PS Mailing Services Ltd
Data Protection Policy
May 2018

PS Mailing Services Limited is a registered data controller: ICO registration no. Z9106387 (www.ico.org.uk

1. Introduction

1.1. Background

We collect personal data about the people we deal with during the course of carrying out our business and delivering our services. Such people include our clients, employees, other business contacts and prospective clients and employees.

This policy document sets out the approach we take towards managing this personal data to ensure we meet the data protection requirements set out in the General Data Protection Regulation ("GDPR"), any UK specific implementation of aspects of the Regulation into UK law and any guidance the Information Commissioner's Office or the Article 29 Working Party provide.

We take data protection seriously and place a high importance on the correct and lawful processing of all personal data as well as respecting the rights and privacy of our clients and employees. As such, this policy sets out the company procedures that are to be followed, by all employees when dealing with personal data across the business.

1.2. Data protection

The GDPR is a European regulation which was ratified on 27th April 2016 and is enforced across the whole of the European Union, including the UK, from 25th May 2018. The Regulation replaces existing member state laws that implemented the previous EU data protection Directive and despite the UK leaving the European Union the Regulation will also replace the UK's Data Protection Act 1998.

1.2.1. Key definitions

- "Personal data" relates to information that enables the identification directly or indirectly of a living individual, this includes the identification of an employee within a business, but does not include generic business data
- "Special categories of personal data" relates to more sensitive personal data including racial or ethnic origin, religious beliefs and health related information
- "Processing" means any activity carried out on the personal data including storage, collection, organisation and general use
- A "Data Subject" is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor
- A "Data Controller" is an organisation who determines the purposes of processing of data – typically this is the organisation that has collected the data in the first place and wishes to process it
- A "Data Processor" is a person or organisation who processes data on behalf of the Data Controller (usually a third party).

1.2.2. Data protection principles

Controls around the use of data are governed by a set of principles, which state that data must be:

- Processed lawfully, fairly and transparently
- Collected only for specified or legitimate purposes and not further processed outside the original purpose for collection

- Relevant and necessary for the purposes for which they have been collected (i.e. we should not collect any data that we don't need)
- Accurate and kept up to date
- Only kept for as long as the data is required. Where data is no longer required it must be deleted or anonymised
- Kept and processed securely

It is up to the Data Controller or Processor to be able to demonstrate compliance with these principles (this is the principle of "accountability").

1.2.3. Lawfulness of processing

For processing to be lawful, data can only be processed when one of the following conditions applies:

- The Data Subject has given consent
- Processing is required for the performance of a contract or delivering a service
- Processing is required to comply with a legal obligation
- Processing is necessary to protect the vital interests of the Data Subject
- Processing is carried out in the public interest
- Processing is carried out in the legitimate interests of the Data Controller, but without detriment to the Data Subject

1.2.4. Data subject rights

Under the GDPR, Data Subjects have the following rights:

- The right to be informed (including when the data was not obtained directly from them) about who has their data, what it's used for, who will have access to and their rights to object, withdraw consent, etc.
- The right to request whether data is being processed by the Data Controller and if so what data and how (this is a subject access request)
- The right to have their data updated and kept up to date
- The right to erasure of their data when the data is no longer needed, when consent has been withdrawn or if it has been unlawfully processed
- To restrict, in certain circumstances, the processing of their data
- The right to data portability allowing a Data Subject to request copies of their data in a format compatible with another system for their own use or to import into a third-party system
- The right to object to the processing under legitimate interests, for direct marketing purposes, for profiling or research
- The right to object to automated decision making

1.3. What data is covered by data protection?

Personal data is defined as any information which identifies a living individual. Generally this will include data such as name, address, email addresses and telephone numbers but may include other information. Whilst PS Mailing Services does not normally hold any personal data over and above these contact details listed above, should a specific client require us to do so it would be covered contractually on a client by client basis.

2. Scope

This policy document applies to <u>all</u> employees, including full-time, part-time, contractors and temporary staff.

