

MCMC MTSFB TC G056:2025

TECHNICAL CODE

INTERNET OF THINGS (IOT) - PRIVACY REQUIREMENTS

Developed by



Registered by



Registered date: 20 November 2025

© Copyright 2025

MCMC MTSFB TC G056:2025

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under Section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to Section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with Section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by Section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under Section 185 of the Act.

A technical code prepared in accordance with Section 185 shall not be effective until it is registered by the Commission pursuant to Section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)

MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)

Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Page

Committee representation iii

Foreword iv

0. Introduction 1

1. Scope 1

2. Normative references 2

3. Abbreviations 2

4. Terms and definitions 2

5. Challenges in managing data privacy 4

6. Privacy risk in Internet of Things (IoT) data management lifecycle 6

 6.1 Internet of Things (IoT) data management lifecycle risk 6

 6.1.1 Data collection 7

 6.1.2 Data storage 7

 6.1.3 Data usage 8

 6.1.4 Data transfer 8

 6.1.5 Data deletion 9

 6.2 Internet of Things (IoT) data privacy risks and stakeholder responsibilities 9

 6.2.1 Data subject 9

 6.2.2 Data controller 9

 6.2.3 Data processor 10

 6.2.4 Stakeholder responsibilities 10

 6.2.5 Additional responsibilities of stakeholders 11

7. Governance and compliance requirements for Internet of Things (IoT) data protection 13

 7.1 Data protection governance 13

 7.2 Compliance and enforcement 14

 7.3 Risk management for Internet of Things (IoT) data protection 14

 7.4 Understand risk considerations and mitigation 15

 7.5 Risk treatment 15

 7.6 Monitoring and review 15

 7.7 Recording and reporting risk 16

8. Internet of Things (IoT) systems data protection controls requirements 16

 8.1 General controls 16

 8.2 Notice and choice controls 17

 8.3 Disclosure controls 18

 8.4 Security controls 18

MCMC MTSFB TC G056:2025

8.5	Data minimisation and retention controls	18
8.6	Data integrity controls	19
8.7	Access controls.....	19
	Bibliography	20

Committee representation

This technical code was developed by IMT-2020, IoT and ITS Security Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CyberSecurity Malaysia

Digital Connect Society

FNS (M) Sdn Bhd

SIRIM Berhad

Smart Tech AP Sdn Bhd

Universiti Kuala Lumpur

MCMC MTSFB TC G056:2025

Foreword

This technical code for Internet of Things (IoT) - Privacy Requirements ('Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INTERNET OF THINGS (IOT) - PRIVACY REQUIREMENTS

0. Introduction

The Internet of Things (IoT) has emerged as a transformative technology, connecting a vast array of devices, from smart home appliances to industrial sensors, to the internet. This interconnectedness has revolutionised various industries, offering unique opportunities for efficiency, innovation, and convenience. However, the rapid production of IoT devices has also raised significant concerns regarding data privacy and security.

As IoT devices are able to collect and transmit vast amounts of sensitive personal data in real-time, either for automation purposes or Artificial Intelligence (AI)- driven analytics, it is crucial to establish robust privacy frameworks to safeguard individual rights and protect sensitive information. In practice, IoT ecosystems face challenges such as inconsistent privacy controls, weak enforcement of user consent, and fragmented compliance with data protection laws, which increase the risk of misuse and unauthorised access to personal information. This Technical Code aims to address these critical data privacy concerns by specifying applicable requirements for IoT systems. By focusing on data protection, user consent, and transparency, this Technical Code ensures that IoT devices and applications handle personal information in a responsible and ethical manner.

This Technical Code defines the requirements for data privacy governance and controls in IoT systems that process personal data, including biometric data, health data, geolocation data, and multimedia content (such as video, photos, and audio recordings). The target users of this Technical Code are entities that undertake roles as data controllers and/or data processors, within IoT deployments and operations.

This Technical Code supports and complements the following Technical Codes that provide a comprehensive framework for IoT security and privacy.

- a) MCMC MTSFB TC G013, provides the IoT security management framework, including the IoT reference model that covers application layer, service support, network layer, device layer, management capabilities and security capabilities.
- b) MCMC MTSFB TC G031, outline the requirements for IoT application security that cover everything from security measures to the threat landscapes and IoT application security best practices.
- c) MCMC MTSFB TC G045, defines the IoT device security requirements for IoT devices and gateways. Focusing on authentication, cryptography, data security, device platform security, and physical security.

1. Scope

This Technical Code specifies the requirements for the protection of personal data within IoT systems. It establishes principles and controls for the collection, processing, storage, transmission, sharing, and disposal of personal data handled by IoT devices, platforms, and applications.

This Technical Code applies only to personal data as defined in Clause 4. Any data which allows for association with, or inference of identity, shall be considered as personal data. Data from which identity association or deduction cannot be inferred is considered not to be personal data. This Technical Code applies to the following.

- a) IoT device manufacturers, system developers, and service providers;
- b) Organisations that process or manage personal data generated by IoT systems; and

MCMC MTSFB TC G056:2025

- c) Third parties with access to personal data within IoT ecosystems.

This Technical Code does not cover:

- a) General cybersecurity requirements not directly related to personal data protection; and
- b) Sector-specific or jurisdiction-specific regulatory requirements, which may apply in addition to this document.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

Personal Data Protection Act 2010 (Act 709)

Code of Practice for Communications of Data Users (2017) - For Licensees Under the Communications and Multimedia Act 1998

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

AI	Artificial Intelligence
API	Application Programming Interface
CIA	Confidentiality, Integrity, and Availability
DPO	Data Protection Officers
DPIA	Data Protection Impact Assessment
IIoT	Industrial Internet of Things
IT	Information Technology
IoT	Internet of Things
MAC	Media Access Control
PET	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
SLA	Service Level Agreement
UI	User Interface

4. Terms and definitions

For the purposes of this Technical Code, the following definitions apply.

