

# Data Protection Policy

MT GROUP part of Manx Telecom Trading Limited (MT GROUP) and its subsidiary companies is committed to gathering and using information about individuals, including customers, contacts, employees, and other stakeholders, in compliance with data protection laws and industry best practices. This policy outlines the procedures for collecting, handling, and storing personal data to ensure compliance with the General Data Protection Regulation (GDPR) and ISO27001-2022 standards.

This Data Protection Policy ensures that MT GROUP:

- Complies with GDPR and follows industry best practices and any key legislation.
- Protects the rights of customers, employees, business partners, and suppliers.
- Maintains transparency in how personal data is stored and processed.
- Mitigates risks associated with data breaches and has clear processes and controls.
- Whilst maintain a key DPO (Data Protection Office/Officer) function with Exec level reporting.
- Complies with Regulation (EU) 2016/679 where applicable.

This policy applies to all personal data processing activities conducted by MT GROUP, where MT GROUP acts as the data controller. It includes processing carried out by joint controllers, contractors, and processors and or whereas MT GROUP act as a data processor.

## Principles of Data Protection (UK & IOM GDPR)

In accordance with GDPR (Article 5 UK GDPR) & GDPR and LED Implementing Regulations (Section 6 Isle of Man), MT GROUP adheres to the following seven principles of data protection:

- i. Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and in a transparent manner.
- ii. Purpose Limitation: Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- iii. Data Minimisation: Data shall be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
- iv. Accuracy: Data shall be accurate and, where necessary, kept up to date. Inaccurate data shall be erased or rectified without delay.
- v. Storage Limitation: Data shall be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- vi. Integrity and Confidentiality (Security): Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

- vii. **Accountability:** MT GROUP shall be able to demonstrate compliance with the above principles and ensure that individuals are not put at risk due to the processing of their personal data.

## 1. Data Classification

In accordance with ISO27001-2022, MT GROUP implements a robust data classification scheme to ensure the appropriate handling and protection of information assets. Data classification is essential for identifying and categorising data based on its sensitivity, value, and criticality. This process meets regulatory requirements but also enhances data security, operational efficiency, and risk management.

Consistent data classification enables us to safeguard sensitive information from unauthorised access, ensure compliance with legal and regulatory standards, and optimise data management practices, ultimately reducing the risk of data breaches and improving overall organisational resilience.

1.1 Data is classified into the following categories:

- i. **Public:** Data that is available for anyone outside the organisation to view for example:
  - Press releases
  - Publicly available reports
  - Marketing materials
  - Company website content
- ii. **Internal-Only:** Default classification for all data for example:
  - Internal memos, E-Mail
  - Employee handbooks
  - Internal project plans
  - Documents, emails, database entries that do not contain any confidential or restricted data
- iii. **Confidential:** Data that requires higher protection due to its sensitive nature for example:
  - Financial records
  - Customer data (not protected under GDPR)
  - Business Partners
  - Sensitive Data
  - CCTV
  - Any system configuration information which could compromise security
  - Contracts and agreements
  - Employee performance reviews
- iv. **Restricted:** Highly sensitive information that requires strict access controls. Unauthorised disclosure could cause significant harm to the organisation or individuals.
  - Passwords or Secret keys which exposed would compromise security

- Trade secrets
- Confidential
- Escrow
- Intellectual property
- Strategic plans
- Personal data under GDPR (Refer to Appendix A)

## **2. Data Handling Controls**

MT GROUP enforces stringent data handling controls to ensure the integrity, confidentiality, and availability of information assets. These controls encompass a range of measures designed to protect data throughout its lifecycle, from creation to disposal. Implementing consistent data handling controls is crucial for mitigating risks, ensuring compliance with legal and regulatory requirements, and maintaining operational efficiency.

