# TECHNICAL CODE

## INTERNET OF THINGS (IOT) - PRIVACY REQUIREMENTS



**Developed by**

**Registered by**

Registered date:

## 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

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

CyberSecurity Malaysia

Deloitte Malaysia

Digital Connect Society

Goopletech

Sirim QAS International Sdn Bhd

Universiti Kuala Lumpur

## 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 AI driven analytics. It is crucial to establish robust privacy frameworks to safeguard individual rights and protect sensitive 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 responsibly and ethically.

This Technical Code supports the foundation laid by existing technical codes. These following codes provide a comprehensive framework for IoT security:

a) MCMC MTFSB TC G013: Internet of Things – Security Management that 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: Internet of Things – Application Security Requirements that outline the requirements for IoT application security that covers everything from security measures to the threat landscapes and IoT application security best practices.

c) MCMC MTSFB TC G045: Internet of Things - Device Security Requirements that defines the IoT device security requirements for IoT devices and gateways. Focusing on authentication, cryptography, data security, device platform security, and physical security.

This Technical Code complements the IoT Application Security and IoT Device Security frameworks by focusing on the following elements:

a) Privacy governance and compliance monitoring;

b) User consent and data minimisation principles;

c) Privacy-Enhancing Technologies (PETs) for IoT; and

d) Cross-border data transfers and risk management.

This Technical Code also defines privacy governance requirements for IoT systems that process Personally Identifiable Information (PII), biometric data, health data, geolocation data, and multimedia content (video, photos, audio recordings). These categories require strict privacy controls with reference to:

a) PDPA 2024 (Malaysia) – Personal Data Protection Act;

b) GDPR (EU) – General Data Protection Regulation;

c) ISO/IEC 27701 – Privacy Information Management Systems;

d) ISO/IEC 27400 – IoT Security & Privacy Guidelines; and

e) NISTIR 8228 - Considerations for Managing IoT Cybersecurity and Privacy Risks.

## 1. Scope

This Technical Code is dedicated to establishing a comprehensive framework that ensures the protection of PII and other sensitive data within the IoT ecosystem. PII may have a combination of the following information:

a) device identifiers;

b) user accounts;

c) MAC addresses;

d) biometric data;

e) health data;

f) geolocation data; and/or

g) multimedia data.

Any data which allows for association with or deduction of identity shall be considered to be PII.

By prioritising privacy-by-design principles, this Technical Code aims to integrate privacy considerations into the design and development of IoT devices and systems from the outset. This includes limiting the collection and retention of personal data to what is necessary for the intended purpose.

This Technical Code applies to IoT deployments such as the following:

a) Smart healthcare

   Wearable health devices, remote patient monitoring.

b) Smart cities and surveillance

   CCTV analytics, automated law enforcement.

c) Consumer IoT and smart homes

   Smart assistants, connected security cameras.

d) Industrial IoT (IIoT)

   Employee tracking, factory automation.

To safeguard data, the Technical Code will promote the implementation of robust data privacy measures such as encryption, anonymisation, data minimisation, etc. Regular risk assessment will be essential to identify and address potential privacy risks. Additionally, the Technical Code will advocate for transparency and accountability by requiring clear and transparent data practices, including privacy notices, privacy policies, and user consent mechanisms.

By connecting key stakeholders in the IoT ecosystem, including consumers, manufacturers and service providers, the Technical Code will facilitate collaboration and establish industry-specific guidelines and best practices. This collaborative approach will ensure that IoT devices and systems are developed and operated in a manner that respects individual privacy and complies with relevant data protection laws.

## 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.

Act A1727 *Personal Data Protection (Amendment) Act 2024*

## 3. Abbreviations

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

| | |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CIA | Confidentiality, Integrity and Availability |
| GDPR | General Data Protection Regulation |
| IT | Information Technology |
| IoT | Internet of Things |
| MFA | Multi-Factor Authentication |
| OS | Operating System |
| PDPA | Personal Data Protection Act |
| PII | Personally Identifiable Information |
| RBAC | Role-Based Access Control |
| SLA | Service Level Agreement |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| UI | User Interface |

## 4. Terms and definitions

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

### 4.1 Anonymisation

Anonymisation irreversibly removes all identifying information, making it impossible to re-identify individuals. Anonymisation is preferred for data that needs to be shared publicly without privacy concerns.

### 4.2 Data minimisation

Data minimisation is the 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 if a data breach occurs.

### 4.3 Data privacy

Data privacy refers to the 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.

### 4.4 Data security

Data security is a comprehensive 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.

### 4.5 Differential privacy

A mathematical technique that allows for the release of statistical information about a dataset while protecting the privacy of individual data points. It achieves this by adding noise to the data, making it difficult to determine whether a specific individual's data was included in the dataset or not. This ensures that the privacy of individuals is preserved, even when analysing large datasets.

### 4.6 Internet of Things (IoT)

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

IoT devices are different from conventional IT devices, they are generally able to sense, affect and interact with the physical world. It cannot be accessed, managed or monitored due to their packaging as black box systems without the conventional control interfaces. Furthermore, it lacks detailed explanation and assurance with regards to their security, privacy attributes.

