MACS Privacy Policy

Users' Responsibilities

Users should familiarise themselves with this document and apply its principles. This document should be reviewed in every user's yearly appraisal, alongside the MACS Acceptable Use Policy.

Policy wording

The wording in this policy reflects the requirements of the General Data Protection Regulation (GDPR), which will come into effect in the UK on 25 May 2018.

Purpose

MACS is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out MACS's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, [including workers, contractors, volunteers, interns, apprentices] and former employees, referred to as HR-related personal data.

MACS has appointed Fay Skevington as the person with responsibility for data protection compliance within MACS. She can be contacted at fay@macs.org.uk. Questions about this policy, or requests for further information, should be directed to her.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.
"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

MACS processes HR-related personal data in accordance with the following data protection principles:

- MACS processes personal data lawfully, fairly and in a transparent manner.
- MACS collects personal data only for specified, explicit and legitimate purposes.
- MACS processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- MACS keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- MACS keeps personal data only for the period necessary for processing.

- MACS adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- MACS tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices and in its 'Data Profiles' spread sheet. It will not process personal data of individuals for reasons other than that outlines in these two documents.
- MACS will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.
- Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in electronic format), and on HR systems.
- MACS keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data -Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

PLEASE SEE ANNEX 1 FOR A CHECKLIST FOR A MACS EMPLOYEE THAT RECEIVED A SUBJECT ACCESS REQUEST

Individuals have the right to make a subject access request. If an individual makes a subject access request, MACS will tell him/her:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think MACS has failed to comply with their data protection rights; and
- whether or not MACS carries out automated decision-making and the logic involved in any such decision-making.

MACS will also provide the individual with a copy of the personal data undergoing processing. This will typically be in electronic form if the individual has made a request electronically.

To make a subject access request, the individual should send the request to fay@macs.org.uk. In some cases, MACS may need to ask for proof of identification before the request can be processed. MACS will inform the individual if it needs to verify their identity and the documents it requires.

MACS will normally respond to a request within a period of one month from the date it is received. In some cases, such as where MACS processes large amounts of the individual's data, it may respond within three months of the date the request is received. MACS will

write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, MACS is not obliged to comply with it. Alternatively, MACS can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which MACS has already responded. If an individual submits a request that is unfounded or excessive, MACS will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require MACS to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override MACS's legitimate grounds for processing data (where MACS relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override MACS' legitimate grounds for processing data.

To ask MACS to take any of these steps, the individual should send the request to fay@macs.org.uk.

Data security

MACS takes the security of HR-related personal data seriously. MACS has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. MACS' security is based on the storage of data on the MACS Microsoft Office 365 Sharepoint (with exceptions in line with the MACS Acceptable Use Policy), with limited access given to staff and volunteers as necessary and revoked when no longer necessary.

Where MACS engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Some of the processing that MACS carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, MACS will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If MACS discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery if appropriate. MACS will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals and, if appropriate, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

MACS will not transfer personal data to countries outside the EEA.

Individual responsibilities

Individuals are responsible for helping MACS keep their personal data up to date. Individuals should let MACS know if data provided to MACS changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals in the course of their relationship with MACS. Where this is the case, MACS relies on individuals to help meet its data protection obligations to staff, volunteers, members and donors.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside MACS) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction) in accordance with the MACS Acceptable Use Policy;
- not to remove personal data, or devices containing or that can be used to access personal data, from MACS' premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device in accordance with the MACS Acceptable Use Policy; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to familiarise themselves with the 'Data Profiles' spreadsheet and ensure that any data that they collect is collected and stored in line with its description in this spread sheet. If this is not the case, or if there are any queries, please contact fay@macs.org.uk.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under MACS' disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, member or donor data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

MACS will provide training to all individuals about their data protection responsibilities as part of the induction process and at yearly appraisals thereafter.

Law relating to this document

Leading statutory authority

The General Data Protection Regulation (GDPR) requires employers to:

- process personal data lawfully, fairly and in a transparent manner;
- collect data for specified and legitimate purposes and not process data in a manner that is incompatible with those purposes;
- collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- ensure that data is accurate and kept up to date, and take every reasonable step to rectify or erase data that is inaccurate without delay;
- keep data only for the period necessary for the purposes of processing;
- ensure that appropriate security is in place to protect data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- process data in accordance with the rights of data subjects; and
- transfer data outside the European Economic Area (EEA) only if there is an adequate level of protection for the rights and freedoms of data subjects.

