

**The EU General Data Protection Regulation (GDPR) Policy**

Introduction

1. Background

1.1 Key Enviro Solutions Ltd along with the Counter Fraud Authority needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as ‘information which relates to a living individual and from which they can be identified, either directly or indirectly’.

1.2 Personal data at Key Enviro Solutions Ltd Head Office can include employees (present, past and prospective), contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998 and the forthcoming General Data Protection Regulations (GDPR).

1.4 The DPA requires Key Enviro Solutions Ltd to comply with the eight Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly.

1.6 The lawful and correct treatment of person-identifiable information by Key Enviro Solutions Ltd is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help Key Enviro Solutions Ltd ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection Act and GDPR principles

1.7 Key Enviro Solutions Ltd has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security.

1.8 All legislation relevant to an individual’s right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to Key Enviro Solutions Ltd. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

1.9 The aim of this policy is to outline how Key Enviro Solutions Ltd meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the Data Protection Act 1998 and the forthcoming GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B.

2. What information is covered?

2.1 Personal data within the respective legislative and regulatory provisions covers ‘any data that can be used to identify a living individual either directly or indirectly’. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3. Policy statement

3.1 This document defines the data protection policy for Key Enviro Solutions Ltd. It applies to all person-identifiable information obtained and processed by the organisation and its employees.

It sets out:

* The organisation’s policy for the protection of all person-identifiable information that is processed
* Establishes the responsibilities (and best practice) for data protection
* References the key principles of the Data Protection Act 1998 and GDPR.

4. Principles

4.1 The objective of this policy is to ensure the protection of Key Enviro Solutions Ltd information in accordance with relevant legislation, namely:

To ensure notification;

Annually notify the Information Commissioner about the Key Enviro Solutions Ltd use of person-identifiable information.

To ensure professionalism;

All information is obtained, held and processed in a professional manner in accordance with the eight principles of the Data Protection Act 1998 and the provisions of the GDPR.

To preserve security;

All information is obtained, held, disclosed and disposed of in a secure manner.

To ensure awareness;

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

Data Subject access;

Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by the Key Enviro Solutions Ltd Leadership Team. Where review and update is necessary due to legislative changes this will be done immediately.

4.3 In accordance with the Key Enviro Solutions Ltd equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5. Scope of this policy

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.

5.2 The procedures cover all person identifiable information whether clinical or non-clinical, electronic or paper which may relate to, employees, contractors and third parties about whom we hold information.

6. Policy

6.1 Key Enviro Solutions Ltd obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

* Staff records and administrative records
* matters relating to the prevention, detection and investigation of fraud and corruption in the wider facilities service
* Complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data Key Enviro Solutions Ltd will comply with the data protection principles within the Data Protection Act 1998.

7. Data protection responsibilities

Overall responsibilities

7.1 Key Enviro Solutions Ltd Board members, collectively known as the ‘data controller’ permit the organisation’s staff to use computers and relevant filing systems (manual records) in connection with their duties. Key Enviro Solutions Ltd Board members have legal responsibility for the notification process and compliance of the Data Protection Act 1998.

7.2 Key Enviro Solutions Ltd Board members whilst retaining their legal responsibilities have delegated data protection compliance to the Data Protection Officer.

7.3 The Data Protection Officer’s responsibilities have been allocated to the organisation’s Information Governance and Risk Management Lead.

Data Protection Officer’s (DPO) responsibilities

7.4 The Data Protection Officer’s responsibilities include:

* Ensuring that the policy is produced and kept up to date
* Ensuring that the appropriate practice and procedures are adopted and followed by Key Enviro Solutions Ltd
* Provide advice and support to the Board on data protection issues within the organisation
* Work collaboratively with Organisational Development and Governance and Assurance to help set the standard of data protection training for staff.
* Ensure data protection notification with the Information Commissioner’s Office is reviewed, maintained and renewed annually for all use of person-identifiable information.
* Ensure compliance with individual rights, including subject access requests.
* Act as a central point of contact on data protection issues within the organisation.
* Implement an effective framework for the management of data protection.

Line managers’ responsibilities

7.5 All line managers across the organisation’s business units are directly responsible for:

* Ensuring their staff are made aware of this policy and any notices.
* Ensuring their staff are aware of their data protection responsibilities.
* Ensuring their staff receive suitable data protection training.

General responsibilities

7.6 All Key Enviro Solutions Ltd employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.7 All Key Enviro Solutions Ltd employees have a responsibility to inform their business unit Leads and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.8 All Key Enviro Solutions Ltd employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Information Governance Officer.

7.9 Employees must follow the subject access request procedure (see Appendix C below).

8. Monitoring

8.1 Compliance with this policy will be monitored by the Finance and Corporate Governance team, together with internal audit reviews where necessary.

8.2 The Information Governance and Risk Management Lead is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

9. Validity of this policy

9.1 This policy will be reviewed at least annually under the authority of Key Enviro Solutions Ltd Board members. Associated data protection standards will be subject to an ongoing development and review programme.

Appendix A - Data Protection Act 1998 - Data protection principles

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B – Summary of relevant legislation and guidance

General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. ‘Controllers’ and ‘Processors’ will be required to document decisions and maintain records of processing activities.

Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts and Primary Care Groups to respect and protect an individual’s human rights. This will include an individual’s right to privacy (under Article 8) and a service user’s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. However, this article also states “there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

Each organisation must act in a way consistent with these requirements. It must take an individual’s rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the “Interception of Communications Act 1985”. The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person-identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Key Enviro Solutions Ltd issues each employee with an individual user id and password which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Key Enviro Solutions Ltd will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

Information Security Management: Key Enviro Solutions Ltd Code of Practice

The guidelines provide a framework for consistent and effective information security management that is both risk and standards-based and is fully integrated with other Key Enviro Solutions Ltd Information Governance areas. Without effective security, Key Enviro Solutions Ltd information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties.

Confidentiality: Key Enviro Solutions Ltd Code of Practice

Gives bodies’ guidance concerning the required practice for those who work within or under contract to Key Enviro Solutions Ltd concerning confidentiality and employees’ consent to the use of their personal data.

The Caldicott Guardian Manual 2017

Provides guidelines relating to sharing of person-identifiable information and advocates the appointment of senior organisational members to the role, to ensure adherence to the principles.

Records Management: Key Enviro Solutions Ltd Code of Practice

The code acts as a guide to the required standards of practice in the management of records for those who work within or under contract to Key Enviro Solutions Ltd organisation in England. It is based on current legal requirements and professional best practice.

Information Commissioner’s Guidance - Use and Disclosure of Health Data

This guidance is concerned with the application of the Act with regards to the processing of information contained within ‘health records.

Approval

This statement has been approved by the KES board of directors who will review and update it annually.

****

Paul Openibo

Director

 Date: 1st January 2021