True Food Community Co-operative

Data Protection Policy and Procedures

Introduction

This document is for members, volunteers and staff of True Food. It has been written to bring True Food's data processing activities into line with current data protection regulations. It is based on guidance from the Information Commissioner's Office www.ico.org.uk although edited and simplified.

The policy is supported by procedures which cover its implementation. These contain further explanations of the principles of our data processing and guidance on how we apply the policy in practice.

True Food and Personal Data

True Food respects the privacy of individuals and is committed to the secure processing of all personal data received. True Food processes personal data from a variety of different groups of individuals for a range of business purposes, for example members, volunteers, staff, customers and suppliers.

Scope

This policy applies to personal data as defined by current UK data protection law, referred to here as GDPR. The policy applies to all staff, members and other volunteers who process personal data on behalf of True Food.

Personal Data

Personal data is information relating to a person who could be identified from the information in question.

The personal data generally processed by True Food staff, members and volunteers will be limited to personal names, addresses, email addresses and telephone numbers.

Certain members of staff and members will process further personal data including financial and personnel records.

CCTV images are also captured, and can be processed by members of staff to aid the investigation of potential crime.

Processing

Processing is the obtaining, recording, updating, storage, sharing, or other use of data.

Data Processing activities are guided by the following principles:

- Lawfulness, fairness and transparency
- Limiting the data collected to what is genuinely needed to run True Food.
- Having a lawful basis, defined by GDPR, for all data processing
- Using data only for the specific purpose for which it is collected
- Ensuring that data is accurate.
- Reviewing the data processed to check it is truly needed
- Keeping data only as long as it is needed
- Having appropriate measures in place to ensure data is kept confidentially and securely.
- Taking responsibility for ensuring that all data processing activities are compliant with GDPR

Lawful Basis

There must be a lawful basis for the processing of any personal data. GDPR sets out what those bases are. The lawful bases that True Food relies on will be one of the following:

- A person has given genuine and explicit consent for specific data to be processed
  e.g a customer gives us their email in relation to a special-order.
- The processing is necessary to fulfil a contractual obligation with a person
  e.g True Food must collect employees' bank details in order to pay them
- The processing is necessary to comply with a common law or statutory obligation
  e.g True Food must collect personal information on committee members to complete statutory reporting to the FCA
- Legitimate interest, except where such interests are overridden by the interests of the data subject
  e.g True Food collects information on preferred activities of members because it has a legitimate interest in knowing how its members want to contribute to the co-operative.

If none of these bases apply, the processing will be unlawful. If someone gives us their data for one reason, it can not be used for any other.

Special Category Data

GDPR defines the following as special category data: race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health, sex life, sexual orientation, history of criminal offences.

It is prohibited to process this data unless there is:

- Explicit consent to process for specified purposes, or
- Processing is necessary for the carrying out of obligations as an employer, or
- Processing is necessary for the purposes of preventative or occupational medicine or assessment of the working capacity of an employee.

The only special category data that True Food currently has any reason to collect relates to the health of employees and volunteers. This is in circumstances where at least one of these grounds apply.

Rights of the individual

True Food respects the rights of the individual and has procedures in place to cater for an individual's right to:

- access their personal data.
- have inaccurate personal data rectified or completed if it is incomplete.
- have personal data erased. The right is not absolute and only applies in certain circumstances.
- request the restriction or suppression of their personal data.
- object to the processing of their personal data in certain circumstances.

The Operations Manager will respond to any request relating to the above. The Operations Manager will comply with such requests except where there is a lawful basis for not doing so.

Privacy Notice

Privacy information is made available to individuals at the time the personal data is collected, in the form of a Privacy Notice on our website. The same information is available in the shop This includes:

- Why it is being collected & what will be done with the data

- For how long it will be kept
- With whom it will be shared

Consent

If consent is the lawful basis then the individual will be asked when the data is collected. Where this is the case, requests for data will specify what the data will be used for and seek consent in each case. Data will not be used for any other purpose than that specified.

Accountability and governance

True Food is not required to have a Data Protection Officer. A nominated member of staff (the Operations Manager) is responsible for the day to day implementation of data protection activities. True Food's Management Committee is responsible for ensuring that True Food has enough staff and resources to discharge its data processing obligations.

Contracts with third parties

Whenever an external body such as a supplier is used to process personal data on our behalf, we will ensure that there is a written contract in place. The contract is important so that both parties understand their data processing responsibilities and liabilities.

True Food will only share data with organisations who can show they have policies and procedures in place to ensure data is processed lawfully. This will be regularly reviewed by the Operations Manager to ensure third party policies and procedures are up to date.

Data Asset Register

The Data Asset Register records all aspects of data processing activities. It includes:

- How captured
- Where stored and how
- What used for
- Who uses it
- Who shares it internally and externally
- On what lawful basis is it processed
- When it should be deleted
- Any risk associated with it

The Register is kept up to date by the Operations Manager. The details of all new data processing activities will be logged on the Data Asset Register.

