PM&M Consulting Solutions Ltd
Data Management Policy

Adopted 10 May 2018

Last updated: 9 May 2018

1. Context and overview

This Policy was prepared by Rachel Escott, Director, PM&M Consulting Solutions Ltd and approved and made operational on 9 May 2018.

It will next be formally reviewed on 30 May 2019.

Introduction:

PM&M Consulting Solutions Ltd, and it's trading names of Creative Communications and David Steel Consulting, occasionally receives and processes certain information about individuals on behalf of clients, including on occasion gathering additional information for example through customer surveys.

These can include customers, suppliers, business contacts, employees and other people the client organisation has a relationship with or may need to contact using the services of PM&M Consulting Solutions Ltd.

This policy describes how this personal data must be collected, handled and stored to meet our data protection standards – and to comply with the law.

Why this policy exists:

This data management policy ensures PM&M Consulting Solutions Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners of our own and those of our clients.
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. 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 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 GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. People and responsibilities

Both Director-employees of PM&M Consulting Solutions Ltd ['the Company'] contribute to compliance with GDPR. Each Director works on his or her own client accounts and takes responsibility for the proper management and safeguarding of clients' data, which may include the data of employees, customers and other stakeholders of the clients, for the duration they hold that data in order to fulfil the client contracts.

The lead GDPR Director (Rachel Escott) has received training and advice on conforming to the GDPR regulations and oversees their enactment within the Company through Director meetings.

This includes (but is not necessarily limited to):

- Keeping up to date about data protection issues, risks and responsibilities
- Documenting, maintaining and developing the Company's data protection policy and related procedures
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each business unit that processes personal data. The policies themselves will stand as proof of compliance.
- Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters
- Checking and approving contracts or agreements with third parties that may handle the Company's or clients' sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services that we are considering using to store or process data, to ensure their compliance with obligations under the regulations
- Checking that clients' privacy notices reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the companies use of their data

- Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles

The Data Protection Officer (DPO) – the person responsible for fulfilling the tasks of the DPO in respect of PM&M Consulting Solutions Ltd is Rachel Escott, Director and Audience Development Consultant.

3. Scope of personal information to be processed

- On occasion, as part of a contract of work for a given client, PM&M Consulting Solutions may act as a Data Processor for the client. As part of such contracts we may receive from the client personal data including:
    - names of individuals
    - postal addresses of individuals
    - email addresses
    - telephone numbers
    - online identifiers
    - social media identifiers
    - any other information relating to individuals
    - information relating to individuals for HR purposes

- Where available, PM&M Consulting Solutions Ltd consultants will log in to the client's own server system using their secure log-in processes, so data for those projects is not held or processed on the Company's own systems.
- Otherwise, the data is collected by the client organisation and transferred to us and subsequently returned to the client solely by secure, encrypted data transfer systems (eg Dropbox Business) based in the EU or conforming to the US:EU Privacy Shield; or if by post on storage material such as USB, CD or other external hard drives, or paper-based material such as feedback surveys, data will only be received from and return to the client by protected methods including Royal Mail Special Delivery, DHL or FedEx.
- New data relating to individuals that is generated by PM&M Consulting Solutions Ltd on behalf of a client, such as in the collection of survey feedback, will be carried out using reputable online software providers based in the EU or conforming to the US:EU Privacy Shield such as Survey Monkey.
- We rely on the client for the accuracy and cleanliness of the data it has collected about its clients, customers and other stakeholders, including where applicable its employees, before the client transfers that data to us for processing.
- All data received by us from clients will immediately be saved to a searchable file structure on our PM&M Consulting Solutions Ltd server (including internal and external back-up drives). Hard copies on paper, CD, USB etc will be kept securely in our offices until returned to the client after the end of the project.
- We will not aim to receive information about individuals that is not relevant for the specific contracted activity we are undertaking. Where additional information has been transferred to us, we will delete or anonymise that information to ensure only relevant information is retained, necessary to carrying out the contract. This includes removal from backed-up versions of the data files.
- We will strongly discourage clients from sending data by email. Where a client does so, we will immediately save the data into a searchable folder system on our server and delete the email attachments from our entire email server system, including the trash.
- We will keep all data on our servers and on all desktop computers and mobile devices (where relevant) encrypted and password-protected; and will strongly encourage clients to do the same before they transfer any data to us.

