GM Freeze Information Assurance Policy

VERSION 2
Adopted 30 October 2018

1. Introduction

The purpose of this policy is to ensure that we gather, store and use information about our staff, volunteers, management committee members, member organisation representatives, supporters and other individuals securely, fairly and legally.

2. Data Protection Act and General Data Protection Regulation (GDPR)

The Data Protection Act 2018 (the Act) is the UK's implementation of the European Union's General Data Protection Regulation (GDPR) and some other related legislation. Both regulate how 'personal data' must be managed and give individuals certain rights around the data that we hold about them.

2.1. GM Freeze is registered with the Information Commissioner to process personal data. We are named as a data controller under the register kept by the Information Commissioner.

2.2. Under the Act, 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.

2.3. The Act states that data must be processed according to seven enforceable data protection principles, included as Appendix 1.

2.4. The Act gives individuals the right to:

2.4.1. obtain their personal information from us except in limited circumstances.

2.4.2. ask us not to process personal data where it causes substantial unwarranted damage to them or anyone else.

2.4.3. claim compensation from us for damage and distress caused by any breach of the Act.

2.5. The act also states that you must have a valid lawful basis in order to process personal data (see appendix 2).

2.6. GM Freeze will maintain its registration as a Data Controller and comply with all requirements under the Data Protection Act 2018.

3. **Personal data collected and held by GM Freeze**

3.1. GM Freeze collects personal data from staff, Management Committee members, volunteers, members, supporters, mailing list members, petition/action signatories and enquirers. Data is collected via website sign-ups, email, telephone, hard copy sign-ups, written correspondence and face to face contact.

3.2. GM Freeze will only collect data for one of the following reasons:

3.2.1. Data subjects (the people to whom the data refers) have told us they would like to hear from us, e.g. through our mailing list, or through the post. For these people we rely on the lawful basis of consent and so will keep a record of when and how the data subject gave their consent. We will maintain and follow written operational procedures for gaining and recording consent consistently and effectively. We will ensure that data subjects know how to stop receiving communications from us and will reconfirm consent every five years.

3.2.2. Data subjects have a financial or other contractual relationship with us, such as being a supporter/member/donor, member of staff, board member, job applicant, supplier or similar relationship. For these people we rely on the lawful basis of contract to process data.

3.2.3. For another lawful basis as described in Appendix 2.

3.3. Whenever personal data is collected, GM Freeze will tell individuals how their data will be used. Wherever possible this will be built into standard text on any printed or electronic forms used to capture data. When individuals offer their personal data proactively we will inform them in our reply or acknowledgement how we will use their data.

3.4. GM Freeze will not sell, rent, distribute or otherwise make people's personal data available to any third party except where they have given us their permission to do so or where the law requires us to do so.

3.5. GM Freeze may, from time to time, use a third party or contractor (such as a mailing house) to process data on our behalf. In this instance we remain responsible for ensuring that data is processed in accordance with the Act and will follow the Information Commissioner's guidance on outsourcing. Specifically, any third party will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

3.6. GM Freeze may, from time to time, work jointly with members or other organisations on activities that include the collection and storage of personal data. Before embarking on such a project (or as soon as it becomes clear that an activity may include such an element if this is later), we will agree an information assurance action plan with the other party/ies, including, but not limited to:

3.6.1. Clear shared understanding of who will be responsible for collecting and storing personal data and what procedures they have in place to ensure compliance with this policy.

3.6.2. Clear shared understanding of who will have access to personal data once the joint project or activity is complete and what procedures are in place to communicate this to data subjects.

4. **Keeping data secure and up to date**

4.1. Electronic files containing personal details will be encrypted with a password. Passwords will only be shared with staff, Management Committee members or volunteers who have completed an information assurance induction and will never be communicated in a method that attaches them in any way to the data itself. For example, passwords must not be stated in emails to which data is attached.

4.2. Electronic files containing personal details will only be stored within online file sharing facilities once the Director is satisfied that adequate security measures have been put in place, either by the provider of the file sharing facility or by GM Freeze itself.

4.3. Hard copies of personal data will be stored securely. Where hard copies of personal data (such as sign-up sheets from events) need to be transferred from one location to another, this must be done in person or via a secure postal service.

4.4. We will take particular care not to accidentally disclose personal information, for example, when trying to match a telephone caller with data held electronically.

4.5. Email accounts which are used to receive, process or store personal data of any kind will be held securely. Access will only be given to staff, Management Committee members or volunteers who have completed the appropriate level of information assurance induction, as detailed under 6.2 or 6.3, below.

4.6. We will endeavour to keep personal data up to date, encouraging contacts to inform us of any changes and noting any such changes promptly. This includes cross-referencing where personal data about an individual is held in more than one place.

5. **Subject access**

5.1. Individuals (known in this context as data subjects) are entitled to see the information that we hold about them. This is often referred to as subject access. Individuals who make a written request and pay the appropriate fee are entitled to be:

5.1.1. Told where any of their personal data is being processed.

5.1.2. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.

5.1.3. Given a copy of the information comprising the data; and given details of the source of the data (where this is available).

5.1.4. There are some exemptions, detailed on the Information Commissioner's Office website

5.2. The Act requires us to comply with any such request within one month of receiving it. We will respond to all requests courteously and aim to comply within 20 calendar days of receiving the request.

5.3. We are no longer entitled to charge a fee for subject access unless it is "manifestly unfounded or excessive" or the individual requests additional copies following a request. In both of these instances, we will charge a "reasonable fee" based on our administrative costs, including staff time.

6. **Training and review**

GM Freeze will ensure that information assurance is prioritised in all interactions with individuals. In order to achieve this, we will:

6.1. Regularly review our procedures for data collection and management, including proof of consent where consent is the lawful basis for processing this person's data.

6.2. Require all staff, Management Committee members and volunteers who may have any contact with personal data to undergo an information assurance induction. This will involve reading and confirming to their Line Manager or the Director, their understanding of this Information Assurance Policy, including appendices.

6.3. Require all staff, Management Committee members and volunteers engaged in regular data collection or processing to read the Information Commissioner's guide to the General Data Protection Regulation (GDPR), view the commissioner's own training videos and discuss their contents with their Line Manager or the Director to ensure that they have fully understood their responsibilities.

6.4. Review and update this policy at least every three years.

7. **Responsibility**

The Director is responsible for ensuring that this policy is effectively implemented.

Appendix 1: Data Protection Principles

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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');

(f) 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').

Article 5(2) adds that:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Appendix 2: Lawful bases for processing

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

(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.)