DATA

PROTECTION

POLICY

15th January 2018

ISM OP14

Version 1.0

CONTENTS

1. Introduction

Shift F7 needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the company 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 to comply with the law.

2. Why this Policy exists

This data protection policy ensures Shift F7:

- Complies with data protection law and follows 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 risks of data breach

3. Data Protection Law

The Data protection Act 1998 describes how organisations – including Shift F7, must collect, handle and store personal information.

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

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 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 up to date
5. Not be held for any longer than 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 unless that country or territory ensures an adequate level of protection

4. People, Risks and responsibilities

4.1 Policy scope

This policy applies to:

- The head office of Shift F7 based at Dorking.

- Any branches of Shift F7 (if applicable)
- All staff of Shift F7
- All contractors, suppliers and other people working on behalf of Shift F7

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

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ….plus any other information relating to individuals

4.2 Data Protection risks

This policy helps to protect Shift F7 from 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 uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

4.3 Responsibilities

Everyone who works for or with Shift F7 has some responsibility for ensuring data is collected, stored and handled appropriately.

Anyone who handles personal data must ensure that it is handled and processed in line 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 Shift F7 meets its legal obligations.
- The Data Protection Officer is responsible for:
    - 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.
    - Arrange data protection training and advice for the people covered by the policy.
    - Handle data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Shift F7 holds about them (also called “subject access requests”)
    - Checking and approving any contracts or arrangements with third parties that may handle the company’s sensitive data.

- The Information Security Manager is responsible for:
    - Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third party services the company is considering using to store or process data. For instance, cloud computing services.

- The Managing Director is responsible for:
    - 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 data protection principles.

5. 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**. Where access to confidential information is required, employees can request it from their immediate line manager.
- **Shift F7 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 not required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

6. Data storage

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

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. (NB. Shift F7 as part of their ISO27001 accreditation have implemented a Clear Desk Policy)

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, these should be kept locked away securely when not being used.
- Data should only be stored on designated devices 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 the general office space.
- Data should be backed up frequently. These 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.

7. Data use

Personal data is of no value to Shift F7 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 their computer screens are always locked when left unattended.
- Personal data should not be shared informally, in particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Information Security 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.

8 Data accuracy

The law requires Shift F7 to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort Shift F7 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 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.
- Shift F7 will make it easy for data subjects to update the information Shift F7 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 Managing Director's responsibility to ensure any marketing databases are checked against industry suppression files every six months.

9 Subject access request

All individuals who are the subject of personal data held by Shift F7 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 email, addressed to the data protection manager. The data protection manager can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £20 per subject access request. The data protection manager will aim to provide the relevant data within 14 days.

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

10 Disclosing data for other reasons

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

Under these circumstances, Shift F7 will disclose requested data. However, the data protection manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisors where necessary.

11 Providing information

Shift F7 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.

References:

Documentation relation to Policies, Procedures for the company's ISO27001:2013 accreditations.