Co-operative Assistance Network Limited

Data Protection Policy

This policy is issued in accordance with the requirements of the Data Protection Act 1998 and General Data Protection Regulations 2018.

Introduction

Co-operative Assistance Network Limited (CAN) sometimes enters into contracts that require it to keep and process certain information about individuals.

CAN also needs to keep and process information about workers so that they can be recruited and paid, and legal obligations to government complied with.

Terms

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.

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 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, including with the consent of the individual.

Policy

CAN will ensure that all personal data is:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes and any further processing is completed 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.

In accordance with the General Data Protection Requirements, CAN will only process personal data where it is required for a lawful purpose. Lawful purposes include (amongst others):

- If the individual has given their consent
- If the processing is necessary for performing a contract with the individual
- For compliance with a legal obligation
- For the legitimate interest of the business.

In the course of business, CAN may collect and process personal data. If personal data is collected from from an individual, they will be informed about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing
- The types of third parties, if any, with which we will share or disclose that personal data
- How individuals can limit our use and disclosure of their personal data
- The period that their personal data 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 Commissioners Office
- 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.

If CAN receives personal data about an individual from other sources, CAN 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.

CAN will inform data subjects whose personal data is processed:

- That CAN is the responsible Data Controller with regard to that data
- The name and contact details of CAN's Designated Data Protection Officer.

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

CAN will ensure that personal data we hold is accurate and kept up to date.

CAN will check the accuracy of any personal data at the point of collection. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

CAN will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. CAN will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required for the function for which it was collected and permission to hold it obtained and will actively purge obsolete and unwanted data from time to time.

CAN 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
- 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.

CAN 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.

CAN will put in place procedures and technologies to maintain the security of all personal data. Personal data will only be transferred to a data processor that agrees to comply with those procedures and policies, or has put in place similar adequate measures.

CAN 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 by CAN 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.

To maintain a secure data storage environment CAN will:

- Pursue an active strategy to minimise the data held in remote storage or on workers' electronic devices
- Use a professional provider of remote data storage offering the highest level of data security

- Encrypt data held on workers' devices provided by CAN
- Encrypt any back-up storage devices used for workers' devices
- Instruct workers to move data as quickly as is reasonably possible to the higher level of security provided by the remote data storage provider
- Instruct workers to avoid allowing data to move from CAN equipment to personal computers, USB drives etc.

Methods of disposal of redundant data
Digital data is to be deleted and purged.
Paper documents are to be shredded and incinerated.
Digital storage devices are be physically destroyed when they are no longer required.

Control transfer of personal data
CAN will never transfer data into any jurisdiction providing less protection for private data.

Notification of personal data held and processed
All persons whose data are held by CAN are entitled to:

- Know what information CAN holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what CAN is doing to comply with its obligations under the Regulations.

Subject access requests
Individuals must make a formal request for information we hold about them. This must be made by email. Directors who receive a request should forward it to the Designated Data Controller immediately.

CAN will make no charge for the first occasion that access is requested but may make a charge of £10 per each subsequent request at its discretion.

CAN aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Individuals who request the data that we hold about them must verify their own identity before that data can be released. Designated Data Controller will determine if that verification is sufficient proof of identity. If it is not then the data will not be released.

Subject consent
In many cases, CAN can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to CAN processing some specified classes of personal data may be a condition of acceptance of some contracts. Agreement to CAN processing some specified classes of personal data is a

condition of employment for staff, including information about previous criminal convictions.

If fulfilment of contractual obligation requires CAN to ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes:

- CAN will only use that information in the protection of the health and safety of the individual
- CAN will need consent to process that information, in the event of a medical emergency, for example, therefore the individuals concerned will be asked to sign a Consent To Process form regarding that type of information. A refusal to sign such a form can result in denial of service.

Processing sensitive personal data

Sometimes it is necessary to process information about a person's health, criminal convictions, ethnicity, gender and family details. This may be to ensure that CAN is a safe place for everyone, or to operate other CAN policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, workers will be asked to give express consent for CAN to do this. Offers of employment may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Designated Data Controller.

Longer term retention of personal data

CAN will keep some forms of information for longer than others, for example in compliance with the requirements of funding authorities to demonstrate that beneficiaries of a programme have met the required mix of gender, ethnicity etc. When such information is held on behalf of other organisations, CAN will abide by these requirements for the retention of that information where it has been possible to explain the requirement and obtain and record the informed consent of the individuals concerned.

Responsibilities of workers

All CAN workers must:

- Check that any information that they provide to CAN in connection with their employment is accurate and up to date
- Inform CAN of any changes to information that they have provided, e.g. changes of address
- Check the information that CAN may send out from time to time, giving details of information kept and processed about workers
- Inform CAN of any errors or changes. CAN cannot be held responsible for any errors unless the worker has informed CAN of them

- Comply with these guidelines if and when, as part of their responsibilities, workers collect information about other people, (e.g. as part of a service to a customer).

Data security

All workers are responsible for ensuring that:

- All data is uploaded to the CAN file server at the earliest opportunity
- Data held on other devices is minimised
- Any personal data held on laptops and other devices is kept securely
- Hard drives on laptops used by workers are encrypted
- Laptops and devices holding data are backed up to external hard drives at least weekly
- External hard drives and backup devices are locked away when not in use
- Backups older than three years are permanently deleted
- When data is shared between workers or devices it is to be done via the CAN server rather than by USB drives or other external drives or other servers whenever possible
- When USB drives are used data must be copied and not moved onto the drive and then deleted from the drive once the transfer is complete
- USB sticks used by CAN workers must only be used for CAN business – keep work and personal USB sticks separate
- CAN USB sticks must be kept kept clean of files and malware
- Data held on paper must be destroyed after seven years, or ten years if European Funding is involved, unless that data is both useful for CAN's business and still current
- Personal information is not accidentally or otherwise disclosed either orally or in writing to any unauthorised third party.

Workers will understand that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Compliance

Compliance with the Regulations is the responsibility of all CAN workers. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Controller.

Status of this policy

This policy does not form part of the formal contract of employment but it is a condition of employment that employees will abide by the rules and policies made by the CAN from time to time. Any failure to follow this policy can therefore result in disciplinary proceedings.

Any worker who considers that this policy has not been followed in respect of personal data about themselves should raise the matter with the

Designated Data Controller initially. If the matter is not resolved, it should be raised as a formal grievance.

Implementation

A plan for the implementation of this policy will be put into place after the adoption of this policy.

The Data Controller and the Designated Data Controller

CAN as a body corporate is the Data Controller under the Data Protection Act and the Board is therefore ultimately responsible for implementation. However, a Designated Data Controller is appointed for dealing with day-to-day matters and to be the first point of contact for enquirers.

The Designated Data Controller is responsible for ensuring that the Information Commissioners Office is properly notified and paid.

The Designated Data Controller also includes the role of GDPR Co-ordinator.

The Designated Data Controller for CAN is **Chris Funnell**. To contact the Designated Data Controller use the email address chris@assist.coop.

Responsible Department: Society Secretary

Implementation Date: 12 May 2018

Review period: 3 years

Next review due: 12 May 2023

Note: this policy does not need to be passed by Members as it is legally required.

Passed at Directors Meeting of 11 May 2018

Agreed at Members Meeting of 07 December 2018

Revisions agreed at Directors Meeting of 31 December 2018

Revisions agreed at Directors Meeting of 19 August 2019