Data Protection Policy

1. Introduction

1.1. This document outlines the data protection policy (the "**Policy**') of CMS Direct Mail Ltd, whose registered office is at Unit 8 Peel Green Trading Estate, Green Street, Eccles, Manchester M30 7HF (the "**Company**') to help ensure compliance with all current UK data protection legislation.

1.2. This Policy relates solely to the personal data and information (the "**Data**") supplied to the Company by its clients or its client's agents for the purposes of carrying out services including, but not limited to, direct mail, marketing, advertising, public relations, promotion, communication and fulfilment (the "**Services**").

1.3 Definitions

Data Protection Legislation: means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the General Data Protection Regulation ((EU) 2016/679) (**GDPR**), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy including any amending or replacement legislation in force from time to time.

Personal Data: any information identifying an individual or information relating to an individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories Personal Data. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices: separate notices setting out information that may be provided to individuals when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.

Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. Purpose of this Policy

2.1. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of Data in both paper and electronic format.

2.2. The Company takes very seriously the Data privacy and Data protection rights of individuals and this Policy is a statement of the Company's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Legislation.

2.3. Every member of staff has a duty to the Company to be aware of and adhere to the Policy set out below, to ensure the Company complies with its moral and legal obligations. Any breach of this Policy may result in disciplinary action.

2.4. Along with a commitment to protecting individual's rights; the Data Protection Legislation is taken very seriously as the Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

2.5. All supervisors are responsible for ensuring all members of staff comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.6. The Data Protection Officer is responsible for overseeing this Policy and, as applicable, developing related policies and other privacy guidelines.

2.7 Please contact the Data Protection Officer with any questions about the operation of this Policy or the Data Protection Legislation or if you have any concerns that this Policy is not being or has not been followed.

3. This Policy

3.1. The Company collects Data from its clients solely for the purposes of undertaking the Services requested by the client. The Company shall process any Data (as defined in the Data Protection Legislation) solely for the purposes of the requested Service and for no other purposes.

3.2. The Company shall hold all Data supplied as confidential and shall not pass such Data on to any other organisation without first obtaining approval from the client. The Company shall not alter the Data other than for the purpose of completing the Service requested and shall first obtain approval from the client.

3.3. Data cleansing alterations will only be carried out through recognised industry approved processes and with the prior approval of the client.

3.4. The Company has in place appropriate technical and organsational measures against the unauthorised or unlawful use of Data and against accidental loss,

destruction or damage. Such Data security measures are outlined in section 5.1 of this document. The Company shall make each of its employees aware of the obligations with regard to the security and protection of Data.

3.5. The Company expects that its clients should also abide by the Data Protection Legislation in the original collection of any Data supplied. It is the client's responsibility to ensure that Data supplied to the Company is validly held, relevant, accurate and supplied with permission for use as specified. This includes the collection of any necessary consents and supplying any necessary privacy notices to individuals. The Company reserves the right to take any reasonable measures deemed necessary if it believes the Data supplied to have been collected inappropriately.

4. Data Protection Principles

4.1. The Data Protection Legislation, in particular the GDPR, sets out strict rules about the way in which Personal Data and Special Category Data are collected, accessed, used and disclosed. The Company shall perform its responsibilities in accordance with the following six principles as outlined in the GDPR:

4.1.1 Processed lawfully, fairly and in a transparent manner;

The Company shall obtain and process Data fairly and in accordance with statutory and other legal obligations.

The Company will only process Personal Data where it has a 'lawful basis' (legal reason) to do so. The 6 legal reasons the Company may use are:

- Where the data needs to be processed to **fulfil a contract** with the individual
- Where the data needs to be processed so the organisation can **comply with a legal obligation**
- Where the data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- Where the data needs to be processed so a public authority can perform a task carried out **in the public interest,** and carry out their official functions
- Where the data needs to be processed for the **legitimate interests** of an organisation (provided the rights and freedoms are individuals' are not overridden)
- The individual has freely given clear **consent**

For Special Categories of Personal Data, the Company will comply with the additional requirements for processing) as set out in the GDPR. These include:

- Where we have obtained **explicit consent** from the individual
- Where the Data needs to be processed so the organisation can comply with a **legal obligation**
- Where the Data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- Where the Data needs to be processed for reasons of **substantial public interest**.

The Data Protection Legislation requires the Company to provide detailed, specific information to individuals depending on whether the information was collected directly from individuals or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.

Whenever we collect Personal Data directly from individuals, including for human resources or employment purposes, we must provide the individual with all the information required by the Data Protection Legislation including the identity of Company, how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the individual first provides the Personal Data.

Where we are acting as a Data Processor for example in relation to personal data and information supplied to the Company by its clients then these Privacy Notices are to be supplied by the client directly as a data controller for that information.

4.1.2 Collected only for specified, explicit and legitimate purposes;

The Company shall keep Data for purposes that are specific, lawful and clearly stated. Data shall be used and disclosed only in ways compatible and necessary for the purposes for which the Data was collected.

The Company will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the individual of the new purposes and they have provided consent where necessary.

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;

The Company shall hold Data only to the extent that it is adequate, relevant and not excessive for the purposes of providing the agreed service to the client.

The Company will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's Data Retention Policy.

