The Mediators' Institute of Ireland

Data Protection Policy

May 2018

Introduction

The purpose of this document is to provide a concise policy document regarding the Data Protection obligations of Mediators' Institute of Ireland (hereafter "the MII"). This includes obligations in dealing with personal data, in order to ensure that the company complies with the requirements of the EU General Data Protection Regulation (GDPR) 2016/679.

Who We Are

The Mediators' Institute of Ireland is a company limited by guarantee, registered under Part 18 of the Companies Act, 2014.

The main object for which the MII is established is to promote the use of mediation as a process of dispute resolution in all areas in Ireland by ensuring the highest standards of education training and professional practice of mediation and by increasing public awareness of mediation.

The MII is a Data Controller of personal data relating to its staff and members.

Scope

The EU GDPR 2016/679 applies to the keeping and processing of Personal Data, both in manual and electronic form.

This policy applies to all Personal Data collected, processed and stored by the MII in relation to its staff and members.

This policy applies equally to Personal Data held in manual and electronic form.

Data Protection Principles

The MII is obliged to comply with the principles the General Data Protection Regulation (EU) 2016/679 (Article 5) which can be summarised as follows:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('*lawfulness, fairness and transparency*');
2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('*purpose limitation*');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('*data minimisation');*
4. 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. 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; (‘*storage limitation’*);
6. 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’*).

Definition of Data Protection Terms

‘Personal Data’ means any information relating to an identified or identifiable natural person (‘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;

‘Sensitive Personal Data’ is data revealing**:**

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- or trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health or data concerning a natural person’s sex life or sexual orientation.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

‘Third Party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

‘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 transmitted, stored or otherwise processed;

Categories of Personal Data

The Personal Data records held by the MII include:

- Name
- Address
- E-mail
- Phone number
- Mediation qualifications
- Work Experience
- Insurance details
- CPD information

- Clients complaints

Please note that the MII does not retain any financial information or bank details submitted by members or affiliates after payments have been processed.

Purposes of processing:

- To provide our services in accordance with our membership requirements
- To fulfil our obligations
- To manage our business for our legitimate interest

Legal basis: Legitimate interest and members' consent

Location:

- *Online Profiles* - members' personal data is stored online on our website (www.themii.ie) and uploaded to our website by the MII members.
- *Computer records* are also stored on the office PCs that only personnel (Office Manager and Registrar) who are authorised to use the data can access on a 'need-to-know' basis.
- *Manual Records* are held in relevant filing system, in a secure, locked filing cabinet that only personnel (Office Manager and Registrar) who are authorised to use the data can access on a 'need-to-know' basis. Personnel is required to maintain the confidentiality of any data to which they have access.

Security:

- Online Profiles are password protected and only the Office Manager who is authorised to use the data can access on a 'need-to-know' basis.
- Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.
- Information on computer screens and manual files are kept hidden from callers to the MII office.
- Manual records are kept in a secure filing cabinet in locked offices.
- All waste papers, printouts are disposed of in a secure manner. Only authorised people should be able to access, alter, disclose or destroy personal data.

Sharing Data:

Information is sought directly from members and affiliates themselves primarily when applying for membership/affiliation or at the annual membership renewal stage.. When applying to become a member/affiliate of the Mediators' Institute of Ireland (MII) individuals are asked to provide personal data so that their application can be considered in line with the assessment criteria utilised by the MII to determine eligibility for membership or affiliation.

All members and affiliates are encouraged to renew their membership or affiliation online utilising a secure financial payment system. In some cases applicants may provide bank or credit card details in order to pay the application fee or annual subscription. The MII does not retain any financial information or bank details submitted by members or affiliates after payments have been processed.

The MII will only use a member/affiliate's information where it is necessary for us to carry out our responsibilities and duties. The MII does not share its members and affiliates details with other organisations other mentioned above.

