MCFT Data Protection Policy

Version 1.2
28th May 2019

Contents of this Policy

Data Protection Statement 2

1. GDPR Compliance 3
1.1 Key details 3
1.2 Introduction 3
1.3 Why this policy exists 3
1.4 GDPR 4
2. People, risks and responsibilities 5
2.1 Policy scope 5
2.2 Data protection risks 5
2.3 Responsibilities 5
2.4 General staff guidelines 6
3. Data storage 7
4. Data use 8
5. Data accuracy 8
6. Subject access requests 9
7. Disclosing data for other reasons 9
8. Providing information 9

Bibliography 10
Appendices 10
Appendix I – Data Access Request Form 10

Data Protection Statement

Doing business is not what it used to be twenty years ago. With the introduction of advanced computing technologies, businesses around the world can reach markets and provide customer service on a global level, as never seen before. Performing business in this manner however, comes with a great dependency on sensitive data. May it be customer contact information, job applicant's address information, or a members of staff's national insurance number.

MCFT recognises the importance of the protection of its clients', employees', and business partners' data. MCFT is - and has always been - committed to protecting the data our business is dependent upon.

In light with the recent regulatory changes (The General Data Protection Regulation) MCFT has created this extensive Data Protection Policy.

This policy describes efforts MCFT is taking to protect and secure its most sensitive data. Furthermore, the present policy dictates which internal stakeholders are responsible for the protection of the applicable data in question. The policy moreover covers in what ways the organization will seek consent from data owners in order to lawfully use those data, within the scopes mentioned in the before mentioned document. Lastly, the policy informs external parties with a contact procedure, should any party have concerns in relation to the protection of their data.

MCFT's intention is to provide full transparency and accountability for the protection of sensitive data. We trust that the compliance with our internal data protection policy would address any concerns to GDPR compliance and to any concerns one might have in relation to the protection of their data.

Terence Horsman
Business Improvement Manager and Data Protection Officer
on behalf of McFarlane Telfer ltd.
28th May 2019
Maidenhead, Berkshire
United Kingdom

1. GDPR Compliance

1.1 Key details

Prepared for McFarlane Telfer ltd. (hereinafter referred to as MCFT) located at B5, McFarlane Telfer Ltd, Westacott Business Centre, Maidenhead SL6 3RT, UK

Policy prepared by:	Terence Horsman & Gerryt Coen Annema
Policy prepared on:	29th May 2019
Approved by management on:	29th May 2019
Policy became operational on:	29th May 2019
Next review date:	29th May 2020

This data protection policy is governed by English law. Any disputes over this privacy policy shall be brought to a court in the United Kingdom.

1.2 Introduction

To operate as a business, MCFT needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

Information gathering is necessary to continuously ensure client needs are fulfilled and provide immediate response to service or remedial requests. Other forms of data gathering include applicant & employees consisting of job requirement screening, person specifications and written records of interviews.

MCFT's policy describes how this personal data is collected, handled and stored to meet the company's data protection standards — and to comply with the law.

1.3 Why this policy exists

This data protection policy ensures MCFT:

- 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 individuals' data
- Protects itself from the risks of a data breach
- Explains in what way it acts in case of a data breach.

1.4 GDPR

The General Data Protection Regulation henceforth referred to as GDPR, adopted in 2016, describes how organisations including MCFT— must collect, handle and store personal information, applying regardless whether 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.

ICO, 2017 states that the General Data Protection Regulation is underpinned by six important principles. These say that personal data must:

a) Be lawfully, fairly, and in a transparent manner.

b) Be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) Data processed is adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

d) 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.

e) Kept in a form which permits identification of data subject for no longer than is necessary for the purposes which the personal data are processed.

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using the appropriate technical or organisational measures.

1.5 Legal Definitions

In this chapter some of the legal vocabulary which is used in the rest of this report will be explained. These are set out in Article 6(1) of the GDPR as clarified by DPA 18.

