MCSA Data Privacy Policy

Mark Hodge

Direct: 01628 810 977

Email: Mark.Hodge@mcsa.co.uk

Maindec House, Holtspur Lane
Wooburn Green, Bucks, HP10 0AB

Document Control

Revision Information					
Revision	2.0	Replaces	1.0	Effective From	18/04/18
Revision Details	1.0 Initial Draft 2.0 First set of amendments				
Authors	Role		Contact Email		Contact Phone
Mark Hodge			Mark.Hodge@mcsa.co.uk		01628 810977

Table of Contents

Data privacy policy

Definitions

Data Protection Laws	means any law, statute, subordinate legislation regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body which relates to the protection of individuals with regard to the processing of Personal Data to which a Party is subject including the Data Protection Act 1998 or Data Protection Act 2017 (as applicable) and the GDPR.
GDPR	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal Data	Has the meaning in Data Protection Laws

1 Introduction

1.1 **The MCSA Group** needs to gather and use certain information about individuals in the course of its business. This information can include customers, suppliers, business contacts, employees and other people the organisation 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

2.1 This data protection policy ensures **The MCSA Group and its employees**:

2.1.1 Complies with **Data Protection Law** and follow good practice
2.1.2 Protects the rights of staff, customers and partners
2.1.3 Is open about how it stores and processes individuals' data
2.1.4 Protects itself from the risks of a data breach

3 Data protection law

3.1 The **Data Protection Laws** describe how organisations including **The MCSA Group** 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 **Data Protection Laws** are underpinned by eight important principles. These say that personal data must:

3.1.1 Be processed fairly and lawfully
3.1.2 Be obtained only for specific, lawful purposes
3.1.3 Be adequate, relevant and not excessive
3.1.4 Be accurate and kept up to date
3.1.5 Not be held for any longer than necessary
3.1.6 Processed in accordance with the rights of data subjects
3.1.7 Be protected in appropriate ways
3.1.8 Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

4 Policy scope

4.1 This policy applies to:

4.1.1 The head office of The MCSA Group
4.1.2 All branches of The MCSA Group
4.1.3 All staff and volunteers of The MCSA Group
4.1.4 All contractors, suppliers and other people working on behalf of The MCSA Group

4.2 It applies to all data that the company holds relating to identifiable individuals.This can include:

4.2.1 Names of individuals
4.2.2 Postal addresses
4.2.3 Email addresses
4.2.4 Telephone numbers
4.2.5 …plus any other information relating to individuals

5 Data protection risks

This policy helps to protect **The MCSA Group** from some very real 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.

6 Responsibilities

Everyone who works for or with **The MCSA Group** 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 **The MCSA Group** meets its legal obligations.
- The **Technical Director,** 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 **The MCSA Group** 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 **IT Manager,** 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 **Director of Marketing Manager,** 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.
    - Ensuring that any data purchased is from a responsible supplier and that they have permission to use the customer information for marketing purposes.
    - Regularly review processes to ensure customer contact preferences are updated on MCSA's CRM database.

7 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 MCSA Group 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 data protection officer if they are unsure about any aspect of data protection.

8 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 data controller.

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.
- All Company laptops are encrypted with BitLocker. Data should **never be saved directly** to tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

9 Data use

An individual's personal data is of no intrinsic value to **The MCSA Group** unless or until the data is used in the course of its business. 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**. In particular, Special Personal Data should never be sent by email, as this form of communication is not secure.
- Special Personal Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area** without appropriate contractual safeguards in place.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

10 Data accuracy

The law requires **The MCSA Group** 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 **The MCSA Group** 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.
- **The MCSA Group** will make it **easy for data subjects to update the information The MCSA Group** holds about them.
- 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 marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

11 Subject access requests

All individuals who are the subject of personal data held by **The MCSA Group** 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 post or email, addressed to the data controller at privacy@mcsa.co.uk. 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 30 days.

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

12 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, **The MCSA Group** 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.

13 Providing information

The MCSA Group 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 data privacy statements, setting out how data relating to employees, clients, suppliers and prospective customers is used by the company.