4.1 Anonymisation

Conversion of personal data into data that cannot be used to identify any individual. Anonymisation is preferred for data that needs to be shared publicly without privacy concerns.

4.2 Data controller

Individual or organisation that directly processes or uses personal data, or has direct control over the processing or use of personal data, or authorises the processing or use of personal data. The entity determines the purposes for which and the manner in which any personal data is or is to be processed.

Note: The Data controller was referred to as the data user in Act 709 (2010).

4.3 Data minimisation

Principle of collecting and processing only the minimum amount of personal data necessary for a specific purpose. This helps to reduce the risk of data breaches and protect individuals' privacy. By limiting the amount of personal data collected and stored, organisations can minimise the potential harm in the event of a data breach.

4.4 Data privacy

Practices and principles that govern the collection, storage, use, and sharing of personal data. It ensures that individuals have control over their personal information and that it is protected from unauthorised access, use, or disclosure.

4.5 Data processor

Any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of their own purposes.

4.6 Data security

Approach to protecting sensitive information from unauthorised access, use, disclosure, disruption, modification, or destruction. It involves implementing a framework of policies, procedures, and technical controls to ensure the confidentiality, integrity, and availability (CIA) of information assets

4.7 Data subject

Individual whose personal data is being processed. Any living person whose information is collected, used, or disclosed by an organisation (data controller) is considered a data subject. Data subjects have various rights, including the right to access, correct, and withdraw consent for the processing of their personal data.

4.8 Internet of Things (IoT)

Network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

4.9 Internet of Things (IoT) device

Device that is able to sense, affect and interact with the physical world.

4.10 Manufacturer

Entities that design, develop, and produce IoT devices and systems.

MCMC MTSFB TC G056:2025

4.11 Personal data

Any information concerning a commercial transaction that directly or indirectly relates to an individual who can be identified from that information or other information held by the data controller. This includes information such as names, identification numbers, online identifiers and encompasses any information that can be used to identify a natural person.

4.12 Privacy-by-design

Holistic approach that integrates privacy considerations into the design and development of products, systems, and practices. It emphasises proactive measures to protect personal data and individual privacy throughout the entire lifecycle of a technology or process, rather than relying on reactive measures after a privacy breach or issue occurs.

4.13 Pseudonymisation

Replacement of personal identifiers with pseudonyms reduces re-identification risks while remaining reversible if auxiliary data is available.

4.14 Sensitive personal data

Personal data that includes information about health, physical or mental condition, religious beliefs, political opinions, criminal records and "biometric data".

4.15 Service providers

Organisations that operate, maintain, and deploy IoT devices and systems.

4.16 Stakeholders

Organisations, service providers, third-party providers, data subjects, data controllers and/or data processors.

4.17 User consent

Explicit permission granted by an individual to an organisation to collect, process, and store their personal data. It is a fundamental principle in data privacy regulations, ensuring that data subjects have control over their personal information. Consent should be freely given, specific, informed, and unambiguous.

5. Challenges in managing data privacy

The challenges in managing data privacy involve the obstacles and complexities in protecting and securing data privacy. The key challenges in managing data privacy and its impact on the organisation are provided below.

Table 1. Challenges in managing data privacy

No.	Obstacles/Complexities	Challenges	Impact
1.	Rapid evolution of the regulatory landscape	Data privacy laws and regulations are constantly evolving and vary significantly across jurisdictions (e.g., PDPA amendment in Malaysia, GDPR in Europe, CCPA in California).	The organisation's data privacy stakeholders shall stay updated on regulatory changes, interpret implications, and ensure organisational compliance, which can be resource-intensive and complex.
2.	Data complexity and proliferation	Organisations handle vast amounts of data across multiple platforms and locations, including IoT, cloud services and third-party systems.	Managing data inventories, mapping data flows, and ensuring data accuracy and security becomes challenging. Data privacy stakeholders shall navigate data complexity to effectively protect personal information.
3.	Privacy by Design and default implementation	Integrating privacy considerations into the design and development of systems, applications, and processes from the outset (privacy by design).	Requires close collaboration across departments (IT, legal, compliance) to embed privacy principles into organisational practices, which can face resistance or require significant cultural and procedural changes.
4.	Data breach preparedness and response	Increasing frequency and sophistication of cyber threats pose significant risks to data security and privacy.	Data privacy stakeholders shall develop robust incident response plans, conduct breach simulations, and coordinate responses swiftly to mitigate harm to individuals and comply with regulatory notification requirements.
5.	Balancing privacy with business innovation	Organisations strive for innovation and efficiency while respecting and complying with data privacy rights.	Data privacy stakeholders shall find ways to enable data-driven initiatives while adhering to legal constraints and ethical standards, often navigating complex trade-offs between privacy and business objectives.
6.	Vendor and third-party management	Organisations increasingly rely on third-party vendors and service providers who handle personal data.	Data privacy stakeholders shall ensure that third parties comply with data protection requirements through robust contractual agreements such as Data Processing Agreements (DPAs) and ongoing monitoring, mitigating risks associated with data transfers and outsourcing.

