Data Protection Policy

The National Holocaust Centre & Museum

Author: Anne Howkins – Finance & Business Manager

Date: March 2018

Review Due: March 2019

Version 0.2.

Contents

Data Protection Policy

Introduction

Legislation covering the use of personal data.

Currently Data Protection in the UK falls under the Data Protection Act (DPA) 1988. However, from 25th May 2018 this Act will be superseded by the General Data Protection Regulation (GDPR). Although the GDPR is an EU regulation, the government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. In preparation of this document, which is intended to promote best practice, the more onerous requirements of DDPR will be assumed.

In addition, The Fundraising Preference Service (FPS) allows the public to stop text, phone, email and direct mail communications from charities of their choice.

The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf.

The overriding principle of GDPR is that ***"The protection of natural persons in relation to the processing of personal data is a fundamental right"*** and that ***"The processing of personal data should be designed to serve mankind"***

Personal data

The GDPR definition of personal information is more detailed then the DPA and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. It applies to both automated and manual filing systems, which is broader than DPA.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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 purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) 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;
e) 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 be 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 the GDPR in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Lawful processing

GDPR requires that Beth Shalom identifies and documents its legal basis for processing personal data – the "conditions for processing". The accountability basis of GDPR is a significant addition to the requirements of the DPA.

This legal basis should demonstrate that at least one of the following conditions is met:

a) Consent of the data subject
b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
c) Processing is necessary for compliance with a legal obligation
d) Processing is necessary to protect the vital interests of a data subject or another person
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

There are certain other provisions for special categories of data, however the overriding principle is that of consent.

Consent

Consent under GDPR requires a clear affirmative action by the owner of the data, and must demonstrate that it is:

a) freely given
b) specific
c) informed
d) an unambiguous indication of the individual's wishes

Silence, pre-ticked boxes or inactivity does not indicate consent.

The right of the individual

Beth Shalom should demonstrate that the following rights to individuals under the requirements of GDPR have been met:

a) The right to be informed
b) The right of access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling

Details of these requirements are shown below.

The right to be informed

The information supplied must be concise, transparent, intelligible and easily accessible. It should be written in clear and plain language, and there should be no charge. The following table indicates what, and when it should be supplied:

What information must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	Yes	Yes
Purpose of the processing and the legal basis for the processing	Yes	Yes
The legitimate interests of the controller or third party, where applicable	Yes	Yes
Categories of personal data		Yes
Any recipient or categories of recipients of the personal data	Yes	Yes
Details of transfers to third country and safeguards	Yes	Yes
Retention period or criteria used to determine the retention period	Yes	Yes
The existence of each of data subject's rights	Yes	Yes
The right to withdraw consent at any time, where relevant	Yes	Yes
The right to lodge a complaint with a supervisory authority	Yes	Yes
The source the personal data originates from and whether it came from publicly accessible sources		Yes
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	Yes	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	Yes	Yes

In addition the following timescales apply to the provision of information:

We provide individuals with privacy information at the time we collect their personal data from them.

Where data is not obtained directly from the data subject, the information should be provided within a reasonable period of having obtained the data (generally one month). Or if the data is used to communicate with the individual it should be provided, at the latest, when the communication takes place. If disclosure to another recipient is envisaged, communication should be before the data is disclosed, at the latest.

The right of access

Individuals have the right to obtain confirmation that their data is being processed, access to their personal data, and other information (largely information that should be supplied in a privacy notice).

This information is to be provided free of charge and within one month of any request.

The right to rectification

Requests must be processed within one month. If the data has been disclosed to a third party, they must be informed of the rectification.

The right to erasure

Also known as 'the right to be forgotten'. The broad principle is to enable an individual to request the deletion or removal of personal data where this is no compelling reason for its continued processing.

The following circumstances apply:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

b) When the individual withdraws consent.

c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

d) The personal data was unlawfully processed (ie otherwise in breach of the GDPR).

e) The personal data has to be erased in order to comply with a legal obligation.

f) The personal data is processed in relation to the offer of information society services to a child.

