



## Irish Motor Neurone Disease Association Data Protection Policy 2018

### Policy Statement

The Irish Motor Neurone Disease Association is conscious of its responsibilities to all its stakeholders (clients, their families/carers, members, statutory bodies, trusts, foundations, corporations, and the public at large), to be fully accountable for all data collected, to make the best possible effort to protect that data and to be accountable to all concerned.

The Association also recognises the importance of safeguarding the privacy rights of individuals in relation to the processing of their personal and personal sensitive data (i.e. data pertaining to physical and mental health). It aims to adhere to the highest standards in this regard and to meet the legal requirements in doing so.

### 1 General Principles

#### 1.1 Scope

The purpose of this document is to set down the principles and ground rules and to provide guidance on all aspects of data collection, processing, filing, storing and sharing. It sets out the requirements of staff and volunteers of the Association in this regard as well as providing some general good practice guidelines on collecting, controlling and protecting data. The Association is not obliged to register with the Data Protection Commission, however, the Association must comply with existing data protection laws.

As part of the internal client registration process the Association will collect, store and process personal and sensitive personal data (i.e. data pertaining to physical and mental health). This data relates to living individuals who can be identified from the data or from the data in conjunction with other information. As such the Association is recognised, by the Data Protection Commission and others, as a **data controller**. By collecting the personal and sensitive personal data, all registered clients, their families and carers will be treated equally and entitled to equal access to services.

As stated the Association is subject to legislation dictated by the Data Protection Acts 1988 to 2018 as well as the General Data Protection Regulation (GDPR). As such, the Data Protection Commission may investigate complaints or carry out investigations to inspect the type of personal information kept by the Association, how it is processed and the security measures in place. Individual data subjects also have rights in respect of their personal data. It is up to the Manager of the Association to communicate with the staff of the Association, the Chairperson, and the Board Members as to the Association's data protection policy and how the policy is maintained.

The policy also acts to:

- Inform MND clients, their families, and carers as to what information is required to register with the Association.

- Inform MND clients, their families and carers how their data will be stored, processed, and protected.
- Inform MND clients, their families and carers if their data will be shared and how third parties (who must be deemed appropriate and lawful e.g. Physical and Sensory Disability Database, HSE, Hospice, Central Remedial Clinic, Community Health Services, Counselling Services, Clinical Research, TCD) intend to use their data.
- Inform staff and volunteers of the IMNDA as to how they should obtain data fairly and the way in which it should be processed once obtained.
- Inform staff and volunteers of the IMNDA of what is relevant data (not excessive) and the length for which it should be retained.

## 1.2 Responsibility

As a data controller, the Association has certain key responsibilities in relation to the information which it processes. These responsibilities are summarised in terms of seven principles which are enshrined in the GDPR and outlined within the procedure below.

The Manager is responsible to the Chairperson and Board of Directors for ensuring that this policy document is adhered to in both spirit and fact. All other staff, members, healthcare professionals, and volunteers are expected to co-operate.

The Manager is responsible for ensuring that all staff and volunteers are aware of their responsibilities through appropriate induction training and the availability of an internal data protection policy.

All requests for personal data must be obtained fairly by an identified staff member of the Association.

If data is to be shared, it can only be done so by having obtained the consent of the data subject (or where they are unable to do so by a family member or carer). The only exception is where it is necessary to share personal data in order to deliver a service requested by the data subject or their family member/carer.

With regard to data, staff of the Association must adhere to the following rules:

- Principle 1 – Transparency: Transparency demands that data processing be undertaken in a transparent manner and data subjects are provided with certain information in relation to processing of their personal data.
- Principle 2 - Purpose Limitation: Purpose Limitation is the principle that personal data is only processed for the particular purpose(s) for which it was collected (and for closely related purpose(s)).
- Principle 3 - Data Minimisation: Data Minimisation demands that collection of personal data is limited to what is adequate, necessary and relevant to the purposes for which it was collected.
- Principle 4 – Accuracy: The principle of Accuracy requires that personal data must be accurate and kept up to date and every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified.

- Principle 5 - Storage Limitation: Under the principle of Storage Limitation personal data is not to be kept in an identifiable form for any longer than the purposes for which it was collected (subject to certain limited exceptions).
- Principle 6 - Integrity and Confidentiality: The principle of Integrity and Confidentiality requires that technical and organisational security measures be put in place to ensure that personal data is protected from various forms of data breaches.
- Principle 7 – Accountability: The seventh key principle is Accountability, which requires that data controllers are able to demonstrate compliance with each of their obligations under the GDPR

### 1.3 Measures

The procedures laid out below list the measures which must be taken to implement the policy.

