Introduction

Martyn Weeks Consultancy trading as FRS hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. This policy sets out how the Company seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their work.

Definitions

Business Purposes

The purposes for which personal data may be used by Martyn Weeks Consultancy: Personnel, administrative, financial, regulatory, payroll and business development purposes.

Personal Data

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other employees, clients, suppliers and marketing contacts.

Personal data Martyn Weeks Consultancy gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Sensitive Personal Data

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all employees. They must be familiar with this policy and comply with its terms. This policy supplements the Company's other policies relating to data protection. Martyn Weeks Consultancy may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to employees before being adopted.

Our procedures

Fair and lawful processing

Martyn Weeks Consultancy must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that the Company should not process personal data unless the individual whose details are being processed have consented to this happening.

Responsibilities of the Director:

- Keeping relevant employees updated about data protection responsibilities, risks and issues

- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all employees and those included in this policy
- Answering questions on data protection from employees, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them
- Checking and approving with third parties that handle the Company's data any contracts or agreement regarding data processing
- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets

The processing of all data must be:

- Necessary to deliver Company services
- In the legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Martyn Weeks Consultancy Terms of Business contains a Privacy Notice on data protection. The notice:

- Sets out the purposes for which the Company hold personal data on customers and employees
- Highlights that the work may require Martyn Weeks Consultancy to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that is held about them

Sensitive personal data

In most cases where the Company process sensitive personal data it will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or Martyn Weeks Consultancy are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

Martyn Weeks Consultancy will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. The Company 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 inaccurate personal data relating to them is corrected. If employees believe that information is inaccurate or if their personal circumstances change, they should inform Martyn Weeks so they can update records.

Data security

Employees must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on Martyn Weeks Consultancy's behalf, the Director will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The Director must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- 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
- Approval must be sought from the Director before any large data downloads occur.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

Martyn Weeks Consultancy must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. Employees must not transfer personal data anywhere outside the UK without first consulting the Director.

Processing data in accordance with the individual's rights

Employees should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Director about any such request. Do not send direct marketing material to someone electronically unless there is an existing business relationship with them in relation to the services being marketed. Please contact the Manager for advice on direct marketing before starting any new direct marketing activity.

Conditions for processing
Martyn Weeks Consultancy will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All employees who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Consent
The data that Martyn Weeks Consultancy collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data Requests
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Training
All employees will receive training on this policy. New starters will receive training as part of their induction process. Further training will be provided periodically or whenever there is a substantial change in the law or our policy and procedure.

Data audit and register
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

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

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

- For a serious breach the ICO must be notified within 72 hours of the Company becoming aware
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Martyn Weeks Consultancy must also inform those individuals without undue delay.

Monitoring

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

Consequences of failing to comply

Martyn Weeks Consultancy take compliance with this policy very seriously. Failure to comply puts both employees and the organisation at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the Company procedures which may result in dismissal.

If employees have any questions or concerns about anything in this policy, do not hesitate to contact the Director.