### 4.7 Personal data

Refers to any information which can identify a person such as name, identification number, address, contact info, biometric data, etc.

### 4.8 Pseudonymisation

Pseudonymisation replaces personal identifiers with pseudonyms, making it difficult but not impossible to re-identify individuals with additional information. Pseudonymisation is often used for research purposes.

### 4.9 Personally Identifiable Information (PII)

Refers to any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other linked or linkable data. This includes direct identifiers such as name, id number, biometric records, and indirect identifiers such as date and place of birth, financial, medical, educational, and employment information.

### 4.10 Sensitive personal data

Refers to any personal data that could cause harm to the individual if leaked or misused such as race, religion, physical or mental health, political opinion, etc.

### 4.11 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 subject have

control over their personal information. Consent should be freely given, specific, informed, and unambiguous.

## 5. Overview

This chapter outlines the key stakeholders in the IoT ecosystem and their respective roles in ensuring data privacy. Understanding these roles is essential for implementing effective privacy measures and fostering collaboration across the IoT value chain. Table 1 describes the IoT key stakeholders.

**Table 1: IoT Key Stakeholders**

| IoT Key Stakeholders | Descriptions |
|---|---|
| Consumers | End users that use or interact with IoT devices and IoT systems. |
| Manufacturers | Entities that design, develop, and produce IoT devices and systems. |
| Service Providers | Organisations that operate, maintain, and deploy IoT devices and systems. |

Table 2 outlines the key stakeholders involved in IoT data privacy and their respective roles, as well as their relationship to IoT application and device security. It highlights the different parties who play a significant role in ensuring that IoT devices and applications obey data privacy standards while maintaining security, ensuring safe and reliable use of IoT technology.

**Table 2: Stakeholders role in IoT application and device security**

| Stakeholder | Role in IoT Data Privacy | Relation to IoT application and device security |
|---|---|---|
| Data Protection Officers (DPOs) | Ensure compliance with Personal Data Protection Act (PDPA), GDPR, ISO 27701. Conduct Privacy Impact Assessments (PIAs) and enforce privacy-by-design policies. | Work with IoT security teams to ensure encryption, access controls, and secure data storage align with compliance requirements. |
| Compliance and legal teams | Oversee cross-border data transfers, privacy policies, and third-party data processing agreements. Ensure IoT deployments follow data sovereignty laws. | Collaborate with IoT security teams on legal frameworks for data retention, breach notification, and regulatory compliance. |
| IoT service providers and platform operators | Implement privacy-by-design for IoT cloud platforms, ensuring secure user data processing and anonymisation. | Align with IoT Application Security to protect API access, cloud storage security, and threat monitoring. |
| IoT device manufacturers | Integrate privacy-enhancing technologies (PETs) (e.g., on-device encryption, data minimisation, anonymisation) into IoT devices. | Follow IoT Device Security best practices (e.g., firmware security, secure boot, and hardware root of trust). |

**Table 3: Stakeholders role in IoT application and device security** *(continued)*

| Stakeholder | Role in IoT Data Privacy | Relation to IoT application and device security |
|---|---|---|
| IoT application developers | Design applications that support user consent, data minimisation, and secure data-sharing protocols. Implement privacy-by-default settings. | Align with IoT Application Security for secure coding practices, API security, and Role-Based Access Controls (RBAC). |
| Enterprise IoT & Industrial IoT (IIoT) deployers | Manage privacy risks in industrial environments, smart cities, healthcare, and logistics IoT deployments. | Work with IoT security teams to implement data protection mechanisms and network segmentation. |
| Regulatory bodies and data protection authorities | Enforce PDPA and sector-specific IoT privacy guidelines. Certify privacy-compliant IoT deployments. | Collaborate with cybersecurity agencies to verify IoT infrastructure compliance with encryption, secure storage, and device authentication. |
| End users & consumers | Control how their personal data is collected, stored, and shared via privacy dashboards and consent settings. | Expected to follow IoT security best practices, such as firmware updates, strong passwords, and device access management. |

In the complicated landscape of the IoT, various stakeholders play crucial roles, each with distinct responsibilities related to personal data protection.

a) **Consumers** are the primary **Data Subjects** in the IoT ecosystem. Their personal data, often generated by IoT devices, is collected and processed by various entities.

b) **Manufacturers** of IoT devices frequently act as **Data Controllers**. They determine the purpose and means of processing personal data collected from consumers. This includes data collected during device setup, usage, and maintenance.

c) **Service Providers** often assume the role of **Data Processors**. They process personal data on behalf of Data Controllers, such as storing, analysing, or transmitting data. This includes cloud service providers, data analytics companies, and network operators.

It is important to note that the specific roles of each stakeholder can vary depending on the nature of the IoT application and the data being processed. Therefore, a careful analysis of each scenario is necessary to accurately determine the mapping of roles under the PDPA.

