Market Research Benevolent Association

Data Privacy and Data Protection Policy.

This document refers to the Data Protection Act 2018 & UK GDPR laws of the UK.

In this document the term 'donors' refers to people or organisations who have made a financial donation or donations to the MRBA, 'supporters' to people or organisations who have contributed to the running of the MRBA in a non-financial way, 'volunteers' to people who give their time for specific tasks, and 'cases' to people who have applied for or received help for general assistance or who have applied or received help under the MRBA Skills scheme.

Privacy Notices.

MRBA collects personal details for a number of purposes:

- to administer financial donations to MRBA funds, including communication with donors and to allow us to recover Gift Aid. This information is held in the Contact Database and includes contact details and amount of donation. This information will be kept for five years beyond a financial donation being made.
- to provide a newsletter, as well as other items relating to progress of the MRBA and invitations to events to persons with an interest in the MRBA including, but not limited to, donors, supporters, volunteers, and cases. This information is held in the Contact Database. This includes contact details, a record of material sent to them, events attended and similar activity. This information will be kept for as long as the individual is on the database, and name and basic contact details will be kept up to five years beyond the point at which the individual asks to be removed from the database. This is to ensure that the individual is not contacted again for at least five years.
- to hold contact details for volunteers such as trustees, management or other committee members and regional managers and others who may assist the MRBA.
- to maintain a record of cases, their circumstance and any assistance that they received.
- To administer the work and payment of employees.

It is the policy of MRBA that when personal data is supplied, the individual supplying the data will be provided with details of how that data will be held, either at the point of supplying the data or through a privacy notice to which their attention will be drawn.

The individual will be informed that their details will:

a) Be held by MRBA as data controller
b) Be held securely
c) Be used only for the legal purpose for which they were given
d) Be accessible only to those persons within MRBA who require the details for the purpose for which they were given
e) Not be used for any other purpose within MRBA other than that for which they were given without explicit consent.
f) Not be passed to any other organisation for their use without the explicit consent of the individual.
g) Be removed at any time at the request of the individual.

For donors, supporters, volunteers, cases and employee's data that relates to their status will be held on the basis of legitimate interest. For other purposes they will be required to give consent to their data being held by MRBA to be used for the specific purposes for which it was given. All other persons will be required to give consent to their data being held by MRBA to be used for the specific purposes for which it was given.

MRBA will not share personal data on any of its databases with any other organisation unless required to do so by law. Were it to wish to do so, consent must be sought from each individual whose data will be involved. The exception is where it may be passed to a Data Processor acting on behalf of MRBA, where the MRBA remains the Data Controller.

Example statement to be included as signature to all email communication for the purpose of marketing:

MRBA takes your privacy seriously. We will hold your personal details securely and they will be used only for the purposes to which you agree. They will be seen by the people who need to and will not be shared with any other organisation for their use without your express consent. You may ask to be removed from our database at any time. See our privacy policy at mrba.org.uk.

Individual's rights

It is MRBA policy to respect the rights of individuals who supply personal data both in accordance with the Data Protection Act 2018 and UK GDPR or other applicable privacy legislation that may vary from time to time.

Individuals who supply personal details to MRBA have a right to expect that:

a) The data will be held securely.
b) The data will be used only for the purpose for which it was given. Consent to use it for that purpose will have been freely given, specific to the purpose, and will require a positive indication that consent has been given.
c) Consent will be sought before it can be used for any other purpose, and that consent must be freely given, specific to the purpose and require a positive statement of consent by the individual.
d) The data will be made available within the MRBA only to people who have a need for access to it in order to carry out the legitimate purpose for which it was given.
e) Personal data will not be shared with any other bodies for their use without the explicit consent of the individual and that consent will be freely given, specific to the purpose and require a positive statement of consent by the individual.

Subject access requests

It is the policy of MRBA to respond to all subject access requests within one month in accordance with the Data Protection Act 2018, UK GDPR or other applicable privacy legislation, and to the satisfaction of the applicant.