- At the end of a client project, we will retain personal data in as much as it was necessary for the completion of the contracted activity, for a shot period in case of any queries or requests to re-analyse the data. Following this short period (to be determined on a project-by-project basis), all personally-identifiable data will be removed from our files and folders, including backup drives, and only anonymised data will be retained as necessary for the analysis and reporting for the contract.
- We will review files and folders quarterly, to ensure data still held is necessary, not excessive and up-to-date.
- Where a client transfers to us details of any sensitive special categories of personal information or protected customers / stakeholders of their own, we will query the necessity for us to receive that information and maintain the actions described about to ensure it is fully protected and respected.

4. Uses and conditions for processing

On instruction from and under contract to the Data Controllers of our clients (via the specific client staff we are contracting with) we may be asked to receive, and process personal data as follows. This list may be added to from time to time.

Outcome/Use	Processing required	Data to be processed	Conditions for processing	Evidence for lawful basis
Show, season, event or launch promotional mailing	Mail-merge of name address details from clients' patron database	Name and address details	Consent	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing
Show, season, event or launch promotional e-mailing	Mail-merge of name address details from clients' patron database	Name and email address details	Consent	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing
Analysis of engagement patterns eg through ticketing frequency or type	Grouping and comparison of behaviour patterns including on occasion household or attendance groups behaviours	Names, addresses, ticketing history, audience segmentation flag	Consent; fulfilment of contract	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing

Invitation to Customer feedback survey	Mail-merge invitations to email addresses;	Name and email address details	Consent; legitimate interest	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing
Customer feedback survey analysis	Automated and manual analysis and reporting of feedback statistics and views	Name and email address details; postal address details; unique identifiers; device or IP identifiers; quantitative and qualitative feedback from individuals	Consent; legitimate interest	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing
Candidate shortlist for recruitment	Grading of applications against a Job Description; selection; invitation to interview	Name, postal and email addresses; phone numbers; personal education and employment information	Legitimate interest	Client ensures validity and proof of consent before transferring the data to PM&M Consulting Solutions Ltd and confirms this in writing OR information received direct form applicant on legitimate interest basis.

5. Privacy Impact Assessments

Our Privacy Impact Assessments (also known as Data Protection Impact Assessments, DPIAs) will be carried out in the following way:

- At the start of each project and where relevant, create a documented analysis of the processing operations required and the purpose of the processing.
- Seeking and obtaining assurance from the Data Controller (the client) of the lawful basis by which they hold and are transferring the data and contracting us to process it.
- An assessment of the necessity and proportionality of the data received in relation to the purpose.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals in relation to PM&M Consulting Solutions Ltd's storage and protection processes for the data.
- Confirmation to the client that the DPIA has been carried out and the necessary protections judged to be in place.

6. Data Sharing

PM&M Consulting Solutions Ltd will not normally engage in personal data sharing of any sort and should a client indicate their intention to use data sharing for promotional or other purposes, will strongly encourage them to review the provisions of the GDPA and their own Data Management Policy in relation to this.

7. Security measures

As detailed in Part 3 above, PM&M consulting Solution's protocols for ensuring the security of personal data transferred to us, collected by us and analysed or processed in the fulfilment of a contract for a Data Controller client are as follows:

- Where available, PM&M Consulting Solutions Ltd consultants will log in to the client's own server system using their secure log-in processes, so data for those projects is not held or processed on the Company's own systems.
- Otherwise, the data is collected by the client organisation and transferred to us and subsequently returned to the client solely by secure, encrypted data transfer systems (eg Dropbox Business) based in the EU or conforming to the US:EU Privacy Shield; or if by post on storage material such as USB, CD or other external hard drives, or paper-based material such as feedback surveys, data will only be received from and return to the client by protected methods including Royal Mail Special Delivery, DHL or FedEx.
- New data relating to individuals that is generated by PM&M Consulting Solutions Ltd on behalf of a client, such as in the collection of survey feedback, will be carried out using reputable online software providers based in the EU or conforming to the US:EU Privacy Shield such as Survey Monkey.
- We rely on the client for the accuracy and cleanliness of the data it has collected about its clients, customers and other stakeholders, including where applicable its employees, before the client transfers that data to us for processing.
- All data received by us from clients will immediately be saved to a searchable file structure on our PM&M Consulting Solutions Ltd server (including internal and external back-up drives). Hard copies on paper, CD, USB etc will be kept securely in our offices until returned to the client after the end of the project.