Table 1. Challenges in managing data privacy (continued)

No.	Obstacles/Complexities	Challenges	Impact
7.	Cultural and organisational change	Building a privacy-aware culture and securing executive buy-in for privacy initiatives can be a challenging task.	Data privacy stakeholders shall educate employees, raise awareness of privacy risks, and advocate for privacy-enhancing measures across all levels of the organisation, which requires effective communication and change management skills.
8.	Emerging technologies and privacy implications	Technologies such as AI, IoT, quantum and blockchain present distinctive privacy challenges due to their data-intensive nature and potential for widespread data collection.	Data privacy stakeholders shall assess and address privacy risks associated with emerging technologies, proactively implementing safeguards and influencing technology design to prioritise privacy.
9.	Global data transfers and cross-border compliance	Data flows across borders raise complex legal and regulatory issues regarding data sovereignty, international data transfers, and compliance with varying privacy laws.	Data privacy stakeholders shall navigate mechanisms such as standard contractual clauses and binding corporate rules to facilitate lawful data transfers while managing risks associated with global data processing.
10.	Maintaining trust and reputation	Data breaches and privacy incidents can damage an organisation's reputation and erode trust with customers, stakeholders, and regulators.	Data privacy stakeholders shall prioritise transparency, accountability, and ethical data practices to maintain trust, manage public perception during incidents, and protect brand integrity.

6. Privacy risk in Internet of Things (IoT) data management lifecycle

The IoT has revolutionised the way users interact with the world, connecting devices and systems to exchange data and automate processes. While IoT offers numerous benefits, it also introduces significant security and privacy risks, particularly due to its interface between digital and physical domains, which involves sensor and actuation capabilities. IoT systems collect and transmit vast amounts of personal and sensitive data. The organisation shall address the potential vulnerabilities, data risks and safeguard user privacy throughout the data management lifecycle.

6.1 Internet of Things (IoT) data management lifecycle risk

IoT systems are a prime target of cyberattacks due to the large amounts of personal data generated by IoT devices. IoT data risk management is primarily related to the understanding of the IoT data management lifecycle that consists of 5 stages, which are data collection, data transfer, data storage, data usage and data deletion.

In Figure 1 below, the organisation shall review the IoT data privacy risks within the IoT data management lifecycle. By understanding the security and privacy risks associated with data collection, storage, usage, transfer, and deletion, an organisation can protect user data privacy and build a secure IoT system with effective measures.

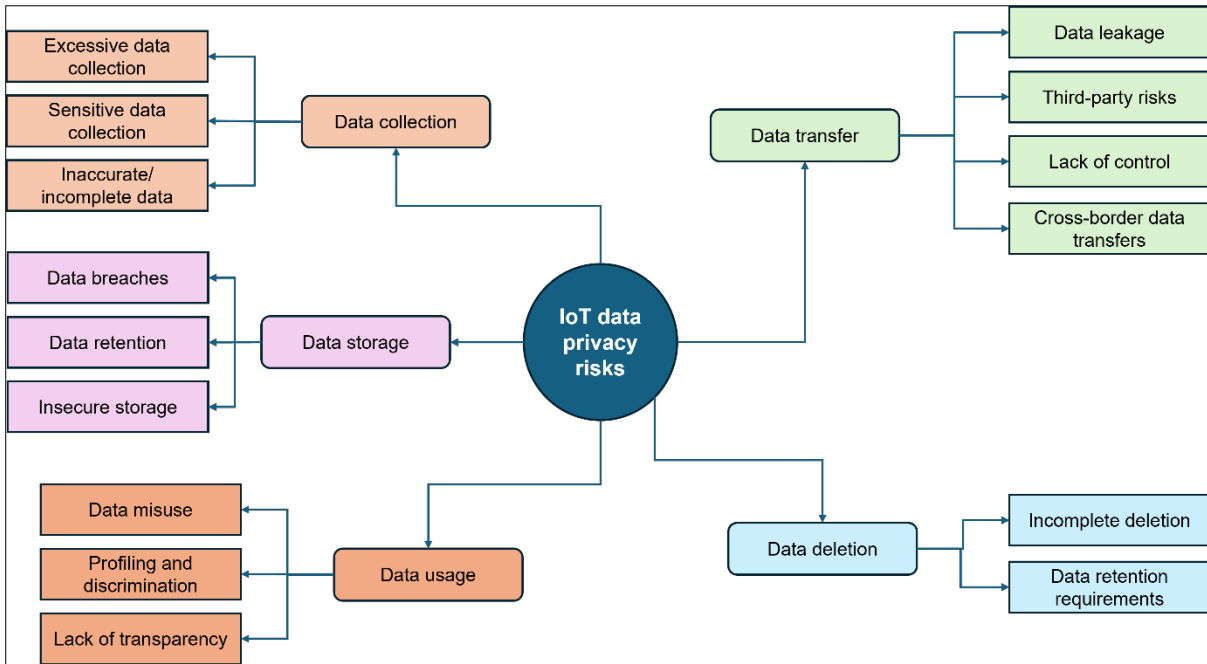


Figure 1. Internet of Things (IoT) data management lifecycle

6.1.1 Data collection

The organisation may collect data from various IoT devices, such as sensors, cameras, and wearables, and collect data on physical parameters like temperature, humidity, motion, and location. Data collection is typically conducted at high frequency and in large volumes, providing the foundation for subsequent analysis and decision-making. The following are the risks associated with data collection.

a) Excessive data collection

IoT devices often collect vast amounts of data, including personal information, location data, and behavioural patterns. Excessive data collection can pose significant privacy risks if not handled carefully.

b) Sensitive data collection

IoT devices may collect sensitive data, including health information, financial data, or biometric data. This data, if compromised, can have severe consequences for individuals. For example, a smart home assistant may inadvertently collect sensitive conversations if not properly configured.

c) Inaccurate or incomplete data

IoT devices can generate inaccurate or incomplete data due to sensor errors, network issues, or software bugs. This can lead to misleading insights and incorrect decision-making.