If the data has been disclosed to third parties, they must be advised of the erasure. This applies to data shared on social networks, forums and websites.

The right to restrict processing

Processing of personal data is to be restricted in the following circumstances:

a) Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

b) Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.

c) When processing is unlawful and the individual opposes erasure and requests restriction instead.

d) If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Procedures should be in place to ensure when there is a requirement to restrict the processing of personal data.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Data must be provided, free of charge, in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The right to object

Individuals have the right to object to:

a) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
b) direct marketing (including profiling)
c) processing for purposes of scientific/historical research and statistics.

Where personal data is processed for direct marketing purposes (fundraising), processing must be ceased immediately as soon as an objection is received. There are no exemptions or grounds to refuse. Individuals must be informed of their right to object "at the point of first communication" and in the privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

These requirements are similar to existing rules under the DPA.

Where personal data is processed for research purposes individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

Rights in relation to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. Beth Shalom should indentify which processing operations constitute automated decision making and consider whether changes are needed to working practices. These rights are significant in HR procedures and practices.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

a) performance at work;
b) economic situation;
c) health;
d) personal preferences;
e) reliability;
f) behaviour;
g) location; or
h) movements.

When processing personal data for profiling purposes, appropriate safeguards must be in place so that:

a) processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
b) appropriate mathematical or statistical procedures are used for the profiling.
c) appropriate technical and organisational measures are in place to enable inaccuracies to be corrected and minimise the risk of errors.
d) personal data is secured in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Accountability principle

The new accountability principle in Article 5(2) requires demonstration of compliance with the principles and states explicitly that this is Beth Shalom's responsibility. The following is required to show compliance:

a) Implementation of appropriate technical and organisational measures that ensure and demonstrate compliance. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

b) Maintain relevant documentation on processing activities.

c) Where appropriate, appoint a data protection officer (DPO). Beth Shalom does not fall under the category of orgnaisations which must appoint a DPO.

d) Implement measures that meet the principles of data protection by design and data protection by default. Data protection by design should be included in any new activities involving the use of personal data, and also in the commissioning of computer systems for that purpose. Measures could include:

    1. Data minimisation;
    2. Pseudonymisation;
    3. Transparency;
    4. Allowing individuals to monitor processing; and
    5. Creating and improving security features on an ongoing basis.

e) Data protection impact assessments where appropriate.

Records of processing activities

Internal records of processing activities should be maintained, which record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

a) Name and details of the organisation (and where applicable, of other controllers, your representative and data protection officer).
b) Purposes of the processing.
c) Description of the categories of individuals and categories of personal data.
d) Categories of recipients of personal data.
e) Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
f) Retention schedules.
g) Description of technical and organisational security measures.

These records are to be made available to the relevant supervisory authority for purposes of an investigation.

Data Protection Impact Assessments (DPIA)

These should be carried out when new technologies are to be implemented, and where profiling or other significant use of personal data is planned. The assessment should include risk, security issues and demonstration of compliance.

Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Communication of information to trustees

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. The trustees are expected to put into place comprehensive but proportionate governance measures, including privacy impact assessments and privacy by design, which are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for Beth Shalom.

In the same manner that Risk and Financial information is communicated to the Trustees. It is proposed that a formal reporting structure be put in place so that the Board is made aware of its legal obligations.

Sources of personal data at Beth Shalom

Beth Shalom collects and stores data using a variety of methods, and for a range of business purposes.

Purpose of data held by Beth Shalom Ltd

Data may be held for the following purposes:

a) Staff Administration
b) Fundraising
c) Realising the Objectives of a Charitable Organisation or Voluntary Body
d) Accounts & Records
e) Advertising, Marketing & Public Relations
f) Information and Databank Administration
g) Journalism and Media
h) Processing For Not For Profit Organisations
i) Research
j) Volunteering