DATA PROTECTION POLICY

POLICY STATEMENT

In order to operate efficiently, MAG must collect information about people with whom we work. These may include members of the public, current, past and prospective employees, funding bodies and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government or of donor governments.

The Data Protection Policy below sets out MAG's commitment to protecting personal data (please see "definitions" below) as a data controller and how we implement that commitment with regards to the collection and use of personal data. MAG

MAG is governed by a range of legislations including (in Europe), the General Data Protection Regulation (GDPR), Data Protection Act 2018 and the Privacy and Electronic Communications Regulation 2003 (PECR).

MAG considers that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. We fully appreciate the underlying principles of the data protection regulations and adhere to the provisions. MAG will seek to ensure that data processed by third parties is compliant with any relevant regulations. MAG will use the principles of the GDPR as a basis for responsible data-protection practices worldwide.

The GDPR is based on six key principles of lawful processing of data along with a further accountability principle which requires organisations to be responsible for and able to demonstrate compliance. Individuals have eight rights under GDPR placing certain obligations on organisations, a key one being transparency of data processing. An approach of privacy by design and default is required to meet these accountability and transparency requirements.

The PECR gives people specific privacy rights in relation to electronic communications such as text messages, phone calls and emails. There are specific rules on marketing calls and cookies which require organisations to obtain specific consent for certain unsolicited activities.

In the UK, MAG is registered with the Information Commissioners Office (ICO) to process personal data.

SCOPE

This policy applies to all staff (HQ, International & National), trustees, consultants and volunteers.
This policy is approved by the Board of Trustees.

DEFINITIONS

Data Protection Act 2018 (DPA) – the UK legislation that provides a framework for responsible behaviour by those using personal information.

EU General Data Protection Regulation (GDPR) – EU regulation that came into force on 25th May 2018.

Information Commissioners Officer (ICO) – the organisation responsible for implementing and overseeing the DPA and GDPR in the UK.

Data Protection Officer (DPO) – the DPO informs and advises on data protection, monitors compliance with law and internal policy, acts as point of contact with the ICO and must be allowed to act independently and report to the highest level of management.

Governance Nominations and Review Committee (GNRC) – Board Committee with responsibility for oversight of MAG's data protection compliance.

Personal Data - Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, posts on social networking websites, medical information, or a computer IP address.

Personal Data 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.

Special Categories – Certain types of personal data which are particularly sensitive in nature and require additional care. This includes data relating to the following: racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic and biometric data, health, sex life or sexual orientation.

Subject Access Request – An individual's right to obtain a copy of the information that is held about them.

1. ACTIVITIES REGULATED BY THE GDPR

Data processing
Processing personal data by or on behalf of the controller.

Data controller
To determine the purpose, conditions and means of the processing of personal data. The controller shall be responsible for, and be able to demonstrate, compliance with data protection principles.

1.1 ORGANISATION OF DATA PROTECTION COMPLIANCE IN MAG

GOVERNANCE NOMINATIONS AND REVIEW COMMITTEE (GNRC)
The Governance Nominations and Review Committee (GNRC) takes delegated responsibility on behalf of the Board of Trustees for oversight of MAG's data protection compliance. The committee reports to the Board as required.

MAG LEADERSHIP TEAM
The Leadership Team will:

- Ensure that MAG is compliant with the data protection regulations
- Promote awareness of data protection regulations throughout MAG
- Ensure that data protection arrangements are adequately resourced
- Provide exemplary leadership in all matters of data protection and promote a culture of privacy by design
- Ensure that a nominated representative within each HQ department is responsible for data protection compliance and provides a point of contact for all data protection issues within the team
- Ensure that each programme/region has a nominated in-country data protection representative who is responsible for data protection compliance and provides a point of contact for all data protection issues within the programme/region
- Report to the GNRC on all matters relating to data protection compliance
- Report all concerns and personal data breaches in line with the data breach process

MANAGERS
All managers in the UK and overseas will:

- Ensure that effective arrangements to deliver on MAG's Data Protection commitments are established and implemented within the team/programme
- Ensure that Data Protection compliance is a standing item at team meetings in HQ and the field

