Data Protection Policy – Cireco

Contents

1. Introduction

Cireco (Scotland) is an arms-length organisation of Fife Council. We were set up to provide services on behalf of the Council such as:

Commercial waste services
Recycling Points
Household Waste Recycling Centres
Skip Hire

To deliver services effectively Cireco (Scotland) needs to collect, process and hold, large volumes of personal information relating to current, past and prospective employees, suppliers, clients, and customers. In addition, it may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies.

2. Policy Statement

Cireco (Scotland) will seek to avoid personal data breaches by having a positive and proactive approach to data collection and management; ensuring we protect the information we collect; ensuring it is used and shared appropriately; actively managing it to ensure it is relevant and up-to-date; is fully compliant with legislation and best practice guidance from the ICO.

Cireco (Scotland) recognises a personal data breach if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned. Where personal data breaches do occur Cireco (Scotland) will, without undue delay, seek to contain the harm to individuals, investigate the breach, report the breach to the Information Commissioner's Office, where appropriate, and look to learn the lessons from any actual or suspected breaches.

3. Scope

This policy is applicable to all personal data held by Cireco (Scotland) whether the information is held or accessed on Council premises or accessed remotely via mobile or home working or by using network access from partner organisations. Personal information held on removable devices and other portable media is also covered by this policy.

Personal data is anything which is capable of identifying a living individual, e.g. name, address, identification number, CCTV image, telephone call recording, e-mail address, location data, postcode, photograph etc. Special category data is information about racial and ethnic origin, political opinions, religious beliefs, physical and mental health, biometric data, sexual life, trade union membership and proceedings.

It applies to all employees, elected members, third party suppliers and any other individuals with access to the Cireco (Scotland)'s information and information systems. This policy also applies to Assessors and Fife Licencing Board, who are separate data controllers in their own right, but associated to Cireco (Scotland) for the purposes of data protection. For Cireco (Scotland) employees, compliance with the policy and associated procedures are a condition of employment. Violations of the policy may result in disciplinary action against an employee.

4. Data Protection Principles

The UK General Data Protection Regulations, together with the UK Data Protection Act 2018, (known as the UK Data Protection Legislation) requires organisations which handle personal data to collect, process and hold personal and confidential information securely and responsibly. This includes maintaining a data processing register of all information held and destroying the information safely when it is no longer required.

The UK Data Protection Legislation sets out six key principles:

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (the individual whose personal data is being used); ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; ('purpose limitation')
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed; ('data minimisation')
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay; ('accuracy')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and

freedoms of the data subject (the individual whose personal data is being used); ('storage limitation') and
- processed 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. ('integrity and confidentiality')

In addition to these principles the law requires organisations to be responsible for, and must be able to demonstrate, compliance with the above principles.

5. Process / Procedure / Guidelines

To ensure compliance with the above data protection principles Cireco (Scotland) will:

- Observe the fair collection and use of personal data.
- Meet its legal obligations to specify the purposes for which data is used.
- Collect and process appropriate data, and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of the data used.
- Apply strict checks to determine the length of time the data is held.
- Take appropriate technical and organisational security measures to safeguard personal data.
- Ensure that personal data is not transferred outside the UK without suitable safeguards.
- Ensure that everyone managing and handling personal data is appropriately trained and supervised; and is fully aware of their data protection responsibilities.
    - Regularly review and audit internal data handling processes and procedures.
- Ensure that rights of people about whom data is held can be fully exercised under the Data Protection Legislation. These include:
    - The right to be informed that processing is being undertaken.
    - The right to prevent processing in certain circumstances.
    - The right to correct, rectify, block, or erase data which is regarded as incorrect.
    - The right of access to one's personal data.
    - The right to withdraw consent.

<u>Subject Access Requests</u>

The UK Data Protection Legislation also allows people to find out what personal information is held by organisations about them by making a Subject Access Request (SAR). A SAR can include both electronic information and paper records. The organisation must provide the information to the individual, or their nominated representative within one month (there are some exceptions to this).

Individuals who wish to make a SAR to Cireco (Scotland) will need to provide evidence of their identity. There is no charge for a SAR made by a data subject to Cireco (Scotland).

The Information Management and Requests Team at Fife Council are responsible for processing and managing Subject Access Requests on behalf of Cireco (Scotland). Employees must not process these requests but should notify the Information Management

and Requests Team upon receipt. The Information Management and Requests Team at Fife Council can be contacted at information.requests@fife.gov.uk

Security Incident & Breach Management

Occasionally Cireco may experience a personal data breach; this could be if personal data is:

- Lost, for example via misplacing documents or equipment that contain personal data, through human error, or via fire, flood, or other damage to premises where data is stored
- Stolen; theft or a result of a targeted attack on our network (cyber-attack)
- Accidently disclosed to an unauthorised individual
- Inappropriately accessed or used

All personal data breach incidents must be reported immediately by e-mail to FRSData.Protection@cirecoscotland.co.uk as the Council has a duty to report any personal data breach to the Information Commissioner's Office (ICO) within 72 hours.

Fife Resource Solutions has a Data Protection team who can provide further advice and guidance in relation to security incidents. They can be contacted at FRSData.Protection@cirecoscotland.co.uk.

Privacy by Design

We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

When introducing any new type of processing, particularly using modern technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out Data Protection Impact Assessment.

All new policies including the processing of personal data will be reviewed by the Service Manager to ensure compliance with the law and establish if a Data Protection Impact Assessment is required.