6.1.2 Data storage

Collected data is securely stored in various storage systems, including local databases, cloud storage, or a combination of both. The data storage systems shall be scalable and reliable to handle the increasing volume and diversity of IoT data. The data storage risks include the following.

a) Data breaches

MCMC MTSFB TC G056:2025

IoT devices often store data on local storage or in the cloud. The devices shall be adequately secured to protect the data from hackers and to prevent data breaches.

b) Data retention

IoT devices may store data for certain periods, subject to the internal storage in the device, increasing the risk of unauthorised access and misuse. In addition, cloud applications and cloud storage also store data pushed by IoT devices, which, if not properly managed, secured and audited, may lead to the risk of data loss, breach and leak.

c) Insecure storage

Many IoT devices and cloud storage used by IoT applications may have weak security measures, such as insecure default passwords, a lack of encryption, and outdated software, making data storage vulnerable to attacks.

6.1.3 Data usage

IoT data may be used for predictive maintenance, personalised experiences, supply chain optimisation, and many other applications. The insights derived from data analysis are utilised to optimise operations, improve decision-making, and develop innovative solutions. However, data usage utilisation may raise several risks as below.

a) Data misuse

IoT data can be misused for various purposes, such as targeted advertising, profiling, or even surveillance.

b) Profiling and discrimination

IoT devices can collect data that can be used to create detailed profiles of individuals, potentially leading to discrimination or unfair treatment.

c) Lack of transparency

IoT device manufacturers and service providers may not be transparent about how they collect, use, and share data, eroding trust.

6.1.4 Data transfer

Data is securely transferred between devices, networks, and storage systems using various protocols and technologies. Efficient data transfer is crucial for real-time applications and timely decision-making. However, several risks related to data transfer are provided below.

a) Data leakage

IoT devices often transmit data over networks, increasing the risk of data leakage.

b) Third-party risks

IoT devices may rely on third-party services to process or store data, introducing additional security risk.

c) Lack of control

Once IoT data is shared, it may be difficult to control its usage, especially if it is transmitted to third-party servers or cloud platforms.

d) Cross-border data transfers

IoT devices may transmit data across borders, raising concerns about data privacy laws and regulations in different jurisdictions.

6.1.5 Data deletion

Data deletion shall be performed securely to prevent unauthorised access and data breaches. Obsolete or unnecessary data shall be deleted to comply with data retention policies and to optimise storage resources. The primary risks in data deletion include the following.

a) Incomplete deletion

IoT devices' data may not be completely erased when decommissioned or sold, leaving them vulnerable to recovery and misuse.

b) Data retention requirements

Legal and regulatory requirements may require IoT device manufacturers to retain data for specific periods, making it difficult to delete.

6.2 Internet of Things (IoT) data privacy risks and stakeholder responsibilities

The stakeholders are responsible and accountable for protecting the security and privacy of Personal data, including managing the related data privacy risks. The organisation shall conduct regular audits and assessments to monitor compliance with data protection laws and internal policies; assess privacy risks, conduct impact assessments, and implement risk mitigation strategies on personal data.

Personal data refers to detailed information that can directly identify an individual, such as a name, NRIC number, or passport number. It also refers to any information concerning a commercial transaction that directly or indirectly relates to an individual who can be identified from that information or other information held by the data controller. This includes information such as names, identification numbers, online identifiers, and encompasses any information that can be used to identify a natural person. Sensitive personal data includes information about health, physical or mental condition, religious beliefs, political opinions, criminal records, and biometric data.

Data privacy roles encompass various scopes and responsibilities depending on the organisation's size, industry, and regulatory environment. The following are the key data privacy roles and responsibilities of stakeholders.

6.2.1 Data subject

Data subjects have specific rights and responsibilities, including the right to be informed about data processing, access their data, correct inaccuracies, withdraw consent, prevent processing that causes damage or distress, and prevent processing for direct marketing, and the right to data portability that allows data subjects to transfer their data to another data controller.

Data subject shall be responsible for providing accurate information and cooperating with the data controller and the data processor when exercising their rights.

6.2.2 Data controller

Data controller processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor. The data controller also acts as the entity that determines the purposes for which and the means by which personal data is processed. The organisation act as a data controller when it decides "why" and "how" personal data is handled.

MCMC MTSFB TC G056:2025

The data controller collects excessive data, including sensitive personal information. The data controller shall ensure that all data collected is accurate and complete, and that the data collected is protected against potential misuse and harm. Data controller shall also ensure that data subjects' rights are primarily protected with adequate transparency or controls.

6.2.3 Data processor

Personal data processing means collecting, recording, holding, or storing the personal data or carrying out any operation or set of operations on the personal data, including:

- a) the organisation, adaptation, or alteration of personal data;
- b) the retrieval, consultation, or use of personal data;
- c) the disclosure of personal data by transmission, transfer, dissemination, or otherwise making available; or
- d) the alignment, combination, correction, erasure, or destruction of personal data;

The key roles and responsibilities of data controllers and data processors are as below.

