



Privacy and Data Protection

All Employee Training

Privacy and Data Protection

Training Overview



After completing this training, you should understand the following:



- » The difference between privacy and security
- » The importance of privacy compliance
- » Privacy-related terminology
- » Our responsibilities as MTS employees
- » How to report a concern
- » GDPR requirements

OUR COMMITMENT

MTS is committed to protecting personal information and following applicable privacy laws and regulations around the world. Our privacy policies and procedures describe the types of information we collect, how we use this information, rights and obligations with respect to the information, and other important privacy-related topics..

Privacy and Data Protection

What is Privacy vs. Security?



MTS is committed to protecting the privacy and security of personal and confidential information of its employees, customers, suppliers and other third parties.

Privacy in the workplace refers to protecting information that is considered personal or private from corruption, compromise or loss.

MTS Policies ORC-012, ORC-013, ORC-014, ORC-015

Examples of Personal Information

- Name
- Age
- Date and place of birth
- Home phone number
- Postal / email address
- Bank account and credit card details
- Medical records

Security is the protection of the confidentiality, integrity and availability of information.

MTS Policies IT-013 and IT-021

Scope

- Protect information from accidental or intentional unauthorized modification, destruction or disclosure
- Secure equipment and software used to process, store and transmit information

Privacy and Data Protection


The Importance of Privacy Compliance




MTS is committed to protecting the privacy of personal information of its employees, customers, suppliers and other third parties, and following applicable laws and regulations.

Why is compliance important?

- We all want our personal data to remain private
- It's the right thing to do
- It's the law

 Data protection and privacy laws are becoming stricter.

 A privacy incident / breach can have serious consequences for MTS.

Examples of Privacy Laws & Regulations

U.S. Health Insurance Portability and Accountability Act ("HIPAA") of 1996

- ❖ Protects certain types of health information


EU General Data Protection Regulation ("GDPR")

- ❖ Intended to strengthen and unify data protection for individuals within the EU

Other Applicable Laws:

- ❖ California Consumer Protection Act (CCPA)
- ❖ National privacy laws in Asia, i.e. China & South Korea

Personal data is information on its own, or when combined with any other information held, identifies a living person.

 **Sensitive personal data** needs additional protection, as processing of this kind of data is heavily regulated by country-specific privacy laws and regulations. Some examples include:

- Social Security or National Identification Number
- Bank/Account Number
- Personal Health Information
- Race, Ethnicity, or Sexual Orientation
- Religious or Philosophical Beliefs



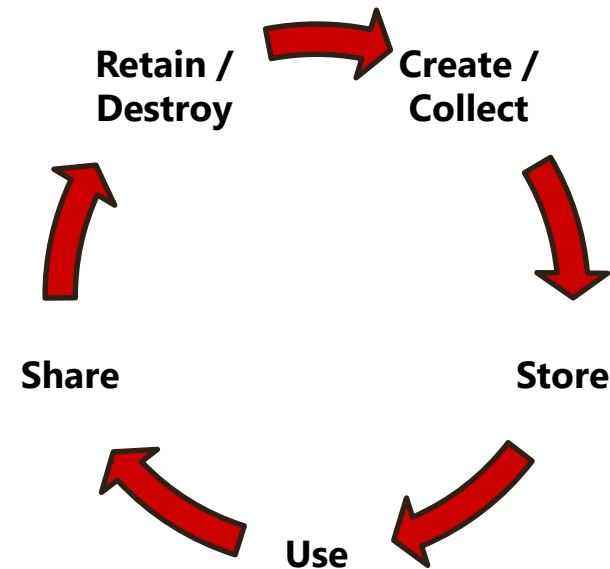
Every MTS employee will come into contact with personal data while executing their business activities. **Processing** involves the handling of personal data and includes the activities listed below.

Activities:

- Create
- Collect
- Record
- Store
- Retrieve
- Share
- Disclose
- Delete
- Destroy



Lifecycle of Personal Data:



Data Breach is any incident or action resulting in data that MTS holds is lost, destroyed, or disclosed to a person/entity that it should not have been disclosed to, or its security has been compromised.

A data breach includes:

- both actual and suspected incidents
- breaches caused accidentally or deliberately

Examples:

- Loss of a laptop, mobile phone, USB stick or other device
- Sending an e-mail to the wrong address
- Leaving papers on a train
- Theft of equipment
- Loss/unauthorized destruction of paper or softcopy records
- Hacking
- Cyber attacks
- Unauthorized people being given access to our systems

Privacy and Data Protection

Our Responsibilities



MTS has a formal Privacy and Data Protection Compliance Program, with related practices and standards managed and executed across different business areas.

