Data Protection Policy

DATA PROTECTION POLICY

Hope4Malawi (the "Organisation")

26 Northey Avenue, Sutton Surrey, SM2 7HR
info@hope4malawi.org

www.hope4malawi.org

DATA PROTECTION COMPLIANCE MANAGER

The person responsible for data protection in the Organisation is Mark Goodman (the Data Protection Compliance Manager / DPCM). If you have any queries about this Policy or the GDPR, please address them to this person in the first instance.

INTRODUCTION TO DATA PROTECTION LEGISLATION

The law regarding data protection is contained in the General Data Protection Regulation (the "GDPR") (Regulation (EU) 2016/679)(in force from 25th May 2018).

The GDPR governs the "processing" of "personal data" by data "controllers" and data "processors".

The GDPR applies to data "controllers" and "processors".

Definitions

- "Processing" is the collection, use, disclosure and handling of personal data.
- "Personal data" is 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 (e.g. IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
- A "controller" is defined under Article 4 (7) as:

"a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws".

The Organisation is the data controller in respect of much of the personal data processed by the Organisation. In relation to *such* data, the Organisation is legally responsible for complying with the GDPR

- A "processor" is defined under Article 4 (8) as:

"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

Liability under the GDPR extends to persons, including staff and volunteers, who are processing the data on behalf of the Organisation.

What Data is Covered?

The GDPR covers all personal data, held on both computers and stored in physical records, where an individual can be directly or indirectly identified.

Breaching the Legislation

Breaches of the GDPR may have serious consequences. "Staff" (including employees, volunteers, agents, temporary and casual workers) are required to read the following information, and to ensure that all handling of personal data is carried out in accordance with the GDPR and this Policy.

Not abiding by the legislation can lead to heavy fines being imposed upon the Organisation or criminal charges being filed against individuals.

Information Commissioner

The Information Commissioner is the government officer responsible for monitoring compliance with the GDPR. Individuals have a right to lodge a complaint with the Information Commissioner's Office (the "ICO") regarding the actions of Organisation if they believe that the organisation has acted wrongly or in breach of the GDPR. The Information Commissioner provides a Helpline service on 01625 545745 and has also issued Codes of Practice and Legal Policy in relation to the GDPR. These can be viewed online at *https://ico.org.uk/*. The Organisation's obligation is to comply with the GDPR, not the Codes of Practice or other Policy.

ABOUT THIS POLICY

This Policy applies to processing of all personal data by the Organisation. This includes data relating to members of staff or third party individuals such as members of the Organisation. The Policy therefore generally refers to “individuals”.

LAWFUL BASIS FOR DATA PROCESSING

The Organisation may not process any personal data for any purpose unless one of the lawful bases under Article 6 of the GDPR is satisfied.

Before collecting and processing any new forms of personal data for the Organisation all individuals must check with the Data Protection Compliance Manager that the appropriate lawful basis has been chosen.

What Are the Lawful Bases?

Under Article 6 (1) of the GDPR, data processing by the Organisation shall be lawful where at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purpose;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Categories

Under Article 9 (1) of the GDPR processing of personal data that falls within the “special categories” of data cannot be processed by the Organisation unless one of the exceptions under

Article 9 (2) has been met. Special categories of data are personal data that relate to the following matters:

- racial or ethnic origin of the individual,
- political opinions,
- religious beliefs or philosophical beliefs,
- trade union membership,
- processing of genetic data, biometric data for the purpose of identifying a natural person,
- data concerning health,
- sexual life or orientation.

The exceptions found Article 9 (2) are as follows:

a) Explicit consent of the data subject has been acquired for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law and may not be lifted by the data subject;

b) Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;

c) Processing is necessary to protect the vital interests of a data subject or another natural person where the data subject is physically or legally incapable of giving consent;

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) Processing relates to personal data which are manifestly made public by the data subject;

f) Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;

g) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;

h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;

i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;

j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

THE DATA PROTECTION PRINCIPLES

Under Article 5 of the GDPR the Organisation must process personal data in accordance with the following six principles:

The First Principle

*Art.5(1)(a) "Personal data must be **processed lawfully, fairly and in a transparent** manner in relation to individuals."*

In line with this obligation the Organisation will ensure that any processing of personal data is carried out fairly and with a lawful basis. Details regarding what data processing the Organisation performs will be made easily accessible to individuals by a privacy notice that is provided in a clear and intelligible manner.

