Fusion Hive
North Shore Road
Stockton-on-Tees
TS18 2NB

GDPR Policy

1 Context and Overview

Key Details:

Policy prepared by:

Approved by board management on:

Policy Operational Date:

Next review:

Introduction

The firm needs to gather and use certain information about individuals.

Individuals can include customers, suppliers, business contacts, employees and other people the firm 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 firm's data protection standards — and to comply with the law.

Please take a moment to read the 'Privacy Policy' we provide to our customers and our enquiries from the footer of any of our websites.

Why this policy exists

This data protection policy ensures that we:

Comply with data protection law and follow good practice;
Protect the rights of staff, customers and partners;
Are open about how we store and process individuals' personal data;
Protect the firm from the risks of a data breach

Data protection law

The General Data Protection Regulation describes how we 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 General Data Protection Regulation is underpinned by six important principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner;
2. Be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Be accurate and, where necessary, kept up to date;
5. Be kept for no longer than is necessary for the purposes for which the personal data is processed; and
6. Be processed in a way that ensures appropriate security of the personal data.

2 People, risks and responsibilities

This policy applies to:

Head office
All branches
All staff and volunteers
All contractors, suppliers and other people working on behalf the firm

It applies to any information which we hold relating to an individual from which an individual can, directly or indirectly, be identified. This can include:

Names of individuals
Postal addresses
Email addresses
Telephone numbers
Training records

Data protection risks

This policy helps to protect the firm from some very real data protection risks, including:

Breaches of confidentiality. For example, information being given out inappropriately.
Excess information collection. For, example collecting more personal information than is necessary for the firm to provide the service.
Failing to offer choice. For example, all individuals should be free to choose how the company uses data relating to them.
Out of date. For example, storing out of date and inaccurate information.
Data retention. For example, keeping personal information indefinitely when no longer in use.
Reputational damage. For example, the firm could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who handles personal information within the firm 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 in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

The **Board of Directors** (Adam Bragg, John Farlam and Graham Lucas) is ultimately responsible for ensuring that the firm meets its legal obligations.

The **Compliance Officer** (Adam Bragg) is responsible for:
Processes:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the firm holds about them (also called ‘subject access requests’).

- Dealing with requests from individuals who want to exercise their rights under GDPR (e.g. request erasure of their personal information)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Carrying out data protection risk assessments
- Carrying out internal data protection audits

IT

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure that security hardware and software is functioning properly.
- Evaluating any third-party services the firm is using to store or process data. For instance, cloud computing services.
- Evaluating any third-party services and companies the firm is using to store or process data. For instance, IT services, trainers and consultants.

Marketing

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by the data protection principles.

3 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 managers.

The firm 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.

In particular, **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 or the Compliance Officer if they are unsure about any aspect of data protection.

4 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or the Compliance Officer.

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 kept **in a locked drawer or filing cabinet**.

Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

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** (like a CD or DVD), 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 services**.
- 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 procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

5 Data use

Personal data is of no value to the firm unless it 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 **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **only be transferred outside of the European Economic Area** if the receiving firm has adequate data security measures.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

6 Data accuracy

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

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

- Data will be held in **as few places as 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.
- The firm will make it **easy for data subjects to update the information** it holds about them. For instance, via the firm's website.
- Data should be **updated immediately inaccuracies are discovered**. For example, if a customer can no longer be reached on his stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression registers** every six months.

7 Individuals' rights

All individuals who are the subject of personal data held by the firm are entitled to:

1. Obtain confirmation about **what information** we hold about them and to **access copies** of that information.
2. Request the **correction** of inaccurate personal information.
3. Request the **erasure** of their personal information.
4. **Restrict** how their personal information is used.
5. Receive their personal information in a **legible** and **transferable** format. For example, in an Excel format.
6. **Stop** the use of their personal data.
7. **Object** to their personal information being used for an automatic decision.
8. **Be informed** about why their personal information is being collected and how it will be used.

The firm must make it easy for individuals to exercise their rights in relation to their personal information. Where an individual makes any of the above requests we must comply within one month.

The firm cannot charge a fee to an individual for exercising his rights unless the request from the individual is excessive. For example, because it is a repetitive request that has previously been complied with.

Any charge should be limited to the administrative cost of complying with the request.

The Compliance Officer will always verify the identity of anyone making a request to exercise his individual rights before actioning the request.

8 Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the individual.

Under these circumstances, the firm will disclose the requested data. However, the Compliance Officer will ensure the request is legitimate, seeking assistance from the board and from the firm's legal advisers where necessary.

9 Providing information

The firm aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- Who their data is being shared with
- How long their data will be stored
- How to exercise their rights
- How to lodge a complaint with the Information Commissioner's Office

To comply with the above, the firm has a privacy statement, which sets out how data relating to individuals is used by the firm.

This is available on request. A version of this is also available on our website.

10 Declaration

I agree I have read and understood the GDPR Policy above and agree to abide by the principals:

Name: :……..

Signed:……..

Date:……..

Positon: ……..