## **2 Procedural guidelines**

### 2.1 Principle 1: Transparency

All requests for personal and sensitive personal data by the Association must be communicated, during the registration process, by an identified administrative or nursing staff using a patient registration form. During this process the following steps must be followed in order to obtain data fairly:

1. Staff member must state their name clearly to the client/family member/carer
2. Staff member must explain, clearly and simply, the purpose for collecting the personal and sensitive personal data (i.e. explain that it is necessary to register all those affected with MND to allow the Association to provide its support and specialised services).
3. Staff should identify the Manager of the Association as the point of contact if the client/family member/carer has any queries regarding Data Protection Legislation or how their data is being processed.
4. Staff member must make the client/family member/carer aware of the persons or categories of persons to whom the data may be disclosed. Data collected by the Association may be shared with members of the multi-disciplinary team. The multi-disciplinary team of healthcare professionals working with MND clients in Ireland is as follows: General Practitioner, Consultant Neurologist, MND Clinical Nurse Specialist, Public Health Nurse, Occupational Therapist, Speech and Language Therapist, Neurology Nurse, Palliative Care Nurse, Social Workers, Social Care Workers, and Physiotherapists from the hospital, hospice, community and remedial environments.
5. Staff member must explain whether the replies to the questions being asked are obligatory and the consequences of not providing replies to those questions.
6. Staff member should make the client/family member/carer aware that the client has a right to access their personal data.
7. Staff member should make the client/family member/carer aware that the client has a right to amend data if it is inaccurate.

8. Staff member should provide any other information that may be deemed necessary to ensure the client has all the information necessary so to be aware as to how their data will be processed (i.e. check that the person is clear about how their data is going to be used).

In addition, where the data has not been obtained directly from the client, all the above must be clearly explained to the family member/carer/healthcare professional so that they may inform the client.

Processing data refers to performing of any operation of set of operations on data, including:

- Obtaining, recording or keeping data.
- Collecting, organising, storing, altering, or adapting the data.
- Retrieving, consulting or using the data.
- Disclosing the information or data by transmitting disseminating or otherwise making it available.
- Aligning, combining, blocking, erasing, or destroying the data.

### Personal Data

To process personal data fairly, it must be obtained fairly (as set out above) and the client must have given consent to the processing or the processing must be necessary to prevent injury or other damage to the health of the client (as determined by a member of the multi-disciplinary team).

### Sensitive Personal Data

To process sensitive personal data fairly, it must be obtained fairly (as set out above) and

(a) The client must have given explicit consent to the processing of their data (i.e. the client has been informed of the purpose(s) in processing the data and supplied their data with that understanding).

or

(b) Processing the data is necessary to prevent injury or other damage to the health of the client or otherwise to protect the vital interests of the client in a case where, consent cannot be given or the Association (data controller) cannot reasonably be expected to obtain such consent.

or

(c) Processing the data is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation.

or

(d) Processing the data is for medical purposes (more information as to what constitutes medical advice is available from [www.dataprotection.ie](http://www.dataprotection.ie)).

## 2.2 Principle 2: Purpose Limitation

The Association may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose(s). Any client/family member/carer has the right to question the purpose for which the Association holds his/her data and the Association must be able to identify that purpose. To comply with this rule:

1. Staff member should clearly explain the reasons for collecting and retaining the data (as set out above in step 2 of obtaining data fairly)
2. The Association will only collect data for lawful purpose(s), these purpose(s) that is to:
  - (a) allow for the provision specialised information
  - (b) allow for the provision of specialised services
  - (c) link clients to the appropriate healthcare professionals
  - (d) to inform the HSE of funding requirements
  - (e) to inform the HSE Physical & Sensory Database
  - (f) to support ethically approved efforts of research
3. Staff member should be aware of the different sets of data held by the Association and the purpose(s) of retaining that information.

Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data i.e.

- (a) The data is used only in ways consistent with the purpose(s) (as outlined above) and
- (b) The data is only disclosed (or shared) with third parties in ways that are consistent with fulfilling the purpose(s) above.

Note: the rules above are lifted only in certain restricted cases (as outlined by Article 9 of the GDPR) where disclosure is required by law or where the client has made contact with the Association and instructed them to share their data with another party.