- a) To secure the collected data storage. Cyberattacks can compromise stored data, leading to identity theft and financial loss. Prolonged data retention and weak security measures further increase the risk of unauthorised access and misuse of data, affecting data subjects.
- b) To secure the appropriate usage of collected data. Data may be used for unintended purposes, leading to biased decisions and discriminatory treatment. Additionally, a lack of transparency regarding data practices can erode trust and hinder informed consent to data subjects.
- c) To securely transfer data to third-party organisations. Sharing data with third-party organisations increases the risk of data breaches and misuse. Individuals may have limited control over how their data is transferred and used by third parties, especially when data is transferred across borders, ultimately affecting data subjects.
- d) To securely and completely delete personal data when it is no longer needed. Failure to completely erase personal data can lead to residual risks, such as unauthorised access or data recovery. Legal and regulatory requirements may necessitate the retention of data for specific periods, reducing the risk of breaches and misuse.

6.2.4 Stakeholder responsibilities

The organisation shall address privacy risks and ensure compliance with data protection regulations. By understanding the roles of key stakeholders and the related data privacy risks, the organisation should be able to implement effective measures to protect user data and build trust in IoT systems. The table below summarises the key stakeholders' responsibilities in relation to IoT data privacy risks within the data management lifecycle.

Table 2. Risk to personal data in IoT systems and stakeholder responsibility

Data lifecycle phase	Risk to personal data in the IoT system	Key stakeholder responsibilities		
		Data subject	Data controller	Data processor
Data collection	Excessive data collection	✓	✓	
	Sensitive data collection	✓	✓	
	Inaccurate/incomplete data	✓	✓	
Data storage	Data breaches	✓	✓	✓
	Data retention		✓	✓
	Insecure storage		✓	✓
Data usage	Data misuse		✓	✓
	Profiling and discrimination		✓	✓
	Lack of transparency		✓	✓
Data transfer	Data leakage		✓	✓
	Third-party risks		✓	✓
	Lack of control		✓	✓
	Cross-border data transfers		✓	✓
Data deletion	Incomplete deletion	✓	✓	✓
	Data retention requirements	✓	✓	✓

6.2.5 Additional responsibilities of stakeholders

As provided below, other stakeholders within the organisation shall also be responsible and accountable for protecting the security and privacy of Personal data, including managing related data privacy risks.

6.2.5.1 Data Protection Officer

The scope and responsibilities are as follows.

a) Strategic Oversight

Develop and implement personal data protection strategies, policies, and procedures aligned with regulatory requirements and organisational objectives.

b) Compliance Management

Ensure compliance with data protection laws (e.g., PDPA, GDPR) and industry standards through audits, assessments, and continuous monitoring.

MCMC MTSFB TC G056:2025

c) Risk Management

Conduct data protection impact assessments (DPIAs) to identify and mitigate personal data protection risks.

d) Education and Awareness

Educate employees on personal data protection best practices, provide training programs, and promote a culture of personal data protection within the organisation.

e) Incident Response

Develop and oversee incident response plans for personal data breaches, coordinate breach notifications, and liaise with regulatory authorities as required.

f) Stakeholder Engagement

Collaborate with legal, IT, compliance, and business units to integrate personal data protection considerations into business processes and new initiatives.

g) Regulatory Liaison

Serve as the point of contact with authorities and ensure communication regarding data processing activities.

h) Monitoring and Reporting

Monitor compliance with data protection laws, maintain records of processing activities, and report to DPAs as required.

6.2.5.2 Data Protection Counsel

The scope and responsibilities are as follows.

a) Legal Compliance

Interpret and apply data protection laws and regulations to ensure organisational compliance.

b) Contract Review

Review and negotiate privacy-related terms in contracts with vendors, customers, and partners.

c) Policy Development

Draft and update privacy policies, notices, and procedures in line with legal requirements and best practices.

d) Risk Assessment

Assess legal risks related to data privacy, advise on risk mitigation strategies, and support DPIAs

e) Litigation Support

Provide legal support in privacy-related litigation, investigations, or regulatory proceedings.

7. Governance and compliance requirements for Internet of Things (IoT) data protection

As IoT ecosystems expand, the organisation's compliance with data privacy governance and regulations will be increasingly complex. Data protection compliance and governance shall be undertaken in accordance with Act 709 and should also refer to ISO/IEC 27701 and NIST 8228.

Unlike traditional IT environments, IoT devices continuously collect and transmit data, often without user interaction. IoT devices operate in resource-constrained environments, which limits their ability to implement strong encryption or on-device processing. In addition, the IoT systems demand standardised privacy management tools to enforce privacy protection across multi-vendor ecosystems.

The IoT data privacy governance and compliance requirements should bridge the gap between legal privacy frameworks and IoT deployment, and provide a practical governance model for stakeholders, IoT device manufacturers, and regulators.

7.1 Data protection governance

The organisation shall implement robust data protection governance to ensure compliance with data protection laws and to build trust with users. A comprehensive data protection governance ensures that applicable laws and regulations are adhered to within the data management lifecycle. The governance should also involve assigning roles and responsibilities to key stakeholders in the organisation. The key elements of privacy governance shall include the following.