By adhering to these controls, MT GROUP can safeguard sensitive information from unauthorised access, prevent data breaches, and enhance overall data security, thereby fostering trust and resilience within our organisation

The following controls detailed in section 2.1 must be adhered to:

### **2.1 Creation and Storage**

- 2.1.1 All data should be classified upon creation.
- 2.1.2 All employees must be educated on where and how data is to be securely stored
- 2.1.3 All employees must store data in approved locations as detailed in Appendix B. Storage of data in non-approved locations is not permitted unless the proper approval is granted to do so.
- 2.1.4 All data by default is classified as 'Internal-only' unless denoted otherwise
- 2.1.5 Data classified as Public, Confidential, or Restricted should be denoted as such through any available method such as:
  - I. Adding the classification in the file name.
  - II. Use of watermarks, labels or other descriptive means
  - III. Storing the data within a folder that denotes its classification.
  - IV. Applying system, file or folder permissions that restrict access to authorised named individuals.
- 2.1.6 All users accessing data must be able to clearly identify its classification as Confidential, Restricted, or Public.
- 2.1.7 Internal-Only data must be stored in secure locations (refer to Appendix B) accessible only to authorised users.

- 2.1.8 Unstructured (file data) Confidential and Restricted data should be stored in encrypted formats.
- 2.1.9 Structured (Data within applications and databases) Confidential and Restricted data should be secured in accordance with the Data Retention Policy and Data Retention Standard where applicable.
- 2.1.10 Confidential and Restricted data held within test systems must adhere to the Data Protection policy.

## **2.2 Access Controls**

MT GROUP implements comprehensive access controls to ensure the security and integrity of information assets. Access controls are vital for regulating who can view or use resources within our systems, based on their roles and responsibilities. These controls include both physical and digital measures, ensuring that only authorised personnel have access to sensitive information.

Consistent implementation of access controls helps mitigate risks, prevent unauthorised access, and ensure compliance with legal and regulatory requirements. By maintaining robust access controls, we enhance data security, operational efficiency, and overall organisational resilience

The following controls detailed in section 3.1 must be adhered to:

## **2.3 File and Folder Permissions**

- 2.3.1 Users must apply appropriate file and folder permissions to prevent unauthorised access.
- 2.3.2 Internal-Only data must be accessible only to authorised personnel.
- 2.3.3 Confidential and Restricted data must have restricted access, with permissions granted only to those with a legitimate need.
- 2.3.4 Public data must be accessible to the public and clearly labelled as such.

## **3. Data Sharing Measures**

MT GROUP implements rigorous data sharing measures to ensure the secure and efficient exchange of information. These measures are designed to facilitate collaboration while safeguarding the integrity, confidentiality, and availability of shared data. Consistent data sharing practices help mitigate risks, ensure compliance with legal and regulatory requirements, and enhance operational efficiency.

By adhering to these measures, we can foster innovation, improve decision-making, and reduce duplicate efforts, ultimately strengthening our organisational resilience and trust among stakeholders

The following controls detailed in section 4.1 & 4.2 must be adhered to:

### **3.1 Internal Sharing (Definition to the added)**

- 3.1.1 Sender must validate the recipient's identity before sharing Confidential or Restricted data.
- 3.1.2 Sender must ensure that access to shared data is limited to authorised personnel.

### **3.2 External Sharing (Definition to the added)**

- 3.2.1 External sharing of data must comply with GDPR regulations
- 3.2.2 Sender must validate the recipient's identity and ensure they have the necessary permissions to send the data.
- 3.2.3 Sender should use secure methods for sharing data, such as encrypted emails or secure file transfer protocols.
- 3.2.4 Sender must use secure methods for sharing confidential or restricted data, such as encrypted emails or secure file transfer protocols.
- 3.2.5 Public data can be shared openly but must be verified for accuracy before sharing.
- 3.2.6 Permission to externally share any data that is classified as confidential or restricted must be obtained from a company director
- 3.2.7 Permission to externally share internal-only data must be obtained from a head of department.

## **4. Revocation of Unauthorised Access**

MT GROUP enforces stringent measures for the timely revocation of unauthorised access to information assets. This process is crucial for maintaining the integrity, confidentiality, and availability of sensitive data. Revoking access rights promptly when they are no longer required helps mitigate risks, prevent data breaches, and ensure compliance with legal and regulatory requirements.