To ensure responsible and ethical handling of personal data in the IoT ecosystem, organisations must adhere to the seven (7) principles of the PDPA. This includes obtaining explicit consent, minimising data collection, implementing robust security measures, and respecting data subject rights. By understanding these mappings and adhering to the principles of the PDPA, organisations involved in the IoT ecosystem can safeguard privacy and build trust with consumers.

Having identified the key stakeholders and their roles, the next chapter delves into the specific data privacy risks associated with IoT systems throughout their lifecycle.

## 6. Internet of Things (IoT) data privacy risks

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 data privacy risks, especially due to its interface between digital and physical domains with respect to sensor and actuation capabilities, encompassing the following.

a) Network-layer connectivity

Inclusive of both Internet and local connectivity.

b) App-layer connectivity

For data collection and processing, and device control. App interactivity might take the form of IoT-associated apps deemed to be official or Application Programming Interface (API), as possibly unpublished.

c) Human-to-device interactivity through the device User Interface (UI)

To browse device internal state and assert settings.

As IoT devices proliferate, they collect and transmit vast amounts of personal and sensitive data, making it essential to address the potential vulnerabilities and safeguard user privacy.

Since security concerns are already addressed in previously published MCMC TC documents as mentioned in Section 1. Figure 1 delves into the key data privacy risks associated with the IoT ecosystem, focusing on the critical phases of data lifecycle such as collection, storage, usage, transfer, and deletion. By understanding these risks, an effective measure can be implemented to protect user privacy and build a secure IoT environment.

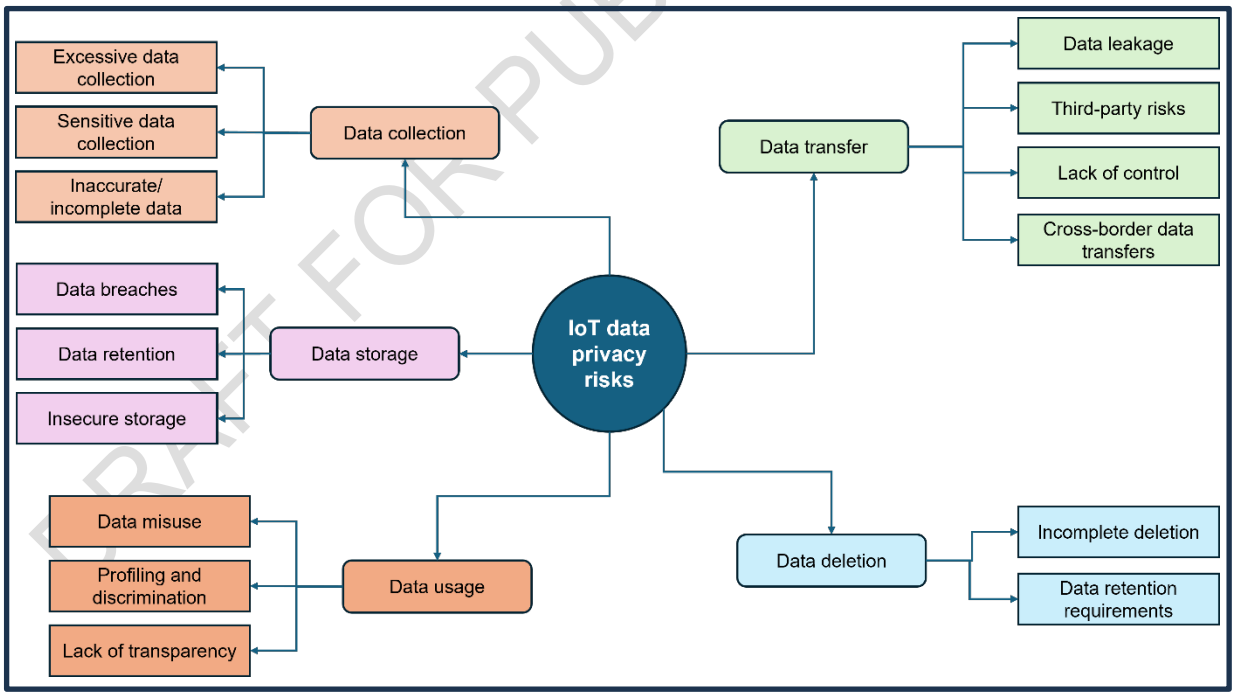


**Figure 1: Overview of IoT Data Privacy Risks**

### 6.1 Internet of Things (IoT) data privacy risks throughout its lifecycle

The data lifecycle in IoT ecosystems involves a series of stages, from data collection to its eventual deletion. Each stage is crucial for extracting value from the massive amounts of personal data

generated by IoT devices. However, this very data abundance makes IoT systems a prime target for cyberattacks.

### 6.1.1 Data collection

IoT devices, such as sensors, cameras, and wearables, collect data on physical parameters like temperature, humidity, motion, and location. This data is collected at high frequency and in large volumes, forming the foundation for subsequent analysis and decision-making. The following are key concerns regarding the collection of data for IoT devices.

a) Excessive data collection

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

b) Sensitive data collection

IoT devices may collect sensitive data such as 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. These systems must be scalable and reliable to handle the increasing volume and diversity of IoT data. The concerns for data storage includes the following.

a) Data breaches

IoT devices often store data on local storage or in the cloud. If these devices are not adequately secured, they can become targets for hackers, leading to data breaches.

b) Data retention

IoT devices may store data for extended periods, increasing the risk of unauthorised access and misuse.

c) Insecure storage

Many IoT devices have weak security measures, making them vulnerable to attacks. This can include insecure default passwords, lack of encryption, and outdated software.