- a) Appoint Data Protection Officers (DPOs), conduct Data Protection Impact Assessments (DPIA), and enforce PDPA compliance
 - i) The data protection governance model involves assigning specific roles and responsibilities to ensure compliance with applicable laws. DPOs shall conduct DPIAs and enforce privacy-by-design principles for IoT devices, considering the unique data collection and processing capabilities of these devices. For example, a DPIA for a smart home device should assess risks associated with continuous data collection, such as voice recordings or video footage.
 - ii) DPOs shall enforce PDPA compliance by ensuring that IoT devices are designed and operated in a way that protects personal data. This includes monitoring data flows, ensuring the proper implementation of consent mechanisms, and implementing effective data protection measures.
 - iii) The organisation should work closely with IoT manufacturers and service providers to ensure that privacy-by-design principles are embedded in the development lifecycle of IoT devices. Additionally, DPOs should provide training to IoT development teams on data protection best practices and ensure that applicable policies are clearly communicated to end-users.
- b) Compliance Teams' accountabilities
 - i) Compliance teams shall be responsible for overseeing cross-border data transfers involving IoT devices and managing legal documentation. The team shall ensure that data collected by IoT devices (e.g., smart home devices, wearables) is transferred in compliance with PDPA and other relevant regulations. For example, if a smartwatch collects health data and sends it to a cloud server in another country, the compliance team shall ensure that the transfer is lawful and secure.
 - ii) The compliance team should manage legal documentation related to IoT data processing, including data processing agreements with third-party vendors and cloud service providers. The team should ensure that IoT devices are configured to comply with localisation requirements, especially when data is processed or stored in different jurisdictions.

MCMC MTSFB TC G056:2025

- iii) Compliance teams should regularly review and update data transfer policies to reflect changes in regulations or business practices.

7.2 Compliance and enforcement

The organisation shall ensure ongoing compliance with data protection regulations and maintain the integrity of IoT systems by implementing robust monitoring and enforcement mechanisms. The practices shall include detecting and responding to unauthorised access, conducting regular audits, and having a structured incident response management. These practices are essential for maintaining data protection and ensuring compliance with legal requirements. The organisation shall follow the following key components for effective compliance monitoring and enforcement.

a) Periodic privacy compliance audits with Act 709

- i) Organisations should conduct periodic privacy audits to ensure that IoT devices comply with regulatory requirements. These audits should include a review of data collection practices, consent mechanisms, and data retention policies.
- ii) Audits should also assess the effectiveness of data protection measures implemented on IoT systems. For example, an audit should test whether a smart home device is properly protecting data before transmitting it to the cloud. The results of these audits should be documented and used to improve data protection practices.

b) Incident response management

- i) IoT service providers should have a robust incident response framework in place to handle data breaches. As an example, if an IoT device is compromised, the provider should be able to quickly isolate the device, notify affected users, and report the breach to the relevant authorities within timelines mandated by Malaysian law, which could be referred to the related Data Breach Notification Circular and Data Breach Notification Guideline documents by Act 709.
- ii) The framework should also include procedures for updating IoT device firmware to address security vulnerabilities and prevent future breaches. In addition, regular incident response drills should be conducted to ensure the team is well-prepared to handle data breaches effectively. These drills should also include activities focused on identifying the root causes of incidents, enabling organisations to implement corrective and preventive measures to strengthen overall system resilience.

a) Compliance monitoring and data protection audits

- i) Effective compliance monitoring and enforcement are critical to safeguard personal data. By conducting regular data protection audits and implementing a comprehensive incident response management, the organisation shall proactively identify risks, ensure adherence to legal and regulatory obligations, and respond swiftly to any breaches. These measures not only help in protecting sensitive user data but also enhance user trust and reinforce the organisation's commitment to responsible data protection.

7.3 Risk management for Internet of Things (IoT) data protection

The organisation shall conduct a risk analysis to understand the associated data protection risks in IoT systems. This risk analysis should be aligned with ISO/IEC 31000, which provides a guide for assessing and evaluating risks associated with IoT systems. The stakeholder shall address data protection risks as they arise throughout the data management lifecycle, based on the following guidance.

- a) Risk identification and classification pertaining to IoT devices, IoT applications and IoT cloud platforms and capabilities with clear mitigation measures.

- b) Policy framework for IoT operations by service provider and stakeholder organisation.
- c) Mitigation framework and processes.
- d) Management review and compliance.

7.4 Understand risk considerations and mitigation

The organisation shall fully understand the risk considerations and mitigation strategies for IoT devices. The following steps are essential in addressing data protection risks, considerations, and mitigation.

- a) Identify and assess the specific data protection risks associated with the IoT system.
- b) Consider the potential likelihood and impact of the personal data protection risks.
- c) Analyse and evaluate the outcome, followed by assessing the effective mitigation strategies.

7.5 Risk treatment

Decisions on risk treatment are based on the overall risk rating and may consider the cost of remediation. The following options should be used for risk treatment.

- a) Risk reduction
 - i) Implement suitable data protection technologies and processes.
 - ii) Having the data controllers and data processors propose minimum solutions that reduce the risks.
 - iii) The data controllers and data processors shall justify the residual risk which do not have mitigation.
- b) Enterprise risk management practices to reduce the likelihood and/or impact of the risks.
- b) Risk retention or acceptance
 - i) The data subjects may decide to tolerate the risk item after further consideration and/or clarification by the data controller.
- c) Risk avoidance
 - i) Avoid collecting sensitive data unless necessary for the device's functionality.
 - ii) The data subjects decide the risk is not acceptable.
- d) Risk transfer
 - i) Risk transfer shall be executed by means of Service Level Agreements (SLAs) and warranties between the data controller and the data processor.