Consistent implementation of access revocation procedures enhances data security, reduces the likelihood of insider threats, and fosters trust among stakeholders

The following controls detailed in section 5.1 & 5.2 must be adhered to:

### **4.1 Unauthorised Internal Users**

- 4.1.1 If data is inadvertently shared with internal users who do not have authorisation to access it, immediate action must be taken to revoke access. This can be achieved by modifying permissions or removing the data from the view of unauthorised users.
- 4.1.2 If the data is classified as Confidential or Restricted, the Data Protection Officer (DPO) must be notified immediately.

## **4.2 Unauthorised External Users**

- 4.2.1 If data is inadvertently shared with external users who do not have authorisation to access it, immediate action must be taken to revoke access.
- 4.2.2 If access cannot be immediately revoked or retrieved, or if the unauthorised recipient has accessed the data before revocation, the Data Protection Officer (DPO) must be notified immediately.

## **5. Data Deletion**

MT GROUP enforces data deletion protocols to ensure the secure and compliant removal of information that is no longer required. Effective data deletion is crucial for mitigating risks associated with data breaches, maintaining compliance with legal and regulatory requirements, and optimising storage efficiency.

By consistently implementing data deletion measures, we can protect sensitive information from unauthorised access, reduce storage costs, and enhance overall operational efficiency.

Such measures are defined in our Data Retention Policy, Data Retention Standard and our Privacy Policy.

The following controls detailed in section 6.1 must be adhered to:

### **5.1 Data Retention & Deletion**

- 5.1.1 Data retention and data destruction must adhere to the Data Retention Policy or the Data Retention Standard.
- 5.1.2 Data must be deleted securely using methods that prevent recovery.
- 5.1.3 Public and Internal-Only data can be deleted using standard procedures.
- 5.1.4 Confidential and Restricted data must be deleted with verification that additional copies such as previous versions, copies for backups etc are also deleted.

## **6. Compliance and Monitoring**

MT GROUP implements rigorous compliance and monitoring measures to ensure adherence to information security standards and regulatory requirements. These measures involve continuous assessment and auditing of our data protection practices to identify and address any compliance gaps or weaknesses.

Consistent compliance and monitoring are essential for mitigating risks, preventing data breaches, and demonstrating our commitment to data protection and accountability.

By maintaining robust compliance and monitoring processes, we enhance stakeholder trust, ensure legal and regulatory compliance, and improve overall organisational resilience

The following controls detailed in section 7.1 & 7.2 must be adhered to:

### **6.1 GDPR Compliance**

- 6.1.1 All data handling practices must comply with GDPR regulations.

- 6.1.2 Data Protection Officer owner must regularly review and update the policy to reflect changes in legislation

## **6.2 Monitoring and Auditing**

- 6.2.1 Data Protection Officer must conduct regular audits to ensure compliance with policy
- 6.2.2 Data Protection Officer must monitor data access and handling practices to identify and address any breaches or non-compliance.
- 6.2.3 Data Protection Officer must log the transfer of confidential and restricted data externally to identify and address any breaches or non-compliance
- 6.2.4 Business Services & Security Operations Teams must put apply measures to enable the monitoring and logging of confidential and restricted data when transferred externally.

## **7. Roles and Responsibilities**

MT GROUP clearly defines and assigns roles and responsibilities to ensure effective management and accountability for information security. This structure is essential for protecting information assets, managing security processes, and addressing information security risks.

Clearly defined roles and responsibilities help mitigate risks, ensure compliance with legal and regulatory requirements, and enhance operational efficiency.

By establishing a well-defined framework, we can foster a culture of security awareness, improve coordination among teams, and strengthen our overall organisational resilience

### **7.1 Data Protection Office/Officer (DPO)**

- Oversee the implementation and compliance of this policy.
- Conduct regular training and awareness programmes for employees.
- Report any losses or suspected breaches of personal data to the information commissioner within 72 hours of becoming aware of the breach (Data Breach)
- Manage any DSAR activity (Data Subject Access Request)
- Determine if any breach of personal data would result in a high risk to the rights and freedoms of individuals. If such a risk is identified, instruct the business to notify the affected individuals in accordance with legal requirements.

