Data Protection Policy

Money Advice Plus
Tisbury Road Offices
Tisbury Road
Hove
BN3 3BQ

01273664000
info@moneyadviceplus.org.uk

Background

The **Data Protection Act 2018** is the UK's implementation of the **General Data Protection Regulation** (**GDPR**). Everyone responsible for using personal **data** has to follow strict rules called '**data protection** principles'. They must make sure the information is: used fairly, lawfully, and transparently.

Data protection law in the UK after Brexit 2020

- The EU's GDPR has been amended into a new "**UK-GDPR**" (United Kingdom General Data Protection Regulation) that took effect on January 31, 2020.
- The **Data Protection Act 2018** has been amended to be read in conjunction with the new UK-GDPR instead of the EU GDPR.
- The European GDPR will apply to the UK in the **transition period** lasting from January 31, 2020 until December 31, 2020 (unless further extensions are agreed upon between the UK and EU).

Money Advice Plus (MAP) is compliant with the requirements of the General Data Protection Regulation (GDPR) 2018.

Therefore, we follow procedures which aim to ensure that all employees, volunteers, trustees, and others who have access to any personal data held by or on behalf of MAP, are fully aware of and abide by their duties under the GDPR.

MAP is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1. Statement of policy

In order to operate, MAP has to collect and use information (data) about people with whom we work. These may include clients; current, past and prospective employees; past and prospective volunteers, trustees, and supporters.

This personal information must be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

Given the nature of MAP's service and our aims and principles, we view the lawful and correct treatment of personal information as important to our successful operations, and to maintaining the confidence of those with whom we work.

To this end, MAP fully endorses and adheres to the principles of data protection as set out in the GDPR.

2. The principles of data protection

Article 5 of GDPR requires that personal data shall be:

a) **processed lawfully, fairly and in a transparent manner** in relation to individuals;
b) **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
d) **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, are erased or rectified without delay;
e) **kept in a form which 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, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) **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.

The GDPR 2018 provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data, which is now referred to as special category data and is broadly similar to the previously titled 'sensitive' personal data under the old Data Protection Act 1998. There are additional rules for processing special category data.

Personal data is defined as data relating to a living individual who can be identified from:

- that data
- that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Special category data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health condition
- sexual life or sexual orientation

- genetic and biometric data

Data and information have the same meaning throughout this document.

3. Handling of personal / special category data

MAP will, through appropriate management and the use of strict criteria and controls:

- Observe fully, conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of people about whom the information is held can be fully exercised

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, we will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about our handling of personal information, whether a member of staff or volunteer or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All employees and volunteers are to be made fully aware of this policy and of their duties and responsibilities, and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular, they will ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by the use of secure passwords.
- Individual passwords are such that they are not easily compromised.

4. EQUIPMENT: To protect data that is held by the Money Advice Plus, work undertaken as an employee of Charity should be completed on equipment provided by Money Advice Plus. If an employee needs to work on a personal computer, they will need to seek permission of their line manager and make the data manager aware.

5. Use of Databases

MAP uses AdvicePro to electronically record the advice given to clients.

Advicepro: AdvicePro is hosted on secure servers and which has password access only. This is their data security statement:

AdvicePro's Commitment to the General Data Protection Regulation (GDPR)

"The new EU General Data Protection Regulation (GDPR) comes into force on May 25th 2018 and will affect every organisation which holds or processes personal data. It will introduce new responsibilities, more stringent enforcement and increased penalties than the current Data Protection Act which it will supersede.

All of our staff and those of our hosting provider are familiar with GDPR and their personal responsibilities.

Our staff are trained on Data Protection issues on commencement of employment and this is updated as and when regulations change or are updated.

All data is held within the UK on servers based in Dundee and Aberdeen.

All storage is secure and our hosting provider has GDPR procedures in place.

We have a notification process in place for any breach.

AdvicePro provides appropriate tools to allow all customers to properly enact the right to erasure process.

AdvicePro provides functionality to allow the details of a client to be extracted in a machine readable format (XML).

ACM Solutions, who develop, manage and provide the helpdesk services for AdvicePro and our current hosting partner (BrightSolid Ltd) are ISO27001 accredited."

TOPAZ: Some face to face, and longer term support cases have archived record stored on TOPAZ. Data is stored on our server within the office. The server can be accessed only by logging in with a secure password.

On both databases, the data belongs to MAP.

5. Implementation

It is MAP policy to appoint a Data Manager (A Data Protection Officer is not required unless the organisation requires large scale, regular and systematic monitoring of individuals.) The Data Controller (MAP), through the

Chief Executive, delegates to a Data Manager responsibility for leading and monitoring policy implementation

The Data Manager will also have overall responsibility for:

- ensuring that all employees and volunteers are fully informed of their responsibilities for acting within the law
- ensuring that the public including employees and volunteers are informed of their rights under the Act
- carrying out compliance checks to ensure adherence with the Data Protection Act
- Leading on actions in the event of a breach

  Andrea Finch is the Data Manager. Any change to the Data Manager must be reported to the Trustees by the Chief Executive
- We will mitigate any risk to data by following our Information Risk Policy

The Chief Executive will ensure compliance of electronic data and its storage and will inform the Data Manager of any breaches.

6. Notification to the Information Commissioner

The Information Commissioner's Office (ICO) maintains a public register of data controllers. MAP is registered as such and our data protection regulation number (ICO registration no) is **Z5736768**

Each registration with the ICO is only effective for 12 months and is renewed by payment of a Data Collection fee.

The Data Controller (MAP) delegates to the Data Manager responsibility for the annual review of and updates of the Data Protection Register (aka Register of Fee Payers) Any changes to the register must be notified to the Information Commissioner within 28 days.

7. Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

Reportable breaches are those where the breach may result in a risk to people's rights & freedoms – in the case that this is likely, we will report the breach to the ICO.

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

We will have robust breach detection, investigation and internal reporting and recording procedures in place. This is detailed in the Information Risk Policy.

8. Relationship with existing policies, procedures and supporting documentation

These are the policies & procedures in place:
Information Risk Policy information risk policy Sept 2020.doc
Confidentiality Policy: **..\confidentiality & disclosure**
Confidentiality Procedure: **..\confidentiality & disclosure**

Data Protection agreement to sign (part of induction pack for all staff, volunteers and trustees) **..\Data protection**
Working from home **..\..\part 3 of 5 personnel\working from home**

Ownership:	Chief Exec
Date Issued:	July 23
Governance Forum responsible	P&G Sub Group
Version:	4
Document history:	V1, V2, V3 with changes, V4with changes
Distribution	email
Review Date of policy:	July 24
Review frequency	1 year
Reason for frequency	AQS