DATA PROTECTION & PRIVACY POLICY

Contents

1. Introduction

Data Protection Laws

This Policy reflects the requirements of the EU General Data Protection Regulation 2016/679 ('GDPR'), the UK Data Protection Act 2018 including its applied GDPR provisions ('DPA 2018'), the UK Privacy of Electronic Communications Regulations 2003 (known as 'PECR' and alternatively 'e-Privacy'), and all relevant EU and UK data protection legislation (collectively referred to herein as 'Data Protection Laws'). This Policy may be amended in response to further guidance that may issue once the UK leaves the European Union (e.g., enactment to replace the EU GDPR with a UK GDPR).

Data Protection Laws relate to any information from which an Individual can be identified (directly or indirectly) either on its own or together with other information. The DPA 2018 increased the level of potential fines for non-compliance depending on the nature of the breach, to the greater of GBP 17 million or 4% of global annual turnover.

Our donors and our regulators expect us take information security very seriously

MAG takes information security very seriously and protecting our information and IT systems is a key component of building and maintaining trust. The consequences of not securing information could expose the organisation and our brand to significant legal and regulatory censure, sanctions and fines. Personal information is legally protected and requires specific attention. Our regulators expect us to comply with best industry practice when securing all types of information.

This policy applies to everyone in the organisation who accesses or otherwise handles Personal Data

This policy applies to all Personal Data processed by MAG and is part of MAG's overall programme and approach to compliance with Data Protection Laws. This policy applies to all Personal Data processed by or on behalf of MAG (including where MAG outsources the management or Processing of Personal Data to third parties or other MAG Organisations).

All MAG Personnel (which for the purposes of this Policy includes all MAG employees, trustees, contractors and associates working for or on behalf of MAG) are expected to understand their responsibilities described in this Policy.

Non-compliance and associated data privacy risks must be identified and managed

Compliance with this Policy is mandatory. Failure to comply will not only put MAG's data protection compliance at risk, but could have disciplinary consequences for any MAG employees, associates or contractors found to be in breach, including adverse risk metrics and/or investigation and disciplinary action pursuant to the MAG Disciplinary Procedure, up to and including dismissal. In addition, breaches of Data Protection Laws can give rise to criminal and/or civil liability for the individuals concerned.

Monitoring and policy enforcement

The MAG Data Protection Lead (DPL) is tasked with monitoring the organisation's compliance with this Policy. This Policy (together with all Related Policies) is an internal document and cannot be shared with third parties, donors or regulators without prior authorization from the DPL.

Subject to applicable law or regulation, MAG reserves the right to:

- monitor, review and examine the use of MAG managed IT and information assets
- monitor and remove any software, files or information stored on any MAG managed device
- rescind access, without notice, to MAG networks and the use of MAG IT assets and resources
- discipline any MAG personnel for breaches of laws, regulation or policy

Contact us

For further information, email dataprotectionteam@maginternational.org if you would like to know more or need help with implementing this policy.

Policy ownership and approval

The Data Protection & Privacy Policy is owned by the Director of Governance and Business Transformation. This is version 0.3 and was approved by the Board of Trustees on 29th January 2021

Full document version control and history can be seen on the final page.

2. Definitions

Consent – is the means by which a Data Subject signifies their agreement to the Processing of Personal Data relating to them. Consent must be freely given, specific, informed and an unambiguous indication of the Data Subject's wishes, and must be expressed by a statement or clear positive action.

Data Controller – means a natural (living) or legal person, public authority, agency or other body which, alone or together with others, determines the purposes and means of the Processing of Personal Data.

Data Processor – means a natural (living) or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

Data Subject – means any identified or identifiable natural (living) person. A Data Subject is not a company or other legal person. This Policy may use the term 'Individual' as an alternative to the term 'Data Subject'.

EEA – means the European Economic Area, which is comprised of the 28 countries in the European Union, together with Iceland, Norway and the principality of Liechtenstein.

MAG Personnel – means employees, contractors and associates of MAG.

MAG – we, our, us means 'Mines Advisory Group'.

Individual – means 'Data Subject'.

Personal Data – means any information from which, alone or together with other information, an Individual can be identified. Personal Data can be factual, such as names, identification numbers, location information, and one or more identifiers such as IP addresses or cookies. Personal Data can also be an opinion about an Individual's actions or behaviour, or related to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of an Individual. Personal Data includes 'Sensitive Personal Data'.

Processing or Process – means any activity, operation or set of operations that is performed on Personal Data, including collecting, holding, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, aligning, combining, restricting, erasing or destroying.

Sensitive Personal Data – means Personal Data that relates to an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation, as well as criminal offences or convictions. Sensitive Personal Data is referred to as Special Categories of Personal Data in the EU General Data Protection Regulation.

