TASMU Data Policy

Document Information

Title: TASMU Data Policy

Policy Reference: TASMU-DAT-POL

Policy Number: 004/2020

Editors: May Li

Date: 2020-06-18

Published Version: V1.0

Status of This Policy: FINAL DRAFT FOR PUBLICATION

Classification: RESTRICTED ACCESS. Do not distribute.

Policy Abstract

This is the TASMU Data Policy and provides the rules for managing data within the TASMU Ecosystem. The data generated by Subscribers of TASMU Smart Services and by the activities of connected devices are key data assets of the TASMU Ecosystem and must be managed appropriately to maintain core functions, operational activities and safeguard personal information from misuse. Every participant within the TASMU Ecosystem has a responsibility to look after data by abiding with this policy, national data policies and laws, including sector data policies as applicable. Mismanagement of data by TASMU Service Operators, may lead to sanctions.

This policy comprises controls of the following data areas within the TASMU Ecosystem:

- Governance
- Data ownership and rights
- Data acquisition
- Data use and sharing
- Data access
- Data retention
- Data quality
- Data standards
- Data Portability

Copyright Notice

Requirements Language

The key words “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as follows:

- **SHALL**: This word, means that the definition is an absolute requirement of the policy.
- **SHALL NOT**: This phrase, means that the definition is an absolute prohibition of the policy.

- **SHOULD**: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY**: This word, or the adjective “OPTIONAL”, mean that an item is truly optional.

Normative References

[IANA Registry]

Internet Assigned Numbers Authority

[ISO 8000]

ISO 8000 Data Quality 2011, ISO

[ISO/IEC 11179-1]

ISO 11179-1 Metadata registries (MDR) Part 1: Framework. 2015, ISO

[ISO/IEC 11179-2]

ISO 11179-2 Metadata registries (MDR) Part 2: Classification. 2019, ISO

[ISO/IEC 11179-3]

ISO 11179-3Metadata registries (MDR) Part 3: Registry metamodel and basic attributes. 2013, ISO

[ISO/IEC 11179-4]

ISO 11179-4 Metadata registries (MDR) Part 4: Formulation of data definitions. 2004, ISO

[ISO/IEC 11179-5]

ISO 11179-5 Metadata registries (MDR) Part 5: Naming principles. 2015, ISO

[ISO/IEC 11179-6]

ISO 11179-6 Metadata registries (MDR) Part 6: Registration. 2005, ISO

[ISO/IEC 11179-7]

ISO 11179-7 Metadata registries (MDR) Part 7: Metamodel for data set registration. 2019, ISO

[ISO 15000-5]

ISO 15000-5 Electronic Business Extensible Markup Language (ebXML) Part 5: Core Components Specification (CCS). 2014, ISO

[ISO 20802-1]

ISO 20802-1 Open data protocol (OData) v4.0 Part 1: Core, 2016, ISO

[ISO 20802-2]

ISO 20802-2 Open data protocol (OData) v4.0 Part 2: OData JSON Format, 2016, ISO

[ISO 29161]

ISO 29161 Information technology Data structure Unique identification for the Internet of Things, 2016, ISO

[JSON]

JavaScript Object Notation (JSON), 1999, JSON-Org

[Data Management Policy]

Data Management Policy, 2015, MOTC, Qatar

[Open Data Policy]

Open Data Policy, 2014, MOTC, Qatar

[OData-ABNF]

OData ABNF Construction Rules Version 4.01, OASIS OData Technical Committee

[OData-CSDL]

OData Version 4.0 Part 3: Common Schema Definition Language (CSDL), OASIS OData Technical Committee

[OData-EDM]

OData Entity Data Model (EDM) Overview, OASIS OData Technical Committee

[OData-EDMX]

XML Name-space Document for OData Common Schema Definition Language (CSDL) XML Representation Version 4.01, OASIS OData Technical Committee

[OData-JSON]

OData JSON Format Version 4.0, OASIS OData Technical Committee

[OData-Protocol]

OData Version 4.0 Part 1: Protocol, OASIS OData Technical Committee

[OData-URL]

OData Version 4.0 Part 2: URL Conventions, OASIS OData Technical Committee

[PAS 180]

Smart Cities Vocabulary PAS 180, 2014, The British Standards Institution (BSI)

[PAS 182]

Smart City Concept Model PAS 182, 2014, The British Standards Institution (BSI)

[RFC2617]

HTTP Authentication: Basic and Digest Access Authentication, 1999, Internet Engineering Task Force (IETF)