### **7.2 MT GROUP Employees**

- Complete data protection training within the specified timeframes as directed by the Data Protection Officer (DPO).
- Escalate any questions to the DPO when the data protection policy does not cover a current scenario, such as difficulties in classifying a data type.

- Adhere to the data protection policy and promptly report any breaches or concerns to the DPO.

## **8. Registration with Information Commissioner**

MT Group has an obligation as a Data Controller to notify the Information Commissioner Office (ICO) of the purposes for which it processes personal data.

Individual data subjects can obtain full details of MT Group's data protection notification from:

- MT Group's the Data Protection Officer (DPO)  
[dataprotection@manxtelecom.com](mailto:dataprotection@manxtelecom.com)
- Information Commissioner Office – Isle of Man  
[ask@inforights.im](mailto:ask@inforights.im) or [www.inforights.im](http://www.inforights.im)
- Information Commissioners Office – UK
- [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk) or [www.ico.org.uk](http://www.ico.org.uk)

MT Group are currently registered for the following:

- Staff Administration
- Advertising, Marketing & Public relations
- Accounts & Records
- Information & Databank Administration
- Research
- Security
- Pensions Administration
- Any applicable and authorised use case

## **9. Registration Numbers**

- MT Group – ICO IOM – R000812
- Synapse 360 – ICO IOM – R001810
- Synapse 360 – ICO UK – ZB552397
- SmartRoam – ICO UK – ZB552389

### **9.0 Privacy Policy**

Our privacy policy is located at:

<https://www.manxtelecom.com/terms-and-conditions/privacy-policy/>

## 10.0 Right to Erasure

This right is also sometimes known as the “right to be forgotten” and affords the data subject the right, under certain conditions, to have the data that MT Group hold about them permanently deleted. Where the right applies, all requests must be actioned within one month.

There are some defined circumstances when the right to erasure applies:

- When the data subject withdraws their consent to MT Group processing their data,
- When the purpose by which MT Group are processing the personal data no longer exists and MT Group no longer need the data,
- When MT Group receive an objection to our processing of the data subjects’ personal data and we cannot provide a legitimate reason for continuing to do so,
- Where MT Group need to comply with a legal obligation,
- Where MT Group’s processing was not done in accordance with the law.

If the circumstances fall outside of these then we do not have to erase the data subjects’ data. If MT Group are unable to delete the personal data, we must inform the data subject of the valid reason why, for example if a piece of legislation mandates us to keep a certain record for a period of time. We must also inform the data subject of the date at which time we will be able to do so.

If the information has been shared, by MT Group, with any third parties we must also make sure that they delete the information and that they complete this within one month of the request.

## 11.0 Right of Access (DSAR)

All data subjects have the right to request access to any information that MT Group holds on them. By having this access, a data subject is able to determine whether the data that is being processed about them is being done so in a fair and lawful manner, and whether there is any data being processed about them that they have not been made aware of.

Under the obligations of the legislation MT Group will not be able to charge an administration fee and once a request has been received it should be actioned and completed within a month. In order to ensure that MT Group are providing the information requested only to the data subject, we may elect to contact them prior to release in order to obtain evidence of their identity. We may also wish to contact the data subject in order to determine if there is a specific piece of information that they require. If we do need to contact the data subject this will not affect the time that we have to respond.

An individual who wishes to exercise his/her right of access is required to contact the DPO function at [DataProtection@manxtelecom.com](mailto:DataProtection@manxtelecom.com) and or if via an internal method, through a supported SNOW ticket raised via:

## **12.0 Right to Rectification**

Where a data subject believes that any of the data held about them by MT Group is incorrect, they have the right to have this rectified. This also relates to any other information that they have obtained from MT Group through their right to access.

If the information that needs to be rectified has been shared by MT Group with any third parties (processors), we must also ensure that the required changes are also reflected in the data that they hold within one month of the request.

