Data Protection Policy

Co-operatives UK Data Protection Policy

Updated July 2019

CO-OPERATIVES UK

www.uk.coop

Co-operatives UK Data Protection Policy

1. Policy Statement

Every day our business will receive, use and store personal information about our members, clients, suppliers, beneficiaries and staff. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process. This policy does not form part of any contracts and may be amended at any time.

As our data protection lead, the Society Secretary is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Society Secretary.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession). Data relating to an organisation is not personal data.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data (referred to in the GDPR as 'special category data') includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, which almost always involve the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that it is:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and any further processing is for a compatible purpose.
- Adequate, relevant and limited to what is necessary for the intended purposes.
- Accurate, and where necessary, kept up to date.
- Kept in a form which permits identification for no longer than necessary for the intended purposes.
- Processed in line with the individual's rights and 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.
- Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

As we have fewer than 250 employees, we will only maintain records of processing activities that are not occasional; could result in a risk to the rights and freedoms of individuals; or involve the processing of sensitive personal data.

Where a new activity is proposed which is likely involve large-scale processing of personal data or the processing of sensitive personal data which may result in a risk to the rights and freedoms of individuals, a data protection impact assessment will be completed before the activity commences.

5. Fair and Lawful Processing

The GDPR and Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose.

The lawful purposes include (amongst others):

- Whether the individual has given their explicit consent by opting into their personal data being used for that specific purpose.
- The processing is necessary for performing a contract with the individual.
- For compliance with a legal obligation.
- Or for the legitimate interest of the organisation.

6. Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in *Schedule 1* of this policy. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in *Schedule 1* or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
- Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
- The third parties, if any, with which we will share or disclose that personal data.
- The fact that the business intends to transfer personal data to a non- European Economic Area (EEA) country or international organisation and the appropriate and suitable safeguards in place.
- How individuals can limit our use and disclosure of their personal data.
- Information about the period that their information will be stored or the criteria used to determine that period.
- Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
- Their right to object to processing and their right to data portability.
- Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
- The right to lodge a complaint with the Information Commissioner's Office.
- Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
- Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and the name of the responsible individual at Co-operatives UK.

8. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Please refer to our Data Retention Policy for a comprehensive guide to the storage, use and deletion of data after the purpose for processing has ended.

11. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Confirmation as to whether or not personal data concerning the individual is being processed.
- Request access to any data held about them by a data controller (see also *Clause 15 Subject Access Requests*).
- Request rectification, erasure or restriction on processing of their personal data.
- Lodge a complaint with a supervisory authority.
- Data portability.
- Object to processing including for direct marketing.
- Not be subject to automated decision making including profiling in certain circumstances.

12. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes, such as auditing. Personal data should therefore be stored on Co-operatives UK's approved data systems and not on individual devices.

13. Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the facilities manager.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Data minimisation.**
- **Pseudonymisation and encryption of data.**
- **Methods of disposal.** Paper documents should be disposed of in confidential waste bins. Digital storage devices should be physically destroyed when they are no longer required.

- **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that devices are password protected when left unattended. All devices should be encrypted and portable devices, such as laptops and tablets, should be securely stored when left unattended.

14. Transferring Personal Data Outside the EEA

We may transfer any personal data we hold to a country outside the EEA or to an international organisation, provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15. Third party contracts

Contracts with third parties should stipulate the role of each party and the limits on the use of the data. The contracts should state which party is the data controller and who is the data processor.

The definitions are broadly:

- A data controller is the organisation who determines how and why the data should be collected and processed.
- A data processor will act on the orders of the controller.

It is possible that a single organisation can be both a data processor and a data controller in relation to different processing activities (it cannot be both a controller and a processor for the same processing activity). The distinction is not always easy to make but the ICO's guidance on 'data controllers and data processors' can help you make it.

16. Subject Access Requests

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to the Society Secretary immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible. It may not always be possible to provide data in hard copy format.

Our employees will refer a request to their line manager or the Society Secretary for assistance in difficult situations.

17. Policy Owner and Review

The current owner of this policy is the Society Secretary who will from time to time review the implementation of the Data Protection Policy in respect of its suitability, adequacy and effectiveness and make improvements where appropriate. The Policy will then be submitted to the Management Team for approval.

SCHEDULE 1: DATA PROCESSING ACTIVITIES

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred
Staff contact and bank details	Staff	Holding contact and bank details Contacting via phone, email and address	Contacting re contracts, payments and organisational information	None
Director contact and bank details	Director	Holding contact and bank details Contacting via phone, email and address	Contacting re role, payments and organisational information	None
Individual contact details of affiliates to member organisations	Member affiliation	Holding contact details Contacting via phone, email and address	Contacting with organisational information and marketing	None
Non-members contact details	Non-members signed up to newsletter	Holding contact details Contacting via phone, email and address	Contacting with organisational information and marketing	None
Suppliers contact details	Suppliers	Holding contact and bank details Contacting via phone, email and address	Contacting re contracts, payments and organisational information	None
Clients contact details	Clients, including tenants	Holding contact details Contacting via phone, email and address	Contacting re contracts, payments and organisational information	None
Beneficiaries contact details	Project beneficiary	Holding contact details Contacting via phone, email and address	Contacting re contracts, payments and organisational information	As specified in any project contracts
Personal Data (society formation)	Founder members	Holding this data Transferring this data to the FCA to form the society	To form corporate entities at the instruction of the client.	The FCA
Personal Data (company formation)	First directors, subscribers and founder members of the corporate bodies we are asked to form.	Holding this data. Transferring this data to a third party (Company Registrations Online) for electronic formation.	To form corporate entities at the instruction of the client.	Company formation agent. Companies House

Personal Data (AML purposes)	First directors, subscribers and founder members of corporate bodies we are asked to form.	Holding this data. Transferring this data to a third party to undertake anti-money laundering checks as per our legal obligations under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, and the Proceeds of Crime Act 2002.	To form corporate entities at the instruction of the client.	Joint Data Controller (Smartsearch) with Co-operatives UK.
Accident book	Individuals who have had an injury or near miss in or around Holyoake House	Record keeping Forwarding to regulator in order to meet statutory obligation	To ensure Health & Safety standards are met	Health & Safety Executive