The Organisation shall make individuals aware of how their data will be processed before it is collected from them or before any subsequent changes are made to the processing of their data.

Where the individual has not provided the personal data directly to the Organisation, the Organisation must provide information to the individual confirming the source of that personal data and the lawful basis for the collection of that data.

The Second Principle

*Art.5(1)(b) "Personal data shall be **collected for specified, explicit and legitimate purposes** and not further processed in a manner that's incompatible with those purposes; further processing for archiving purposes in the public interest or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes."*

The Organisation must be clear when it collects personal data that the personal data is required for a legitimate and lawful purpose. This purpose must be made clear to the individual when the data is collected and must not be used for any other purpose without the consent of the individual.

If the personal data collected will be used for an additional purpose, such as adding an individual's details to a mailing list, then an 'opt-in' consent box should be included on the data collection form. A statement along the following lines could be used to gain this consent from the individual:

"By ticking this box, you are consenting to the details you provide being added to the Hope4Malawi's database and used only for the Hope4Malawi's mission. We'll periodically let you know about other events. Your details will only be used by the Hope4Malawi and not disclosed to third parties. You can opt-out of these communications at any time – just let us know by contacting info@hope4malawi.org*."*

All new privacy notices and data collection forms must be reviewed by the Data Protection Compliance Manager for approval before they can be used by the Organisation.

The Third Principle

Art.5(1)(c) "Personal data shall be ***adequate, relevant and limited to what is necessary*** *in relation to the purposes for which they are processed*."

The Organisation should only collect enough personal data to achieve the aim of the given purpose. The Organisation shall not collect data beyond what is necessary to achieve a purpose.

All forms that require to be completed by individuals must be checked by the Data Protection Compliance Manager, who will ensure that the questions will result in adequate personal data being provided for the purpose and to ensure that no unnecessary information is collected.

The Fourth Principle

Art.5(1)(d) "Personal data shall be ***accurate and, where necessary, kept up to date****; every reasonable step must be taken to ensure that personal data that's inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay."*

The Organisation asks individuals to ensure that their records are kept up to date by advising the Organisation of any relevant changes. The Organisation will make any necessary changes to personal data held on individuals to ensure that it is accurate. The Organisation will review all

personal data held on an annual basis, and where necessary will either update or delete personal data that is not accurate.

The Fifth Principle

Art.5(1)(e) "Personal data must be ***kept in a form that 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, historical research or statistical purposes… subject to implementation of the appropriate… measures required by… [the GDPR] in order to safeguard the rights and freedoms of the data subject."*

The Organisation will review all personal data held on an annual basis and where appropriate will delete personal data that is no longer necessary for the purposes for which the personal data is processed in line with Organisation's Data Retention Policy.

The Sixth Principle

Art.5(1)(f) "Personal data must be ***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*."

Personal data must be looked after safely and securely and access to personal data will be suitably restricted by the Organisation. Physical records will be stored on secure premises in locked filing cabinets. Access to digital records will be restricted to those individuals who require access and will be protected by strong passwords on secure networks. Any computer held records must also be backed up on a secure encrypted back up. Only those individuals authorised to do so may take personal data off-site. It is the individual's responsibility for the security of any personal data taken off site and must keep the data secure in accordance with this policy and the Organisation's Cyber Security Policy.

Where any third party collects or handles personal data on behalf of the Organisation, the Organisation will ensure that they are compliant with GDPR and have taken appropriate security measures to protect the personal data.

For more information and advice, please contact the Organisation's Data Protection Compliance Manager.