3. Roles and responsibilities

3.1. All employees have a responsibility to ensure data protection compliance, however, these people have key areas of responsibility:

<u>The Managing Director</u>
The MD is ultimately responsible for ensuring adequate data protection controls are in place across the business and this includes:

- Ensuring all IT systems and use of technology is compliant and in line with this policy

- Maintaining IT security across the business and ensuring the security of systems is kept up to date
- Assisting the Data Protection Officer with assessing the security aspects of any third party systems that may be used to handle the company's data
- Ensuring all marketing is compliant with the GDPR rules relating to consent and the marketing rules as set out in the Privacy and Electronic Communications Regulations ("PECR")
- Ensuring that employee data is processed in line with this policy and any other rules or guidance relating to the use of employee data.

Data Protection Officer

The Data Protection Officer is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues across the business
- Overall data protection compliance for the business
- Reviewing (annually) all data protection resources made available to the business, including this policy, guidance and support information
- Ensuring adequate training is in place for all employees, depending on the role they fulfil within the company.
- Dealing with data protection and privacy related questions from any part of the business
- Dealing with subject access requests from Data Subjects (clients or employees)
- Dealing with any requests to access data (clients or employees) from external third parties, for example law enforcement and government offices
- Carrying out due diligence and ensuring appropriate contractual terms are in place for any third parties we use to share or store personal data

Our Data Protection Officer is:

Gwen O'Sullivan
Telephone No: 01935 810051
Email: gwen.osullivan@psmailingservices.co.uk

3.2. All employees will familiarise themselves with this policy and any associated policies, relating to the processing of personal data and ensure their processing of personal data is within the rules set out within these policy documents. Specifically, all employees should ensure:

- All personal data accessed, used or processed during their duties is kept and processed securely
- No personal data should be disclosed verbally, in writing or by any other means to any third party, without consent from the company's Data Protection Officer
- No company systems should be accessed for any reason other than for the purposes of carrying out their duties as an employee
- They contact the Data Protection Officer if they are aware of an issue or are uncertain about any aspect of processing data

3.3. Any breach of this policy or any associated policy may result in disciplinary action in line with the company's employee contracts

4. Collection of personal data

4.1. Whenever we collect data, we will only ask for data that is needed for the services we provide or for recruitment

4.2. Where we need consent for the purposes of processing we will:

- Be open and transparent about why we are collecting the data and what is being consented to
- Provide an option for the Data Subject to provide their consent
- We will not provide any pre-ticked options or use any wording that could be missed or misconstrued by the Data Subject to "trick" them into consenting
- We will record the place, time and situation by which that consent was given

4.3. In all circumstances, when collecting data, we will provide the following information:

- Details of who we are, why we're collecting the data, what it will be used for and how long we will use and keep the data, and the legal basis for processing

- Details of our Data Protection Officer and how they can be contacted
- Details of the Data Subject's rights:
    - Data Subject access requests
    - Have their data corrected if details change
    - Have their data deleted when it is no longer needed
    - Object to processing
    - Right to complain to the Information Commissioner's Office
- Details of how to withdraw consent (when consent is the lawful basis of processing)

4.4. Where we make use of data supplied by a third party, in addition to the items listed in 4.3, we will also provide details of where the data came from. The information will be given to the Data Subject at the first opportunity (but not more than one calendar month from receiving the data).

5. Use of personal data

5.1. We will only process personal data supplied to us for its original purpose. We will not reuse the data for any other purpose unless it is lawful for us to do so (e.g. we have consent from the Data Subject).

5.2. Where "legitimate interest" is the lawful basis for processing it will be possible to demonstrate that such processing is not harmful to the Data Subject's rights and the reason for processing as a legitimate interest documented

5.3. Where personal data is held by the business for marketing purposes, it is the responsibility of the Managing Director to ensure that before, each time, data is used, it is cleansed against relevant marketing preference databases (e.g. Telephone Preference Services, Mail Preference Service and Corporate Mail Preference Service) to ensure that the Data Subjects have not opted out of marketing.

