Data Protection Policy

What is Data Protection?

The Data Protection Act (the Act) aims to protect individual's fundamental rights and freedoms, notably privacy rights, in respect of personal data processing.

The Act applies to paper and electronic records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data.

Data protection operates by giving individuals the right to gain access to their personal data. This is done by making a request in writing to Daneo Services which they are entitled to:

- a description of their personal data
- the purposes for which they are being processed
- details of whom they are or may be disclosed to

DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

DANEO SERVICES shall:

1 Process personal data fairly and lawfully and, in particular, not process data unless these principles and the rules set out here are followed.

2 Obtain personal data only for specified and lawful purposes, and not process data in any manner incompatible with that purpose or those purposes.

3 Obtain personal data that is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay

5 Not keep personal data for longer than is necessary for their legitimate purposes.

6 Process personal data in accordance with the rights of data subjects under the Data Protection Act.

7 Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

9 The Daneo Services data protection officer will consult with **individual** therapists to ensure that an appropriate level of data protection consistent with the above statements exists in regard to any necessary data record keeping.

TYPES OF DATA HELD

Daneo services holds basic information for contacting purposes. Individuals therapists keeps personal data on our service users in order to carry out our work effectively. Individual therapists keep this data in a file relating to each service user in written or electronic form. All electronic files are password protected.

Specifically, we hold the following types of data:

a) Clients personal details such as name, address, phone numbers
b) Clients gender, marital status, information of any disability you have or other medical information
c) Clients information gathered through clinical notes
d) Staff employment details
e) Staff education and training details including access N I, clinical practice insurance.

SERVICE USER RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in the section headed “Access to Data” below.
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as ‘rectification’;
d) the right to have data deleted in certain circumstances. This is also known as ‘erasure’;
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as ‘portability’;
g) the right to object to the inclusion of any information
h) Daneo Services’ records and stores clinical notes and this is not subject to any further processing or subject to third party engagement.

CLIENT ACCESS TO RECORDS:

Clients may see their own records. To do so they need to make a request in writing to their individual therapist. Before anyone is allowed to see any record, the manager must fulfil a legal duty of care to:

1. Ensure the person making the request for access is entitled to it.

2. Review the record itself to ensure anyone else's right to confidentiality will not be compromised by such access.

3. Ensure access is granted in a professional manner

4. Any data about third parties within the record will be withheld to preserve the confidentiality of the third party, unless the consent of the third party has been obtained for you to see this.

5. Information written by third parties which is about or refers to you will not be given until confirmation is obtained that access would not be harmful, or indeed requesting access through the third party, not us.

If you detect any factual inaccuracy in your records you may request changes.

Requests for client records will be responded to within 40 calendar days of receiving the request.

RESPONSIBILITIES

All relevant individuals, who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed an employee with responsibility for reviewing and auditing our data protection policy.

ACCESS TO DATA

Individuals have a right to access the personal data that we hold on them. To exercise this right, they should make a Subject Access Request. This request will be acted on without delay and within one month unless, in accordance with legislation, we decide that an extension is required. Should this be the case individuals will be kept fully informed.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the person making the request. In these circumstances, a reasonable charge will be applied.

DATA DISCLOSURES

Counsellors will not disclose personal information about a client to anyone outside the counselling service without the client's permission, but may do so in exceptional circumstances such as:

- Where the counsellor would be subject to civil or criminal legal proceedings if the information was not disclosed to a court. (i.e. a counsellor cannot be required by an employment contract to break the law for you).
- If a child under the age of 18 is being abused
- If an abuser from the past currently has access to the children
- If you are at significant risk to yourself or others
- If you inform us of any act of terrorism
- If you break the law and others are at risk of harm

Confidentiality is a qualified right not an absolute one, but to break confidentiality a counsellor must act within the law and have a legitimate objective, such as those detailed above.

No counsellor will break confidentiality without a great deal of reflection, time permitting. Before breaking confidentiality, a counsellor will usually consult a colleague and perhaps take independent professional advice from a body such as the British Association for Counselling and Psychotherapy and the British Psychological Society and professional indemnity insurers. In addition, counsellors have professional codes to which they adhere that guide and help inform such actions

Every effort will be made to ensure that such disclosure is both reasonable and proportional.

DATA SECURITY

All Daneo staff are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

All staff are aware of their roles and responsibilities when their role involves the processing of data. All staff are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Individual therapists must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to service users should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

DATA DISPOSAL

Paper records are shredded after the mandatory six years of record holding is over, or when the organisation closes. Should a computer reach the end of its life the hard drive will be over written prior to disposal as this ensures the data is really destroyed.

INTERNATIONAL DATA TRANSFERS

Daneo services does not transfer personal data to any recipients outside of the EEA.

REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

TRAINING

All staff will receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data officer and all Daneo services personnel have received training regarding GPDR.

All employees who need to use the computer system are trained to protect service user's private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Margaret Maguire
Contact: 028 90711608

Appendix

DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race and ethnic origin.

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is 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.

Data Subjects

Data Subjects are defined as being individuals about whom information is held.

- Registrant Psychotherapists and Psychotherapeutic Counsellors Supervisors.
- Complainants, correspondents and enquirers
- Advisors, consultants and other professional experts