7.6 Monitoring and review

The organisation shall conduct regular audits to monitor and assess the effectiveness of data protection controls. The audits should include vulnerability scans, penetration testing, and reviews of access logs. The audit information should be made available to compare data privacy risk levels for each data controller and determine whether they meet the data subjects' risk tolerance thresholds. This information shall be shared with management and stakeholders to refine risk criteria, risk assessments,

MCMC MTSFB TC G056:2025

and risk treatment, and to consider cost-benefit analysis, organisational constraints, business priorities, and other relevant factors.

7.7 Recording and reporting risk

The organisation shall record and report the risk management plan and the risk management audit reports to obtain management approval within the decision-making context of the organisation. This involves presenting the results that will ensure effective management of IoT data protection, governance, and compliance.

8. Internet of Things (IoT) systems data protection controls requirements

The data protection controls requirements of the IoT systems shall be within the context of the seven principles of Act 709 to ensure responsible and ethical handling of personal data in IoT systems. The organisation shall be guided by the seven principles to safeguard data privacy and to build trust among the stakeholders.

8.1 General controls

The organisation shall integrate data protection considerations into the design and architecture of IoT systems, including the following.

- a) Proactive, not reactive: Anticipate and prevent privacy issues before they occur, rather than reacting to them after the fact.

The organisation should manage data protection policies for IoT devices, ensuring that data collected by these devices is protected both at rest and in transit. As an example, a smart doorbell camera should encrypt video footage before storing it locally or transmitting it to the cloud.

- b) Data protection as the default setting: Build systems and practices that protect privacy by default, requiring no action from the user.

Data processors and data controllers should ensure IoT systems are capable of receiving firmware updates to address emerging data protection vulnerabilities. Regular updates should be provided to patch vulnerabilities and improve device protection capabilities.

- c) Data protection embedded into design: Integrate privacy considerations into the design and architecture of systems and processes from the start.

The organisation shall implement data protection-by-design principles, ensuring that privacy considerations are integrated into the design and functionality of IoT systems from the beginning. For example, a smart thermostat should be designed to collect only the minimum amount of data necessary to function, such as temperature settings, rather than unnecessary details like user location.

- d) Full functionality: Positive-sum, not zero-sum, to ensure that data protections do not compromise the functionality or usability of a system or service.
- e) Visibility and transparency: Be open and transparent about data collection, processing, and sharing practices.
- f) Respect for user privacy: Prioritise user data protection and empower users to make informed choices about their data.

8.2 Notice and choice controls

Data controller shall inform data subjects in writing about the purpose for which personal data is collected, how it will be used, and the choices they have regarding the processing of their data. Personal data cannot be processed without the data subject's consent, unless the processing is necessary for a specific purpose, such as fulfilling legal obligations or protecting vital interests.

The data subject consent and transparency are essential to ensure that users retain control over their personal data when interacting with IoT systems. The notice and choice principles should foster trust between data subjects and data controllers by providing data subjects with clear, accessible, and effective ways to manage data collected, stored, and shared by their IoT devices.

Service providers and manufacturers, as data controllers, shall comply with the following controls, which are crucial for achieving consent and transparency in IoT systems.

- a) Granular opt-in/out settings: user control over specific data types.
 - i) IoT systems should provide data subjects with granular control over the types of data they collect. For example, data subjects should be able to opt in or opt out of specific data collection features, such as location tracking, voice recording, or health monitoring. This is particularly important for IoT devices such as smart speakers, wearables, and home security systems, where data subjects may want to control what data is collected and how it is shared.
 - ii) Granular settings should be easy to access and configure, either through the device itself (user interface) or through a companion mobile application or web application in the cloud. For example, a fitness tracker should enable data subjects to choose whether to share their heart rate data with third-party applications.
 - iii) Data subjects should also be able to change their preferences at any time, and these changes should take effect immediately.
- b) Multi-layered consent notifications (QR code disclosures, voice-assisted privacy settings, etc.)
 - i) The organisation shall provide clear and accessible consent mechanisms tailored to the IoT devices' capabilities. For devices with limited interfaces (e.g., no screens), consent may be obtained through companion mobile applications or web-based interfaces during the initial setup process. For example, a smart thermostat should guide data subjects through a step-by-step consent process on a paired smartphone application, explaining what data is collected and how it will be used.
 - ii) For devices with voice capabilities (e.g., smart speakers), voice-assisted privacy settings can be used to explain data collection practices and obtain data subject consent in an interactive manner. For example, a smart speaker could ask the data subject, "Would you like to enable voice recording for personalised responses?" and provide a clear explanation of how the data will be used.
 - iii) QR codes on device packaging or user manuals should link to detailed privacy disclosures for data subjects who want more information. The organisation shall ensure that consent remains multi-layered but is implemented in a manner that is feasible for resource-constrained IoT devices.
- c) Real-time privacy dashboards (data subjects can view, modify, or delete collected IoT data)
 - i) The organisation shall ensure that the IoT devices offer real-time privacy dashboards that allow data subjects to view, modify, or delete the data collected by the devices. For example, a smart home hub should provide a dashboard that allows users to view the data being collected by each connected device and manage their privacy settings accordingly.

MCMC MTSFB TC G056:2025

- ii) The IoT systems dashboards should be accessible via mobile applications or web interfaces, ensuring that data subjects should be able to manage their privacy settings remotely. For example, a data subject should be able to log into a mobile application to view the data collected from a smart security camera and delete any footage that is no longer needed.
- iii) The IoT systems dashboards should also provide transparency reports, showing data subjects how their data is being used and shared with third parties. This helps build trust and ensures that data subjects are fully informed about their privacy.