Certification with the Information Commissioner's Office /Fees

As True Food uses CCTV for the prevention and detection of crime, we are registered with the ICO.

Security

Personal data is securely processed by means of appropriate technical and organisational measures. This includes risk analysis, organisational policies, and physical and technical measures, as set out in the Information Security Policy.

Personal Data Breaches

A data breach is a breach of security leading to the unlawful loss or destruction of, or unlawful access to, personal data. Examples include the hacking of membership database, theft of laptop or personal phone containing personal data obtained through work for True Food.

In each case the Operations Manager will be informed. They will investigate and establish whether the breach must be reported to the ICO and to the person/s involved, following

ICO guidance from their website or helpline. Incidents which may need to be reported to the ICO are those where there is a likelihood of 'severe risk to the rights and freedoms of an individual'.

Whether a breach is reported to the ICO or not, a record will be kept of the incident by the Operations Manager.

Retention & Deletion

Personal data will not be retained once there is no longer a lawful basis for keeping it.

Some data must be retained for legal or regulatory reasons. Full details of this are available in the Privacy Notice. If there is no legal requirement to retain the data it will be deleted. The Business Development Lead and Operations Manager will review data that we keep and ensure that we delete anything there is no longer a reason to retain.

Storage

Personal data will be stored securely. Staff, members and volunteers will ensure:

- Paper copies are locked away when necessary or
- Personal details are not on obvious public display e.g kept in desk drawers or folders
- IT devices are protected by passwords.

Home Working and Own Devices

Employees and members work from home and use their own devices for True Food business. Employees and members will take reasonable steps to ensure that data stored on these devices, or on paper, is kept secure ie:

- All devices must be protected with a secure password
- Paper copies of data must be stored securely
- Data should not be accessible to family and visitors or other users of the devices
- Data breaches must be reported to the Operations Manager

Training

New staff, committee, any member or other volunteer having access to personal data will receive briefing and guidance on their responsibilities in complying with this policy and the GDPR. Members and other volunteers will be reminded of the guidance annually, if risk or concerns are identified or if new data processing is introduced.

Review of policy and procedures

The policy, procedures and privacy notice will be reviewed annually, if risk or concerns are identified or if new data processing is introduced. This is done by the Operations Manager and the committee to ensure True Food continues to meet the requirements of current legislation and regulation.

Reviewed October 2024

True Food Community Co-operative
CCTV Policy and Procedures

This policy is to inform True Food staff, volunteers and members about the use of CCTV at the shop and to provide information about the use of and access to CCTV images .

This document sets out the accepted use and management of CCTV equipment and images to ensure that True Food complies with current data protection legislation. We process personal data in line with our Data Protection Policy and Privacy Notice.

True Food will also follow of the Guiding Principles of the Surveillance Camera Code of Practice as published by the Home Office and updated in 2021. [i]

The lawful basis for gathering and using CCTV footage

CCTV has been installed in our shop to assist in deterring crime, and also the prevention and detection of crime. The system is also intended to assist with the identification, apprehension and prosecution of offenders, and the identification of actions that might result in disciplinary action.

Responsibility for CCTV

The Operations Manager has overall responsibility for the maintenance of the system. He will periodically check the equipment and arrange for the suppliers to carry our periodic maintenance checks.
The Operations Manager will ensure that images are deleted in accordance with the retention policy. Selected members of staff (all permanent members of staff and all casual shop managers) and selected, authorised members will have access to the recorded images during the maintenance of the systems but will under no circumstances routinely view, disclose or retain copies of the recorded images.
Members of staff will be trained in the operation of the CCTV system, and will be aware of the data protection compliance requirements in line with the Code of Practice.

The Committee and Operations Manager are responsible for ensuring that this policy and its implementation is compliant with Data Protection Legislation and will audit the system's use on a periodic basis.
The Operations Manager is responsible for dealing with and responding to any requests for access to images made by CCTV of individuals under the Data Protection Act.
The Operations manager is responsible for viewing images when investigating an incident or suspected incident.
Images may also be accessed by the Operations Manager, if necessary, as part of a disciplinary investigation.

Security measures to protect the CCTV Data

The Operations Manager has responsibility for ensuring that the equipment and the routinely recorded images have the appropriate security. The CCTV equipment is all located within the store, which is securely locked outside of working hours both with locked doors and locked metal shutters. During working hours, there is always a trained member of staff on the premises. Access to the images is securely controlled through a password protected

login screen. The password is regularly changed, and is known only to trained members of staff. It is never shared outside of the trained staff.

Images are routinely retained for 90 days but may be retained longer if they are required as part of an investigation.

The Operations manager has overall responsibility for viewing images when investigating an incident or suspected incident, but can delegate this activity to other, trained, members of staff when required.

[i] https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

Reviewed October 2024