## **13.0 Right to Restrict Processing**

If some of the conditions identified in section above exist and the data subject indicates that they do not wish for their data to be erased, they can request from MT Group, the restriction of processing of their data. In effect, this means that we must cease processing their data until such time that processing is once more permitted, or they decide that their data can now be deleted.

The law allows that:

- If a data subject contests the accuracy of some of the data that MT Group holds about them, we can attempt to verify the accuracy of what we have. Until such time that we have been able to do this, the data subject can request that we cease the processing of this data.
- If MT Group's processing of the data is found to be unlawful and the data subject does not wish for their data to be deleted, they can ask that we cease any further processing of the data until such time that they wish it to be erased.
- If MT Group no longer need the data, but the data subject wishes it to be retained, they can ask us to do so.

If the data subjects' personal data has been shared by MT Group, with any third parties we must also make sure that they restrict the processing of the personal data in accordance with the instruction and that they complete this as soon as is practicable.

## **14.0 Right to Data Portability**

Under the legislative requirements data subjects have the right to acquire their data from MT Group in a commonly used machine-readable format that allows them to re-use their data for their own purposes.

This right applies when:

- personal data is processed by automated means,
- personal data has been provided by the data subject to MT Group,
- where the processing is based on the data subjects' consent or for the completion of a contract with the data subject.

## **15.0 Right to Object**

The law provides data subjects with the right to object to certain processing activities. They have the right to object to certain activities such as direct marketing, profiling or when MT Group are processing their data using legitimate interests as our legal basis for processing. Each of these categories are detailed below and provides information about the application of each one.

### **15.1 Legitimate Interests**

Legitimate interests is one of a number of processing conditions however it is the one that provides the most ambiguity. Within our Privacy Notice on our website MT Group will detail a number of examples and reasons for the processing of personal data. If the reason we have provided for the processing of a data subjects personal data is legitimate interests, we will have to provide them the right to object to this processing. If they wish to invoke this, they must inform us in writing. In such circumstances, for MT Group to continue processing their data, we would have to provide them with compelling evidence of our legitimate interests. If we are unable to do so, we are no longer legally allowed to undertake this processing, and should the data subject wish, delete any data that was collected because of, or, in order to complete this processing.

### **15.2 Profiling**

Where systems undertake profiling about an individual or attempt to provide information to a data subject based on their usage of a system, product etc they are afforded the right to object to such processing.

The ICO defines profiling as any form of automated processing of personal data consisting of using data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that natural person's:

- performance at work
- economic situation
- health
- personal preferences
- interests
- reliability
- behaviour

- location or movements

Where an individual objects to this processing we must make sure that the processing of the personal data in this manner is ceased within one month of their request.

This can include automated individual decision-making profiling whereby the data subject shall not be subject based solely on automated processing, including profiling whereby automated.

### **15.3 Direct Marketing**

In order for MT Group to be able to send marketing communications to a data subject they must provide their consent for us to do so. Where this consent is through an online system and the data subject is selecting a box regarding their preferences the box is not pre-selected, and the default position must be of the individual not receiving communications meaning that they have to positively opt-in to receiving them.

At any time, a data subject has the right to withdraw this request (i.e. objecting to receiving marketing communications) and we must provide them with the ability to do this. The easiest way for us to this is to:

- Provide an unsubscribe facility within the marketing email which, opens a webpage in order to allow the data subject to request no further marketing contact from MT Group; or
- Allow the data subject to reply to the email communication requesting no further marketing contact; or
- Allow the data subject to contact our sales and marketing departments, or our Data Protection Officer requesting no further marketing; or
- Provide the data subject with the ability to amend their preferences from within the system in which they previously provided them.

After any of these have occurred, MT Group must not directly contact the data subject again in this regard unless they provide a subsequent request to start receiving them again.

It is worth noting that system update messages, notifications about changes to terms and conditions etc. are not considered marketing materials (providing that they do not also contain marketing within them) and do not apply to this right.