All Employees must safeguard personal data as applicable for your job in accordance with MTS privacy policies.

Business Area Roles

Office of Risk and Compliance sets organizational compliance expectations through policies and trainings.

Human Resources adheres to compliance requirements to safeguard personal data as they manage daily HR practices.

Information Technology and Security owns security measures to protect MTS networks and systems and safeguard data from loss, misuse, unauthorized access, disclosure, alteration or destruction.

Privacy and Data Protection

Our Responsibilities



As MTS employees, you are responsible for protecting the personal data you have access to as you execute your business activities. Follow the key principles outlined below.

Key Privacy Principles

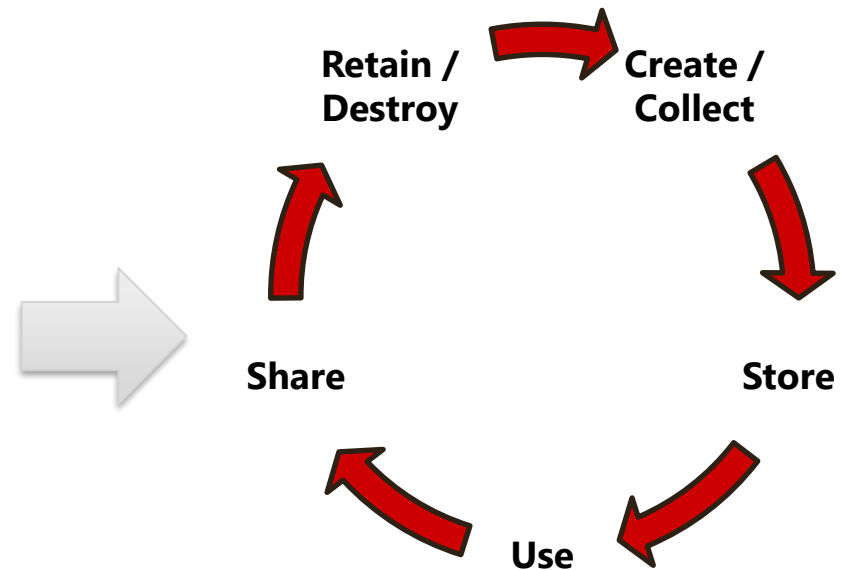
Only use and share personal data for its intended **business purpose**

Follow operational and technical safeguards to avoid unauthorized **access**

Use the **minimum amount** of personal information necessary for your work

Retain personal data for no longer than necessary

These key principles apply to the full lifecycle of personal data:



Privacy and Data Protection

Our Responsibilities



Creating, Collecting, Storing, & Using Personal Data

- ✓ Only create or collect the personal data needed to specifically perform an operational task or business-related project.
- ✓ Store information on approved devices and locations only.
- ✓ Ensure that documents that contain personal data are kept in secure locations with access only to those employees that need it to perform their job function.
- ✓ For sensitive personal data, safeguard data through file-level security controls (e.g., password protecting files, email encryption, etc.) and dispose of immediately after business use.
- ✓ Avoid downloading or saving personal data that is not needed for a specific operational task or project.
- ✓ Lock your screen and secure personal data when you are away from your desk.



Sharing Personal Data

- ✓ Only share personal data with those who need it to fulfill their job responsibilities.
- ✓ Never share personal data with anyone unless you know who they are and that they are entitled to the data.
- ✓ Do not use personal email accounts to carry out business activities.
- ✓ Prior to sending an email that contains personal data, review the distribution list to ensure only those who need data have been included on the email.
- ✓ When transferring personal data internally between MTS employees, it is best practice to secure with an email encryption feature.
- ✓ When transferring personal data between an MTS employee and a third party, it is required to use a secure method such as an email encryption feature.



Retaining and Destroying Personal Data

- ✓ Strictly follow document retention policy and related guidelines – review, archive and delete electronic and paper documents when no longer needed or retention timeframe has been met.
- ✓ Take caution with disposal method of sensitive data on hard drives and network drives, when no longer needed.
- ✓ Take caution with disposal method of sensitive data in paper files, ensuring disposal is handled using currently approved secure handling methods (e.g., shred).
- ✓ Delete any documents with personal data that are saved on personal drives and no longer serve a business or legal need.



