Privacy and Data Protection

Part 1/2

We are committed to respecting the privacy of all individuals with whom we work and protecting their personal data in compliance with applicable privacy and data protection laws. **Personal data** is any information that can be used to identify a person either directly or indirectly. We handle personal data responsibly by collecting only what's needed, using it fairly and transparently, keeping it accurate and secure, and only storing it for as long as necessary.

We ensure all TMICC's digital assets are safe, properly maintained and used only for appropriate work purposes. We protect all forms of TMICC information by classifying, storing, securing, sharing, updating and deleting it in line with our standards and relevant laws, including privacy, security, employment and data retention.

Why is it important?

Protecting personal data is fundamental to respecting people and the human right to privacy. It builds trust with our employees, consumers, customers and business partners. It ensures compliance with legal obligations, helping us avoid fines and reputational harm. It safeguards sensitive information from misuse, loss or unauthorised access, and enables individuals to exercise their rights over their own personal data.

What must I do?

- Only collect or access personal data when necessary for my role or business purpose.
- Limit the amount of data I collect to the minimum I need for the specific purpose.
- Use personal data fairly.
- Consider potential harm to individuals when using their data and take steps to mitigate these risks.
- Be transparent with individuals about how their data is used.
- Store personal data securely using approved systems and tools in accordance with our information security policies.
- Keep personal data accurate and up to date.
- Respect individuals' rights (e.g. for access, correction, or deletion) and get consent to use it where necessary (e.g. for e-marketing).
- Complete a **Privacy Risk Assessment** before any new project, campaign, or activity that involves personal data.
- Do not keep personal data longer than needed – delete or anonymise it in accordance with our retention policies.
- Do not put confidential information, including personal data, into publicly available AI tools or on social media, and do not share it with third parties without authorisation and appropriate contract terms, including after my TMICC employment ends.

Privacy and Data Protection

Part 2/2

TMICC has an **obligation to cooperate** with requests from government agencies for information stored on TMICC devices or used for TMICC business. That means that if I receive a request to keep certain information, I must ensure that the requested information is secure, will not be deleted or altered, and is available for review or production by TMICC or relevant third parties, even if the data retention period has expired. If I fail to follow this request, I and TMICC could face fines, liability and reputational harm.

Always speak to Data Privacy Team before:

- Collecting or using any sensitive or special category personal data or data relating to vulnerable people (including children);
- Using innovative technology, AI, or automated decision making to process personal data;
- Monitoring people or their behaviour; or
- Using large volumes of personal data (>100,000 for marketing and >10,000 for HR / R&D).

What are Examples of Personal Data?

Names, email addresses, home addresses, phone numbers, medical information, online cookies, IP addresses, location data, employee ID number, photographs or videos where individuals are identifiable.

Certain categories of personal data, such as race, ethnicity, religion, health, sexuality or biometric data are classified as “sensitive” or “special category” data and require additional protection.

All data on company-issued devices is subject to collection, transfer and inspection, as is company-related data on personal devices used for business purposes.

What is a Personal Data Incident?

A Personal Data Incident is any incident that has the potential for personal data to be lost, damaged or misused. This could be the result of a security failing, and it could be accidental or malicious in nature. A Personal Data Breach is when there is a confirmed loss, alteration, destruction, unauthorised disclosure of, or access to, personal data.

Examples of Personal Data Incidents:

- Accidental Disclosure: HR data (names, salaries) sent to the wrong recipients.
- Malware Attack: Consumer accounts database compromised by malicious software.
- Accidental Destruction: Payroll records deleted, causing payment delays.
- Loss of Paper Records: Health declaration forms mislaid at reception.

Report any Personal Data Incidents immediately to the Privacy Team.

Where do I go for more information?

Chief Privacy Officer, Global Privacy Team, Legal and Business Integrity Teams, Privacy & Data Governance Hub.