The GDPR not only requires employers to comply with the data protection principles but to demonstrate that they comply. This is known as the Principle of Accountability.

Employers are also required to implement appropriate technical and organisational measures (including implementing appropriate data protection policies and providing employee training) to ensure and demonstrate that they carry out processing in accordance with the requirements of the GDPR.

MACS is not required to appoint a data protection officer, and so responsibility for data protection compliance has been assigned to Fay Skevington.

The GDPR requires organisations that hire third parties to conduct data processing activities on their behalf (known as "data processors") to put in place certain contractual requirements, including that the third-party processes data only on the basis of written instructions and that individuals processing the data will be subject to a duty of confidentiality. Additionally, MACS must contract only with third parties that implement appropriate technical and organisational measures for GDPR compliance and relies on their declaration of compliance to establish compliance.

Where MACS conducts data processing that is likely to result in a high risk to the rights and freedoms of individuals, particularly if it is using new technologies, the GDPR requires MACS to conduct a privacy impact assessment.

In the event of a data breach, the GDPR requires organisations to notify the Information Commissioner and individuals whose data has been breached within 72 hours of becoming aware of the breach. Where a breach is not likely to result in a risk to the rights and freedoms of individuals, MACS does not need to notify the Information Commissioner or the

individuals affected. However, MACS must keep a record of all data breaches, they should be recorded in the ‘Data Profiles’ spread sheet under the tab ‘Record of Data Breaches’.

Under the GDPR, the transfer of personal data outside the EEA is subject to strict rules. Personal data can be transferred to countries that have received an adequacy decision from the European Commission without additional security protections. However, employers transferring personal data to non-EEA countries that have not received an adequacy decision will need to apply additional safeguards, such as binding corporate rules or standard data protection clauses. Transfers of personal data include instances where data is stored, backed up or accessed outside the EEA.

Notes

The GDPR and the Data Protection Bill create new definitions for special categories of personal data and data on criminal convictions and offences. Under the Data Protection Act 1998, these types of data were previously known as "sensitive personal data". The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. To process such data, employers are likely to rely on the grounds that processing is necessary to perform or exercise obligations or rights of the employer under employment law. Under the Data Protection Bill, employers must have a policy on the use, retention and erasure of the data where it is processed to exercise obligations or rights under employment law.

Although documents such as the data security policy are likely to be outside the scope of HR responsibility, employers should refer to such applicable policies where relevant, and ensure that data protection measures are implemented consistently across MACS.

Given the serious penalties for breach of the GDPR (see Warning below), employers should set out employees' responsibilities with respect to data protection and clearly state that the failure to follow data protection requirements can amount to a disciplinary offence.

Warning

Employers that fail to comply with their obligations under the General Data Protection Regulation (GDPR), including breaching the data protection principles, data subject rights and requirements regarding international data transfers, can be subject to significant administrative fines of up to €20 million or 4% of the undertaking's worldwide annual turnover, whichever is higher. Although the Information Commissioner will take into account a number of factors when determining the level of a fine, employers would be well advised to take the implementation of data protection measures seriously to mitigate the risk of liability or enforcement action.

Organisations may also be subject to direct claims for compensation by individuals who have suffered damage as a result of a breach of the GDPR.

The Data Protection Bill supplements the GDPR and contains additional requirements regarding special categories of personal data, data on criminal convictions and offences, information requirements for individuals and subject access requests. These requirements have been incorporated into this model policy where relevant. However, the Bill is still being considered by Parliament and is subject to change before it comes into force.

Annex 1. MACS employee subject access request checklist

- Ensure that the request has been sent to fay@macs.org.uk, if the task of responding to the request has been delegated to you then:
- Establish that the requestor has the right of access to the data, this is the case if
    - It is their data
    - It is the data of someone for whom they are a guardian
- Responses should be limited to questions asked
- MACS will confirm what data is held.
- If the actual data has to be disclosed and the data is sensitive or beyond that which they provide request proof of identification, this can be through confirmation of details over the phone or by email.
- If a subject access request is manifestly unfounded or excessive, MACS is not obliged to comply with it.
- All requests must be responded to within one month with, at the least, a response indicating how long the full response will take. A full response cannot take longer than 3 months.