6. Storing data

6.1. All personal data, particularly data classified as "special category" data must be encrypted at rest and during transmission

6.2. The sharing of data within the business must only be done so through secure means

6.3. Data should only be shared by email when no other secure means are available. If data is shared via email it should be locked with a password (using a password which meets the requirements of the company's password policy). Email should always be collected and sent via a secure connection

6.4. Any devices (PCs, laptops, tablets, mobiles, etc.) that enable access to the company's data should be locked with appropriate password controls (in line with the company's security guidelines)

6.5. Data should not be downloaded to local devices (PCs, laptops, tablets, mobiles, memory sticks, etc.) or to network storage devices unless authorised by the Data Protection Officer. If data is downloaded to a local device then it must only be stored for the minimal time necessary on that device and deleted once it is no longer needed on that device

6.6. Data should not be printed out, unless authorised by the Data Protection Officer. If data is printed out then the printed copy of the data will be destroyed once it is no longer needed and the print out should be stored securely (e.g. in a locked filing cabinet) when it is not being used

6.7. Any devices (PCs, laptops, tablets, mobiles, etc.) that can be used to access personal data should be locked down according to the company's device security policies

6.8. Where personal data is being viewed on a device, the screen or device lock must be activated if the device is to be left unattended for any period of time

6.9. Employees must observe if there is a risk that any unauthorised third party would be able to view personal data whilst they, themselves, are viewing the data on a device (e.g. whilst travelling on public transport, etc.) to prevent unauthorised viewing of personal data. Screen guards should be used whenever possible, in such situations

6.10. No personal data will be transferred to personal devices belonging to an employee without authorisation from the Data Protection Officer

6.11. Where personal data is, with permission, downloaded, copied or printed the storage of that data should be secure at all times

6.12. Where the use of third party systems are used (and have been authorised by the Data Protection Officer), access controls will be put in place to ensure access is secure and limited to only those employees who have a need to access the data

6.13. All company systems which are used for storing or processing of personal data should be adequately and regularly backed up (in line with the company's IT policy). All backups should be encrypted and stored securely

7. Access to personal data

7.1. No employee will access data unless they are authorised to do so for the purposes of carrying out their duties as an employee

7.2. Employees will only have access to data that is required for them to carry out their duties. If they need access to data they are not currently authorised to access, they should seek access via their line manager

8. Accuracy of data and keeping it up to date

8.1. If we are told by a client or employee that the data we hold on them is out of date or incorrect we shall make sure the incorrect data is either deleted or updated

8.2. If we are updating information about a client we must do so immediately to ensure the old data is not processed in the meantime

8.3. If we have shared the data with any third party, we will immediately inform the third parties to ensure their copies of the data are updated

9. Retention of data

9.1. We will only process (including store) data for as long as we have a business reason to do so. We can retain data where there is a legal duty for us to keep data (e.g. to meet the requirements set out by HMRC) but any data not required must not be retained, once it is no longer needed

9.2. Where data is no longer required and we are unable to justify a legal reason for keeping it, we will either delete the data or anonymise it, within one month

10. Subject access requests

10.1. A client or employee has a right to request access to the data we process and to ask how we process that data (a so called "Subject Access Request"). All subject access requests should be processed by the Data Protection Officer in line with the Subject Access Request policy

11. Right to erasure

11.1. All requests from a Data Subject for the deletion of their data should be dealt with in consultation with the Data Protection Officer to ensure we don't delete data we have a lawful basis, or legal requirement, to continue processing

11.2. Unless where we can demonstrate otherwise, if a Data Subject requests the deletion of their data we will comply with the request, within one month of the request, and confirm to the Data Subject what data has been deleted

11.3. Where the personal data in question has been disclosed to a third party, we will notify the third party of the need for them to also erase the data

12. Right to data portability

12.1. The IT team will ensure that any systems we use that meets the requirements for a data portability option has the data portability option available either directly to the customer or for a member of the customer services team to activate.