Retention Period:

The MII is committed to ensuring that all members and affiliates data and complaint details are retained securely consistent with the mandatory periods of retention outlined below:

Purpose	Category of Files	Period not less than	Statutory or Regulatory reference
Protection of MII member – period of limitation within which clients can bring complaints against mediators	All Files – both in hard copy and in electronic storage format	6 Years	Statute of Limitations Act 1957
Compliance with Accounts regulations	All Accounts Files – both in hard copy and in electronic storage format	6 Years	Accounts Regulations, S.I. 421 of 2001

In line with the Statute of Limitations Act 1957, when a person ceases to be a member or affiliate of the MII their file and data (both in hard copy and electronic format) will be retained by the Institute for a period of 6 years.

If after 6 years a former member or affiliate has not sought to re-join, their hard-copy file will be shredded and electronic data deleted. Only their basic details (name, contact details, member/affiliate history etc.) will be retained by the MII and will be archived on the online system. After 6 years, Expired members will no longer be contacted by the MII in connection with their membership status.

Data contained in an Online Profile will be removed from the MII website on cessation of their membership or affiliation.

In addition the MII will retain for a period of 6 years details of all unsuccessful applications for MII membership/affiliation. Incomplete applications (where the applicant has not supplied one or more component of the application requirements) are deleted after 3 months.

Data Subject Rights

As a member/affiliate of the Mediators' Institute of Ireland you have certain legal rights to control your information and the manner in which we process it. This includes:

1) Right to be informed

This right provides the data subject with the ability to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing.

2) Right to access

This right provides the data subject with the ability to get access to his or her personal data that is being processed. This request provides the right for data subjects to see or view their own personal data, as well as to request copies of the personal data.

3) Right to rectification

This right provides the data subject with the ability to ask for modifications to his or her personal data in case the data subject believes that this personal data is not up to date or accurate.

4) Right to withdraw consent

This right provides the data subject with the ability to withdraw a previously given consent for processing of their personal data for a purpose. The request would then require a data controller to stop the processing of the personal data that was based on the consent provided earlier.

5) Right to object

This right provides the data subject with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent, if consent was appropriately requested and no processing other than legitimate purposes is being conducted.

6) Right to object to automated processing

This right provides the data subject with the ability to object to a decision based on automated processing.

7) Right to be forgotten

Also known as right to erasure, this right provides the data subject with the ability to ask for the deletion of their data. It is important to note that this is not an absolute right, and depends on retention schedule and retention period in line with other applicable laws.

8) Right for data portability

This right provides the data subject with the ability to ask for transfer of his or her personal data. As part of such request, the data subject may ask for his or her personal data to be provided back (to him or her) or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Dealing with a Data Access Requests

Under Article 15 of the GDPR, an individual has the right to be informed whether the MII holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept.

Prior to complying with a Data Subject Access Request, we require proof of the applicant's identity and address to ensure that personal information is not given to the wrong person. Information requested will be provided by the MII **within one month** of the identity of the individual of the data subject being verified. *See Data Access Request Form template in Appendix 1.*

In the normal course of events, the MII is obliged to respond to your access request within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where the MII is extending the period for replying to your request, it must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.

There is no fee payable by you to make an access request - the MII will deal with your request for free. However, where the MII believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the MII may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s).

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the MII refuse to furnish the data to the applicant.

Personal Data Security Breach

Article 4(12) of the EU General Data Protection Regulation (GDPR) 2016/679 defines **"personal data breach"** as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

"Destruction" happens where the data no longer exists, or no longer exists in a form that is of any use to the controller.
"Damage" takes place where personal data has been altered, corrupted, or is no longer complete.
"Loss" of personal data should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorized to receive (or access) the data, or any other form of processing which violates the GDPR.

