The Movement Centre for Targeted Training Policy

Data Protection

Version: 3
Updated: November 2018
Review date: November 2020

Data protection

1. Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

GDPR replaced the data protection directive (officially Directive 95/46/EC). The regulation was adopted on 27 April 2016 and has applied from 25th May 2018 after a two-year transition period. The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect The Movement Centre (TMC).

The Regulations cover both written and electronic information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

All TMC staff are required to follow this Data Protection Policy at all times.

The Chief Executive is registered with the ICO and has overall responsibility for data protection within TMC but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Further information on Patients records can be found in TMC's Patients Records Policy.

Further information on HR can be found in TMC's Employees Data Protection Policy.

2. Definitions

Processing of information – how information is held and managed.
Information Commissioner - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. TMC is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data.
Personal data – any information which enables a person to be identified. Processing such data refers to any operations performed on this personal data. Common types of personal data processing include (but are not limited to) collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.

Special categories of personal data – information under the Regulations, which requires the individual's explicit consent for it to be held by the Charity.
The special categories are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- health
- sex life and sexual orientation
- any criminal convictions and offences.

3. Data Protection Principles

As data controller, TMC is required to comply with the principles of good information handling.
The GDPR sets out seven key principles, as outlined by the ICO:

1. **Lawfulness, fairness and transparency:** processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
2. **Purpose limitation:** 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 ('purpose limitation'
3. **Data minimisation:** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. **Accuracy:** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. **Storage limitation:** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6. **Integrity and confidentiality (security):** 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 ('integrity and confidentiality')
7. **Accountability:** "The controller (TMC) shall be responsible for, and be able to demonstrate compliance with, point 1 ('accountability')."

TMC must also ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

4. Processing Data

In order to process Data TMC must establish the most appropriate lawful basis.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

TMC uses different types of lawful bases depending on the type of data being processes. Full details can be found in TMC's Privacy Policies.

4.1. Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email/electronic

Face-to-face/written: A pro-forma should be used.
Telephone: Verbal consent should be sought and noted on the case record and on Salesforce.
E-mail: The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of insurance products were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record (e.g. Salesforce). The verbal consent is to be recorded in the appropriate fields on the database or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and online. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by TMC then the Head of Clinical Services should discuss with the CEO at the earliest opportunity.

5. Legitimate interests

Legitimate interests are the most flexible lawful basis for processing, but TMC should not assume it will always be the most appropriate.
It is likely to be most appropriate where TMC uses people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Where it is believed that legitimate interests apply TMC should ensure that people's rights and interests are protected.

The ICO outlines three elements to the legitimate interest's basis:

- Identify a legitimate interest;
- Show that the processing is necessary to achieve it; and
- Balance it against the individual's interests, rights and freedoms.

The legitimate interests can be TMC's interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary. If TMC can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply. When exercising legitimate interest TMC must balance the organisation's interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override TMC's legitimate interests.
TMC should keep a record of the legitimate interests assessment (LIA) to help demonstrate compliance if required and include details of your legitimate interests in your privacy information. Please see TMC's Privacy Policy for more details.

6. Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.
3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis
4. A client's individual consent to share information should always be checked before disclosing personal information to another agency.
5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive should first be sought.
6. Personal information should only be communicated within TMC's staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

6.1 Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If TMC's work involves you having personal / and/or special categories of personal data at home or in TMC's car, the same care needs to be taken. Patients records must also be dealt with in accordance with TMC's Patient Records Policy.

6.2 Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

6.3 Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only. All information on the database (salesforce) is also held securely and is password protected.

Computer monitors in the reception area, or other public areas, should be positioned in such a way so that visitors and patients cannot see what is being displayed. All members of staff should lock computers when leaving it unattended.