### 6.1.3 Data usage

The insights derived from data analysis are utilised to optimise operations, improve decision-making, and develop innovative solutions. IoT data can be used for predictive maintenance, personalised experiences, supply chain optimisation, and many other applications. However, how this data is utilised raises several concerns such as the following.

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 arise during the transfer of data across IoT devices, such as following.

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

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

a) Incomplete deletion

IoT devices may not completely erase data when they are decommissioned or sold, leaving it vulnerable to recovery and misuse.

b) Data retention requirements

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

### 6.2 Mapping of Internet of Things (IoT) data privacy risks against key stakeholders

Table 3 provides a breakdown of the potential IoT data privacy risks associated with its lifecycle and the key stakeholders involved. It highlights the responsibilities of manufacturers, service providers, and consumers in mitigating these risks. By understanding these responsibilities, stakeholders can take targeted actions to address privacy risks and ensure compliance with data protection regulations.

**Table 4: IoT Data Privacy Risks vs Key Stakeholders**

| Data Lifecycle | IoT Data Privacy Risks | Responsible | | |
|---|---|---|---|---|
| | | Consumers | Manufacturers | Service Providers |
| 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 | | ✔ | ✔ |

#### 6.2.1 Data collection

Manufacturers and service providers often collect excessive data, including sensitive personal information. This data may be inaccurate or incomplete, leading to potential misuse and harm. Consumers are primarily affected by these risks, as their data is being collected without adequate transparency or control.

#### 6.2.2 Data storage

Manufacturers and service providers are responsible for securely storing collected data. 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 consumers.

#### 6.2.3 Data usage

Manufacturers and service providers are responsible for 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 consumers.

#### 6.2.4 Data transfer

Manufacturers and service providers often 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 consumers.

#### 6.2.5 Data deletion

Manufacturers and service providers are responsible for the complete deletion of 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.

By understanding the roles of each stakeholder and the specific privacy risks they face, organisations can implement effective measures to protect user data and build trust in IoT technologies.

## 7. Internet of Things (IoT) risk management

Manufacturers and service providers shall address data privacy risks as arises throughout the lifecycle, based on the following.

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

b) Policy framework for IoT operations by service provider (SP) organisation, as subject to adjustment.

c) Mitigation framework and processes, as similarly subject to adjustment.

To enable the use of IoT that properly addresses data privacy risks, the key stakeholders shall perform a risk management approach towards understanding associated data privacy risk to the IoT devices.

The overall risk management process is not expected to be a waterfall process and should be aligned with the ISO 31000, Risk Management, which provides a guide to assess and evaluate the risk. An effective risk management involves in identifying potential privacy risks, assessing their impact, and implementing measures to mitigate them. This process should be iterative, with regular monitoring and review to ensure ongoing compliance.

At minimum, the risk assessment process shall be carried out as follows.

### 7.1 Understand risk considerations and mitigation

It is crucial in understanding risk considerations and mitigation strategies for IoT devices. The following steps are essential in addressing data privacy risks.

a) Identify and assess the specific data privacy risks associated with your IoT devices may impact the CIA.

b) Consider the potential likelihood and impact of the risks on individuals and organisations.

c) Analyse and evaluate the outcome followed by assessing the effective mitigation strategies.

### 7.2 Risk treatment

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

a) Risk reduction

   i) Implement encryption for data at rest and in transit to reduce the risk of data breaches.

   ii) Having the service providers to propose minimum solutions that reduces the risks.

   iii) The service providers successfully justify why the risk is irrelevant.

   iv) Enterprise risk management practices to reduce probability and/or impact of the risks.

   v) Plan for failures by defining failure countermeasures to reduce the risks.

b) Risk retention or acceptance

   The consumers may decide to tolerate the risk item after further consideration and/or clarification by the service providers.

c) Risk avoidance

   i) Avoid collecting sensitive data unless absolutely necessary for the device's functionality.

   ii) The consumers decide the risk is not acceptable.

d) Risk transfer

   Service Level Agreements (SLAs) and warranties that transfer the risks to the Operator or Manufacturer.

### 7.3 Monitoring and review

At this stage, information should be available to help to compare the data privacy risks levels for each of the service providers and determine if they meet the consumers risk tolerance thresholds. This information shall be shared with the decision-makers and the other stakeholders, and further deliberation on refining the risk criteria, risk assessments, risk treatment which now may take into account cost-benefit analysis, organisational constraints, business priorities and others. Regular audits should be conducted to assess the effectiveness of privacy controls. These audits should include vulnerability scans, penetration testing, and reviews of access logs.

### 7.4 Recording and reporting risk

The objective is to obtain approval within the decision-making context of the enterprise. This involves presenting the results that will help make the final decision about the selection of the service providers or manufacturers.