To this end, the process for dealing a subject access request is:

1. When a request is received, MRBA will determine whether the subject data is held on any of the databases and other formats, together with what information is held on each.

Checks will include whether the entry on the database or other format is currently active or is flagged to avoid further contact.

2. The outcome of these checks will be communicated to the subject within one month of the receipt of the request with identification of the subject.

3. Requests to remove all or part of the information held on MRBA databases will be complied with within one month of the receipt of the request with identification of the subject. All reasonable efforts will be made to delete information from back up servers.

4. No charge will be made to the individual for checking the databases nor for removing information.

Children

The MRBA holds no personal data of children, nor has any contact with children either as financial donors, cases or as volunteers. It is not expected that personal data relating to children will be collected by MRBA.

The material collected by MRBA is not expected to contain any identifiable information regarding children. It is noted that from time to time applicants for funding may mention or detail children in a general sense, such as number of children or ages, but explicitly identifiable information will be collected or retained.

We therefore do not consider it necessary to adopt any policies regarding the handling of data relating to children. Should this situation change, the need for a policy will be reviewed.

Secure holding of information

It is the policy of the MRBA to hold all personal data securely in accordance with requirements of the Data Protection Act 2018, GDPR and PECR.

The MRBA DPO and Chair of the Management Committee are responsible for data protection compliance within MRBA and thereby responsible for matters of data security.

To meet adequate standards of security for personal data, all databases and other documents containing personal information will be handled as follows:

- Electronic databases shall not be loaded onto USB memory devices unless password protected.
- Electronic data is kept securely.
- Electronic databases shall not be transferred by email unless password protected. Passwords will be notified to the recipient separately.
- Electronic databases are held within the UK or EEA and compliant with privacy regulations..
- Hard copy data will be held in a locked cabinet, unless being used when it is the responsibility of the responsible data holder to ensure that it is kept secure.
- Only one copy of each database and a back-up copy shall exist. These will be held by the person designated as being the responsible data holder for that information or someone designated by them. An exception will be made for databases of contact details amongst closed groups (e.g. volunteers and committee members) for the purpose of contacting each other, where each person on the database may have a copy of that database.
- Where second copies are required for operational reasons they will be destroyed or deleted immediately after use. If they are not, they become a new database with a new responsible data holder. This can only occur, though, where there is a legitimate purpose for the new database. The existence of the new database and the person designated as the responsible data holder must be notified to the Secretary to the Trustees.
- Information will be updated as quickly as possible after the receipt of new information regarding either existing or new subjects.
- Where information is duplicated on different databases, the updating of information on one database will be informed to the holders of the same information. To this end, the administrator will hold a register of databases and the information which is held on each.

Data breaches

A data breach occurs when personal details become available to someone outside of MRBA who is not authorised to see them. It is the policy of MRBA to investigate such breaches, inform those affected and take corrective action as quickly as possible.

Should a breach occur the DPO/Chair of the Trustees as the persons responsible for data protection compliance, must be notified as soon as it is discovered. They will commence an investigation into:

a) The nature of the data involved and its sensitivity.
b) The extent of the breach in terms of number of individual records put at risk.
c) How the breach occurred.
d) The person or persons who may have seen the personal data as a result of the breach.

A report of the breach shall be made to the ICO within 72 hours if the breach is deemed to be likely to risk the rights and freedoms of the individual or individuals concerned or is on a large scale. The DPO/Chair will report to the Executive Committee as soon as possible, with implications for the data subjects, implications for MRBA and recommendations regarding changes in procedure to prevent any further occurrence. Full records will be kept of the breach and subsequent actions.

All individuals whose data has been or may have been compromised will be informed of the nature of the breach as quickly as possible.

All passwords protecting the database or databases involved must be changed immediately.

Privacy Impact Assessments

MRBA does not anticipate involvement with, nor the holding of personal data about, children or vulnerable people. There is therefore no requirement for a Privacy Impact Assessment.