### **15.4 Rights in relation to automated decision making and profiling**

The law provides data subjects with rights in relation to decisions that are made by a computer and not by a person, allowing them to object to those decisions and request that they are made by a person. These rights however do not apply in the following circumstances:

- when the data subject is providing their consent to such decisions being made; or
- when the law requires such decisions to be made; or
- when such decisions are necessary for the performance of a contract

## 16.0 Notifications Regarding Breaches

When acting either as a data controller or data processor, from the moment MT Group becomes aware of a breach of data protection legislation, it has 72 hours to report this to the relevant Information Commissioner.

This notification must include:

- Information about the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects; and
- The name and contact details of the data protection officer, or other contact point where more information can be obtained;

If the breach is sufficiently serious that it needs to be communicated to the public, we must do so without undue delay.

The Information Commissioner can be contacted through the following means:

**See section: 8**

## 17.0 Processing of Sensitive Information

Sometimes it may be necessary to process information about a person's criminal convictions, race, gender, health and family details. This is required in order to operate some of MT Group's HR policies, such as the equal opportunities policy. We may also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma, diabetes or any disabilities. Unless we have the express consent of the data subject, we will only be able to use such information in the protection of the health and safety of the individual concerned. In the event of a medical situation where such information would be important for saving an individual's life, we will not need their consent to pass this information on to life saving professionals. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, we will need to ask individuals to give their express consent for MT Group to process this data.

In many cases, MT Group can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to MT Group processing some specified classes of personal data, is a condition of employment for staff. This includes information about previous criminal convictions in

accordance with the Rehabilitation of Offenders Act 1974. Staff who have access to client information may be required to undergo a Security Clearance process through the Police. Therefore, prospective or existing members of staff will be asked to consent to their data being processed when an offer of employment / change of role offer is made. A refusal to agree may result in any offer withdrawn.

## 18.0 Employee Responsibilities

### 18.1 Processing by MT Group Employees

“Processing”, in relation to information or data, means obtaining, recording or holding the information or data, or carrying out any operation, or set of operations, on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- storage of the data, ensuring its security;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or

alignment, combination, blocking, erasure or destruction of the information or data

### 18.2 Staff Checklist for Processing Data

Before processing any personal data, all staff should consider the questions below:

- What is the legal basis for processing data that I am using?
- If it is consent, do we have the data subject's consent to process their data? Is it unambiguous and freely given?
- What collection activities do I have the lawful right to undertake? Is this everything that I want to process about the individual?
- Is the information 'ordinary' or is it 'sensitive'?
- Do I really need to collect the information?
- Do I really need to collect all of it?
- Can any or all of the data be pseudonymised or anonymised?
- For how long should the data be retained? When should it be updated or destroyed? What steps should be taken to ensure that this happens?
- Who else will be using the data? Is this authorised?
- Am I authorised to collect/store/process the data?
- Have I informed the data subject that I have their data, and provided them access to MT Group's fair processing / privacy policy?
- Where has the data been obtained from? Is this a reliable source? Can we prove the data subject provided consent to MT Group (or an approved third party) processing their data?
- Has the data been checked with the data subject for accuracy?
- Can I be certain that the data is kept secure and only accessible by those who have permission?

- If the answer to any of the above questions is no, or of a negative nature, then processing activities should be stopped and an investigation undertaken to determine how it can be corrected, involving the Data Protection Officer.
- Depending upon the circumstances, a notification to the Information Commissioner may also be required.

### 18.3 Prohibited Activities

All employees of MT Group who process personal data in any form must ensure they comply with the requirements of the Legislation and with any additional data protection procedures and guidelines that may be issued from time to time.

In particular, no employee of MT Group may, without the prior written authorisation of the Data Protection Officer:

- 1 Process data that MT Group does not have a legal basis for processing, including;
  - Continuing to process data where consent has been withdrawn by the data subject;
  - Development of a new paper filing system, computer system or database for processing personal data;
  - Use of an existing paper filing system, computer system or database to process personal data for a new purpose;
- 2 Intentionally retain data for longer than the time frame identified in the Data Retention Policy

All employees of MT Group are also responsible for ensuring that:

- 1 Any personal data they hold is classified and managed in accordance with MT Group's Information Security Policy;
- 2 Personal data is not disclosed to any unauthorised third party, and that every reasonable effort is made to see that data is not disclosed accidentally. If there is any doubt about whether personal data might have been accidentally disclosed to unauthorised persons, consult the Data Protection Officer;
- 3 Personal data is kept secure in an approved place. For example,
  - Keeping the data locked in a filing cabinet, drawer or room;
  - If the data is computerised, ensuring the data is password protected, or in a secure area of the network.