Having established risk management framework, the next chapter outlines the specific data privacy controls that can be implemented to mitigate these risks.

## 8. Relevant data privacy controls in Internet of Things (IoT) system

Data privacy risks arise at every stage of the data lifecycle-collection, storage, usage, transfer and delete, ensuring they comply with relevant applicable laws and respect users' rights to data privacy. Addressing these risks requires a proactive and holistic approach that includes robust security and privacy measures, transparent user consent mechanisms, and strict adherence to data privacy regulations. This includes the following.

a) Provide clear and concise consent management tools

   i) Informed Consent

      Obtain explicit and informed consent from consumers for data collection and processing.

   ii) Transparency

      Clearly communicate the purpose of data collection and how it will be used.

   iii) Revocation of Consent

      Allow consumers to revoke their consent at any time.

b) Collect, store, and process only the minimum amount of data necessary.

   i) Purpose Limitation

      Collect only the necessary data for the intended purpose.

   ii) Storage Limitation

      Retain data only for the required duration.

   iii) Access Control

      Implement strict access controls to limit who can access and process the data.

c) Integrate privacy considerations into the design and architecture of IoT systems from the start. This includes the following.

   i) Proactive not Reactive

      Anticipate and prevent privacy issues before they occur, rather than reacting to them after the fact.

   ii) Privacy as the Default Setting

      Build systems and practices that protect privacy by default, requiring no action from the user.

iii) Privacy Embedded into Design

Integrate privacy considerations into the design and architecture of systems and processes from the start.

iv) Full Functionality

Positive-Sum, not Zero-Sum to ensure that privacy protections do not compromise the functionality or usability of a system or service.

v) End-to-End Security

Full Lifecycle Protection to protect data throughout its entire lifecycle, from collection to deletion.

vi) Visibility and Transparency

Be open and transparent about data collection, processing, and sharing practices.

vii) Respect for User Privacy

Prioritise user privacy and empower users to make informed choices about their data.

d) Adhere to the seven (7) PDPA principles as stated in Annex A and any relevant data privacy regulations.

e) Conduct regular security and privacy audits including risk assessments to identify and address the gaps.

f) Train employees on data protection best practices and incident response procedures.

By implementing these data privacy controls, the IoT ecosystem can significantly mitigate the risks outlined in the table and foster a more secure and privacy-respecting environment for users. At minimum, the controls defined in Annex B shall be considered. The next chapter explores the governance and compliance framework necessary to ensure ongoing privacy protection.

# 9. Internet of Things (IoT) privacy governance and Personal Data Protection Act (PDPA) compliance framework

As IoT ecosystems expand, ensuring compliance with privacy laws (PDPA, GDPR, ISO 27701) is becoming increasingly complex. Unlike traditional IT environments, IoT devices continuously collect & transmit data, often without user interaction. It operates in resource-constrained environments, limiting their ability to implement strong encryption or on-device processing. It lacks standardised privacy management tools, making enforcement difficult across multi-vendor ecosystems.

This chapter bridges the gap between legal privacy frameworks and real-world IoT deployment challenges, providing a practical governance model for IoT device manufacturers, service providers, and regulators.

## 9.1 Privacy Governance Model

A comprehensive privacy governance model ensures that privacy laws and regulations are adhered to when managing data collected by IoT devices. This model involves assigning roles and responsibilities to key stakeholders to protect users' privacy, particularly in the context of IoT data collection, processing, and storage. Key elements of this model includes the following.

a) Data Protection Officers (DPOs): Conduct PIAs, enforce PDPA compliance.

The privacy governance model involves assigning specific roles and responsibilities to ensure compliance with privacy laws. Data Protection Officers (DPOs) play a key role in conducting Privacy Impact Assessments (PIAs) and enforcing privacy-by-design principles for IoT devices, considering the unique data collection and processing capabilities of these devices. As an example, a PIA for a smart home device should assess risks related to continuous data collection, such as voice recordings or video footage.

DPOs should enforce PDPA compliance by ensuring that IoT devices are designed and operated in a way that respects user privacy. This includes monitoring data flows, ensuring proper consent mechanisms, and implementing data protection measures.

They should also 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 privacy best practices and ensure that privacy policies are clearly communicated to end-users.

b) Compliance Teams: Oversee cross-border data transfers, legal documentation.

Compliance teams are responsible for overseeing cross-border data transfers involving IoT devices. They must ensure that data collected by IoT devices (e.g., smart home devices, wearables) is transferred in compliance with PDPA and other relevant regulations. As an example, if a smartwatch collects health data and sends it to a cloud server in another country, the compliance team must ensure that the transfer is lawful and secure. This can be achieved by implementing end-to-end encryption and ensuring that data is stored in jurisdictions with adequate privacy protections.

These teams should also manage legal documentation related to IoT data processing, including data processing agreements with third-party vendors and cloud service providers. They should ensure that IoT devices are configured to comply with localisation requirements, especially when data is processed or stored in different jurisdictions.

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

c) IoT Service Providers: Implement privacy-by-design, manage encryption policies.