4.1.4 Accurate and where necessary kept up to date;

The Company expects its clients to abide by the Data Protection Legislation and industry best practice standards for the supply of accurate, complete, relevant and up to date Personal Data. The Company shall, upon the client's request, provide data cleansing services to improve the accuracy of Data. The Company shall, upon the client's request, provide information regarding returned mail to improve accuracy of Data. The Company shall not otherwise accept responsibility for keeping records of returned mail for the purposes of maintaining data accuracy or any other purposes.

With regards to the Company's own data we will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

4.1.5 Not kept in a form which permits identification of data subjects for any longer than necessary;

Data shall be retained only as necessary in conjunction with providing the service requested by the client. Unless agreed in writing, data shall be deleted 8 weeks after completion of the Service.

4.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction of damage, using appropriate technical or organisational measures.

5 Security

5.1 The Company will keep Personal Data secure by taking appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage The following procedures are in place to help prevent unauthorised access to, alteration, disclosure or destruction of Personal Data:

5.1.1.1 Data is held in a secure environment protected by security key pad entry lock. All windows are protected with security grills. The premises are protected by ADT alarm system with police response.
5.1.1.2 Responsibility for the day to day security of data lies with the IT Manager.
5.1.1.3 Access to the Data storage and Data processing area is restricted to authorized staff.
5.1.1.4 All computers within this area are protected by power-on passwords. A second tier of password authentication will allow the user the appropriate level of data access on the main server. The IT Director controls the levels of permission.
5.1.1.5 If a computer is left unattended for a period of five minutes then a screen saver password is activated. Passwords are reviewed every four months or when a member of staff leaves.
5.1.1.6 Data is stored on the main server and shall not be transferred to other computers, except for a limited period in connection with carrying out the Service. Direct access to the server is password restricted and restricted to IT manager level.
5.1.1.7 External Data transfers from the Company are password protected.
5.1.1.8 Data backups are taken every evening, except for weekends. Historic backups are stored in the Company safe.
5.1.1.9 Set-up documents are separated from standard paper recycle and shredded on site.
5.1.1.10 Not transferred to countries that have inadequate protection. Data shall not be transferred outside of the UK.

6 Sharing Data

6.1 The Company will not normally share Personal Data with anyone else without the consent of the individual. However, there certain circumstances where the Company will be required to share Personal Data with other organisations and it will comply with Data Protection Legislation when disclosing this information.

6.2 The Company will sometimes share Personal Data with suppliers and/or contractors who enable it to provide services to clients and employees – e.g. IT companies or energy suppliers. The data shared is limited to the specific information the supplier requires in order to carry out their service as well as any additional information that ensures the Company fulfils its health and safety obligations to the people carrying out the work. The Company will ensure that suppliers handle this Personal Data correctly through the contract terms and it will only use suppliers and/or contractors that comply with Data Protection Legislation.

6.3 The Company is responsible for the fair and lawful processing of Personal Data shared with third parties. The Company will make sure this occurs through data sharing agreements, either in contracts or as standalone agreements.

6.4 The Company will share Personal Data with law enforcement and government agencies or public bodies where it is legally required to do so or for the prevention or detection of crime and/or fraud. Examples include:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations; or
- Research and statistical purposes provided Personal Data is sufficiently anonymised or consent has been provided.

7 Individual Rights and Requests

7.1 Individuals have rights when it comes to how the Company handles their Personal Data. These include rights to:

- withdraw their consent to processing at any time;
- receive certain information about the data controller's processing activities;
- request access to their Personal Data that the Company holds;
- prevent use of their Personal Data for direct marketing purposes;
- in certain circumstances, to ask to erase Personal Data;
- to rectify inaccurate Data or to complete incomplete Personal Data;
- in certain circumstances to restrict the processing of their Personal Data;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on automated decision making or profiling;
- prevent processing that is likely to cause damage or distress;
- in certain circumstances, be notified of a Personal Data Breach;
- to make a complaint to the Information Commissioner’s Officer (ICO); and
- in limited circumstances, ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

7.2 Employees must immediately forward any request to exercise data protection rights which they receive to the Data Protection Officer.

8 Data Protection by Design and Default

8.1 The Company will put measures in place to show that we have integrated data protection into its processing activities. This includes:

- Appointing a suitably qualified Data Protection Officer.
- Implementing privacy by design when processing Personal Data and completing privacy impact assessments where processing presents a high risk to rights and freedoms of individuals.
- Integrating data protection into internal documents including this Policy, any related policies and any Privacy Notices.
- Regularly training members of staff on Data Protection Legislation, this Policy, any related policies and any other data protection matters. The Company will maintain a record of training attendance by members of staff.
- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

9 Personal Data Breaches

9.1 The Company will make all reasonable endeavors to ensure that there are no Personal Data Breaches.

9.2 The Company has put in place procedures to deal with any suspected Personal Data Breach. Please see the Data Breach Notification Policy for further guidance. Any suspected Personal Data Breach must be reported immediately to the Data Protection Officer.

9.3 In the unlikely event of a Personal Data Breach, the Company will report this to the ICO within 72 hours of becoming aware of it, where the individual is likely to suffer some form of damage e.g. through identity theft or a breach of confidentiality.

10 Training

Data protection will form part of continuing training needs for employees and where changes to legislation or the Company's processes make it necessary. All employees must complete all mandatory data protection related training as and when required.

11 Related Policies

This Policy is linked to:

- Fair Processing Policy;
- Data Retention Policy;
- Data Breach Notification Policy;

12 Policy Review

This Data Protection Policy will be reviewed periodically or in light of any legislative or other relevant developments. The next periodic review is April 2019.