Urban Theology Union

Data Protection Policy

Introduction

Purpose

The Urban Theology Union (UTU) is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data. The organisation has the Office Administrator as its data protection lead, office@utusheffield.org.uk.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

UTU processes personal data in accordance with the following data protection principles:

- UTU processes personal data lawfully, fairly and in a transparent manner.
- UTU collects personal data only for specified, explicit and legitimate purposes.
- UTU processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- UTU keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- UTU keeps personal data only for the period necessary for processing.
- UTU adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

UTU tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notice. It will not process personal data of individuals for other reasons or share with third parties without prior consent.

Where UTU processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with the requirements of the UK's GDPR.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and

UTU will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

[If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.]

To make a subject access request, the individual should send the request to office@utusheffield.org.uk. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires. UTU will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case. If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;

- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask UTU to take any of these steps, the individual should send the request to office@utusheffield.org.uk

Data security

UTU takes the security of personal data seriously. UTU has internal controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties e.g locking filing cabinet, office with locking door, robust software security. Where UTU engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

In the unlikely event that processing would result in a high risk to individual rights and freedoms, the organisation would carry out a data protection impact assessment to determine the necessity and proportionality of processing. This would include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If UTU discovers that there has been a notifiable breach of personal data, one that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery and notify those involved. UTU will record all data breaches regardless of their effect.

International data transfers

Personal data may be transferred to countries outside the UK for legitimate interest in carrying out the work of UTU with its members: membership, courses etc. Data is transferred outside the UK on the basis of only using personal addresses, email addresses.

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals: members, tutors, staff or volunteers . Where this is the case, the organisation relies on individuals to help meet its data protection obligations. Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The UTU will provide training to all individuals about their data protection responsibilities as part of the induction process [and at regular intervals thereafter].

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

J. Forde

March 2023