A personal data breach can happen for a number of reasons, for example:

- Loss or theft of data or equipment on which data is stored, or through which it can be accessed
- Loss or theft of paper files
- Hacking attack
- Inappropriate access controls allowing unauthorised/unnecessary access to data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

Data Breach Handling Procedure

The purpose of the Data Breach Procedure is to ensure that all necessary steps are taken to:
(i) contain the breach and prevent further loss of data
(ii) ensure data subjects affected are advised (where necessary)
(iii) comply with the law on reporting the incident to the Data Protection Commissioner if necessary
(iv) learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future.

Under Article 33 (1) of the EU General Data Protection Regulation (GDPR) 2016/679, the MII as Data Controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, notify the personal data breach to the supervisory authority (Data protection Commissioner) competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the

supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Individuals have to be notified if adverse impact is determined (Article 34).

Data Breach Management Plan

The MII response to any reported data security breach will involve the following four elements.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed. *See Data Breach Reporting template at Appendix 2*

Policy Review

This policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines from the Data Protection Commissioner, legislation and feedback from members, staff and others.

Contact Us

If you have any concerns over the manner in which your personal information may have been retained or used, you can contact the MII by email at info@themii.ie or by post to

The Mediators' Institute of Ireland
Unit 2.1
The Distillers Building
Smithfield
Dublin 7

Under Article 77 of the GDPR, you have **the right to lodge a complaint** with the Data Protection Commission if you consider that processing of your personal data is contrary to the GDPR.

A complaint can be made directly to the Office of the Data Protection Commissioner at: info@dataprotection.ie

Postal Address
Data Protection Commissioner
Canal House
Station Road
Portarlington
R32 AP23 Co. Laois

APPENDIX 1

Mediators' Institute of Ireland

Data Access Request Form

Date issued to data subject:

Access Request Form: Request for a copy of Personal Data under Article 15 of the EU General Data Protection Regulation (GDPR) 2016/679

Important: Proof of Identity must accompany this Access Request Form (e.g. official/State photographic identity document such as driver's licence, passport). Please note we have the right to require that you identify yourself before we will respond to any access request.

SECTION 1

Full Name	
Maiden Name *(if name used for MII membership)*	
Address	
Contact number *	Email addresses *

** We may need to contact you to discuss your access request*

Please tick the box which applies to you:

Current member/affiliate ☐	Former member/affiliate ☐
	Insert Years From/To:

SECTION 2 Data Access Request:

I, ……..[insert name] wish to be informed whether or not the Mediators' Institute of Ireland holds personal data about me and to be provided with a description of this data

and to be informed of the purpose for holding such data. I am making this access request under Article 15 of the EU General Data Protection Regulation (GDPR) 2016/679.

Signed …… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full? ☐
2) Signed and dated the Access Request Form? ☐
3) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.) ☐

Please return this form to the following address:

The Mediators' Institute of Ireland
Unit 2.1
The Distillers Building
Smithfield
Dublin 7

FOR MII USE ONLY:

Reference No:	DP/
Date request received:	
Identity verified:	YES/NO
If Yes: Original ID supplied in person: If Yes, original evidence of ID checked and returned to requester: Copy ID attached to request: If yes, ID verified and documents shredded by:	 YES/NO YES/NO YES/NO

APPENDIX 2

Data Breach Reporting Template

	Report by:	**Name:** **Job Title:** **Date:**
1.	Summary of event and circumstances	Who, what, when, who etc.
2.	Type and amount of personal data	Title of document(s)-what information is included-name, contact details, financial, sensitive or special category data.
3.	Action taken by recipient	
4.	Action taken to retrieve data and respond to breach	
5.	Procedure/policy in place to minimise risk	Communication, secure storage, sharing, exchange.
6.	Breach of policy/procedure by officer/member	Has there been a breach of policy and has appropriate management action been taken?
7.	Details of notification to data subject. Complaint received?	Has data subject been notified? If not, explain why. What advice has been offered?
8.	Details of Data Protection training provided.	Date of most recent training by staff/ councillor involved
9.	Risk assessment and changes need to prevent further data loss	
10.	Conclusions and learning points	