Table of Contents

Data Protection Policy Statement

[Organisation] will uphold people's privacy rights and comply with legal and contractual obligations, while making effective use of personal data to support our [business/charitable] objectives.

[Organisation] will take a risk-based approach to data protection decision-making; keeping in mind the intent of data protection law and effective operational outcomes; adopting best recommended practice where there is ambiguity about minimal compliance requirements.

Data protection risk is ultimately owned by the [Board of Directors | Board of Trustees], with operational decisions delegated to [Directors | department heads | local managers] as specified within is Data Protection Policy Framework.

Scope

This Policy applies to all “processing” of "personal data" (terms as defined by law)

- where [Organisation] is Data Controller, and
- where [Organisation] is Data Processor

Implementation

Our Data Protection Policy comprises of this Data Protection Policy Framework document and the supporting policies, procedures and guidance to which it refers to throughout.

An index of supporting materials is outlined below:

- **Management of Key GDPR Requirements – Accountability summary**
- **Management of Key GDPR Requirements – Monitoring and Reporting**
- **Record of Processing Activity (ROPA)**
- **Privacy Information Strategy**
- **Baseline of specific privacy information**
- **Privacy Information Assessments**

The requirements of this Policy will be incorporated into the [organisation] operational procedures and contractual arrangements.

See Section

A2: Our approach to accountability for managing personal **data**, for detail on the roles and responsibilities we have allocated to manage data protection risk.

Review

[Organisation] undertake to review the Policy and the latest best practice at least every 12 months. The Policy will also be reviewed when necessary – for example, in the event of legislative or organisational change.

Data Protection Fee – Registration

[Organisation] will pay the required data protection fee, and is registered with the Information Commissioner's Office (ICO) with following reference:

Authorisation

This Data Protection Policy Statement and Framework has been adopted by the [Board / Trustees] as follows:

Signed:

Name:

Role:

Meeting (including reference to agenda item where relevant):

Date:

A: Accountability

A1: How we adhere to the data protection principles

A1.1: Lawfulness, fairness and transparency

We maintain a **Record of Processing Activity (ROPA)** which outlines our lawful basis for processing; processing of special categories of personal data, and processing of personal data relating to criminal convictions and offences

Section B2: Our approach to providing privacy information, details how we will fulfil our transparency obligations.

We also carry out the following additional activities to judge whether our processing meets the 'reasonable expectations' of the data subjects

[INSERT description of activities, e.g. surveys, reviewing feedback and complaints].

A1.2: Purpose limitation

Our **ROPA** outlines our Business Objectives, the purposes for which we process personal data to deliver those Business Objectives, and a description of the processing activities we undertake for each.

When a new purpose for processing personal data is identified, we use the decision-making process described in A5.1.2: Our approach to re-using personal data.

A1.3: Data minimisation

The following sections describe how we implement the minimisation principle in day-to-day operations:

A5.1.1: Our approach to data minimisation

A5.1.2: Our approach to re-using personal data

A1.4: Accuracy

The following sections describe how we implement the accuracy principle

A5.1.3: Our approach to maintaining accurate personal data

B4.1: Our approach to implementing the right to rectification

A1.5: Storage limitation

The following sections describe how we implement the storage limitation principle

A5.1.4: Our approach to record retention and disposal

A5.1.5: Our approach to pseudonymisation and anonymisation

B4.2: Our approach to implementing the right to erasure

A1.6: Integrity and confidentiality

The following section describes how we implement appropriate security if personal data

C1: Our approach to managing the security of personal data

A2: Our approach to accountability for managing personal data

A2.1: Data Protection Officer (DPO) and other roles

We have assessed the criteria outlined in the GDPR and have concluded that [we must appoint a DPO | are not required to appoint a DPO, but will allocate a role to be [Data Protection Lead. This role is held by [role title]].

This decision is based on the following assessment:

[insert assessment of whether statutory DPO is required]

>>> INSERT Output #1 from *Management and Delivery of Key GDPR Requirements (Data Protection Office decision tree and guidance).*

The [Board of Directors | Board of Trustees] for [Organisation] is ultimately accountable for strategic approach to data protection.

The role of [Data Protection Officer | Lead] is responsible for providing data protection oversight and expertise to the organisation as a whole.

The [Data Protection Officer | Lead] has operational responsibility for the organisation's good practice and will be accountable for maintaining the **Records of Processing Activity** and Data Controller notification.

All staff, including [volunteers,] contractors and temporary workers, are required to understand and comply with data protection standards and procedures.

We will meet our accountability obligations by

(i) committing the following resources:

INSERT: Allocation of budget: [describe budget or process for including data protection in budget decisions]; Allocation of human resource: [describe resources]; [evidence of commitment].

(ii) allocating the roles and responsibilities outlined in our **Management of Key GDPR Requirements – Accountability summary** document, to deliver strategic, operational and tactical accountability.