Any processing of personal or sensitive personal data by a third party must also be taken in compliance with the Acts. This requires that, as a minimum, any such processing takes place subject to a contract between the Association (controller) and the third party (processor) which specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data be deleted or returned upon completion or termination of the contract.

The Association, as data controller, is also required to take reasonable steps to ensure compliance by the third party with these requirements.

### 2.3 Principles 6: Integrity and Confidentiality

The Association must take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. High standards of security are essential for all personal data, even more so for sensitive personal data. As such the Association complies and exceeds the minimum standard of security as recommended by the Data Protection Acts. Security measures at the Association include but are not limited to the following:

- (a) Access to secure Computing Cloud Infrastructure which is restricted to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors.
- (b) Access to any personal data within the Association is restricted to authorised staff on a 'need-to-know' basis in accordance with policy.

- (c) Access to computer systems are password protected with other factors of authentication as appropriate to the sensitivity of the information.
- (d) Information on computer screens and manual files are kept hidden from person(s) calling into the office.
- (e) A back-up procedure is in operation for computer held data, including the support of an IT Security Company for back-up.
- (f) All reasonable measures have been taken to ensure that staff is made aware of the organisations security measures (as per the staff handbook and ongoing supervision/training) and they comply accordingly.
- (g) All waste paper, printouts, etc., are disposed of carefully and appropriately (i.e. using the shredding facility)
- (h) A designated person i.e. Manager is available for periodic reviews of the measures and practices in place.

Article 34 of the GDPR obliges Data Controllers to notify the Data Protection Commission and affected data subjects in the case of certain types of personal data security breaches. The Association will manage a Data Breach in accordance with this requirement.

#### 2.4 Principle 4: Accuracy

The Association may be liable to an individual for damages if it fails to observe the duty of care provision in the Acts applying to the handling of personal or sensitive personal data which tends to arise in relation to decisions or actions based on inaccurate data. In addition, it is also in the interests of the Association to ensure all data held is accurate for reasons of efficiency and effective decision making. As such the Association complies with the following:

- (a) Clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy.
- (b) There is a general requirement within the Association that any personal or sensitive personal data is kept up-to-date and is regularly and fully examined.
- (c) Appropriate procedures are in place, including review and audit, to ensure data is kept up-to-date.

#### 2.5 Principle 3: Data Minimisation

Data controlled by the Association, is only sought and retained to achieve a specific purpose or function (services, fundraising, finance, human resources etc.).

The Association uses a registration process to collect personal and sensitive personal data. The process involves completion of a patient registration form. The data collected on this form is the minimum specific criteria necessary to fulfil all purpose(s) (as outlined above). This data must be deemed:

- (a) Adequate in relation to the purpose(s) for which it was sought.
- (b) Relevant in relation to the purpose(s) for which it was sought.
- (c) Not excessive in relation to the purpose(s) for which it was sought.

Ongoing reviews are carried out on the relevance of personal and sensitive personal data sought from clients their families and carers through the use of various channels i.e. forms, website etc. and on current data already held.

## 2.6 Principle 5: Storage Limitation

The Association, as data controller, has a responsibility to be clear about the length of time for which data will be kept and the reason why the information is being retained. As per Data Protection legislation, data collected for one purpose cannot be retained once the initial purpose(s) cease. The data already held by the Association is subject to

- (a) A defined policy on retention periods for all items of personal and sensitive data held.
- (b) Management, clerical and computer procedures.
- (c) Appropriate anonymisation of personal and sensitive personal data after a defined period if there is a need to retain non-personal data.
- (d) Regular clearing and shredding of data by an appropriate staff member.

Usually we will retain personal data on file for the duration of the purposes for which it is provided plus a period thereafter (usually 6 years) for evidential, legal compliance or audit purposes.

## 3. Data Subject Rights

Data protection laws provide data subjects with various rights in respect of their personal data which are summarized below. The Association, as data controller, is obliged to comply with data subject rights requests within one month of receipt and no fee may be charged (unless there are exceptional circumstances).