If you have questions on retention or destruction of data, please consult with your legal or compliance partners.

A data subject access request is when an individual makes a request to MTS about the nature and use of their personal data.

A data subject rights request may be:

- Verbal (i.e. by telephone or face to face).
- In writing (i.e. by letter, email, fax, or via any of our social media channels).
- Sent to anyone within MTS - we cannot require data subjects to send their requests to a specified person within MTS.

Examples of these requests might be:

- "stop marketing to me"
- "please delete my information"
- "remove me from your email listing"
- "please share the information your company has for me"

If you receive a request which is, or you suspect may be a data subject access request, email privacy@mts.com.

Privacy and Data Protection

How to Report a Privacy Incident



If you become aware of or suspect a privacy incident or breach:

- ✓ You must not delay. Some jurisdictions have 72 hour notice requirements.
- ✓ You should not take any further action in relation to the breach unless directed to do so by the ORC.
- ✓ Do not notify any affected individuals or the regulators – the ORC will take these steps as appropriate.
- ✓ Refer to ORC-013 Privacy Incident Response Policy for more information on how breaches are handled.
- ✓ Failure to report could result in disciplinary action.

Be aware that MTS may need to:

- » Notify the individuals concerned – employees, customers, etc.
- » Notify Data Protection Authorities
- » Inform the police or and/or other third parties (e.g. insurers).

Privacy and Data Protection

How to Report a Privacy Incident



Promptly report a potential incident immediately to
privacy@mts.com

ORC, Legal, IT, and HR teams work together and follow the Privacy Incident Response Policy to address a reported incident.

Timing is critical for MTS to take the necessary steps – so please report immediately!

The remaining slides are focused on
EU General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR):

- Enhances legal and regulatory requirements to bring data protection and **privacy laws** into the 21st century, which is **industry and sector neutral**.
- Applies broadly across data processing activities and relationships with individuals, customers, staff, service providers, third parties and beyond.
- Enhances individuals' position and rights with:
 - Improved transparency
 - More accountability for businesses
 - Greater control of own personal data
 - Significant regulatory powers of authorities

Non-compliance with GDPR can result in:

- **Regulatory fines** of up to 4% of worldwide annual revenue or 20 million EUROS (whichever is higher)
- **Criminal sanctions** can be imposed in addition to regulatory fines
- **Individual** compensation claims
- **Class action** possible for “judicial remedies” (administrative remedies, e.g. to stop processing, or delete data)
- Fines, civil and criminal liability possibly in **multiple countries**
- **Stop orders** by Data Protection Authorities
- **Reputational risk and brand damage**
- **Burden** on management time and legal expenses in case of investigations/actions

Privacy and Data Protection

Where GDPR Applies



GDPR expects us to act as responsible stewards of EU personal information and build privacy and security safeguards into our policies, practices and applications.

We hold personal data of:

- MTS employees
- Customers' employees
- Suppliers and sub-contractors
- Other third parties

We hold personal data in IT systems, such as:

- SAP
- SuccessFactors
- Salesforce
- IT security tools

GDPR applies to Data Controllers and Data Processors.

- A **Data Controller** determines the purposes and means of processing personal data.
- A **Data Processor** processes personal data on behalf of the data controller.

MTS is primarily a data controller. MTS service providers (such as payroll service, etc.) are data processors.

Privacy and Data Protection

GDPR - Data Protection Officer Role



In addition to the roles of all MTS employees, IT, HR and ORC in upholding MTS's commitment to privacy, MTS contracts with an external Data Protection Officer (DPO) to assist in the oversight of the compliance program.

DPO Responsibilities include:

- Advise ORC in relation to any questions regarding GDPR and data protection.
- Partner with compliance team and represent MTS before data protection authorities.
- Act as primary contact for EU data subject requests.