IoT service providers must implement privacy-by-design principles, ensuring that privacy considerations are integrated into the design and functionality of IoT devices from the outset. 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.

They should manage encryption policies for IoT devices, ensuring that data collected by these devices is encrypted 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.

Service providers should also ensure that IoT devices are capable of receiving firmware updates to address emerging privacy and security vulnerabilities. Regular updates should be provided to patch vulnerabilities and improve device security.

By implementing a robust privacy governance framework, stakeholders can ensure ongoing compliance with privacy laws and build trust with users. The following annexes provide additional guidance on compliance with PDPA principles and recommended security countermeasures.

### 9.2 Consent & Transparency

Consent and transparency are essential to ensuring that users retain control over their personal data when interacting with IoT devices. These principles help build trust between users and service providers by giving users clear, accessible, and effective ways to manage the data being collected, stored, and shared by their devices. The following components are crucial to achieving consent and transparency in IoT systems.

a) Granular opt-in/out settings: User control over specific data types.

IoT devices should provide users with granular control over the types of data they collect. For example, users 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 like smart speakers, wearables, and home security systems, where users may want to control what data is collected and shared.

Granular settings should be easy to access and configure, either through the device itself (if it has a user interface) or through a companion mobile app. As an example, a fitness tracker should allow users to choose whether to share their heart rate data with third-party apps.

Users 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.

IoT devices should provide clear and accessible consent mechanisms tailored to their capabilities. For devices with limited interfaces (e.g., no screens), consent can be obtained through companion mobile apps or web-based interfaces during the initial setup process. For example, a smart thermostat could guide users through a step-by-step consent process on a paired smartphone app, explaining what data is collected and how it will be used.

For devices with voice capabilities (e.g., smart speakers), voice-assisted privacy settings can be used to explain data collection practices and obtain user consent in an interactive manner. For example, a smart speaker could ask the user, “Would you like to enable voice recording for personalised responses?” and provide a clear explanation of how the data will be used.

QR codes on device packaging or user manuals can link to detailed privacy disclosures for users who want more information. This ensures that consent is still multi-layered but is implemented in a way that is feasible for resource-constrained IoT devices.

c) Real-time privacy dashboards: Users can view, modify, or delete collected IoT data.

IoT devices should offer real-time privacy dashboards that allow users to view, modify, or delete the data collected by their devices. For example, a smart home hub could provide a dashboard where users can see what data is being collected by each connected device and manage their privacy settings accordingly.

These dashboards should be accessible via mobile apps or web interfaces, ensuring that users can manage their privacy settings remotely. For example, a user could log into a mobile app to see what data their smart security camera has collected and delete any footage they no longer need.

Dashboards should also provide transparency reports, showing users how their data is being used and shared with third parties. This helps build trust and ensures that users are fully informed about their privacy.

### 9.3 Data Minimisation & Retention

Data minimisation and retention principles ensure that IoT devices only collect, retain, and process the minimum amount of data necessary to perform their intended functions. These principles help mitigate

the risks of unnecessary data retention and improve user privacy. The following practices are essential for effective data minimisation and retention in IoT systems.

a) Automated data deletion after retention period expires.

IoT devices should be configured to automatically delete data after the maximum retention period specified by the PDPA or other applicable regulations expires. As an example, a smart doorbell camera should delete video footage after 30 days unless the user explicitly chooses to retain it for a longer period.

There is no need to specify a minimum retention period, as the focus is on ensuring that data is not retained longer than necessary. Users should have the option to manually delete data before the retention period expires if they no longer need it.

IoT devices should provide clear notifications to users when data is nearing the end of its retention period, giving them the opportunity to extend retention if needed.

b) Self-destructing metadata to prevent tracking after deletion.

To prevent tracking after data deletion, IoT devices should use self-destructing metadata. For example, metadata associated with IoT data (e.g., timestamps, device IDs) should be automatically erased once the data is deleted.

This is particularly important for IoT devices that collect sensitive data, such as health monitors or location trackers. By ensuring that metadata is also deleted, IoT devices could provide stronger privacy protections and reduce the risk of data being reconstructed or misused after deletion.

c) Blockchain timestamping for audit-proof privacy enforcement.

IoT devices can use blockchain timestamping to create an immutable record of data deletion, ensuring that privacy policies are enforced in an audit-proof manner. As an example, a smart meter could use blockchain to record when energy usage data is deleted, providing a transparent and tamper-proof audit trail.

This approach is particularly useful for IoT devices that handle sensitive or regulated data, as it provides a verifiable record of compliance with data retention and deletion policies.

### 9.4 IoT Security & Cross-Border Transfers

Ensuring robust security for IoT devices and managing cross-border data transfers are vital for protecting user privacy and complying with data protection regulations. Strong security protocols and strategies are necessary to safeguard IoT systems from potential threats and unauthorised access. Key practices for IoT security and minimising cross-border transfers are as follows.

a) End-to-End Encryption (E2EE): at least AES-128 for stored data, TLS 1.2 for transmission.