Advice will be provided by the Service Manager on conducting Data Protection Impact Assessments in line with Cicero's Data Protection Impact Assessment Procedure.

6. Data Sharing

For the planned, regular sharing of personal information between Cireco (Scotland) and other partners or agencies, appropriate information sharing agreement's, protocols and supporting guidance materials must be agreed and in place. Information sharing agreements and other governance elements will be reviewed, amended, and updated on a regular basis, and in accordance with operational requirements.

Appropriate security measures will be used when sharing any personal data.

Data Subjects will be advised of any data sharing in the Privacy Notice.

Data Processors

Where Cireco engage Data Processors to process personal data on our behalf, we will ensure:

- Data processors have appropriate technical security measures in place
- No sub-processors are used without prior written consent from Cireco
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

7. Responsibilities

Cireco Scotland has responsibility for ensuring that the information under their control is collected, processed, and held in accordance with this policy and the requirements of the Data Protection Legislation

All employees, elected members, and any other individuals with access to Cireco Scotland's information must be familiar with the requirements of the Data Protection Legislation and have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with the Cireco Scotland's information policies, procedures, and other guidance.

Chief Executive Officer

The Chief Executive has ultimate responsibility to ensure that all elements of the company's data protection policies are implemented and maintained. The Chief Executive Officer will also:

- Maintain a sufficient level of understanding of data protection within the organisation and ensure the data protection policy is reviewed, amended, and reflects the current undertaking of the business
- Ensure sufficient competent data protection advisory resource is maintained
- Ensure resources and personnel are in position to positively influence and maintain data protection provisions
- Ensure business processes, tenders and future business plans incorporate data protection at the core
- Chair oversight group meetings that include attendance by the DPO, minutes and that the Cireco Scotland's board considers data protection issues reported by the oversight group

Service Manager (with specific responsibility for Data Protection)

The Service Manager has specific responsibility for data protection within Cireco Scotland. The Service Manager will be supported by a Technical Officer in delivery of these responsibilities.

- Establish and maintain sufficient resources (including competent employees, equipment, and workplaces) to maintain safe operating procedures
- Lead by example in matters of data protection compliance
- Measure compliance with the safety management system via regular audit, monitoring and review
- Ensure data protection performance is a regular feature at management meetings

- Ensure all matters of significant non-compliance (whether arising from accident investigation, audit, competent report, or intervention by the Information Commissioner's Office Scotland) are promptly brought to their attention and monitor appropriate corrective actions to completion in good time
- Maintain adequate systems of communication and consultation with employees and employee groups to enable key messages and safety instructions to be promptly delivered and to enable the views, concerns, and opinions of employees about health and safety matters to be brought to the attention of the Senior Management Team
- Ensure competent employees are in position, provide training, instruction, and supervision relevant to their work activities.
- Ensure compliance with all legislative aspects of data protection
- Provide all employees working for Cireco Scotland with the necessary information, instruction, training, and supervision necessary to maintain data protection while discharging their individual responsibilities
- Ensure the above principles and values are embedded at all levels of the Organisation.

Other Service Managers

Service Managers have specific responsibility for personal information within their service. This includes ensuring that:

- Employees only have access to personal information where that access is necessary to enable them to undertake work duties. Employees should discuss with their line manager any instance where access rights require clarification. Access rights must not to be regarded as permanent and are subject to change at any time dependent upon the nature of the duties being fulfilled by an employee.
- Employees should only record information about an individual which is relevant to the purpose or purposes that the information is being collected for, and should be aware that they may be required to justify what has been recorded and be aware that all recorded personal information may be released as part of a Subject Access Request.

Employees

All employees working for Cireco Scotland and those operating on behalf of Cireco Scotland will be expected to cooperate in the implementation of this data protection policy by:

Cooperate with and participate in, so far as is necessary, any activity that will assist the council in complying with any requirements as a result of data protection legislation. This includes the need to participate in data protection training.

- Not to intentionally access personal data they are not required to access or misuse any personal data staff have access to. Any employee who is found to have inappropriately divulged personal information will be subject to investigation under Cicero's disciplinary procedure, which may result in dismissal and possible legal action.
- Report all breaches, incidents and near misses. Cooperate with your employer during investigation proceedings.
- Cooperate with their employer in all matters relating to data protection and highlight short fallings in data protection across the business.

8. Training

Regular Data Protection training is mandatory for all Elected Members and employees of Fife Resource Solutions. Training requirements will be assessed based on work role.

The Service Manager are responsible for ensuring that employees within their Service are trained appropriately.

Fife Resource Solution's Data Protection team will assist Services in evaluating training needs and ensuring adequate resources are provided.

9. Policy Compliance

If any officer is found to have breached this policy, they may be subject to Cireco (Scotland)'s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Service Manager.

10. References

This policy statement is underpinned by supporting policies, procedures, and guidelines. The documents listed below are all available online. The Data Protection and Freedom of Information Subject page is a good starting point.

National Code of Conduct for Councillors
Electronic Mail and Messaging Policy
Employee Code of Conduct
Employee Data Policy
Information Requests Policy
Information Security Policy
Information Security Incident Management Policy
Mobile Electronic Computing Devices & Removable Storage Media
Password Management Policy
Records Management Policy
System Access Policy for Non-Council Employees
Transfer of data out-with the EU
Privacy Impact Assessment Template and Guidance
Data Sharing Guidance