3. MAG Requirements for Handling Personal Data

In our role as a charity and an employer, MAG takes data protection very seriously, whether the Personal Data relates to our donors, suppliers, contractors, business associates or current, past, or prospective MAG personnel.

In all cases, we expect MAG Personnel and all third parties Processing Personal Data for us or on our behalf to comply with these data protection principles:

Lawfulness, Fairness, and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner.

We will provide Individuals with clear and relevant information about how we process their Personal Data in order to ensure that the processing meets the requirements of Data Protection Laws.

Data Protection Laws permit processing of Personal Data for specific purposes to ensure data is processed fairly and does not adversely affect the Individual.

MAG must only process Personal Data when it is necessary and meets at least one of these six lawful bases for Processing:

- **Consent** – where the Individual has given their Consent for their Personal Data to be processed. Any processing must be strictly within the purposes for which the Consent is given. Explicit Consent is required in most cases when processing Sensitive Personal Data.
- **Contract** – where the processing is necessary for the performance of a contract with the Individual. This includes the performance of contracts to which the Individual is party or in order to take steps at the request of the Individual prior to entering into a contract.
- **Legal Obligation** – where the processing is necessary to comply with legal obligations to which we are subject.
- **Vital Interests** –where the processing is necessary to protect the vital interests of the Individual or another natural person.
- **Public Interests** – where the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in us. (Public interests must be 'substantial' when we are processing Sensitive Personal Data).
- **Legitimate Interests** – where the processing is necessary for our (or a third party's) legitimate interests provided they do not override the interests and fundamental rights of the Individual. Where we rely on this lawful basis, we may need to perform a legitimate interest assessment (see 'Privacy Risk Assessments below).

Purpose Limitation

We collect and process Personal Data for specified, explicit and legitimate purposes. We will not process Personal Data in a manner that is incompatible with the originally stated purposes.

Secondary use of personal data will be reviewed and approved by the Data Privacy Office, the DPL or authorised delegate.

Accuracy

We will ensure the Personal Data we process is accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure Personal Data is accurate, having regard to the purposes for which it is processed.

Security and Confidentiality

We will take reasonable precautions to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access. These precautions include technical, physical and organisational security measures to prevent unauthorised access, as documented in the Related Policies. More information can be found in the Information Security Policy.

Data Subject Rights

Individuals' Rights. Individuals have the following rights when it comes to the processing of their Personal Data:

- Withdraw their previously given consent at any time
- Request access to their Personal Data
- Object to our processing of their Personal Data for direct marketing purposes
- Request erasure of their Personal Data if it is no longer necessary for the
- purposes for which it was collected or required to be retained for legal and regulatory purposes
- Request rectification of inaccurate or incomplete Personal Data
- Challenge our processing of their Personal Data where we are exercising our legitimate interests

Responding to Data Subject Rights Requests. Where MAG is the Data Controller (determining the means and purpose of processing the Personal Data), we will ensure that we comply with the following requirements:

- Information – we will ensure Individuals are informed about our privacy policies and their rights in relation to their Personal Data at the point of collection, in easily accessible notices. This includes Personal Data collected on paper, website registration forms, surveys, and telephone and email marketing campaigns.
- Request Forms – we will provide reasonable and accessible means for Individuals to submit their requests by emailing us using the contact information within the Privacy Policy that is available on the MAG website. MAG Personnel must be able to quickly identify a DSAR, which does not have to take any specific form and can be submitted by any method.
- Safeguards – we will confirm the identity of any Individual submitting a DSAR before providing a response.
- Response – within 30 days of validating the identity of any Individual submitting DSAR, we will provide the requested information, or provide legitimate reasons for not complying with their request. In certain limited circumstances, we may need to extend our response time by up to 60 days.

Sensitive Personal Data

In providing our services, we would not usually expect to process sensitive personal data, however, we are likely to process sensitive MAG personnel information, and therefore, we will take additional measures, including applying the MAG Highly Confidential classification and safeguarding it in accordance with Related Policies. Likewise, additional measures should be applied when we are required to process sensitive personal data of MAG personnel. Where MAG acts as an independent Data Controller, we require written notification before donors disclose sensitive personal data to us.

Personal Data used for Marketing Purposes

Our marketing activities will comply with Data Protection Laws. The following direct marketing obligations will apply:

- ePrivacy. At the time we collect an Individual's Personal Data for current or future direct marketing purposes using electronic communications (fax, text, recorded telephone messages, and email), we will obtain an affirmative indication of agreement (opt-in) from that Individual to receive further marketing communications from us. A pre-checked opt-in box (requiring an Individual to opt out) will invalidate the Consent and will be non-compliant.
- GDPR. All invitations for Consent (opt-in) will be clearly written, and easy to find at the point of collection. It will be made clear at the point of collection that Consent can be withdrawn at any time, as well as the effects of withdrawal (including options for opting back in). Relying on legitimate interests for direct marketing profiling is permitted if that fact is disclosed at the time of collection, and it is made clear to the Individual that they can object to such profiling at any time.

