Data Protection Policy

1. Context and Overview

1.1 Introduction

MT Cold Storage Solutions **(MTCSS)** 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 MTCSS's data protection standards – and to comply with the law.

1.1.1 Why this policy exists

This Data Protection Policy ensures MTCSS:

• 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

1.2 Data Protection Law

The General Data Protection Regulations and related Data Protection legislation describe how organisations – including MTCSS – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper and on other materials.

To comply with law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection legislation is underpinned by eight important principles which state that personal data must:

1. Be processed fairly and lawfully
2. Be obtained for only specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept 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 (EEA), unless than country or territory also ensures an adequate level of protection

2. People, Risks and Responsibilities

2.1 Policy Scope

This Policy applies to:

• The head office of MTCSS

• All hubs, branches, departments and teams of MTCSS

• All staff of MTCSS

• All contractors, suppliers and other people working on behalf of MTCSS

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

• Names of individuals

• Postal addresses

• Email addresses

• Telephone numbers

• … plus any other information relating to individuals

2.2 Data Protection Risks

This Policy helps to protect MTCSS 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 MTCSS uses data relating to them

• Reputational damage; for instance, MTCSS could suffer if hackers successfully gained access to sensitive data

2.3 Responsibilities

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

Each hub, branch, department or 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 at MTCSS is ultimately responsible for ensuring that MTCSS meets its legal obligations

• The Office Manager is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies
- 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 MTCSS holds about them (also called ‘subject access requests’)
- Checking and approving any contracts or agreements with third parties that may handle the MTCSS sensitive data

- Addressing any data protection queries from journalists or media outlets like newspapers

• The Office Manager is responsible for:

- Ensuring all IT 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 any third-party services MTCSS 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
- Where necessary, working with other staff to ensure marketing communications such as emails and letters

3. 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

• **MTCSS will provide training** to all relevant 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 MTCSS 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 Office Manager, if they are unsure about any aspect of data protection.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Office Manager or your line manager.

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,** for example on a printer or hot desk

• **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 removal media** (like a CD, DVD, memory stick or tape), 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 service**

• 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 MTCSS standard back up procedures

• Data should **never be saved directly** to laptops or other mobile devices such as tablets or smart phones

• All servers and computers containing data should be protected by **approved security software and a fire wall**

5. Data Use

Personal data is of no value to MTCSS unless the business can make use of it ie. the business must have a reason for obtaining and keeping 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 looked** 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**

• Personal data should **never be transferred outside of 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

Notwithstanding the above, personal data may be processed to comply with a law e.g. relating to a customs entry or clearance and to perform an agreed contract or service for a customer.

6. Data Accuracy

The law requires MTCSS 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 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

• MTCSS will make it easy for **data subjects to update the information** it 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 Managers responsibility to ensure **marketing databases are checked regularly against suppression files**

7. Subject Access Request

All individuals who are the subject of personal data held by MTCSS are entitled to:

• Ask **what information** MTCSS holds about them and why

• Ask **how to gain access** to it

• Be informed **how to keep it up to date**

• Be informed how MTCSS is **meeting its data protection obligations**

If an individual contacts MTCSS requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Head of Legal and Company Secretary or Group HR Advisor of MTCSS at sales@mtcss.co.uk

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

8. Disclosing Data for Other Reasons

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

Under these circumstances, MTCSS will disclose requested data. However, MTCSS will ensure the request is legitimate, seeking assistance from board the board and from MTCSS legal advisers where necessary.

9. Providing Information

MTCSS 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, MTCSS has Privacy Notices, setting out how data relating to individuals is used by MTCSS.

10. Related MTCSS Policy Documentation

• Privacy Notices, related to

- Recruitment
- Employees
- Website Users
- Customers

• IT Policy

• Records Management Policy