Natural Fertility Consultant
DATA PROTECTION POLICY

1 Introduction

1.1 Purpose of Policy

I, Brendan O'Brien, trading as the Natural Fertility Consultant, and owner of www.naturalfertilityconsultant.com, gathers and uses in the course of my business certain information about individuals in the EU and thus I am subject to the laws governing information storage as laid out in the General Data Protection Regulation. Such information can include names, addresses and contact information for clients, suppliers, and other people the organisation has a relationship with or may need to contact.
Pursuant to this regulation I am obligated to make this document available online describing how this personal data will be collected, handled, and stored in such a way as to comply with the General Data Protection Regulation.

1.2 Policy Statement

I am committed to a policy of protecting the rights and privacy of clients, staff, and others in accordance with General Data Protection Regulation.
I commit to:
• complying with both the law and good practice
• respecting individuals' rights
• being open and honest with individuals whose data I hold
• Registering my details with the Data Protection Commissioner.

1.3 Personal Data

The reason I hold personal data is as follows:
- Provision of direct healthcare through written and online contact
- Marketing and newsletters
- Case histories

In the course of providing healthcare certain special categories of personal data may be captured included race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health and sexual orientation.
In lay terms any given client could in theory share any personal information with me and therefore I would end up holding that information and as such it would be subject to the regulations.

1.4 Data Protection Principles

There are six data protection principles that are core to the General Data Protection Regulation. I will make every possible effort to comply with these principles at all times in my information-handling practices.

The 6 principles are:

1) Lawfulness, fairness and transparency.

- Data collection must be fair, for a legal purpose and I must be open and transparent as to how the data will be used.

2) Limited for its purpose

- Data can only be collected for a specific purpose.

3) Data minimisation

- Any data collected must be necessary and not excessive for its purpose.

4) Accurate

- The data I hold must be accurate and kept up to date.

5) Retention

- I cannot store data longer than necessary. My professional governing body NTOI and my insurance provided require me to hold client details related to therapy for at least 7 years.

6) Integrity and confidentiality

- The data I hold must be kept safe and secure.

1.5 Key risks

In my work the main risks to the the privacy of your information are:

- That it may fall into the wrong hands through poor security
- inappropriate or unprofessional disclosure of information
- Inappropriate therapy advice as a result of the information I hold being inaccurate or insufficient.

2 Responsibilities

I am the data controller for all personal data held on my systems and I am responsible for:

1. Analysing and documenting the type of personal data I hold
2. Checking procedures to ensure they cover all the rights of the individual
3. Identifying the lawful basis for processing data
4. Ensuring consent procedures are lawful
5. Implementing and reviewing procedures to detect, report and investigate personal data breaches
6. Storing data in safe and secure ways
7. Assessing the risk that could be posed to individual rights and freedoms should data be compromised

3 Data Recording, Security and Storage

3.1 Data accuracy and relevance

I will ensure that any personal data I process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. I will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

3.2 Data security

I will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, I will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

3.3 Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place within a locked filing cabinet where unauthorised personnel cannot access it.
- Printed data will be shredded when it is no longer needed after the cessation of my governing body's retention of records policy (7 years) has expired.
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used
- Cloud services used to store personal data will be assessed for compliance with GDPR principles. An authenticator app will be used to access cloud data.
- Data will be regularly backed up.
- All reasonable technical measures will be put in place to keep data secure

3.4 Data retention

- I will retain personal data for no longer than is necessary. This shall be in accordance with the guidelines of our professional association, NTOI.

4 Accountability and Transparency

1. I will ensure accountability and transparency in all our use of personal data.
2. I will keep written up-to-date records of all the data processing activities that I do and ensure that they comply with each of the GDPR principles.
3. I will regularly review our data processing activities and implement measures to ensure privacy by design including data minimisation, pseudonymisation, transparency and continuously improving security and enhanced privacy procedures.

5 Consent

1. I will ensure that any consents sought are specific, properly explained, and in plain language such that individuals can clearly understand why their information will be collected, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data.
2. Consents will be granular to provide choice as to which data will be collected and for what purpose.
3. I will seek explicit consent wherever possible.
4. I will maintain an audit trail of consent by documenting details of consent received including who consented, when, how, what, if and when they withdraw consent.
5. For online consent, I may use a cryptographic hash function to support data integrity, alternatively I will maintain the consents information in a spreadsheet with links to the consent forms.
6. I will regularly review consents and seek to refresh them regularly or if anything changes.

6 Direct Marketing

1. I will comply with both data protection law and Privacy and Electronic Communication Regulations 2003 (PECR) when sending electronic marketing messages. PECR restricts the circumstances in which I can market people and other organisations by phone, text, email or other electronic means.
2. I will seek explicit consent for direct marketing. I will provide a simple way to opt out of marketing messages and be able to respond to any complaints.

7 Subject Access Requests

7.1 What is a subject access request?

An individual has the right to

1. receive confirmation that their data is being processed
2. access their personal data and supplementary information

7.2 How to deal with subject access requests

1. I will provide an individual with a copy of the information requested, free of charge, within one month of receipt of request using commonly used electronic formats.
2. If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual will be informed within one month.
3. I can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, I can request the individual specify the information they are requesting.
4. Once a subject access request has been made, I will not change or amend any of the data that has been requested. Doing so is a criminal offence.

7.3 Data portability requests

1. I will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a PDF file, although other formats are acceptable.
2. I must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to within one month.

8 Transferring data internationally

There are restrictions on international transfers of personal data. I will not transfer personal data abroad without express consent.

9 Third Parties

9.1 Using third party controllers and processors

A. As a data controller and/or data processor, I will have written contracts in place with any third-party data controllers (and/or) data processors that I use. The contract will contain specific clauses which set out our and their liabilities, obligations, and responsibilities.
B. As a data controller, I will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.
C. As a data processor, I will only act on the documented instructions of a controller. I acknowledge our responsibilities as a data processor under GDPR and I will protect and respect the rights of data subjects.

9.2 Contracts

1. Our contracts will comply with the standards set out by the Data Protection Commissioner and, where possible, follow standard contractual clauses.
2. Our contracts with data controllers (and/or) data processors will set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

10 Reporting breaches

1. Any breach of this policy or of data protection laws will be reported as soon as practically possible after I become aware of a breach.

2. I have a legal obligation to report any data breaches to Data Protection Commissioner.