[RFC3986]

Uniform Resource Identifier (URI): Generic Syntax, 2005, Internet Engineering Task Force (IETF)

[RFC7159]

The JavaScript Object Notation (JSON) Data Interchange Format, 2014, Internet Engineering Task Force (IETF)

[TASMU Security Policy]

TASMU Security Policy, 2020, MOTC

[TASMU Societal Impact Policy]

TASMU Societal Impact Policy, 2020, MOTC

[TASMU Interoperability Policy]

TASMU Interoperability Policy, 2020, MOTC

[W3C JSON-LD 1.0]

W3C JSON-LD 1.0, A JSON-Based Serialization for Linked Data, 2020, W3C

[W3C JSON-LD 1.1]

W3C JSON-LD 1.0, Processing Algorithms and API, 2020, W3C

[W3C LD-DCAT]

W3C Linked-Data Data Catalog (DCAT) Vocabulary, Data Catalog Vocabulary (DCAT), 2020, W3C

[W3C-RDF Concepts]

W3C-RDF Concepts RDF 1.1 Concepts and Abstract Syntax, 2014, W3C

[W3C Web Annotated Protocol]

W3C Web Annotated Protocol, Web Annotated Protocol, 2017, W3C

[XML-Schema-2]

W3C XML Schema Definition Language (XSD) 1.1 Part 2: Data types, 2004, W3C

[XML]

Extensible Markup Language (XML), 2006, W3C

Informative References

[Facebook Data Policy]

Facebook Data Policy, 2018, Facebook

[GDPR]

General Data Protection Regulation, 2016, European Union (EU)

[Google Privacy Policy]

Google Privacy Policy, 2016, Google

[Uber Privacy Notice]

Uber Privacy Notice, 2020, Uber

Contents

Definitions

The definitions used in this policy have been written to provide contextual clarity and where necessary specificity, and should not be interpreted to be contradictory to any laws in the State of Qatar.

[Anonymisation]

The process in which Personal Data is altered in such a way that it irreversibly prevents the identification of the Subscriber. Personal Data which has been irreversibly anonymised ceases to be Personal Data.

[Analytics Data]

This refers to the collection of data that is used to support decision making and/or research in TASMU Systems:

- (E) Sector Platforms, and
- (F) Central Platform

[Central Platform Analytic Data]

This refers to a collection of raw or processed data that is used to support decision making and/or research in the TASMU System (F) Central Platform.

[Consent]

Consent is an affirmative, freely given and informed agreement of a Subscriber for the Processing of their data. Natural persons ("individuals") must be able to control the Processing of their Personal Data within the TASMU Ecosystem and where necessary provide explicit Consent, which signifies their agreement, expressly confirmed in words, to specific Processing.

[Corporate Data]

Corporate data is data that is captured through the operation of the TASMU Service Operator's corporate functions. It can include, but is not restricted to: staff data, company data, financial data, facilities data, product data and system specific configuration data etc.

[Data Sharing Agreement]

Refers to a form of contractual agreement between a TASMU Service Operator and a National Service Owner or Third Party Partner for exchanging data.

[Data Custodian]

Refers to the role within the TASMU Service Operator's organisation responsible for data management and accountable for Data Rights.

[Data Portability]

Refers to the the fundamental right of the individual to move their Personal Data across different TASMU Service Operators or TASMU Smart Services.

[Data Owner]

A data owner is a Subscriber, who owns and is accountable for their data.

[Data Ownership]

Data ownership is the act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use, and distribution policy implemented by the Data Owner.

[Data Rights]

Data Rights consist of the set of permitted Data Custodian actions that TASMU Service Operators undertake on TASMU Data for the functioning and operating of a TASMU Smart Service, including:

- data acquisition

- data analysis
- data storing
- data sharing
- data monetisation
- data deletion or destruction

[Data Source]

A data source refers to the individuals or an entity from which a specific set of data is obtained.

[Device Data]

Refers to all the data collected from an IP address, web beacon, pixel tag, ad tag, cookie, JavaScript, local storage, software, or by any other means, or from a particular computer, web browser, mobile device, or other connected device or application.

[Internet of Things]

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, uniquely identified with the ability to transfer data over a network to (E) Sector Platforms and/or the (F) Central Platform.

[Metadata]

Refers to the set of data that describes and gives peripheral information about TASMU Data. It ensures the resusability of data within the TASMU Ecosystem, helps drive efficiencies in processing and publication of data, hence making management of underlying data easier and more simplified using data catalogues, dictionaries, and taxonomies.