>>> Output #4 from *Management and Delivery of Key GDPR Requirements*

(iii) ensuring that Strategic monitoring of data protection risk is overseen by the [Data Protection Officer | Lead] and is reported to [Board of Directors | Board of Trustees] on a [interval] basis and when urgent risks arise.

(iv) Ensuring that Operational monitoring and reporting of data protection compliance will be carried out and recorded as described in the **Management of Key GDPR Requirements – Monitoring and Reporting** document.

>>> Output #3 from *Management and Delivery of Key GDPR Requirements*

A2.2: Data protection training and awareness

We will conduct a training needs assessment to ensure all training and awareness is appropriate based on the nature, scope and context of the processing of personal data which is undertaken, and the data protection responsibilities of the role.

>> **INSERT Output #1 from *Management and Delivery of Key GDPR Requirements (Data Protection Skills Framework)***

We will ensure staff receive data protection training and awareness by:

[describe mandatory training, schedules for refresher training, role-specific training and other awareness/education mechanisms]

We will ensure volunteers receive data protection training and awareness by:

[describe mandatory training, schedules for refresher training, role-specific training and other awareness/education mechanisms]

A3: Our Record of Processing Activities (ROPA)

The ROPA is updated each time a new purpose of processing is identified, and a review of the lawful basis for that processing is carried out.

The ROPA is reviewed for accuracy and currency by [role title or department] every [interval].

>> **INSERT Output from *Record of Processing Activity (ROPA)***

A4: Our approach to working with suppliers and partners

When researching or negotiating with new suppliers, we [describe or link to the process to be followed].

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #8 Procurement***

We use standard Data Processor contract clauses for suppliers who are acting as Data Processors on our behalf.

When data is disclosed to other Data Controllers, we

[describe data sharing arrangements,

describe how ad-hoc disclosure requests are handled

reference or link to templates and procedures]

A5: Our approach to proactive management of Data Protection risk

A5.1: Data protection by design and default

Data protection by design and default will be embedded into our change and project management processes by

[describe how Data Protection by design and default is considered, monitored and evaluated within change and project management processes]

A5.1.1: Our approach to data minimisation

When a purpose for processing personal data is identified, we will identify the processing activities required and design systems, data collection forms and processes to comply with the principle of minimisation.

Where there are multiple purposes with differing minimum data requirements, we will put in place suitable access controls and procedures to reduce excessive processing.

A5.1.2: Our approach to re-using personal data

If the re-use of personal data is for the same purpose as it was originally collected for then we will carry out the processing, ensuring that we adhere to

B1: Our approach to transparency and fairness to **individuals**.

If the re-use of personal data is for a new purpose then we assess whether the new purpose is compatible with the original purpose for which the personal data was collected by:

[Example:

1. Referencing our ROPA to ascertain the original purpose and context of processing
2. Consulting data journey documents to determine the nature and scope of the processing
3. Determining whether a purpose compatibility assessment is required
4. Carrying out the assessment if required]

>> **NOTE: consider using Protecture's Decision Tree "Do I need to do a Compatibility Assessment?"**

>> **NOTE: consider using Protecture's "Purpose Compatibility Assessment Tool"**

A5.1.3: Our approach to maintaining accurate personal data

We adopt the following measures to maintain the accuracy of personal data:

For example:

- When a purpose for processing personal data is identified, we will identify the processing activities required and meet the level of accuracy required for the purpose (wherever personal data is collected, input, transferred or updated) by designing suitable systems, data collection forms and processes.

- Staff will follow the following processes and procedures:

A5.1.4: Our approach to record retention and disposal

Our records retention schedule[/policy] is [link or reference where this document can be found]

A5.1.5: Our approach to pseudonymisation and anonymisation

[describe triggers and mechanisms for applying pseudonymisation or anonymisation]

A5.2: Data protection impact assessment

Before starting any high-risk processing activity, the decision as to whether a Data Protection Impact Assessment is required will be taken by [person responsible for deciding] based on the criteria described in the GDPR and the Article 29 Working Party Guidance on Data Protection Impact Assessment.

[describe or link to the procedure]

>> **NOTE: consider using Protecture's Decision Tree "Do I need to do a Data Protection Impact Assessment?"**

A6: Our approach to transfers of personal data outside the EEA

The requirement for data to be transferred outside the European Economic Area will depend on the purposes of processing, which is documented in our **ROPA**.

The condition for transfer will also be determined by the purpose.

We do not transfer data outside the EEA without a valid condition for processing and appropriate safeguards for the rights and freedoms of the data subjects.

