Data Protection Policy

Contents

1. Introduction

Envirovent Limited hold personal data about employees, clients, suppliers & other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data & ensure that employees understand the rules governing the use of personal data to which they have access in the course of their work. This policy requires employees to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	Business purposes include: ➢ *Compliance with legal, regulatory & corporate governance obligations & good practice* ➢ *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* ➢ *Ensuring policies are adhered to (such as policies covering email & internet use)* ➢ *Operational reasons, such as recording transactions, training & quality control, confidentiality of commercially sensitive information, security vetting, credit scoring & checking* ➢ *Investigating complaints* ➢ *Checking references, ensuring safe working practices, monitoring & managing employees access to systems & facilities & employees absences, administration & assessments* ➢ *Monitoring employees conduct, disciplinary matters* ➢ *Marketing our business* ➢ *Improving services*
Personal data	Information relating to individuals, such as job applicants, current & former employees, clients, suppliers & marketing contacts ➢ *Data may include: individuals' contact details, educational background, financial & pay details, details of certificates & diplomas, education & skills, marital status, nationality, job title, & CV*
Sensitive personal data	➢ *Sensitive date refers to an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data will be strictly controlled in accordance with the GDPR*

2. Scope

This policy applies to all employees, who must be familiar with the contents & comply with its terms. This policy supplements our other policies relating to internet & email use. We may supplement or amend this policy by additional policies & guidelines from time to time.

3. Who is responsible for this policy?

Our DPO has overall responsibility for the day-to-day implementation of this policy.

4. Procedures

Fair & lawful processing

We must process personal data fairly & lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing have consented to this happening, unless there is a contractual obligation.

The DPO's responsibilities

- Keeping the board updated about data protection responsibilities, risks & issues
- Reviewing all data protection procedures & policies
- Arranging data protection training & advice for all employees
- Responding to individuals who wish to know what data is being held by EnviroVent

Responsibilities of the IT Department

- Ensure all systems, services, software & equipment meet acceptable security standards
- Checking & scanning security hardware & software regularly to ensure it is functioning properly
- Researching third-party services & systems that the company is considering using to store or process data

Responsibilities of the Marketing Department

- Approving data protection statements attached to emails & other marketing material
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests & not unduly prejudice the individual's privacy

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health & safety at work).

Accuracy & relevance

We will ensure that any personal data we process is accurate, adequate, relevant & not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals may ask that we correct inaccurate personal data relating to them.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate & updated as required.

Storing data securely

- Where data is stored on paper, it should be kept in a secure place such a locked cabinet / draw
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by passwords that are changed regularly
- Data stored on external storage devices must be locked away securely when not in use
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- Servers containing sensitive data will be approved & protected by security software & strong firewall.

Data retention
We will retain personal data for no longer than is necessary. This will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Subject access requests
Individuals are entitled to request access to information held about them. There are restrictions on the information to which they are entitled under applicable law. Any such requests should be made to the HR department in the first instance.

Processing data in accordance with the individual's rights
We will abide by any request from an individual not to use their personal data for direct marketing purposes & notify the DPO about any such request. We will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

Training
All employees will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy & procedure.

Training is provided through an in-house seminar & regular refresher training.
It will cover:

- The law relating to data protection
- Our data protection & related policies & procedures.

Reporting breaches
All employees have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure & take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioners Office of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring
Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply
We take compliance with this policy seriously. Failure to comply puts both you & the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Andy Makin

Managing Director
Date 01.11.24