[Service Oriented Architecture]

Service-oriented architecture (SOA) is a style of design that defines a way to make software components reusable via service interfaces. These interfaces utilise common communication standards in a way that they can be rapidly incorporated into new applications without having to perform deep integration each time.

[National Data]

Refers to the data in (J) National (External) Services in the TASMU Ecosystem and provides common services and other sector services.

[National Service Owner]

Refers to the owners of services and platforms in (J) National (External) Services.

[Network Data]

Refers to the networking configuration data that enables devices to connect and communicate within the TASMU Ecosystem across the following:

- (D) any networking between platforms (E) and services (C)
- (G) any networking between platforms (F) and devices (H)

[Operations Data]

Refers to the operational data required in the following TASMU Systems to manage Subscribers, platform operations and security operations:

- (I) The TASMU Control Centre
- (K) The TASMU Security Management
- (L) The Operation Management

[Open Data]

Refers to the open data approach that is defined in the Open Data Policy adopted within the TASMU Ecosystem to ensure data is exchange freely without technical barriers, copyright, patents or other mechanisms of control.

[Open Interface]

Refers to a public standard interface for connecting one component to another component regardless of their brands. In the case of software, it also implies that more than one program exists to interface with the application that has the open interface or that a program can be readily written to communicate with it.

[Open Standards]

Refers to a set of specifications that are standardised by a formal body and are then published and made freely available to the technical community.

[Personal Data]

Data of a natural person ('individual') which is specifically identifiable or can be reasonably identified either by the Personal Data itself or through a combination of other data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[Production]

This refers to the environment, system and/or data of a TASMU System that provides a "live" service to Subscribers. This includes pre-production and live disaster recovery environments and is in contrast to non-production environments such as test or development which are not used for "live" services.

[Processing]

Any operation or set of operations which is performed on data, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.

[Retention Schedule]

Refers to the documented instructions describing the retention and disposition aspects of relevant TASMU Data under the TASMU Service Operator's custody.

[Retention Period]

Refers to the length of time prescribed in the defined Retention Schedule for which certain TASMU Data must be kept before their final disposition.

[Sector Platform Analytic Data]

Refers to a collection of raw or processed data that is used to support decision making and/or research in the (E) Sector Platforms.

[Services Data]

Refers to the data that is collected, generated, and stored within the TASMU Systems related to (H) Smart Devices or Subscribers. Examples include application data, history of service usage, search activities, cookies, transaction records, traffic and location data, etc.

[Subscriber]

An organisation or natural person who utilises a TASMU Smart Service. They subscribe to and are authenticated by the TASMU Ecosystem. In some contexts they may be referred to as consumers.

[TASMU Data]

Refers to the following data types, specified in the TASMU Data Model which are acquired, generated, configured and processed within TASMU Systems for functioning and operating of the TASMU Ecosystem:

- Personal Data
- Device Data
- Network Data
- Services Data
- Analytics Data
- Operations Data
- National Data

- Third Party Data

[TASMU Ecosystem]

This is the Smart Qatar (TASMU) platform and any TASMU Smart Service that is either connected to this Central Platform or is branded as TASMU compliant. Refer to (A) in the TASMU Conceptual Diagram.

[TASMU System]

Refers to any of the following elements from the TASMU Conceptual Diagram:

- (C) Any smart application or service
- (D) Any networking between platforms and (C)
- (E) Sector data analytics platforms
- (F) Central data analytics platform
- (G) Any networking between platforms and devices (H)
- (H) Any smart devices
- (I) The TASMU Control Centre
- (K) Security Management System of the TASMU Ecosystem
- (L) Operations Management System of the TASMU Ecosystem

[TASMU Smart Nation Regulator]

The entity in the State of Qatar who regulates the TASMU Ecosystem. It is responsible for drafting, promoting, governing, updating, monitoring compliance with, and enforcing this policy.

[TASMU Service Operator]

This is the owner and operator of the TASMU System, who has overall responsibility for its secure, compliant operation.

[TASMU Smart Service]

A TASMU Smart Service is a national service, leveraging one or multiple technologies, to resolve an identified challenge or enable a desired outcome and that operates in the TASMU Ecosystem. Collectively, they focus on detailing and contextualizing services relevant for the State of Qatar.

[Third Party Data]

Refers to external data originating from systems or services outside of the TASMU Ecosystem.

