US Data Protection Policy

UPDATED: MAY 2018

US Data Protection Policy

Introduction

The United Synagogue (US) controls and processes personal information about its members, employees and volunteers under EU data protection legislation.

This policy sets out:

- Our processes for legitimately processing data
- How the accuracy of the data will be maintained
- What security measures must be in place prior to any processing of information.
- The correct parameters of when it is appropriate to process data.

Scope

This policy applies to all members, employees and volunteers who may be involved in the collection and/or processing of personal information on behalf of the US and extends to data whether it is held on paper or by electronic means.

Objectives

The objectives of this Data Protection Policy are:

- To comply with all applicable data protection legislation.
- To outline, guide and monitor the coordination of the information, security and data handling procedures in force within the US.
- To promote confidence in the US's information, security and data handling procedures.
- To provide assurances for third parties dealing with The US.
- To provide a benchmark for employees on information, security, confidentiality and data protection issues.

Data Protection Principles

Data protection legislation covers all personal information relating to living individuals. The US will not share this information with other organisations without the consent of the individual concerned unless we are required by law to do so.

This Policy sets out how the organisation complies with data protection principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall only be obtained and further processed for specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose that they are processed.
4. Personal date shall be accurate and kept up to date.
5. Personal data shall not be kept longer than necessary.
6. Personal data shall be processed in line with the rights of the data subject.
7. Personal data must be kept secure.
8. Personal data must not be transferred to a country without adequate protection.
9. The right to be informed
10. The right of access
11. The right of rectification

12. The right to erase
13. The right to restrict processing
14. The right to data portability
15. The right to object
16. Rights in relation to automated decision making and profiling

Statement of commitment

The US is committed to maintaining the highest standards and levels of security and confidentiality for information in our custody and control. Safeguarding this information is critical to the successful functioning of the organisation. The US will treat all information in its care and control with the same high degree of security and confidentiality. This Policy applies to all synagogues, departments and divisions within the US. The organisation further undertakes to inform members, employees, volunteers and members on how it uses information and the purposes for which information is processed.

Data Protection Processes

In order to achieve its objectives, The United Synagogue will:

- Ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information, security and compliance with all applicable data protection legislation.
- Ensure that all contracts and service level agreements between any part of The US and external third parties (including contract staff), where personal data is processed, make reference to the regulations where appropriate.
- Ensure that third parties acting on behalf of The US are given access to personal information that is appropriate to the duties they are undertaking and no more.
- Ensure that all staff (including contract staff) and volunteers understand their responsibilities regarding data protection and information security under data protection regulations.

Data Sharing

There are a limited number of occasions where it is necessary and appropriate for the organisation to share personal data it holds.

Under the regulations, the US are required to explain to all individuals how they will use personal data which is collected and shared. This information is provided to all new members, employees and volunteers as part of their respective agreements with the organisation.

Individuals are told:

- Who we are
- Purpose for sharing data
- Our legal basis or bases, if more than one, for processing data

The organisation has appropriate Information Processing Agreements (IPA) with all relevant third parties, these are reviewed on a regular basis and recorded on a central IPA log. All decisions to share data are based the current needs of the organisation and comply with regulations. The US remains the data controller throughout a members, employees or volunteers relationship with the organisation and has overall control over the purpose and the manner in which personal data is processed. The organisation is also responsible for the protection of such data.

Exemptions

In certain circumstances, it may be appropriate or necessary to disclose information held by the organisation to specific third parties for example, in order to prevent a criminal offence from being committed, or to prevent the continuation of a criminal offence, or to comply with other legal obligations.

Data Retention

Personal data must only be kept for the length of time necessary to perform the process or function for which it was collected. This applies to both electronic and hard copy data.

Under new legislation, an additional provision is the right to be forgotten; Individuals (data subjects), can request that certain information about them be deleted in the following circumstances:

- Where the personal data is no longer required for the purpose for which it was originally collected/processed and deletion has not already taken place.
- Where the individual withdraws consent.
- Where the individual objects to the processing and there is no overriding legitimate interest or other legal obligation that justifies continuing the processing.
- Where personal data was unlawfully processed (i.e. in breach of regulations).
- Where personal data must be erased in order to comply with a legal obligation.

Nothwithstanding the above, sufficient data may be retained on a suppression list as to allow the individual to be identified so as to prevent the accidental processing of their data in future without permission.

Disposal of Data

Where personal and confidential information is no longer required, it will be safely and securely destroyed.

Right of access to data - Subject Access Requests (SARs)

Individuals have a right of access to personal information held by the US, if they are the "data subject" of that information. Requests must be made by the data subject themselves in writing and addressed to the Synagogue office or the Data Protection Officer as appropriate. The person requesting the data must complete an Access Request Form (available on the US Website), providing details of the information required as well as their current address and an acceptable form of identification. There is normally no charge for responding to the request.

In those rare cases were the request is deemed to be either unreasonable or excessive the Data Protection Officer may choose to refuse the request entirely, or comply subject to an administrative fee being paid. SAR's will normally be processed within a month of receipt.

The US will only accept SARs from the data subject (individuals) concerned or holders of an appropriate Power of Attorney thereof.

Data Breaches

The US has appropriate processes and procedures in place to ensure that any personal data breaches are promptly detected, investigated and duly reported to the Information Commissioners Office (ICO) and were necessary, to the individual concerned.

Regular data mapping and the utilisation of the US IT Infrastructure ensures that any potential data breech can be detected and addressed promptly. Any wilful disregard or intentional breach of the Data Protection Policy by employees may be considered a disciplinary offence and thereby subject to The US's Disciplinary Procedure.

Any data breech caused or allowed by third party data processors (e.g. printers etc) acting on the organisation's behalf under contract will be considered and treated as a breach of contract.

Equality impact assessment (EIA)

Following a Stage 1 EIA, it was found that this policy will affect all members, employees and volunteers' in the same way as all personal data should be processed in accordance with the regulations, consequently there is no adverse impact on any one of these groups in particular.

The Data Protection Officer is ultimately responsible for all data compliance and monitors the organisation's Data Protection processes.