IoT devices should implement lightweight encryption protocols that are suitable for their resource constraints while still providing strong security. As an example, AES-128 can be used instead of AES-256 for devices with limited processing power, as it provides a good balance between security and performance.

For data transmission, TLS 1.2 can be used as a fallback for devices that cannot support TLS 1.3, provided that the implementation is properly configured to avoid known vulnerabilities. For highly sensitive data (e.g., medical or financial data), AES-256 and TLS 1.3 should still be prioritised, but only on devices with sufficient resources to handle these protocols.

IoT manufacturers should also consider hardware-based encryption solutions, such as secure enclaves or cryptographic chips, to offload encryption tasks and reduce the burden on the device's main processor.

Regular firmware updates should be provided to ensure that encryption protocols remain up-to-date and secure.

b) Zero-Trust Authentication: Role-based access controls for IoT platforms.

IoT platforms should adopt zero-trust authentication models, where access to data is strictly controlled based on user roles and permissions. As an example, a smart home system should only allow authorised users to access camera feeds or control smart appliances.

Multi-Factor Authentication (MFA) should be required for accessing IoT device data, especially for devices that control critical infrastructure or sensitive environments. As an example, a user accessing a smart security system should be required to enter a password and a one-time code sent to their mobile device.

IoT devices should also implement device authentication to ensure that only authorised devices can connect to the network. As an example, a smart lock should only accept commands from registered smartphones.

c) Localisation strategies: Edge computing to reduce cross-border data transfers.

To minimise cross-border data transfers, IoT devices should leverage edge computing strategies, where data is processed locally on the device or at the network edge rather than being sent to centralised cloud servers.

As example, a smart security camera could process video footage locally and only send alerts to the cloud, reducing the amount of data that needs to be transferred across borders.

Localisation strategies not only reduce the risk of data breaches but also improve response times and reduce bandwidth usage, making them ideal for resource-constrained IoT devices.

### 9.5 Compliance Monitoring & Enforcement

To ensure ongoing compliance with privacy regulations and maintain the integrity of IoT systems, organisations must implement robust monitoring and enforcement mechanisms. This includes detecting and responding to unauthorised access, conducting regular audits, and having a structured incident response framework. These practices are essential for maintaining security and meeting legal requirements. The following key components are vital for effective compliance monitoring and enforcement.

a) Real-time anomaly detection for unauthorised data access.

IoT platforms should implement real-time anomaly detection systems to identify unauthorised access to data. As an example, if an IoT device detects unusual access patterns (e.g., multiple failed login attempts), it should trigger an alert and temporarily lock down access. This is particularly important for IoT devices that are part of critical infrastructure, such as industrial IoT systems or smart city devices.

Anomaly detection systems should be integrated with incident response frameworks to ensure that any suspicious activity is quickly investigated and mitigated.

b) Quarterly privacy audits to monitor compliance with PDPA & GDPR.

Organisations should conduct quarterly privacy audits to ensure that IoT devices comply with PDPA and GDPR requirements. These audits should include a review of data collection practices, consent mechanisms, and data retention policies.

Audits should also assess the effectiveness of encryption and security measures implemented on IoT devices. As an example, an audit might test whether a smart home device is properly encrypting

data before transmitting it to the cloud. The results of these audits should be documented and used to improve privacy and security practices.

c) Incident response framework.

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 72 hours, as required by PDPA.

The framework should also include procedures for updating IoT device firmware to address security vulnerabilities and prevent future breaches. Regular incident response drills should be conducted to ensure that the team is prepared to handle data breaches effectively.

# Annex A
(informative)

## Compliance to seven (7) PDPA principles

Organisations must adhere to the following seven PDPA principles to ensure the protection of personal data and maintain compliance with privacy laws. These principles guide the lawful and responsible handling of personal data, fostering trust and transparency between organisations and individuals.

a) General principle

Organisations must process personal data fairly and lawfully, ensuring that individuals are aware of the purposes for which their data is being collected.

b) Notice and choice principle

Individuals must be provided with clear and accurate information about the collection and processing of their personal data, including the purpose, categories of data collected, and the right to opt-out or provide consent.

c) Disclosure principle

Organisations must only disclose personal data to third parties with the consent of the individual, unless required by law or for contractual purposes.

d) Security principle

Organisations must implement appropriate security measures to protect personal data from unauthorised access, disclosure, alteration, and destruction.

e) Retention principle

Personal data should not be kept longer than necessary for the purpose for which it was collected, unless required by law or for legitimate business reasons.

f) Data integrity principle

Organisations must ensure that personal data is accurate, complete, and up to date to the best of their knowledge.

g) Access principle

Individuals have the right to access their personal data and request for correction, updating, or deletion if it is inaccurate, incomplete, or misleading.

# Annex B
(normative)

## Recommended security & privacy countermeasures

This Technical Code provides a comprehensive set of guidelines designed to mitigate risks and protect user data from unauthorised access, breaches, and other potential threats.

The countermeasures detailed in this annex covers a wide range of security practices, including encryption, secure authentication, regular software updates, and robust privacy policies. Additionally, it emphasises the importance of transparency in data handling, particularly in the event of data breaches and third-party data sharing.