Consent – Where explicit consent is given by the data subject to store and use his/her personal details for specified legitimate reasons
Contract – Where the processing of personal data is necessary to fulfil the terms of a contractual obligation or as part of entering in to a contract
Legal Obligation – Where processing personal data is necessary for compliance with common law or statutory obligation
Vital Interest – Where processing or disclosure of personal data is necessary to protect life.
Public Interest – Where processing is necessary to perform a specific task in the public interest that is set out in law
Legitimate Interest – Where processing is necessary for the purpose of a legitimate interest.

2. People, risks and responsibilities

2.1 Policy scope

This policy applies to:

- The head office of MCFT
- All branches of MCFT within the European Union or EEA
- All staff, applicants and volunteers of MCFT
- All contractors, suppliers and other people working on behalf of MCFT

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the *General Data Protection Regulation*. This can include:

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

2.2 Data protection risks

MCFT is committed to a policy that makes the greatest effort to protect individual's information. However, in case of a data breach event, MCFT ensures it immediately reports to the Information Commissioner's Office (ICO) within 24 hours (at least within 72 hours).

- **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.

2.3 Responsibilities

Everyone who works for or with MCFT 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, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that MCFT meets its legal obligations.
- The **Data Protection Officer, Terence Horsman** 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.
    - 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 MCFT holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Business Improvement Manager, Terence Horsman** ***(****Ad interim position is fulfilled by Colin Platt)* is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet 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, Mark Brooker and CEO, Chris Craggs** are 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.

2.4 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.
- **MCFT 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,** which need to be changed at least once every 90 days 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 data protection officer if they are unsure about any aspect of data protection.

3. Data storage

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

When data is **stored on paper,** it is 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 is kept **in a locked drawer or filing cabinet**.
- Employees make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts are 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 as follows:

- Data is **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 is kept locked away securely when not being used.
- Data is only stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data are **sited in a secure location**, away from general office space.
- Data is **backed up frequently**. Those backups are tested regularly, in line with the company's standard backup procedures.
- Data is **never saved directly** to laptops or other mobile devices like tablets or smart phones, unless these data are part of a MCFT corporate application and are secured under a Virtual Private Network.
- All servers and computers containing data are protected by **approved security software and a firewall**.

4. Data use

Personal data is of no value to MCFT 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 ensure **the screens of their computers are always locked** when left unattended.
- Personal data **is not shared informally**. It is never sent by email, as this form of communication is not secure.
- Data is **encrypted before being transferred electronically**. The Business Development Manager can explain how to send data to authorised external contacts.
- Personal data is **never transferred outside of the European Economic Area,** unless the data owners have given implied, verbal or written consent.
- Employees **do not save copies of personal data to their own computers.** Always access and update the central copy of any data.

5. Data accuracy

The law requires MCFT 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 reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data is held in **as few places as necessary**. Staff do not create any unnecessary additional data sets.
- Staff **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- MCFT makes it **easy for data subjects to update the information MCFT** holds about them. For instance, via the company website or customer portal.
- Data is **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it is flagged as inaccurate data on the database.

6. Subject access requests

All individuals who are the subject of personal data held by MCFT 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 controller, Terence Horsman at Terence.Horsman@MCFT.com. The data controller has supplied a standard request form, which can be found in Appendix I – Data Access Request Form.

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.

7. 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, MCFT 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.

8. Providing information

MCFT 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.

This is available on request. A version of this statement is also available on the company's website.

Bibliography

ICO. (2017, February 28). *Guide to the General Data Protection Regulation (GDPR)*. Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

ICO. (2017, February 28). *Guide to the General Data Protection Regulation (GDPR)*. Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Appendices

The appendices to this report can be found in this chapter.

Appendix I – Data Access Request Form

This form is to be used for any subject access requests from MCFT by any interested party. MCFT aims to respond to the request in question within 14 working days.

Name	
Company (as stated on any by MCFT provided documentation, such as quotations, invoices, etc.)	
Telephone Number	
Email Address	
Request	
Signature	

Please enclose a lawful proof of identification with this request form. Due to privacy concerns, the data controller will disregard any requests filed without valid proof of identification.

Please send this completed document in PDF to Terence Horsman, at Terence.Horsman@MCFT.com. Any requests sent through other channels will be disregarded.