[Third Party Partners]

Refers to third party entities outside of the TASMU Ecosystem that Process data, and/or operate the TASMU System for TASMU Service Operators.

1. Introduction

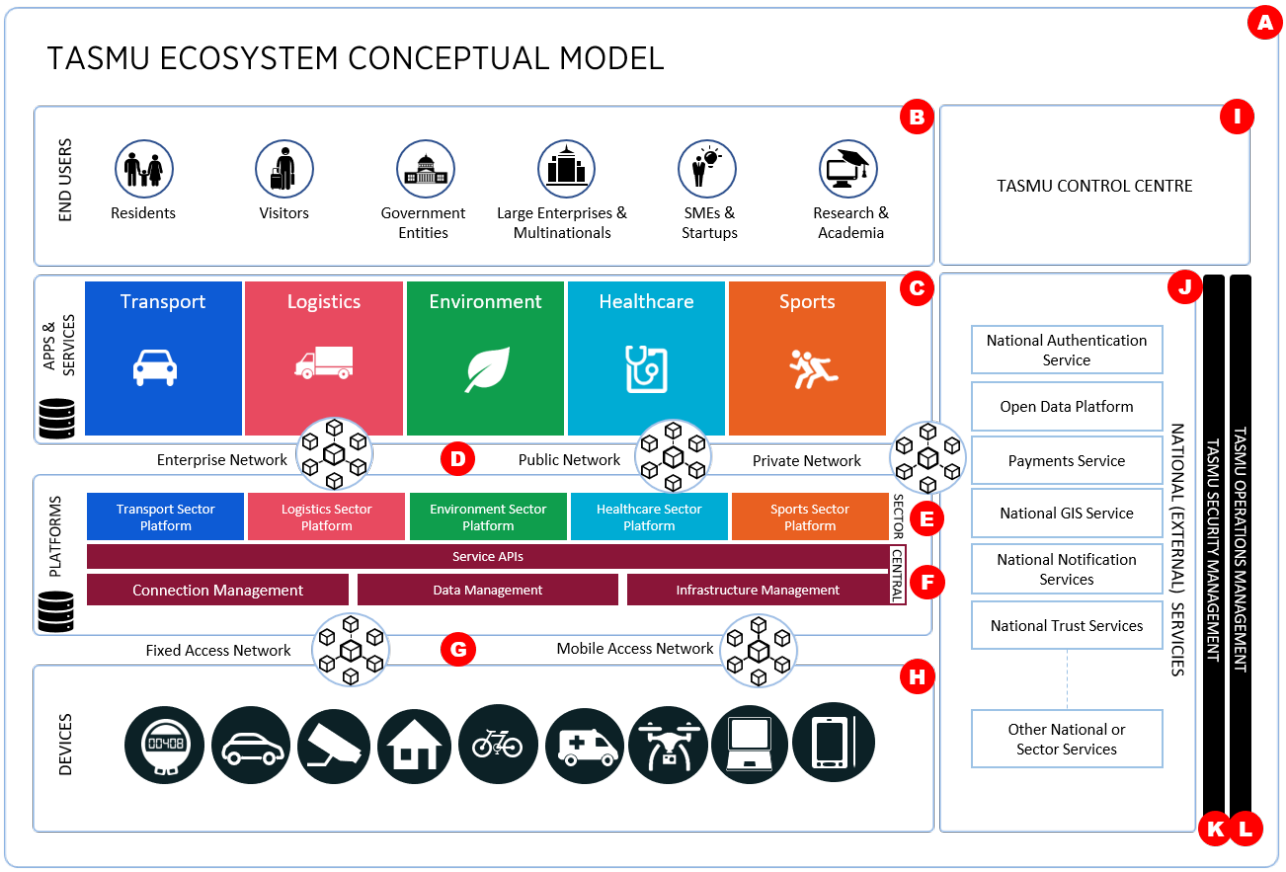
1.1 TASMU

The Qatar National Vision 2030 aims to “transform Qatar into an advanced society capable of achieving sustainable development.” TASMU, or the Smart Qatar program, is a digital response to the goals that have been set out in the National Vision 2030. It is about harnessing technology and innovation to improve quality of life and help drive economic diversification.

TASMU aims to leverage innovative applications of technologies to provide targeted services for residents, businesses and government across priority sectors. The foundation of this whole-of-nation effort relies on the ability to collect and manage vast amounts of data, share and open it up for spawning broad-based innovation and entrepreneurship within a set of defined rules and regulations. This is then processed and analysed by different actors for the build-up of innovative services and applications. As such, governance of TASMU on a national level has been designed to harmonize efforts across the different actors and drive Smart Qatar development with a key focus on ensuring efficiency and building resilience and interoperability.