This annex provides actionable steps to implement effective security and privacy controls, ensuring compliance with regulatory requirements and industry best practices.

1) Encryption

   a) Data at Rest

      Implement strong encryption algorithms (e.g., AES-256) to protect data stored on IoT devices and backend systems.

   b) Data in Transit

      Use secure communication protocols (e.g., TLS/SSL) to encrypt data as it travels between IoT devices, applications, and cloud services.

   c) End-to-End Encryption

      Ensure data remains encrypted throughout its journey from the device to the final destination, preventing unauthorised access at any point.

2) Secure Authentication

   a) Multi-Factor Authentication (MFA)

      Require MFA for accessing IoT devices and management systems, combining at least two of the following - something the user knows (password), something the user has (token or device), or something the user is (biometrics).

   b) Role-Based Access Control (RBAC)

      Implement RBAC to ensure that only authorised personnel can access sensitive data and system functionalities.

   c) Secure Boot and Firmware Validation

      Utilise secure boot processes to verify the authenticity and integrity of firmware and software updates, preventing the installation of malicious code.

3) Regular Software Updates

   a) Automated Updates

      Enable automatic software and firmware updates to ensure that IoT devices are protected against the latest security vulnerabilities.

b) Patch Management

Establish a patch management process to rapidly address and distribute patches for newly discovered security flaws.

c) User Notification

Inform users about critical updates and provide guidance on how to apply them, ensuring their devices remain secure.

4) Privacy Policies
Develop and maintain a comprehensive privacy policy that is easily accessible to users. This policy should include the following.

a) Detailed Explanation

Detailed information on what data is collected, how it is used, who it is shared with, and for how long it is retained.

b) Regular Updates

Update the privacy policy regularly to reflect any changes in data handling practices, legal requirements, or technological advancements.

c) Multi-Language Support

Provide privacy policies in multiple languages to accommodate users from different regions and backgrounds.

5) Data Breach Notifications

a) Implement a transparent process for notifying users in the event of a data breach. This process should include the following.

i) Timely Notification

Inform affected users as soon as a breach is detected, ideally within 72 hours.

ii) Detailed Information

Provide detailed information about the breach, including the nature of the breach, the data affected, and the steps being taken to mitigate the impact.

iii) Mitigation Advice

Offer practical advice to users on how they can protect themselves from further harm, such as changing passwords or monitoring their accounts for suspicious activity.

b) Third-Party Data Sharing

Be transparent about any third-party organisations with whom user data is shared. This should include the following.

i) Disclosure

Clearly disclose the identity of third parties and the specific purposes for which data is shared.

ii) Data Processing Agreements

Ensure that all third parties adhere to the same data privacy standards through binding data processing agreements.

iii) Opt-Out Options

Provide users with the ability to opt out of having their data shared with third parties.

c) Transparency Report

Publish regular transparency report that detail the data handling practices of the organisation. This report should include the following.

i) Data Requests

Information about government or law enforcement data requests and how they were handled.

ii) Compliance Audits

Results of internal and external audits of data privacy practices.

iii) User Feedback

Summarise feedback from users regarding privacy practices and how it has been addressed.

## Bibliography

[1] MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

[2] MCMC MTFSB TC G031, *Internet of Things – Application Security Requirements*

[3] MCMC MTFSB TC G045*, Internet of Things – Device Security Requirements*

[4] NISTIR 8228 - *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

[5] ISO/IEC 29100: 2011 - *Privacy Framework*

[6] ISO 31000: 2018 - *Guidelines for Risk Management*

[7] ISO/IEC 27400: 2022 - *Guidelines for IoT Security and Privacy*

[8] ISO/IEC 27701: 2019 - *Requirements and Guidelines for Privacy Information Management*

## Acknowledgements


### IMT-2020, IoT and ITS Security Sub-Working Group

**Working Group Leaders**

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

**Drafting Committee Members**

| | |
|---|---|
| Assoc. Prof. Dr Ahmad Shahrafidz Khalid (Draft lead) | Universiti Kuala Lumpur |
| Alisa Rafiqah (Secretariat) | Malaysian Technical Standards Forum Bhd |
| Muhammad Azmin Mohamed Ghazali | Universiti Kuala Lumpur |
| Mayasarah Maslizan | CyberSecurity Malaysia |
| Ahmad Syuhaidi Mohd Rozi | CyberSecurity Malaysia |
| Noor Emy Zuraina Baharudin | Sirim QAS International Sdn Bhd |
| Nur Hidayah Ibrahim | Sirim QAS International Sdn Bhd |
| *Alwyn Goh* | *Goopletech* |
| *Azlan Mohamed Ghazali* | *Deloitte Malaysia* |

**Contributors**

| | |
|---|---|
| Prof. Dr. Shahrulniza Musa | Universiti Kuala Lumpur |
| Thaib Mustafa | Smart Tech AP Sdn Bhd |
| Norkhadhra Nawawi | FNS (M) Sdn Bhd |
| Ng Kang Siong | Digital Connect Society |
| *Datuk Syahril Aziz* | *Secure Insight Sdn Bhd* |