GDPR requirements.

(f) We may be required to disclose some of your personal data to your health insurance company. For instance, if we invoice your health insurance company directly in respect of your treatment, we may be required to provide certain information including your Contact Information, appointment and attendance dates, progress notices and the applicable consultation or treatment fee.

(g) If an accident, illness or death prevents your practitioner from being able to contact you, another practitioner from within the Microbiome Group will be able to access the practitioner's client list and contact you if necessary. They will destroy personal and sensitive data and archive clinical notes safely at the appropriate time in line with GDPR requirements.

(h) from time to time we may transfer personal data to our processors or sub-processors which will include Wix, Stripe, G-drive and other secure and encrypted service and technology providers;

(i) we may be required to disclose certain data to regulators or other lawful authorities;

(j) if we are under a duty to disclose or share your personal data in order to comply with any legal obligation (for example, if required to do so by a court order or for the purposes of prevention of fraud or other crime);

(k) in order to enforce any terms and conditions or agreements for our services that may apply;

(l) as necessary in order to protect both our and your rights, property and safety (for instance in relation to fraud protection).

### What happens if there is a data breach?

Although we take measures to protect your data, information can be intercepted and breaches can occur. If there is a data breach, we will follow the regulations set out in Article 33 of the GDPR. This includes notifying the ICO of the nature and consequences of the breach within 72 hours, and any measures we have taken to address it, unless the personal data breach is unlikely to result in high risk to your rights and freedoms. We will also notify you without undue delay if the breach is likely to result in a high risk to your rights and freedoms.

### How long is your personal data stored for?

We review the personal data (and the categories of personal data) we hold on a regular basis to ensure the data is still relevant to our business and is accurate. If we discover that certain data we are holding is no longer necessary or accurate, we will take reasonable steps to update, correct or securely delete this data as may be required. Generally, we will aim to review all personal data held by us every 12 months.

Except where you explicitly agree otherwise or there is legal reason for us to continue storing it, your Contact Information, Financial Information, Communication Information and any other information not specifically mentioned in this section or privacy notice will be stored securely for a period of seven years from receipt of the data or after your final session with

the Microbiome Group, or until the client's 25th birthday in the case of a child, or for as long as is required under relevant law, regulation, policy, practice or procedure.

Marketing Information (such as names, telephone numbers and email address) will be stored for up to five years from the date on which you last interacted with us or until you unsubscribe.

Medical Information will be stored securely for a minimum period of seven years from the date of your last consultation with the practice or until the client's 25th birthday in the case of a child, or for as long as is required under relevant law, regulation, policy, practice or procedure.

## D. SECURITY

We will take reasonable steps to ensure that appropriate technical and organisational measures are carried out in order to safeguard the information we collect from you and to protect against unlawful access, accidental loss or damage. These measures may include (as necessary):

(a) protecting our servers with software firewalls;

(b) locating our data processing storage facilities in secure locations;

(c) encrypting all data stored on our server with an industry standard encryption method that encrypts the data between your computer and our server so that in the event of your network being insecure no data is passed in a format that could easily be deciphered;

(d) securely disposing of or deleting your data;

(e) regularly backing up and encrypting all data we hold.

We will take reasonable steps to ensure that we and our staff are aware of their privacy and data security obligations.

## E. COOKIES AND IP ADDRESSES

(a) A cookie is a piece of data stored locally on your computer or mobile device and contains information about your activities on the internet. The information in a cookie does not contain any personally identifiable information you submit to our website.

(b) On our website, we use cookies to track users' progress, allowing us to make improvements based on usage data. A cookie helps you get the best out of the website and helps us to provide you with a more customised service.

(c) Once you close your browser, our access to the cookie terminates. You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. To change your browser settings you should go to your advanced preferences.

(d) We are required to obtain your consent to use cookies. We will obtain this consent with a toolbar which appears when you first visit our website.

(e) If you choose not to accept the cookies, this will not affect your access to the majority of information available on our website. However, certain online services may not be available.

(f) An Internet Protocol (IP) address is a number assigned to your computer by your Internet Service Provider (ISP), so you can access the Internet. We may use your IP address to diagnose problems with our server, report aggregate information, and determine the fastest route for your computer to use in connecting to our website, and to administer and improve the website.

## F. INTERNATIONAL TRANSFERS

Our practitioners are based around the world, so we often conduct online consultation services from outside of the UK. Your personal data may also be transferred where some of our service providers (such as web hosting service provider) are based outside of the UK and in this instance, we will ensure that we have an agreement with such service providers to provide adequate safeguards and a copy of such agreements or information as to what these safeguards are will be made available.

## G. THIRD PARTY SERVICES

Our site may contain links to and from the websites of related services, our partner networks, advertisers or affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please review these policies before you submit any personal data to these websites.

Our testing companies also have their own privacy policies. Please ensure you are happy with these policies before you proceed with testing.

## H. NOTIFICATION OF CHANGES TO THE CONTENTS OF THIS NOTICE

We will post details of any changes to our policy on the website to help ensure you are always aware of the information we collect, use, and in what circumstances, if any, we share

it with other parties. Please check www.themicrobiomegroup/policies regularly for any updates.

## I. CONSENT

On booking a consultation through our online booking function, or subscribing to our email list, you will be asked to use a check-box to give consent for the Microbiome Group *"to collect, process, store and erase my personal data as set out in this Privacy Notice only to the extent that my consent is required in accordance with this Privacy Notice."*
Please discuss any concerns with us and we will try to accommodate your needs.