TASMU Smart Services are services designed to solve evolving challenges targeted constituents (people, businesses, or government) face, leveraging technology and innovation. TASMU Smart Services cut across industry sectors focusing on human, social, economic, and environmental development. They can be focused on providing convenience or entertainment, or could address critical needs such as national safety and security. As such, the type of information they leverage can range from publicly open to sensitive or private information.

The policy covers the TASMU Ecosystem and interactions with it. The diagram below shows the TASMU Ecosystem in the context of this policy.



Only the following elements are within the scope of this policy:

- A: is the overall ecosystem
- B: is the end-user ecosystem
- C: is the TASMU Smart Services and services ecosystem
- D: are the network connections from the central platform, over enterprise, public and private networks
- E: are the sector data analytics platforms (‘Sector Platforms’)
- F: is the central TASMU data analytics platform (‘Central Platform’)
- G: is the Internet of Things (IOT) access network, either over fixed of wireless networks
- H: is the IOT devices ecosystem
- I: is the TASMU Control Centre
- J: is the ecosystem of national services/platform that connects to the TASMU Central Platform and (C) above
- K: is the TASMU security management ecosystem
- L: is the TASMU operations ecosystem

1.2 TASMU Data Policy

This policy applies to the following TASMU Data that is generated, created, collected and maintained within the TASMU Ecosystem.

1. Personal Data
2. Device Data

3. Network Data
4. Services Data
5. Analytics Data
6. Operations Data
7. National Data
8. Third Party Data

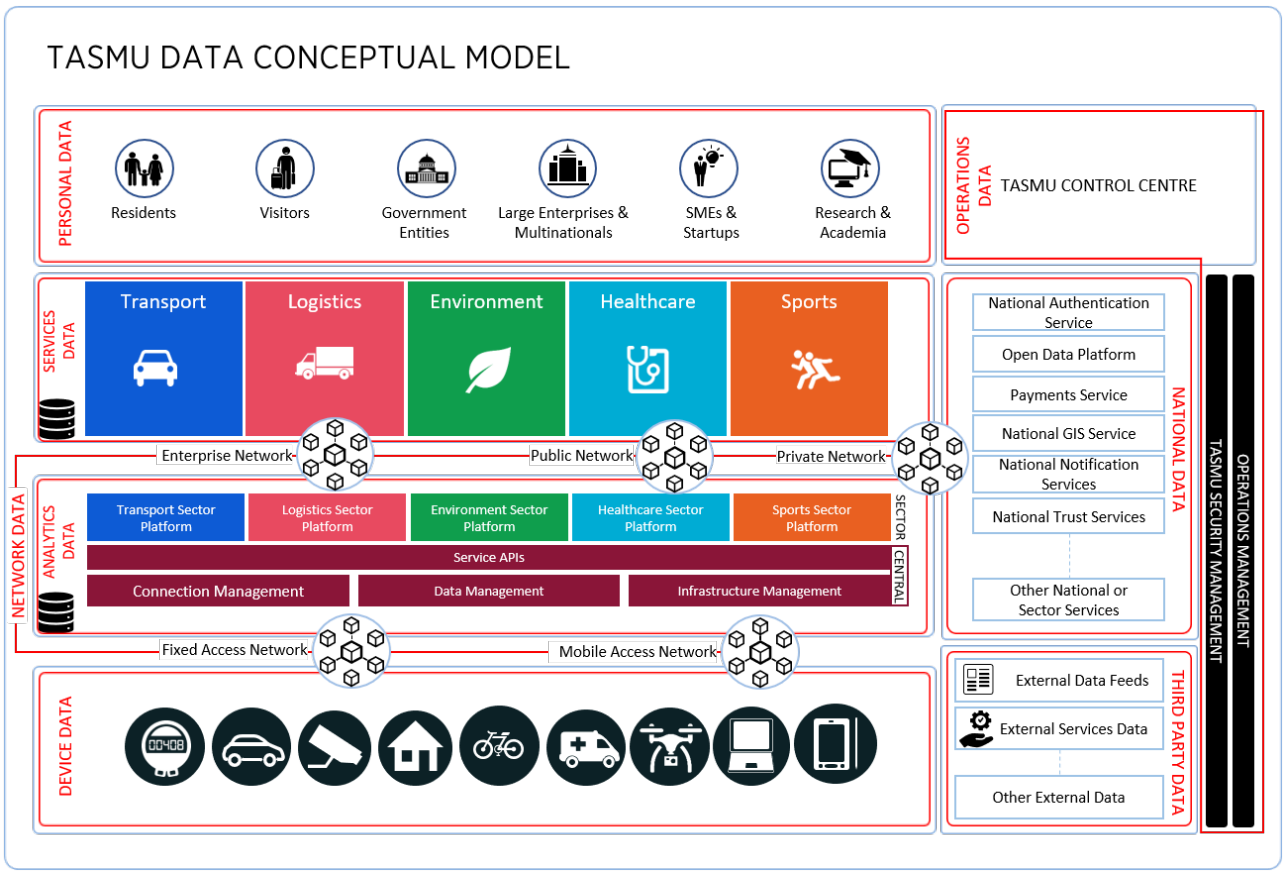
This policy does not explicitly provide the controls for Personal Data, which are specified in the TASMU Security Policy. Additionally, this policy does not apply to Corporate Data for which TASMU Service Operators SHOULD create their own data policy.