- We will not aim to receive information about individuals that is not relevant for the specific contracted activity we are undertaking. Where additional information has been transferred to us, we will delete or anonymise that information to ensure only relevant information is retained, necessary to carrying out the contract. This includes removal from backed-up versions of the data files.
- We will strongly discourage clients from sending data by email. Where a client does so, we will immediately save the data into a searchable folder system on our server and delete the email attachments from our entire email server system, including the trash.
- We will keep all data on our servers and on all desktop computers and mobile devices (where relevant) encrypted and password-protected; and will strongly encourage clients to do the same before they transfer any data to us.
- At the end of a client project, we will retain personal data in as much as it was necessary for the completion of the contracted activity, for a shot period in case of any queries or requests to re-analyse the data. Following this short period (to be determined on a project-by-project basis), all personally-identifiable data will be removed from our files and folders, including backup drives, and only anonymised data will be retained as necessary for the analysis and reporting for the contract.
- We will review files and folders quarterly, to ensure data still held is necessary, not excessive and up-to-date.
- In the rare even of additional temporary staff being employed by PM&M Consulting Solutions Ltd in fulfilment of a project contract, the temporary staff will be instructed in GDPR and data protection and privacy policies and supervised in their use of the data. Any data holding and manipulation will happen on the Company's computers and devices and not transferred to the temporary staff member's computers or devices.
- Where PM&M Consulting Solutions Ltd's Directors/ employees enter into an associateship contract to deliver a project, our Data Management Policy will be explained, and steps taken to ensure that Associates also abide by the policy.
- Where available PM&M Consulting Solutions Ltd Directors/ employees will use two-step authentication for all log-ins on the company's computers and devices, to protect against hacking, password theft and viruses, etc.
- Passwords will be stored in a secure vault system.
- Should we become aware of any data breach while data is held within our systems and premises, we will immediately notify our client and, through them, the ICO within the required timescales.

8. Automated processing

- Automated processing, as detailed above in Part 4, may include mail-merge systems, excel spreadsheet formulae and online survey software for analysis. In the main, however, most processing will be by manual means.
- On occasion data may be forwarded to external service providers for analysis by audience or population segmentation models. This will be by separate contract between PM&M Consulting Solutions Ltd's client and the external service company.
- All decisions to undertake automated processing on their data, and any decisions based on the outcome of that automated processing, will remain the responsibility of the client as Data Controller.

9. Subject access requests

- Personal data and the relationships with those individuals remain the property and responsibility of our clients as Data Controllers.
- We will respond to any request from clients to reveal the information we hold on an individual at a given moment, to assist them to respond to a Subject Access Request within the legal timescale. Such requests will be subject to authentication of the identity of the request originator eg by confirming phone call, visual identification via Skype or other means.
- If requested by our client on behalf of an individual, we will correct or delete the specified data on individuals, to help the client comply swiftly with their obligations under the GDPR.
- Our system of holding any data for a project only within a searchable file structure on our servers, and only for as long as it is needed to fulfil a contract, will enable this swift response to client requests.

10. The right to be forgotten

In certain circumstances, subjects have the right to be deleted from databases. As above, we will act on our clients' request to completely delete data on an individual in accordance with the client's policies and processes.

11. Privacy notices

PM&M Consulting Solutions Ltd will seek assurances from its clients that individuals, whose data is being transferred to us to fulfil a contract, are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights.

And that they make available their organisation's privacy statement.

12. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. PM&M Consulting solutions Ltd will:

1) As required by projects, apply the privacy measures described and maintain records of the implementation and outcomes.
2) Use the experience of implementation to demonstrate both existing and continuous compliance improvement efforts.
3) Keep records showing training of new employees or temporary contracted staff on privacy and data protection matters.