12.2. Where this system is not accessible directly to the client or employee, all requests for an export of a data from a Data Subject will be dealt with by the Data Protection Officer within one month of the original request

12.3. The data will be made available at least in CSV format or in a format standard that has been established between suppliers of similar systems

13. Objections to processing

13.1. Any objections to the use of data for marketing (e.g. requests to stop receiving marketing information) should be passed to the Managing Director, who will ensure that the details of the Data Subject are removed from any marketing lists

13.2. Any other objections are to be dealt with by the Data Protection Officer to ensure that the business does not have a lawful basis for processing

14. Third party due diligence

14.1. Where a third party is used for the processing of personal data, due diligence checks will be carried out on the third party, in consultation with the Data Protection Officer, to ensure they are data protection compliant and will enable our own data protection compliance. Such checks will include asking about how they are GDPR compliant and asking them for a GDPR statement

14.2. Contractual obligations will also be put in place with any third parties we use. Where we provide a contract to be agreed with the third party we shall ensure these contractual obligations are included in the contract either via a new contract or by an addendum to an existing contract; where we are taking a service from a third party who have their own terms of service, to which we have to agree, we must ensure that the contractual obligations are included within those terms

14.3. We will not use any third party who is unable to provide evidence of their data protection compliance or willingness to agree to the appropriate contractual terms

15. Data protection impact assessments

15.1. When new technologies, systems or processes are introduced the Data Protection Officer should be involved and carry out a Data Protection Impact Assessment to ensure the new technologies are compliant with the data protection rules and protect, by default, the privacy and rights of the Data Subjects whose data will be processed by the new technology. Consideration by the Data Protection Office should include:

- The purposes for which personal data is being processed and the kinds of processing carried out
- An assessment of the necessity and proportionality of the processing with respect to the purposes for which it is being processes
- As assessment of the risks to the Data Subjects from the processing
- Details of steps to be taken to minimise any risk to the Data Subjects from the processing

16. Data breaches

16.1. A data breach occurs when any personal data is processed or accessed unlawfully. This may be due to a breach in security but relates to the situation where data is accessed, destroyed or altered without the appropriate authority

16.2. All employees have a duty to report any suspected breaches of data protection to the Data Protection Officer. If an employee is in any doubt as to whether a breach has occurred, they must report it to the Data Protection Office regardless

16.3. Any data breaches will be handled by the Data Protection Officer in line with the Data Breach policy

17. Access by third parties

17.1. Any requests to access employee or client data from external parties such as the Police or a government department, should be checked by the Data Protection Officer to ensure it is lawful for us to disclose the data requested

17.2. The approach to dealing with these requests will be governed by a separate Authorised Third Party policy

18. Complaints

18.1. Any complaints made to the business about the processing of personal data are to be passed, immediately, to the Data Protection Officer. This includes complaints from data subjects and information requests or correspondence from the Information Commissioner's Office

19. International transfer

19.1. The company may, from time to time, transfer or process personal data outside the EU. Transfer or processing of data outside the EU will only take place when:

- The transfer is to a country that the European Commission has determined ensures an adequate level of protection for personal data
- The transfer is to a country or organisation which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the Information Commissioner's Office; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the ICO
- The transfer is made with the informed consent of the relevant Data Subjects
- The transfer is necessary for the performance of a contract between the Data Subject and us (or for pre-contractual steps taken at the request of the Data Subject)

19.2. When data is to be transferred, or processed outside the EU for the first time the transfer must be authorised by the Data Protection Officer

20. Policy review

This policy will be reviewed periodically by the Data Protection Officer to ensure it is still relevant and up to date with any changes in the law, guidance or precedents set.

21. Document control

Version	Date	Author	Status	Comments
1.0	24.05.18	Gwen O'Sullivan	FINAL	