A deliberate breach of Data Protection legislation and/or MT Group's data protection policy may result in disciplinary proceedings.

### 18.4 Unfair Processing

Any recorded opinion about, or intentions regarding a person are considered personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (including hand written notes, e-mails and audio recordings, in addition to

computer and manual files) and when information is to be destroyed. The following is a useful test to apply to 'doubtful' comments.

## **19.0 Privacy by Design**

It is important to MT Group, and our customers that Data Protection is considered at the very start of any project that we undertake. By ensuring that the principles, and the rights of individuals are considered from the offset in software development we are able to ensure that functionality can be embedded into the design of our software to facilitate and enhance data protection.

If we try to implement data protection requirements as an afterthought, we run the risk of not doing it properly, of breaking existing functionality and / or inadvertently exposing the data to security vulnerabilities.

Through the use of Data Privacy Impact Assessment (DPIA) we are able to establish what processing activities are to be taking place and ensure the appropriateness of any remediation that is put in place, before the work is conducted.

The DPIA (if it is required – see the form for guidance) must always be signed off by the Data Protection Officer before work begins on the project. This is managed via the DPO function.

## **20.0 E-Mail**

It is acceptable and appropriate for MT Group to keep records of internal communications which are relevant to an individual's work at MT Group, including information concerning performance and conduct issues, provided such records comply with the Data Protection principles.

It is recognised that email is used for such communications and that such emails form part of MT Group's records. All employees of MT Group need to be aware that:

- Data Protection Legislation applies to emails which contain personal data about individuals which are sent or received by employees of MT Group;
- subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for MT Group to locate the personal data in the emails; and
- the legislation applies to all emails from and to members of MT Group which are sent and received for MT Group purposes, whether or not the emails are sent through MT Group email system or on an individual's own email account.

## **21.0 Disclosure of Information**

Manx Telecom does not anticipate any need to transfer personal data in relation to EU citizens to a country outside of the EU, other than the Isle of Man, which holds an adequacy ruling with the EU making such transfers legal.

However, the names, job titles and contact details of our members of staff on the website could constitute a transfer of personal data worldwide. Manx Telecom will seek the express consent of data subjects before posting such personal information on the Manx Telecom website.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply, or protective measures are taken, be disclosed or transferred outside the European Economic Area (EEA) to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

Personal data for UK, IOM Customers, Employees will only be transferred to approved 3<sup>rd</sup> party suppliers whereby they are providing a direct service and are contracted under GDPR terms and conditions which clearly defines who is acting as a Data Controller and or a Data Processor and a legitimate basis is present to do so.

## **22.0 Data Controller vs Data Processor**

It is essential for MT Group when we are involved in the processing of personal data to be able to determine whether we are acting as a data controller or as a data processor. The difference between the two is the determination of the responsibility for what data is collected and how it is processed.

For the vast majority of the systems that we use to process data, MT Group are the Data Controller, Irrespective of the relationship between MT Group and Customer the formalities and responsibilities should be formalised by a contract between all parties. We must ensure that in all scenarios (MT Group as the processor, MT Group as the controller, MT Group as a controller in common, or MT Group as a joint controller) there is a contract in place so that the data processor is able to provide the controller with “sufficient guarantees to implement appropriate technical and organisational measures” that their processing complies with the requirements of the legislation. This contract requirement should flow down the data chain ensuring that a processor cannot sub-contract to a second processor without the explicit approval of the data controller. In some cases, MT Group may contract a 3<sup>rd</sup> party to act as a Data Processor and or we may act as a Data Processor on behalf of a Business Partner.