Privacy and Data Protection

GDPR Principles of Processing Data



| Privacy Principle | Requirement |
|-------------------------------|--|
| Lawful basis | <ul style="list-style-type: none"> ✓ Ensure there is a lawful basis for processing personal data. |
| Purpose Limitation | <ul style="list-style-type: none"> ✓ Use and share personal data for its legitimate business purpose only. |
| Data Retention | <ul style="list-style-type: none"> ✓ Retain personal data for no longer than necessary. ✓ Destroy, delete, or anonymize personal information once it is no longer needed, in accordance with record retention guidelines. |
| Data Minimization | <ul style="list-style-type: none"> ✓ Use the minimum amount of personal data necessary for your work. ✓ Don't collect or accumulate more personal data than you need. |
| Data Collection | <ul style="list-style-type: none"> ✓ Collect and use personal data with care and caution. ✓ If personal data is processed for marketing purposes, the data subject has the right to object the processing of their data for marketing. ✓ GDPR increases the amount of information MTS needs to disclose to employees and other data subjects. |
| Data Transfers | <ul style="list-style-type: none"> ✓ Transfer and share personal data between internal entities only if it is relevant in serving its business purpose. |
| Data Security | <ul style="list-style-type: none"> ✓ Secure personal data when it is in your possession - follow technical and operational safeguards to avoid unauthorized access. ✓ Further protect <u>sensitive</u> personal information by adding additional security controls on documents, such as password protection. |
| Data Integrity | <ul style="list-style-type: none"> ✓ Maintain the accuracy and completeness of personal data. |
| Third Party Processing | <ul style="list-style-type: none"> ✓ Ensure third parties you work with have completed necessary due diligence assessments, agreements and/or contracts. |
| Using Data Processors | <ul style="list-style-type: none"> ✓ Data processing on behalf of and by instruction of MTS |
| Data Subject Rights | <ul style="list-style-type: none"> ✓ As an employee, you may submit a written request asking what personal data is being processed; MTS honors valid requests with appropriate care and caution. |
| Data Breach | <ul style="list-style-type: none"> ✓ We may need to tell the data protection regulator or other EU data protection regulator within 72 hours of a reported incident or breach. |

MTS has the following structure and practices in place to address the various GDPR privacy principles.

MTS Privacy Policies and Procedures

MTS privacy-related policies and procedures support our commitment to protecting personal data and following applicable privacy laws and regulations around the world, including GDPR.

MTS Privacy Notices

MTS Privacy Notices call out the lawful basis for processing of personal data for both employees and third parties. MTS is responsible for ensuring that such notices are sent to potential data subjects prior to MTS collecting or processing their personal data.

MTS Privacy & Security Incident Response Policies

ORC, Legal, IT, and HR teams work together and follow the Privacy and Security Incident Response Policies to address reported incidents / breach.

MTS has the following structure and practices in place to address the various GDPR privacy principles.

MTS Register of Processing Activities (RoPA)

MTS documents in-scope processes and validates a lawful basis, capturing information about data processing, data categories, the group of data subjects, the purpose of the processing and the data recipients. Transfers of personal data with third parties is documented here as well.

MTS Data Processing Agreement (DPA) Template

MTS identifies service providers that process or transfer personal data. MTS partners with in-scope service providers to review third party standard terms and ensure agreed-upon MTS DPA is included.

MTS Data Protection Impact Assessments (DPIA)

DPIAs are used to build GDPR-compliant processes and safeguards into day-to-day work. DPIAs assess whether the processing is lawful and identifies the lawful basis.

Privacy and Data Protection

GDPR Principles of Processing Data



MTS has the following structure and practices in place to address the various GDPR privacy principles.

MTS Intercompany Transfer Agreements

Transfers of personal data between employees of MTS subsidiaries and affiliates are protected by Intracompany Agreements, with inclusion of appropriate GDPR language, and have been approved by Data Protection Officer.

Data Subject Access Request (DSAR) Protocol

MTS has a mechanism in place to support individual requests for copies of their personal data and supplementary information. Individuals have the right to have their personal data deleted (“the right to be forgotten”). The right is not absolute and only applies in certain circumstances. Individuals have the right to object to processing based on legitimate interests or direct marketing.

MTS Website Opt-In

MTS websites include an opt-in consent for all website users.

When working with third parties, please follow these practices:

- ✓ If you work with a third party and review the contract for your role, partner with ORC to make sure your third party is included on ORC's inventory listing.
- ✓ Work with your third party to ensure inclusion of an updated Data Processing Agreement (DPA).
- ✓ Ensure that any future third party agreements include the DPA.
- ✓ Do not transfer data if MTS does not have a contract (and Data Processing Agreement) with the 3rd party.



**Promptly report a potential incident immediately to
privacy@mts.com**

ORC, Legal, IT, and HR teams work together and follow the Privacy Incident Response Policy to address a reported incident.

For more information, please review MTS Privacy Policies:

Europe Privacy
Policy ORC-012

Incident Response
Policy ORC-013

Global Privacy
Policy ORC-014

North America
Privacy Policy
ORC-015