ACCOUNTABILITY AND RECORD KEEPING

Article 5(2) of the GDPR states that controllers shall be responsible for, and must be able to demonstrate, compliance with the data protection principles laid down in Article 5(1). In order to ensure that the Organisation is fulfilling its duties and responsibilities under the GDPR the Organisation shall:

1. Review and update, where necessary, this policy on a regular basis.
2. Provide training to staff on the legal requirements and organisational procedures in place for data processing within the Organisation.
3. Regularly review and update human resources policies as necessary.
4. Keep an accurate and up-to-date record of its data processing activities.
5. Keep a database of individuals who have given their consent to certain forms of data processing. This will detail:
    1. Who consented,
    2. when consent was received,
    3. how it was obtained,
    4. what they have consented to.
    5. Maintain accurate records of 'high risk' data processing.
    6. Carry out a Data Protection Impact Assessment (DPIA) before implementing new data processing technologies or where processing is likely to result in a high risk to the rights and freedoms of individuals.
    7. Regularly review the personal data processed by the Organisation to ensure that the Organisation;
        1. minimises the amount of data it processes;
        2. is transparent in its data processing activities;
        3. maintains an appropriate level of security to protect personal data from potential data breaches.
        4. Deletes and/or archives personal data that is no longer required.

INDIVIDUALS' RIGHTS

The GDPR affords individuals certain rights on how their personal data is processed by organisations.

Right to be informed

The Organisation recognises an individuals' right to be informed and shall provide notice to an individual when and how their personal data is collected and processed by the Organisation. The Organisation's full privacy notice will be made easily available to the public on the Organisation's

website. As well as this full notice the Organisation will also provide a clear and simple notice at the point data is collected from individuals. Such notices will include the following:

1. What information is being collected?
2. Who is collecting it?
3. How is it collected?
4. Why is it being collected?
5. How will it be used?
6. Who will it be shared with?
7. What will be the effect of this on the individuals concerned?
8. Is the intended use likely to cause individuals to object or complain?

Right to access

Individuals have the right to obtain the following information from the Organisation:

- Confirmation of whether, and where, the Organisation is processing their personal data;
- Information about the purposes of the processing;
- Information about the categories of data being processed;
- Information about the categories of recipients with whom the data may be shared;
- Information about the period for which the data will be stored (or the criteria used to determine that period);
- Information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- Information about the existence of the right to complain to the ICO;
- Where the data was not collected from the data subject, information as to the source of the data; and
- Information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects.

Additionally, data subjects may request a copy of the personal data being processed.

If the Organisation receives a request for any of the information above the request is to be referred immediately to the Data Protection Compliance Manager. The DPCM must provide the information requested to the individual free of charge as soon as possible and no later than one month after receiving a request.

Before releasing any of the information to an individual the DPCM must verify the identity of the individual by one of the following means:

1. Viewing photographic identification such as a UK Driving Licence or Passport, or where this is not reasonable to achieve;
2. Asking the individual to confirm at least two of their personal details that the Organisation holds. E.g. full name, address, date of birth, email address.

If it is deemed that the request is 'manifestly unfounded or excessive' (e.g. repetitive) then the Organisation can refuse to meet the access request and must point the individual to the complaints procedure through the ICO. **Any decision to refuse a request can only be taken by the DPCM.**

Right to rectification

Individuals have a right to have their personal data rectified where it is inaccurate. If the Organisation is made aware of inaccurate data that it holds it must make any necessary changes the individual requests to make that data accurate.

Any individual within the Organisation that received a rectification notification must either make, or arrange for, the necessary corrections to be made. If the individual is unable to do this they must contact the DPCM.

Right to erasure ("Right to be forgotten")

Individuals have the right to erasure of personal data (the "right to be forgotten") if:

- the data is no longer needed for their original purpose (and no new lawful purpose exists);
- the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- the data have been processed unlawfully; or
- erasure is necessary for compliance with EU law or the law of the United Kingdom.

If the organisation receives an erasure request this must be passed to the Data Protection Compliance Manager immediately. The DPCM will then decide if the request is within the scope of the GDPR and, if appropriate, arrange for the data to be erased as necessary.

Right to restrict processing

Individuals have a right to restrict the use of their data. E.g. Request to be removed from a mailing list.

The Organisation is permitted to hold any necessary data to maintain a restriction request.