GDPR Consent. We will ensure that we can demonstrate:

- when the Individual has consented to the Processing (including the Purposes and Rights described at the time of the collection);
- that Consent was freely given (i.e. that the performance of a
- contract or services was not conditioned on the Consent being given); and
- when Consent was withdrawn (if applicable)

Automated Processing of Personal Data

Where we process Personal Data on a purely automated basis, Individuals have the right to object at any time to our processing of the Personal Data concerning them if it produces legal effects concerning them

or similarly significantly affects them. We will handle such objections through the DSR procedures outlined above.

Data Minimisation

Personal Data will be adequate, relevant and limited to what is necessary in connection with the purpose(s) for which it is processed. If we receive personal data during the course of a donor engagement which is excessive, we will endeavour to apply data minimisation by deleting the information that is not required; or returning the information to the donor and requesting a clean copy.

Storage Limitation

Personal Data will be maintained in a form identifying or rendering the Individual identifiable only for so long as it serves the purpose(s) for which it was initially collected or subsequently authorised, except to the extent permitted or required by applicable law.

Information Transfer and Compliance

We may transfer Personal Data to MAG Organisations and/or third parties on our behalf outside the UK, including to countries outside the EU or the EEA for legitimate business activities in accordance with Data Protection Laws.

Assurances. We will not transfer Personal Data to another country or organisation outside the UK/EU/EEA unless we are satisfied that the Personal Data is adequately protected in accordance with Data Protection Laws, this Policy and our Related Policies. MAG Personnel will ensure that any such transfer of Personal Data is governed by written agreements with third parties that impose obligations that reflect the requirements of Data Protection Laws and this Policy.

If there are no UK 'adequacy regulations' about the country, territory or sector for an information transfer, it should be determined if MAG can make the transfer subject to 'appropriate safeguards'. There is a list of appropriate safeguards in the UK GDPR, such as:

- A legally binding and enforceable instrument between public authorities or bodies
- UK Binding corporate rules ("UK BCRs")
- Standard contractual clauses (SCCs)

Privacy by Design and by Default; Pseudonymisation

We are required to implement Privacy by Design and Privacy by Default by ensuring we have appropriate technical and organisation measures (such as pseudonymisation) to ensure compliance with Data Protection Laws at the outset.

- Privacy by Design. This concept promotes the identification and mitigation of privacy risks at the time a product or service is designed, so that privacy and compliance with Data Protection Laws are applied at the earliest stages of a project involving Personal Data and data protection issues are identified and addressed in advance.
- Privacy by Default. This concept ensures that, by default, Personal Data is safeguarded to the greatest extent possible. MAG will ensure that it processes such Personal Data as necessary for specific purposes of the processing, for the shortest period of time possible and with the most appropriate access controls in place.
- Pseudonymisation and Anonymisation of Personal Data. Data Protection Laws apply to information from which an Individual can be identified. Pseudonymisation and anonymisation are methods by which elements of Personal Data are removed or separated so that they cannot be linked back to an Individual without additional information. These processes require the implementation of technical and organisational measures to mitigate the risks of reversal and re-identification, where applicable.

Privacy Risk Assessments

We will assess potential Personal Data privacy risks when personal data is being processed through a change in existing process or development of a new process and or application, and apply appropriate

mitigation steps depending on the outcome(s) of established processes, beginning with an analysis and applicable assessments outlined herein.

- Privacy Threshold Analysis (PTA). Answering basic questions regarding the processing of Personal Data will become an element of approving a new supplier, process, system or service. Where Personal Data is being processed, a Data Protection Impact Assessment must be completed.
- Data Protection Impact Assessment (DPIA). Completing the DPIA allows us to evaluate how Personal Data will be collected and processed, whether adequate safeguarding measures are in place, and how and when Individuals will be informed. Identified privacy risks will be evaluated and consideration given to how those risks can be mitigated in compliance with Data Protection Laws and this policy.

Where high residual risks remain, the DPL will determine what additional steps are necessary to mitigate the privacy risks identified, including reframing or abandoning the project. A record will be kept of all DPIAs, which will be periodically reviewed and updated with the process or business owners.

- Legitimate Interests Assessment (LIA). Performing LIAs are necessary in circumstances where Personal Data is being processed using the legitimate interest legal basis. The LIA will be carried out and decisions documented to evidence the balancing of legitimate interests and ensure they do not override the rights and freedoms of the Individual.