## **23.0 Artificial Intelligence (AI) Data Protection Enhancements**

### **AI Processing of Personal Data**

This policy applies where personal data is processed using Artificial Intelligence (AI), including Generative AI, Large Language Models (LLMs), machine learning and AI capabilities embedded within approved business applications. Such processing shall comply with UK GDPR, Isle of Man GDPR and the Company ISMS Artificial Intelligence (AI) Usage Policy.

### **AI Processing Principles**

AI processing must have a lawful basis, use data minimisation, maintain transparency where required, include human oversight, preserve security controls and comply with information classification requirements.

#### **AI Processing Controls**

Only approved AI platforms may process personal data. The minimum amount of personal data shall be used and AI outputs must be validated before business use.

#### **AI Service Providers**

Approved AI suppliers must be subject to due diligence, Data Processing Agreements, security assessments and appropriate international transfer safeguards.

#### **Privacy by Design**

Projects involving AI processing personal data shall undergo appropriate assessments including DPIAs where required, AI Risk Assessments and Information Security Reviews.

#### **Automated Decision Making**

MT Group shall not rely solely on AI for decisions producing legal or similarly significant effects unless lawful safeguards and human intervention are in place.

#### **Employee Responsibilities**

Employees must only use approved AI services, must not upload personal data into unauthorised AI services and must comply with the AI Usage Policy.

#### **Compliance**

AI processing involving personal data may be monitored and audited by the DPO and Information Security teams.

## **Appendix A**

Under the GDPR, personally identifiable information (PII) is referred to as personal data. This includes any information that relates to an identified or identifiable natural person (data subject). Here are some examples of what is considered personal data under the GDPR:

### **Examples of Personal Data:**

- Basic identifiers: Name, address, phone number, email address, CCTV & video surveillance.
- Online identifiers: IP addresses, cookies, device identifiers
- Identification numbers: National insurance number, passport number, driver's license number
- Location data: GPS data, location tracking
- Biometric data: Fingerprints, facial recognition data, retina scans
- Genetic data: DNA sequences
- Health data: Medical records, health conditions, treatment details
- Financial data: Bank account details, credit card information
- Cultural and social identity: Ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation

### **Special Category Data:**

The GDPR also identifies certain types of personal data as special category data, which require additional protection due to their sensitive nature. These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (for the purpose of uniquely identifying a natural person)
- Health data
- Data concerning a person's sex life or sexual orientation

## Appendix B: Default Storage locations

Exceptions to the default storage locations are permitted only under the following conditions:

- a. An active and approved MT GROUP Policy explicitly specifies an alternative storage location to the table below.
- b. Explicit approval is granted by Company Director or Data Protection Officer for an alternative storage location.

| Storage Location                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Permitted data classifications                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MT GROUP centralised and managed storage locations: <ul style="list-style-type: none"><li>• MT GROUP file services presented as a Drive mapping within users' desktop</li><li>• MT GROUP provided Microsoft365 SharePoint, OneDrive, Teams and other Microsoft MT GROUP Applications that are allocated to users and accessible with MT GROUP user account</li><li>• Services which users are provisioned and accessible with MT GROUP user account such as Service, Operational, HR, Procurement &amp; Financial applications.</li></ul> | Any classification type can be stored on MT GROUP Centralised and managed storage locations: <ul style="list-style-type: none"><li>• Public</li><li>• Internal-only</li><li>• Confidential</li><li>• Restricted</li></ul>                                                                                                                                                                                  |
| Laptop local drives* (C:\ & D:\) supplied by MT GROUP which are: <ul style="list-style-type: none"><li>• Encrypted</li><li>• Logged in with Users Active Directory account only</li><li>• Secured by MT GROUP Endpoint protection services</li></ul> <p><i>*Local drives do not include removable storage of any type (USB, SSD Cards, Cloud based etc)</i></p>                                                                                                                                                                           | When necessary to complete a task or objective as ordered by manager then data classified as: <ul style="list-style-type: none"><li>• Public</li><li>• Internal-only.</li></ul> Data classified as: <ul style="list-style-type: none"><li>• Confidential</li><li>• Restricted</li></ul> must not be stored on Laptop local drives unless explicit permission is granted by manager or any position higher. |