Right to Data Portability

Individuals have a right to be able to transfer their data between different organisations. If requested an individuals' data must be provided to them by the Organisation in an open electronic format such as a .csv file. It must also be recorded within the file in a way that allows other organisations to read the data.

If an individual requests to transfer sensitive data then this should be referred to the DPCM.

Right to Object

Individuals have a right to object to their data being processed for research, statistical analysis, legitimate interests and direct marketing.

For direct marketing – an organisation must stop processing as a soon as it receives an objection. There are no exemptions or grounds to refuse such a request.

CONSENT

The Organisation recognises that consent must be freely given and specific to the purpose that it is being collected for. If the lawful basis relied upon to collect and process a person's data is 'consent' then the Organisation when requesting consent will:

1. Ensure that it is done so in an obvious way and will require a positive action to opt in by an individual.
2. Make the request prominent, unbundled from other terms and conditions, concise and easy to understand and user-friendly.
3. Display the Organisation's name clearly.
4. Display the names of any third party organisations that will rely upon this consent.
5. Give the reason why the Organisation wants the data being collected and explain what the Organisation will do with that data.
6. Make it clear that an individual can withdraw their consent at any time.

In accordance with the accountability requirements in this policy all consent will be recorded to provide evidence of the consents that have been collected.

CHILDREN

Consent

Where the Organisation relies on consent, for the collection and processing of data of an individual under the age of 16, it will ensure that it has the written permission of the parent or guardian for the individual. When the individual turns 16 the Organisation shall obtain permission directly from the individual to continue processing their personal data. If permission cannot be obtained the data must be deleted or archived in accordance with this policy and the GDPR.

In order to manage its consents, the Organisation will keep a database of individuals detailing when the consent was received, who it was given by and when they are due to turn 16 years old.

Legitimate Interest

Where relying on 'legitimate interests' to process a child's data the Organisation will be responsible for identifying the risks and consequences of the processing and will put age appropriate safeguards in place.

SECURITY AND DATA BREACHE

In order to prevent data breaches the following security measures must be taken by employees and volunteers of the Organisation.

All employees and volunteers must read the Organisation's Cyber Security Policy and ensure they follow the procedures and requirements of that policy in conjunction with this one.

Physical Files

Personal data contained on physical files must be stored in locked filing cabinets or in a safe. The keys and/or combinations for such cabinets must only be in the possession of authorised individuals and/or stored in a locked office or home.

Individuals must not leave personal data files unattended. Individuals should take reasonable care not to allow unauthorised individuals to view any personal data files.

Digital Files

Digital personal data files must be stored on computers and drives that are at least password protected and ideally encrypted. All digital files should be backed up on a separate encrypted drive or encrypted digital ‘cloud’ service such as Dropbox.

Computers and drives must not be left unlocked when unattended.

Files must never be stored on a public cloud service. Any files stored in a cloud service must only be accessible by authorised individuals of the Organisation and must not be shared with individuals or organisations outside of the Organisation without the appropriate legal basis and/or consent.

All computer software must be kept up to date with a software provider’s recommended security updates in accordance with the Organisation’s Cyber Security Policy. The Organisation’s computers should also be protected by up to date antivirus and firewall software where appropriate.

Individuals should take reasonable care when viewing personal data files on their computers not to allow unauthorised viewing of such files.

DATA BREACHES AND REPORTING

A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The Organisation will provide training to staff to recognise the different types of data breaches that may occur and what they should do if they suspect a breach has occurred.

Reporting

In the event that a breach is detected it must be reported to the Organisation’s Data Protection Compliance Manager as soon as possible.

The DPCM will need to report any breach that may result in a risk to the rights and freedoms of individuals to the ICO. If the nature of the breach is likely to result in a high risk to the rights and freedoms of individuals then the DPCM will need to notify the individuals concerned as well.

Reporting to the ICO needs to take place within 72 hours of the breach being detected. Failure to report within this time could lead to a fine of up to £8.5 million. It is therefore of the utmost importance that breaches are quickly reported to the DPCM. If the DPCM is not available the breach should be reported to the most senior member of the Organisation who is available.