DATA PROTECTION POLICY

v1.1

Table of Content

1. Introduction

1.1.1. We need to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

1.1.2. This policy describes how data (including personal identifiable data) must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

1.2. Policy aim

1.2.1. This data protection policy ensures that 5th Street Ltd.:

1.2.1.1. Complies with data protection law and follow good practice

1.2.1.2. Protects the rights of team members, customers and partners

1.2.1.3. Is open about how it stores and processes individual's data

1.2.1.4. Protects itself from the risks of a data breach

2. Data Protection Law

2.1. The Data Protection Act 2018 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether the data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

2.2. The UK General Data Protection Regulation is underpinned by six important principles which say that personal data must be;

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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 the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures

3. People, risks and responsibilities

3.1. Policy Scope

3.1.1. The policy applies to;

3.1.1.1. Remote Workers (Home Based).

3.1.1.2. All team members and volunteers of 5th Street Ltd..

3.1.1.3. All contractors, suppliers and other people working on behalf of 5th Street Ltd..

3.1.2. It applies to all data that the company holds relating to identifiable individuals.

3.2. Data protection risks

3.2.1. This policy helps to protect 5th Street Ltd. from data security risks, including;

3.2.1.1. **Breaches of confidentiality -** information being given out inappropriately.

3.2.1.2. **Failing to offer choice -** all individuals should be free to choose how the company uses data relating to them.

3.2.1.3. **Reputational damage -** the company would suffer if hackers gain access to sensitive data.

3.3. Responsibilities

3.3.1. Everyone who works for or with 5th Street Ltd. has some responsibility for ensuring data is collected, stored and handled appropriately. Everything mentioned within this policy applies to freelancers and teleworkers.

3.3.2. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

3.3.3. Miguel Pardo-Marin is responsible for;

3.3.3.1. Keeping the board updated about data protection responsibilities, risk and issues.

3.3.3.2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.

3.3.3.3. Arranging data protection training and advice for the people covered by this policy.

3.3.3.4. Handling data protection questions from team members and anyone else covered by this policy.

3.3.3.5. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

3.3.3.6. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

3.3.3.7. Performing regular checks and scans to ensure security hardware and software is functioning properly.

3.3.3.8. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

3.3.3.9. Approving any data protection statements attached to communications such as emails and letters.

3.3.3.10. Addressing any data protection queries from journalists or media outlets like newspapers.

3.3.3.11. Where necessary, working with other team members to ensure marketing initiatives abide by the data protection principles.

3.3.4. Miguel Pardo-Marin is responsible for;

3.3.4.1. Dealing with requests from individuals to see the data 5th Street Ltd. holds about them (also called "subject access requests").

3.3.4.2. Informing and communicating with the Information Commissioner's Office (ICO) where necessary.

4. Policy statement

4.1. General Guidelines

4.1.1. Access to data should be restricted to those who need it for their work.

4.1.2. Data should not be shared informally.

4.1.3. When access to CONFIDENTIAL or RESTRICTED data is required, team members can request it from Miguel Pardo-Marin.

4.1.4. 5th Street Ltd. will provide training to all employees to help them understand their responsibilities when handling data.

4.1.5. Keep all data secure, by taking sensible precautions and following the guidelines below.

4.1.6. All software the company provides or recommends is correctly licenced. This applies to software that has access to company or customer data.

4.1.7. Bitwarden is being considered as a password manager.

4.1.8. Passwords should never be shared between users to maintain an audit trail.

4.1.9. Personal data should not be disclosed to unauthorised people, either within the company or externally.

4.1.10. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it must be securely deleted or disposed of.

5. Data storage

5.1. These rules describe how and where data should be safely stored.

5.2. Data should only be stored on paper when essential or for legal purposes. It should be standard practise to only store data electronically (digital data).

5.3. Data printouts should be shredded or disposed of securely when no longer required.

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

5.5. Data must be protected by strong passwords that are changed regularly and never shared between team members.

5.6. If data is stored on removable media (like a CD or DVD), its storage must be authorised by Miguel Pardo-Marin and all personnel use only approved storage media. These media must be kept locked securely when not in use and protected by a strong password and encryption when at rest.

5.7. Data should only be stored on designated drivers and servers, and should only be uploaded to approved cloud computing services.

5.8. Servers containing personal data should be sited in a secure location, away from general office space..

5.9. All sensitive data such as customer data and personal identifiable information must be **encrypted-at-rest** using AES-256 or similar.

5.10. All sensitive data must be **encrypted-in-transit** during handling using TLS, SFTP, SSH or similar.

5.11. All team members devices should use **full disk encryption**.

5.12. Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard for backup procedures.

5.13. Data should **never be saved directly to laptops or other mobile devices** like tablets or smartphones **unless you have** the full suite of security protection installed and configured.

5.14. All servers and computers containing data should be protected by **approved security software and a firewall**.

6. Data use

6.1. Personal data is of no value to 5th Street Ltd. 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.

6.2. When working with personal data, employees should **ensure the screens of their computers are always locked** when left unattended.

6.3. Personal data **must not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.

6.4. Personal data should **never be transferred outside of the European Economic Area; however,** data may be processed by a service provider based in countries outside of the EEA. Such countries do not always provide the same level of data protection as the UK; however, where such transfers of data occur, contracts are put in place that include security obligations on 5th Street Ltd. service providers to ensure that personal data is protected under UK standards.

6.5. Team members should **not save copies of personal data to their computers**. Always access and update the central copy of any data.

7. Data accuracy

7.1. The law requires 5th Street Ltd. to take reasonable steps to ensure data is kept accurate and up to date.

7.2. The more important it is that the personal data is accurate, the greater the effort 5th Street Ltd. should put into ensuring its accuracy.

7.3. 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.

7.4. Data will be **held in as few places necessary**. Team members should not create any unnecessary additional data sets.

7.5. Team members **should take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.

7.6. 5th Street Ltd. will make it **easy for data subjects to update the information** 5th Street Ltd. holds about them. For instance, via the company page on our platform.

7.7. 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.

8. Subject access requests

8.1. All individuals who are the subject of personal data held by 5th Street Ltd. are entitled to;

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

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

8.3. Subject access requests from individuals should be made by email addressed to the data controller. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within the time permitted by the regulations.

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

9. Disclosing data for other reasons

9.1. In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. 5th Street Ltd. is also required to disclose personal data to enforce 5th Street Ltd.'s EULA or to protect the property, rights or safety of 5th Street Ltd., users of 5th Street Ltd.'s services or others. In such a case, information may be exchanged with third-party companies or organisations to prevent fraud or reduce credit risk.

9.2. Under these circumstances, 5th Street Ltd. will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

10. Disclosing data to third parties

10.1. Disclosure of personal data (including, without limitation, Client Data) to third parties will only occur if:

- 5th Street Ltd. sells or purchases any business or assets. In such a case, 5th Street Ltd. may authorise the disclosure of personal data to prospective sellers or buyers of such business or assets.
- All or the substantial majority of 5th Street Ltd. is sold to a third party. In such a case, personal data may be one of the transferred assets.

11. Further Information

11.1. Further information and advice on this policy can be obtained Miguel Pardo-Marin.

11.2. Comments and suggestions to improve security are always welcome.