Sample Data Management Policy Structure

This document has been produced by The Audience Agency. You are free to edit and use this document in your business. You may not use this document for commercial purposes.

Important information:

This document forms a suggested approach to addressing personal data management in such a way as to provide a framework/structure for working towards and maintaining compliance with data protection regulations. As every company is different, and the nature and context of the personal information companies hold and the uses to which they might wish to put that data are different, it is vital that you seek professional or legal advice when creating your data management policy. Your business may face circumstances and issues that are not covered by this sample policy. As such, this document represents an approach which might not comprehensively address all the issues faced by any organisation. The Audience Agency cannot take responsibility for the consequences of errors or omissions. Any reliance you place on this document will be at your own risk.

Neither The Audience Agency, nor its employees, sponsors or partners are liable for any losses or damages arising from your use of this document.

How to use this document:

This document provides a suggested structure in which to produce your organisation's Data Management Policy. The structure suggested here is not the only way to produce a data management policy - it can be adapted to meet the needs and circumstances of each individual organisation. However, the sections that are included provide a structured process through which to consider and document key considerations and requirements that will help your organisation to plan and demonstrate how you comply with the regulations.

Each section addresses distinct but related areas of data management. The information in italics describes the type of information that should be presented in each section, and key considerations which should be addressed. Information presented in regular type can be included in your document as is, but there may be information specific to your organisation that should be included –this is indicated where there are square brackets [ ].

Please remove this cover page from your final document and remember to remove the 'SAMPLE' watermark.

Data Management Policy

1. Context and overview

Key details:

- Policy prepared by: [ ]
- Approved by board/management: [ ]
- Policy became operational on: [ ]
- Next review date: [ ]

Introduction:

[Company Name] needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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

Why this policy exists:

This data management policy ensures [company name]:

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners
- 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. Who? People and responsibilities

Everyone at [company name] contributes to compliance with GDPR. Key decision makers must understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance. You should set out here the key areas of responsibility which must be assigned, so that there is clarity about who in the organisation is responsible for leading on compliance with the regulations, what training is required by whom, and how policy and procedural information is disseminated within the team. These responsibilities should include (but are not necessarily limited to):

- *Keeping senior management and board updated about data protection issues, risks and responsibilities*
- *Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule*
- *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.*
- *Dissemination of policy across the organisation, and arranging training and advice for staff*
- *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 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 the company is considering using to store or process data, to ensure their compliance with obligations under the regulations*
- *Developing privacy notices to 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*

Data Protection Officer (DPO) - the person responsible for fulfilling the tasks of the DPO in respect of [company name] is [employee name, employee job title].

Under GDPR organisations in certain circumstances are obliged to appoint a DPO. However, regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR. Best practice dictates that, irrespective circumstances, organisations should appoint a named individual as DPO to lead on ensuring that data protection obligations are met. The minimum tasks of the DPO are:

- *To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws*
- *To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits*
- *To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)*

3. Scope of personal information to be processed

In this section you should detail:

- *the scope of the data you process, including whether you process any of the following:*
  - *names of individuals*
  - *postal addresses of individuals*
  - *email addresses*
  - *telephone numbers*
  - *online identifiers*
  - *any other information relating to individuals*
- *where the data is collected from and stored*
- *details of how you have made consideration to ensure that the data is accurate, (for example, what measures you have in place to check accuracy/duplication/completeness of data) relevant to the purpose, not excessive, up-to-date (for example, what measures you have in place to clean and update records) and not kept for longer than is necessary*
- *When and how relevant data will be checked against industry suppression files, such as the telephone preference service, the mailing preference service and the fundraising preference service*
- *Details of any sensitive special categories of personal information that it is necessary for [company name] to process. Describe the enhanced measures that are set in place to protect this information, and respect the rights and freedoms of the individuals to whom it relates*

4. Uses and conditions for processing

Here, document the various specific types of processing that you carry out, intended purpose for that processing, the data to be processed and what is the lawful basis for

processing, and how these conditions for processing are supported. Expand and add to the fields in the following table as required to give appropriate level of detail.

Outcome/Use	Processing required	Data to be processed	Conditions for processing	Evidence for lawful basis
Annual brochure mailing	*Mail-merge of name address details from patron database*	*Name and address details*	*Consent*	*Evidence of date consent given, how, permitted use and, permitted comms channels.*

***Consent** – in cases where you rely on consent as the lawful condition for processing, you should be able to demonstrate and describe how you have reviewed your processes and systems to make sure that consent is freely and unambiguously given for specific purposes, and that you can evidence an affirmative action on the part of the data subject to have indicated consent, and such that data subjects can reasonably understand who is using their personal information, what information, and for what purposes, and using which communications channels. Do your practises and systems incorporate a suitable audit trail which would enable you to demonstrate how and when consent was obtained, upon request? Do your practices and systems communicate an individual's right to withdraw consent at any time, and do your processes and systems support the functionality to do so?*

Where 'soft opt-in' is used in as the lawful basis for processing for electronic communications (email/SMS/automated-telephone) contact, you should record the notification statement detailing the intended use of personal information given at the point of collecting personal information during the course of sale or negotiation for sale which gave the customer the opportunity to opt out, and also how subsequently notify the customer of their right to unsubscribe with every following communication.