- Provide exemplary management in all matters of data protection and promote a culture of privacy by design
- Provide adequate training within the team/programme for all staff responsible for or with access to personal data
- Ensure that everyone handling personal data within the team/programme knows where to find further guidance and understands their responsibilities to good data handling
- Ensure that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly including dealing with Subject Access Requests in accordance with MAG's SAR Process
- Ensure that all personal data breaches are reported in accordance with MAG's Breach Reporting Process
- Regularly review data protection procedures and guidelines within the team/programme
- Report all concerns and personal data breaches in line with the data breach process

EMPLOYEES

All employees in the UK and overseas will:

- Ensure compliance with arrangements to deliver on MAG's Data Protection commitments including safe storage, deletion and data security as laid out in the MAG ICT Policy
- Make themselves aware of the legal obligations of applicable local laws and to seek information from the Data Protection Representative within the department/programme for advice or guidance
- Report all concerns and personal data breaches in line with the data breach process

DATA PROTECTION REPRESENTATIVES

- To act as the data protection focal point within departments/programmes and champion good data protection practices
- Deal with data protection issues and liaise with the DPO as required
- Assist the DPO with breach reporting
- Deal with subject access requests with support from the DPO

1.2 DATA PROTECTION PRINCIPLES

MAG will comply with the six data protection principles in the GDPR and will ensure that these are adhered to whenever processing any personal data. The Principles are:

1. The Transparency Principle – personal data shall be processed lawfully, fairly and in a transparent manner
2. Purpose Limitation – personal data shall be collected for specified, explicit and legitimate purposes. The purpose must be limited and lawful
3. Data Minimisation – personal data shall be adequate, relevant and limited to what is necessary for the purpose of the processing
4. Accuracy - personal data shall be accurate and, where necessary, kept up to date
5. Storage Limitation – personal data shall be kept for no longer than is necessary for that purpose or those purposes. Please see departments' individual guidelines for data retention periods.
6. Integrity and Confidentiality – personal data shall be processed securely with appropriate technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

As a data controller, MAG is responsible for and required to demonstrate compliance with these principles.

1.3 PERSONAL DATA BREACHES

MAG must report all personal data breaches to the ICO within 72 hours of becoming aware of the breach. The MAG Breach Reporting Process shall be followed when a breach has been identified.

When reporting a breach, the appropriate form obtained from the ICO must be used depending on the nature of the breach. The following information will be provided by the Data Protection Officer in liaison the Data Protection representative from the department/programme concerned and with their Line Manager if required:

- A description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, MAG will inform those individuals without undue delay.

The Data Protection Officer will keep a record of any personal data breaches and will ensure that the Charity Commission are informed of all personal data breaches reported to the ICO

1.4 SUBJECT ACCESS REQUESTS

Under the GDPR, individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information

The MAG Subject Access Request Process shall be followed as soon as an SAR is received.

MAG will acknowledge all subject access requests within five working days and provide a full response without delay and at the latest within one month of receipt. The nominated Data Protection Representative will manage requests for their department or programme in liaison with their Line Manager and the Data Protection Officer

REFERENCES

- **MAG ICT Policy**
- **Privacy Policy**
- **Breach Reporting Process**
- **Subject Access Request Process**
- **Fundraising Compliance Handbook**
- **Cookie Policy**
- **EU General Data Protection Regulation (GDPR) -** https://www.eugdpr.org/eugdpr.org.html
- **Data Protection Act 2018:** https://www.gov.uk/government/collections/data-protection-act-2018
- **Report a breach to the ICO:** https://ico.org.uk/for-organisations/report-a-breach/
- **Information Commissioners Office:** https://ico.org.uk/
- **Think Privacy Toolkit for Charities:** https://ico.org.uk/media/for-organisations/think-privacy/2586/ico-think-privacy-toolkit-charities.pdf
- **Please contact individual departments for details of record retention periods**

APPROVAL AND DATES

Governance, Nominations and Review Committee (GNRC) – 16 April 2019
Leadership Team – 16 April 2019
Board of Trustees – 10 May 2019
This Policy will be reviewed every year and is next due for review in May 2020

POLICY OWNER

Chief Executive