4. Reporting a Personal Data Breach

MAG Personnel who suspect or become aware of a Personal Data breach will immediately contact IT and the DPL at DataProtectionTeam@maginternational.org

MAG employees will not attempt to investigate the incident, or contact any relevant donor, until they have reported the matter and have been contacted by the DPL or IT for help.

Where the incident is confirmed to include Personal Data, the DPL or authorised delegate will assist the Investigations Team, monitor and review the incident response process and provide advice regarding any donor communication.

The Data Protection Laws may require data controllers to notify a Personal Data Breach to the appropriate data protection authority and, in certain circumstances, the affected individual. Where appropriate, the DPL or authorized delegate in consultation with the Chief Risk Officer (CRO) will inform the appropriate data protection authority and, if necessary, affected individuals within the statutory notification period (within 72 hours of becoming aware of a breach involving Personal Data.)

5. MAG as Data Controller and Data Processor

MAG as Data Controller

MAG will act as Data Controller in relation to the processing of all MAG personnel Personal Data.

MAG is a Data Controller in most of its donor engagements. This position is supported by guidance issued by the Information Commissioner. In this context we are likely to be co-controllers alongside our donor, also a Data Controller. We will not be joint controllers, which has a specific meaning in Data Protection Laws.

MAG as Data Processor

MAG will only act as a Data Processor where we process Personal Data on behalf of the donor or other relevant party (where they are the Data Controller) and there is little or no discretion as to how the Personal Data is processed by MAG. Where we consider we are a Data Processor, we will act in accordance with the instructions of the Data Controller of the Personal Data.

As Data Processor, MAG will have a duty to help the controller comply with its own obligations under the Data Protection Laws, and the engagement terms will reflect this.

6. Records of Processing Activities

MAG has created and will maintain a register of all Personal Data Processing activities in accordance with our record-keeping obligations under Data Protection Laws. The tool used to register our records of processing activities (whether automated or manual) will be maintained by the DPL. The completeness and accuracy of the information recorded in the register of processing activities will be the responsibility of the heads within each business function.

When we are a Data Processor, we will cooperate with controllers' requests for sight of the register relating to our Processing of their data subject's personal data, subject to confidentiality and other legal and regulatory considerations. Relevant sections of the register must be available to relevant data protection authorities upon request.

7. Training and Awareness

MAG will issue mandatory annual data protection training and periodic privacy awareness communications to MAG Personnel and contractors. Records of training attendance will be maintained and monitored. Non-completion of this mandatory training will be a breach of this Policy. All MAG Personnel are expected to regularly review the systems and processes under their control to ensure their ongoing compliance with this Policy.

8. Data Protection Governance

The DPL is responsible for implementing and maintaining a data privacy management programme to ensure the Processing of Personal Data meets the requirements outlined in this Policy.

The DPL for MAG is responsible for the following:

- Informing and advising MAG Personnel of their obligations under the Data Protection Laws.
- Providing appropriate data protection training to all MAG employees on the Data Protection Laws and their obligations under this Policy, and ensuring a record of training attendance is retained.
- Providing advice on Data Protection Impact Assessments (DPIAs) and monitoring their performance.
- Cooperating with relevant data protection authorities.
- Acting as contact point for the data protection authorities on issues relating to the Processing of Personal Data by MAG, and consulting with them on any other matter where appropriate.
- Keeping the risks associated with the Processing of Personal Data by MAG under review, having regard to the nature, scope context and purposes of its Processing activities.
- Conducting regular audits and compliance reviews to assess compliance with Data Protection Laws and this Policy, along with Related Policies where they relate to the processing of Personal Data.

9. Related Policies

This Policy is being implemented in conjunction with (and relies on compliance with) the following MAG policies ("Related Policies") all of which include additional requirements relating to Processing of Personal Data:

- Information Security Policy
- MAG Third party Security Policy
- MAG Information Classification and Handling Policy

10. Appendix

Document Version Control

Document Ownership	
Document Name	MAG – Data Protection Policy
Document Status	
Policy Owner	Director of Governance and Business Transformation
Required Readers	All MAG Personnel
Permitted Readers	All MAG Personnel
Approved by	Board of Trustees
Date Approved	29/01/2021
Document Location	Sharepoint

Document Review History (most recent first)				
Date	**Version**	**Reviewer**	**Approval**	**Summary of changes**

Document Review Cycle
This policy is reviewed on an annual basis by the LT lead and every 3 years a formal review and assurance report is provided to the GNRC Board Committee. Significant changes to the organisation (including risk appetite) or the threat landscape may trigger an interim review and could escalate the policy to the Board for re-approval.