Firewalls and virus protection are to be employed at all times to reduce the possibility of hackers accessing TMC's system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

6.4 Cloud Computing

When commissioning cloud based systems, TMC will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

- **Salesforce**

  TMC currently uses one cloud based data management systems to hold and manage information about its service users, donors/supporters and contacts. Salesforce is a Customer Relationship Management (CRM) platform. Salesforce takes the safety of its clients' data very seriously. It has been certified to comply with a number of international standards, including PCI DSS, FISMA, ISO/IEC 27001:2005, SAS 70 Type II, SysTrust, and Eu-US and Swiss-US Safe Harbor. Full details of how Salesforce ensures client's data is protected can be found here: http://www.nicva.org/data-protection-toolkit/templates/legitimate-interests-assessment-template. Salesforces' Privacy Policy can be found here: https://www.salesforce.com/uk/company/privacy/.

- **Xero**

  Xero is cloud accounting software used by TMC. Xero is committed to protecting personal data and have appropriate technical and organisational measures in place to make sure that happens. For more information about security, check out Xero's security pages. Xero's Privacy Policy can be found here.

6.5 Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. TMC will not share or sell its supporter data with outside organisations. Service user information will only be shared with written consent from the family.

TMC holds information on TMC's staff, volunteers, clients and other supporters, to whom we will from time to time send copies of TMC's newsletters, magazine and details of other activities that may be of interest to them. Specific consent to contact will be sought from TMC's staff, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from TMC's mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

The following statement is to be included on any forms used to obtain personal data:

I agree to The Movement Centre contacting me with marketing information (relating to my enquiry) and on the other services that they offer. This may include email and postal information and marketing. In order to do this The Movement Centre will retain details of my name, company, address and other data on the services I am interested in and commission from them. I understand that this information will not be shared with other parties and that I may request a copy of the data held and may also request that The Movement Centre stop sending me this information at any time by email to info@the-movement-centre.co.uk or by telephone on 01691 404248.

6.6 Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on TMC's website.

6.7 Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for TMC should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception should operate a clear desk practice so that any paperwork containing personal and/or special categories of personal data is not left unattended or in public view on the desk, where passers-by could see it.

When sending emails to outside organisations, e.g. physiotherapist or GP, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g. patients' notes taken to ORLAU) should be treated as confidential and kept securely as if it were held in the office. Please see the Patients Records policy for further details.

6.8 Retention of Records

Paper records should be retained for the following periods at the end of which they should be securely disposed of:

- Patient Records - please see TMC's Patients Records Policy.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.

- Declaration of Confidence forms - 6 years
- Other documentation, e.g. clients care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

All records are to be anonymised 25 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.) Please see TMC's Patients Records Policy.

7. What to Do If There Is a Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

If you discover, or suspect, a data protection breach you should report this to the Chief Executive who will review TMC's systems, in conjunction with the Management Team to prevent a reoccurrence. The Trustees should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner.

From 25th May 2018, organisations are required to consider whether a data breach poses a risk to people. It is important to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When this assessment has been made, if it's likely there will be a risk then the ICO must be notified; if it's unlikely then you don't have to report it. It is not necessary to report need every breach to the ICO. Where a breach is required to be reported to the ICO it must be within 72 hours of becoming aware of the breach, where feasible.
If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, TMC must also inform those individuals without undue delay.
TCM is also required to keep a record of any personal data breaches, regardless of whether you are required to notify.
In the event that the breach involves a service user please see TMC's Patients Records Policy for further guidance.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

Further guidance form the ICO on Data Breaches can be found here.

8. The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld)
- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, TMC is permitted to store the personal data but not further process it. TMC can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

TMC will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. TMC must comply with such requests within 30 days of receipt of the written request.

Please see TMC's Privacy Policy for further details of an individual's rights.

9. Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further information is available at www.ico.org.uk.

10. Details of the Information Commissioner

The Information Commissioner's office is at:
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Switchboard: 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

11. Review

This policy will be reviewed every two years (November 2020), or earlier if appropriate, to take into account any changes to legislation that may occur, and/ or guidance from the Information Commissioner.