DATA PROTECTION POLICY

Version 0.0

25th April 2018

VERSION HISTORY

Version	Author	Revision Date	Approved By	Approval Date	Comments
0.0	Stephen Grant	25/04/2018			Initial Draft

Table of Contents

1. Introduction 4

1.1 Why This Policy Exists 4

1.2 Data Protection Law 4

1.2.1 Background to the General Data Protection Regulation (GDPR) 4

1.2.2 Definitions Used (Drawn from GDPR) 4

1.2.3 Article 4 Definitions 4

2. Roles and Responsibilities 6

2.1 Who and What Does This Policy Apply To? 6

2.2 Data Protection Risks 6

2.3 Roles and Responsibilities 6

3. Data Storage 8

4. Data Use 9

5. Data Accuracy 10

6. Subject Access Requests 11

7. Disclosing Data for Other Reasons 12

8. Providing Information 13

9. Changes to this Data Protection Policy 14

9.1 Updates 14

10. Contacting Us 15

1. Introduction

Mouse Click Systems Ltd. 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.

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.

1.1 Why This Policy Exists

This data protection policy ensures Mouse Click Systems Ltd.:

- Complies with data protection law and follow 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

1.2 Data Protection Law

1.2.1 Background to the General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2.2 Definitions Used (Drawn from GDPR)

Material Scope (Article 2) – The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial Scope (Article 3) – The GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

1.2.3 Article 4 Definitions

Establishment – The main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside of the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal Data – Any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in

particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning healthy or data concerning a natural person's sex life or sexual orientation.

Data Controller – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Subject – A living individual who is the subject of personal data held by an organisation.

Processing – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – Is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data Breach – A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data Subject Consent – Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third Party – A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing System – Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Roles and Responsibilities

2.1 Who and What Does This Policy Apply To?

This applies to all those handling data on behalf of Mouse Click Systems Ltd. e.g.:

- All locations of Mouse Click Systems Ltd.
- All employees and volunteers
- All contractors, third party suppliers and other people working on behalf of Mouse Click Systems.

It applies to all data that Mouse Click Systems Ltd. holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Any other personal information held (e.g. financial)

2.2 Data Protection Risks

This policy helps to protect Mouse Click Systems Ltd. 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.

2.3 Roles and Responsibilities

Mouse Click Systems Ltd. is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for Mouse Click Systems Ltd. is **Stephen Grant**.

- The **director** is ultimately responsible for ensuring that Mouse Click Systems Ltd. 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.
    - 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 Mouse Click Systems Ltd. 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.
    - Any questions relating to the collection or use of data should be directed to the Data Protection Officer.
- 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 that the company is considering using to store or process data. For instance, cloud computing services.
- The **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.

Everyone who has access to data as part of Mouse Click Systems Ltd. has a responsibility to ensure that data is collected, stored and handled appropriately.

- 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.
- Mouse Click Systems Ltd. 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.

3. 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 (such as 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.

4. Data Use

Personal data is of no value to [company name] 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 the screens of their computers 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 IT 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.

5. Data Accuracy

The law requires Mouse Click Systems Ltd. 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 Mouse Click Systems Ltd. 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.
- Mouse Click Systems Ltd. will make it easy for data subjects to update the information Mouse Click Systems Ltd. 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 marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

6. Subject Access Requests

All individuals who are the subject of personal data held by Mouse Click Systems Ltd. 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 at datacontroller@mouseclicksystems.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. 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, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Mouse Click Systems Ltd. will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the director and from the company's legal advisers where necessary.

8. Providing Information

Mouse Click Systems Ltd. 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 policy, 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.

9. Changes to this Data Protection Policy

We reserve the right to make changes to this Data Protection Policy at any time. Any changes will be posted in this Data Protection Policy and material changes will be prominently notified on the respective website or application this Data Protection Policy applies to or will be otherwise communicated to you prior to the change becoming effective. We encourage you to regularly review this Data Protection Policy to make sure you are aware of any changes and how your information may be used.

9.1 Updates

This Data Protection Policy was last updated on **25th April 2018**

10. Contacting Us

If you any questions or comments about this Data Protection Policy, please contact us:

Mouse Click Systems Ltd
Brunel House
340 Firecrest Court
Centre Park
Warrington
Cheshire
WA1 1RG

Email: dataprotection@mouseclicksystems.co.uk

Website: http://www.mouseclicksystems.co.uk/contact-us

You can contact the Information Commissioners Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

Website: https://ico.org.uk/global/contact-us/email/