Data Protection Policy

Context and Overview

Key Details

Introduction

Payment Kiosks Limited gathers and holds information on behalf of itself and its clients. Information gathered by Payment Kiosks' customers in order for them to offer a service to their clients can include Traders, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This Policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and comply with the law.

Why This Policy Exists

This data protection policy ensures Payment Kiosks Limited:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risk of a data breach

Data Protection Law

The Data Protection Act 1998 and 2018 describes how organisations including Payment Kiosks Ltd, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that the personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific lawful purposes
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than is necessary

6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

We comply with new Information Rights within DPA2018/GDPR.

People, Risks and Responsibilities Policy Scope

This policy applies to:

- The head office of Payment Kiosks Limited
- All branches of Payment Kiosks Limited
- All staff and volunteers of Payment Kiosks Limited
- All contractors, suppliers and other people working on behalf of Payment Kiosks Limited

It applies to all data the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 / 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Data Protection Risks

This policy helps to protect Payment Kiosks Limited from some very real data security risks, including:

- Breaches of Confidentiality. For Instance, information being given out Inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company use data relating to them.
- Reputational Damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for, or with Payment Kiosks Limited has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed inline with this policy and

data protection principles.

However, these people have key areas of responsibility:

- The board of Directors is ultimately responsible for ensuring that Payment Kiosks meets its legal obligation.
- The data protection officer, Tom Quarry, is responsible for:

    1. Keeping the board updated about data protection responsibilities, risks and issues
    2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    3. Arranging data protection training and advice for the people covered by this policy.
    4. Handling data protection questions from staff and anyone else covered by this policy.
    5. Dealing with requests from individuals to see the data Payment Kiosks Limited holds about them (also called Subject Access Requests).
    6. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Technical Manager, Richard Somerset, is responsible for:

    1. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    2. Performing regular checks and scans to ensure security hardware and software is functioning properly.
    3. Evaluating any third-party service's the company is considering using to store or process data. For instance, cloud computing services.

- The Marketing Manager, Tom Quarry, is responsible for:

    1. Approving any data protection statements attached to communication such as e mails and letters.
    2. Addressing any data protection queries from journalists or media outlets like newspaper or social media.
    3. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line

manager/ Director.

- Payment Kiosks Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date, if no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager/ Director or data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Technical Manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required the paper or files should be stored in a locked filing cabinet or drawer.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer or desk.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, (CD, DVD's memory sticks etc.), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup

procedure.
- Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by approves security software and a firewall

Data Use

Personal data is of no value to Payment Kiosks Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure that the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by e mail, as this form of communication is not secure.
- Data must be encrypted before being sent electronically. The Technical Manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires Payment Kiosks Limited to take reasonable steps to ensure data is kept accurate and up to date.

The more important the personal data is, the greater the effort Payment Kiosks Limited should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as is necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Payment Kiosks will make it easy for data subjects to update the information Payment Kiosks Limited holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing managers responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject Access Requests

All individuals who are the subject of data held by Payment Kiosks Limited are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by e mail, addressed to the data controller at enquiries@paymentkiosks.co.uk The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances Payment Kiosks Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and the company's legal advisors where necessary.

Providing Information

Payment Kiosks Limited aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends the company has a privacy statement, setting out how data relating to individuals is used by the company.