Data Subject Right	Scope	Comment
Access (Art 15)	<ol style="list-style-type: none"> <li>1. Confirmation whether or not personal data are being processed by the Association;</li> <li>2. If so, access to the personal data; plus               <ol style="list-style-type: none"> <li>2.1. the purposes of the processing;</li> <li>2.2. the categories of personal data concerned;</li> <li>2.3. the recipients or categories of recipient to whom the personal data have been or</li> </ol> </li> </ol>	<p>The Association shall provide a copy of the personal data undergoing processing (not necessarily copies of documents). Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided by email.</p>

	<p>will be disclosed;</p> <p>2.4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;</p> <p>2.5. the existence of the Rights of Rectification, Restriction, Erasure and Objection;</p> <p>2.6. the right to lodge a complaint with the Data Protection Commission;</p> <p>2.7. where the personal data are not collected from the Data Subject, any available information as to their source;</p> <p>2.8. the existence of automated decision-making (n/a to the Association).</p>	
<p>Rectification (Art 16)</p>	<p>The right to have inaccurate personal data rectified and incomplete data completed.</p> <p>Art 19 GDPR requires the Data Controller to communicate any rectification or erasure of personal data or Restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Data Controller shall inform the data subject about those recipients if the data subject requests it.</p>	<p>Art 5(1)(d) GDPR applies the principle that “<i>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</i>”.</p>
<p>Erasure (Art 17, 19)</p>	<p>The right to have personal data erased where one of the following grounds applies:</p> <p>1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p>	<p>See Rectification above re Art 5(1)(d).</p>



	<ol style="list-style-type: none"> <li>2. the data subject withdraws consent;</li> <li>3. the data subject exercises the Right to Object and there are no overriding legitimate grounds for the processing;</li> <li>4. the personal data have been unlawfully processed;</li> <li>1.1 the personal data have to be erased for compliance with a legal obligation on the Association We will keep Personal Data only for as long as the retention of such Personal Data is deemed necessary for the purposes for which that Personal Data are Processed. Further details of the retention period for Personal Data is set out in our Records Management Policy.</li> <li>5. .</li> </ol> <p>See Rectification above re Art 19 GDPR.</p>	
<p>Restriction (Art 18, 19)</p>	<p>The right to restriction of processing where one of the following applies:</p> <ol style="list-style-type: none"> <li>1. the accuracy of the personal data is contested by the data subject, for a period enabling the Association to verify the accuracy of the personal data;</li> <li>2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;</li> <li>3. the Association no longer needs the personal data but they are required by the data subject for the establishment, exercise or defence of legal claims;</li> <li>4. the data subject has exercised the</li> </ol>	<p>Art 18(2) requires that where processing has been restricted such personal data shall, with the exception of storage, only be Processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.</p> <p>A data subject who has obtained restriction of processing shall be informed by the Data Controller before the restriction of processing is</p>

	<p>Right to Object pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.</p> <p>See Rectification above re Art 19 GDPR.</p>	<p>lifted (Art 18(3)).</p>
<p>Objection (Art 21)</p>	<p>The right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on “legitimate interest” legal basis in Art 6(1)(f), including profiling based on those provisions.</p> <p>Separate right to object to direct marketing.</p> <p>Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>	<p>The Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.</p>

#### Access to Health and Social Work Data

There are modifications to the right of access in the interest of the client or the public interest, designed to protect the client from hearing anything about him/herself that may cause serious harm to his/her physical or mental health or emotional well being. If a staff member is concerned by an access request, they must report the concern to the Manager, and the appropriate action will be taken. This action will be guided by the modifications and guidelines of the Data Protection Acts. The Association must also ensure that the client is aware that they can apply to have inaccurate data rectified or erased and that they have a right to complain to the Data Protection Commission.

In order to comply with data subject rights requests the following procedure is in place;

- (a) An appropriate staff member is available to receive the request and will inform the client that they are entitled to a copy of the data that the Association is holding pertaining to that client only.
- (b) The client must be informed as to what data is held by the Association pertaining to them and for what purpose(s).
- (c) The client must be told the identity of any third parties to whom this data has been disclosed.

To make an access request the client must

- (a) Apply to the Association in writing (this can include email)
- (b) Give clear details required to identify him/her and locate all information the Association may keep on that person.

The Association must then respond by

- (a) Supplying the data to the individual promptly and within one month of receiving the original request.
- (b) Provide the information in a form which will be clear to the person e.g. any codes or terms used must be explained.
- (c) If the Association does not hold any data pertaining to the person, an appropriate staff member must tell the individual within one month of the request.
- (d) If the Association restricts the request in accordance with one of the exceptions or restrictions set down in the Acts, an appropriate staff member must notify the individual in writing within one month of the request. The Association must also inform the individual of their right to complain to the Data Protection Commission about this refusal.

#### **4. Policy Review**

This policy will be reviewed by the Committee of the Board of Directors annually. The purpose of review is to ensure that the Association complies with any new legislation or regulation and that best practice standards are maintained.