Our process for ascertaining the appropriate condition for transfer and safeguards is [describe or link to process]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #9 Transfers***

B: Transparency

B1: Our approach to transparency and fairness to individuals

Our strategic approach to providing privacy information is defined in our **Privacy Information Strategy.** This outlines

- the means (methods) we will use to provide privacy information, in order that this results in information that is accessible and can be comprehended by the different individuals (Data Subject Categories) we engage with, and

- how we will provide access to general privacy information, i.e. the privacy information that every Data Subject should be able to access.

>> **INSERT Output from *Privacy Information Strategy – Parts 1 and 2***

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #2 Privacy***

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #3 Consent***

B2: Our approach to providing privacy information

Our approach to providing privacy information to individuals is achieved by

- defining **baseline of specific privacy information**, and

- undertaking **Privacy Information Assessments** when required to define how privacy information will be provided to individuals.

>> **INSERT Output from *Privacy Information Strategy – Parts 3 and 4***

B3: Our approach to providing individuals with access to their personal data

B3.1: Our approach to implementing the right of subject access

We ensure that data subjects are informed of their right to access their personal data and the options available to them for exercising this right by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When a data subject access request is received, we

>>[describe or link to process document]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #5 Access***

B3.2: Our approach to implementing the right of data portability

We ensure that data subjects are informed of their right to data portability where it applies, and the options available to them for exercising this right by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When a request for data export or transfer for portability is received, we

[describe or link to process document]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #6 Portability***

B4: Our approach to enabling individuals to manage their personal data

B4.1: Our approach to implementing the right to rectification

We ensure that data subjects are informed of their right to rectification and the options available to them for managing their own data by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When a request for rectification of inaccurate data is received, we

[describe or link to process document]

B4.2: Our approach to implementing the right to erasure

We ensure that data subjects are informed of their right to erasure, where it applies; by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When a request for erasure of personal data is received, we

[describe or link to process document]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #7 Erasure***

B4.3: Our approach to implementing the right to restriction of processing

We ensure that data subjects are informed of their right to restriction of processing, where it applies to their personal data; by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When an individual asserts the right to restriction, we

[describe or link to process document]

B4.4: Our approach to implementing the right to object

We ensure that data subjects are informed of their right to object as it applies to their personal data; by including this right in privacy information, as documented in our **Privacy Information Strategy.**

Where processing is carried out under the lawful basis of legitimate interests or in the public interest; [describe or link to process document]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #4 Object***

Where the objection is to the processing of personal data for direct marketing, [describe or link to process document]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #4 Object***

B4.5: Our approach to rights in relation to automated decision-making

When implementing processing which involves automated decision-making or profiling of individual which may have legal effects or similar, we will ensure that there are appropriate safeguards for the individuals' rights and freedoms by considering and building in those safeguards as described in A5.2: Data protection impact assessment

We ensure that data subjects are informed of their rights in relation to automated individual decision-making (including profiling) as it applies to their personal data; by including this right in privacy information, as documented in our **Privacy Information Strategy.**

When an automated decision is challenged, we will; [describe or link to process document]

C: Security and personal data breaches

C1: Our approach to managing the security of personal data

The “nature, scope, context and purposes of processing” will come from our **ROPA** and the information obtained from our **Data Journey Maps**. This information will be used to determine the “appropriate technical and organisational measures” that need to be taken in order to protect the personal data from unlawful or unauthorised processing and against accidental loss, destruction or damage.

The following policies and associated procedures describe how we protect information assets used by [Organisation].

[describe how information security risk is assessed and managed, e.g.

- Information Security Policy;

- Remote Working Policy;

- Bring Your Own Device (BYOD) Policy

- Access Control Policy]

C2: How we handle personal data breaches

C2.1: Our approach to managing security incidents

Guidance on how to recognise and report information security incidents is provided to staff [and volunteers] by [describe how guidance is provided]

The process for investigating, reporting and responding to information security incidents is [describe or reference process]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #1 Breach***

C2.2: Our approach to notifying the Supervisory Authority of a breach

Where an information security incident meets the definition of a “personal data breach” from Article 4 of the GDPR, an assessment is made as to whether there are sufficient mitigating measures in place to protect the rights and freedoms of the affected data subjects.

If the affected data subjects’ rights or freedoms may be affected by the breach, then the Information Commissioner’s Office will be notified.

This process is [documented at this location]/[describe here]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #1 Breach***

C2.3: Our approach to informing individuals of a security breach

Where an information security incident meets the definition of a “personal data breach” from Article 4 of the GDPR, an assessment is made as to whether there are sufficient mitigating measures in place to protect the rights and freedoms of the affected data subjects or whether there is a likelihood of high risk to their rights or freedoms as a result.

If there is a high likelihood that data subjects’ rights or freedoms will be affected by the breach then a communications plan for informing the affected data subjects will be implemented.

This process is [documented at this location]/[describe here]

>> **INSERT Output from *Management and Delivery of Key GDPR Requirements - GDPR Requirement Framework #1 Breach***