Where 'legitimate interest' is the lawful condition for processing, evidence should be given of the process by which the rights and freedoms of the individual have been weighed against the interests of the company, and how consideration/mitigation of the outcomes of the process have been made. How has the individual been informed of this processing, and what information have they been given to help them exercise their rights?

5. Privacy Impact Assessments

Privacy Impact Assessments (PIAs - also known as Data Protection Impact Assessments, DPIAs) form an integral part of taking a privacy by design, best practice approach, and there are certain circumstances under which organisations must conduct PIAs. They are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy, and protect against the risk of harm through use or misuse of personal information. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

PIAs undertaken by your company may be detailed here, or else referenced here and presented as an appendix to this data management policy document. The DPIA should contain:

- *A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.*
- *An assessment of the necessity and proportionality of the processing in relation to the purpose.*
- *An assessment of the risks to individuals.*
- *The measures in place to address risk, including security and to demonstrate that you comply.*
- *A DPIA can address more than one project.*

6. Data Sharing

In this section provide details of any/all Third Party organisations that [name of company] intends to share personal information with.

Where consent is the basis for sharing, describe how [company name] has obtained and recorded the necessary specific, clear, granular permissions for sharing data with NAMED third parties, for specifically defined uses, and in specified communications channels. Where other lawful conditions for processing are relied upon for data sharing, these should also be described.

Details should be given as to when data sharing agreements, describing and ensuring the arrangements concerning the collection of the necessary permissions, defining the scope of the personal data to be shared – along with the meta-data that will enable the receiving party to be able to create an audit trail, sufficient to enable them to respond to any challenge as to why an individual's data has been processed, or to facilitate a data subject access request, and which details the security measures that will be put in place to protect the data in transit, and which establishes the shared understanding of the receiving organisations' obligations as a data controller with responsibility for all aspects of the regulation as data controllers of the new copy of the data which is being shared with them.

7. Security measures

Here, describe the measures that are in place to protect the personal information that you store from breach.

Details should be documented here of the technical infrastructure considerations and measures put in place to leverage technology to require or ensure compliance, such as restricting and protecting access to the data to those people for whom it is necessary to perform the processing - such as measures like security software and firewalls, encryption, the use of secure Virtual Private Networks (VPN), log-in restricted access and two step authentications, etc.

The procedural and organisational policy measures, such as protocols for safe transfer of data in transit, and protocols for password management, and data back-up should also be detailed.

Describe also the measures in place to enable your organisation to know if a data breach has taken place and what measures are in place to ensure that reporting of any breaches are reported to the ICO within the required timescales. You should also articulate the measures you have in place to ensure that any data to be deleted, is deleted securely and without further risk of breach.

8. Automated processing

Provide details of any automated processing or decision making undertaken by your company name, including profiling. You should describe the lawful condition for that processing, what the outcomes are, and that in a case where such processing leads to a significant legal or other effect on the individual, how you have weighed the outcomes of that processing against the rights and freedoms of the individuals. The process of weighing the organisation's interest against the rights of the individual should always be transparently demonstrated. Privacy statements should include details of any automated processing, (including details of any third party profiling tools or datasets that are used to append information which will build a profile of individuals) and the outcomes of this processing, together with details of how individuals can exercise their right not to be subjected to such.

9. Subject access requests

All individuals who are the subject of data held by your company are entitled to:

- *Ask what information the company holds about them and why*
- *Ask how to gain access to it*
- *Be informed how to keep it up to date*
- *Be informed how the company is meeting its data protection obligations*

Details should be given here of the process by which [company name] will fulfil subject access requests and how individuals are notified of this process.

10. The right to be forgotten

In certain circumstances, subjects have the right to be deleted from your database.

Here, articulate your organisation's policy and process for evaluating this right, and how you would comply technically with those cases where you will carry out the individual's right to be forgotten – what would be deleted and what data would be retained anonymously.

11. Privacy notices

[Company name] aims to ensure that individuals 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.

To these ends the company has a privacy statement, setting out how data relating to these individuals is used by the company.

Detail here where and how the privacy statement can be viewed by individuals.

12. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. [Company name] details here the ongoing measures implemented to:

1) Maintain documentation/evidence of the privacy measures implemented and records of compliance

2) Regularly test the privacy measures implemented and maintain records of the testing and outcomes.

3) Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.

4) Keep records showing training of employees on privacy and data protection matters.

Once you have completed your first draft of this document, it will need ongoing review whenever any changes occur to personnel, practices or policies, or technical infrastructure that impact any of the information given. A formal date for holistic review is given in section 1, but the document should be considered a dynamic articulation of the organisations data management policy which is under constant revision.