8.3 Disclosure controls

Data controllers shall not disclose a data subject's personal information without their consent, except in specific circumstances, such as when required by law or to protect public safety.

8.4 Security controls

Data controllers shall take reasonable security measures to protect personal data from unauthorised or unlawful access, loss, misuse, or disclosure.

The IoT security controls and guidance should be in accordance with Technical Codes MCMC MTSFB TC G013, MCMC MTSFB TC G031 and MCMC MTSFB TC G045.

8.5 Data minimisation and retention controls

The organisation should ensure that IoT devices only collect, retain, and process the minimum amount of data necessary to perform their intended functions. Personal data should only be retained for as long as necessary to fulfil the purpose for which it was collected and should be destroyed or anonymised when no longer needed.

The data minimisation and retention controls should help the organisation mitigate the risks of unnecessary data retention and improve privacy protection. The following practices are essential for effective data minimisation and retention controls in IoT systems.

- a) Automated data deletion after the retention period expires.
 - i) The organisation's IoT devices should be configured to automatically delete data after the maximum retention period specified by the PDPA or other applicable regulations requirements. For example, a smart doorbell camera should automatically delete video footage after 30 days unless the user explicitly chooses to retain it for a longer period.
 - ii) Data subject should have the option to manually delete data before the retention period expires if they no longer need it. There is no need to specify a minimum retention period, as the focus is on ensuring that data is not retained longer than necessary.
 - iii) The organisation's IoT devices should provide clear notifications to data subjects when data is nearing the end of its retention period, giving them the opportunity to extend retention if needed.
- b) Delete metadata to prevent tracking after data deletion.
 - i) The organisation's IoT devices should delete the associated metadata to prevent tracking after data deletion. For example, metadata associated with IoT data (e.g., timestamps, device IDs) should be automatically erased once the data is deleted.
 - ii) The organisation shall ensure that IoT devices' metadata is deleted to provide stronger data protection and reduce the risk of data being reconstructed or misused after deletion, and this is

particularly important for IoT devices that collect sensitive data, such as health monitors or location trackers.

c) Deletion upon the data subject's request

- i) The organisation's IoT devices and services should enable data subject-initiated data deletion. This control should be visible at pertinent instances in the device and service lifecycle, for instance, at device reset and service termination.

8.6 Data integrity controls

Data controllers shall ensure that personal data is accurate, complete, and kept up-to-date, and that it is not misleading.

8.7 Access controls

Data subjects have the right to access their personal data held by a data controller and to request corrections if the data is inaccurate, incomplete, or misleading. The organisation shall ensure that data subjects have the right to access their personal data and sensitive personal data as regulated under Act 709.

Bibliography

- [1] MCMC MTSFB TC G013, *Internet of Things - Security Management*
- [2] MCMC MTSFB TC G017, *Information Network Security - Cloud Service Provider Selection (First Revision)*
- [3] MCMC MTSFB TC G031, *Internet of Things - Application Security Requirements*
- [4] MCMC MTSFB TC G045, *Internet of Things - Device Security Requirements*
- [5] ISO/IEC 27001:2022, *Information security, cybersecurity, and privacy protection – Information security management systems – Requirements*
- [6] ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [7] ISO/IEC 27018:2019, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [8] ISO/IEC 27400:2022, *Cybersecurity – IoT security and privacy – Guidelines*
- [9] ISO/IEC 27402:2023, *Cybersecurity – IoT security and privacy – Device baseline requirements*
- [10] ISO/IEC 27701:2025, *Information security, cybersecurity, and privacy protection - Privacy information management systems - Requirements and guidance*
- [11] ISO/IEC 29100:2024, *Information technology - Security techniques - Privacy framework*
- [12] ISO/IEC 31700-1:2023, *Consumer protection - Privacy by design for consumer goods and services*
- [13] NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

Acknowledgements

Members of IMT-2020, IoT and ITS Security Sub-Working Group

Sub-Working Group Leaders

Assoc Prof Dr Ahmad Shahrafidz Khalid (Chair)	Universiti Kuala Lumpur
Mr Hasyimi Shaharuddin (Vice Chair)	TM Technology Services Sdn Bhd

Drafting Committee Members

Assoc. Prof. Dr Ahmad Shahrafidz Khalid (Draft lead)	Universiti Kuala Lumpur
Ms Alisa Rafiqah Adenan (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Ng Kang Siong	Digital Connect Society
Mr Thaib Mustafa	Smart Tech AP Sdn Bhd
Mr Muhammad Azmin Mohamed Ghazali	Universiti Kuala Lumpur
<i>Mr Alwyn Goh</i>	<i>Goople Tech Sdn Bhd</i>

Contributors

Mr Ahmad Dahari bin Jarno	CyberSecurity Malaysia
Mr Ahmad Syuhaidi Mohd Rozi	CyberSecurity Malaysia
Ms Mayasarah Maslizan	CyberSecurity Malaysia
Ms Norkhadhra Nawawi	FNS (M) Sdn Bhd
Ms Noor Emy Zuraina Baharudin	SIRIM Berhad
Ms Nur Hidayah Ibrahim	SIRIM Berhad
Prof. Dr. Shahrulniza Musa	Universiti Kuala Lumpur
Mr Azlan Mohamed Ghazali	<i>Deloitte Malaysia</i>
<i>Mr Goh Ser Yoong</i>	<i>Advance.AI</i>
<i>Mr Yuwanthiran Sukalingam</i>	<i>Mindvalley, Inc.</i>
<i>Datuk Syahril Aziz</i>	<i>Secure Insight Sdn Bhd</i>