This policy builds upon the existing Ministry of Transport & Communications (MOTC) Data Management Policy and Open Data Policy and covers the full data lifecycle, including:

- **Governance:** the overall management of data
- **Ownership and Data Rights:** who owns the data and provides Data Rights for others
- **Data Acquisition:** how is data captured or enters the TASMU Ecosystem
- **Data Use and Data Sharing:** how is data used and shared
- **Data Access:** who has access to data, and how is access provided
- **Data Retention:** what data needs to be retained, and for how long
- **Data Quality:** good practices for ensuring data quality
- **Data Standards:** the approach for establishing or adopting data standards
- **Data Portability:** how does data move from one system to another

This TASMU policy is regulated by the TASMU Smart Nation Regulator.

The diagram below shows the data ecosystem in the context of this policy, and highlights data acquisition from various Data Sources:



1.3 Compliance

All TASMU Service Operators SHALL:

1. Comply with this policy where they operate a TASMU System or provide a TASMU Smart Service to a Subscriber, prior to operating in the TASMU Ecosystem and on a regular basis as directed by the TASMU Smart Nation Regulator.
2. Ensure that this policy is applied to all aspects of the TASMU System, whether that is maintained or operated by a Third Party Partner, prior to operating in the TASMU Ecosystem.
3. Ensure this policy is considered in conjunction with the specific TASMU Smart Service policy that is issued by the TASMU Smart Nation Regulator and/or other relevant sector policies, which will cover specific requirements of the TASMU Smart Service.
4. Allow for an independent audit to check compliance, as and when necessary, or as directed by the TASMU Smart Nation Regulator.
5. Notify the TASMU Smart Nation Regulator, when the TASMU System undergoes, as applicable, any changes to the following:
    a. data acquisition methods
    b. use of data fields
    c. data formats
    d. additional data acquisition needs
    e. data analytic methods
    f. data access methods and service terms
    g. data retention schedules and terms
    h. Data Sharing Agreement terms
    i. Data Portability methods
    j. data quality, arising from issues

2. Data Policy Controls

2.1 Governance

TASMU Services Operators need to ensure that they manage the data related to their TASMU System, including key aspects such as privacy, security, accessibility, retainability, portability, sharing and quality. Hence TASMU Service Operators SHALL:

1. Be responsible for overall planning, guiding and supervising the data management of their TASMU System, ensuring it:
    a. has the ability to provide and consume Open Data
    b. uses Open Interfaces
    c. uses Open Standards
    d. has the ability to share data, as required and permitted, and comply with the Open Data Policy, and/or sector policies
2. Coordinate the investigation and resolution of any major data issues in the development and operation of TASMU Smart Services with other affected TASMU Service Operators.
3. Ensure the privacy, confidentiality, integrity and availability of data, in line with the TASMU Security Policy that is essential for the operation of the TASMU Smart Service.
4. Ensure that data Processing technologies used in their TASMU System:
    a. comply to the TASMU Interoperability Policy

b. when any emerging technology is used, comply to the ethical specifications in the TASMU Societal Impact Policy

5. Appoint the Data Custodian role and ensure they undertake the following for any TASMU Data related to their TASMU System:

   a. its safe custody, transport and storage
   b. management of the full data lifecycle, including related processes
   c. its quality

2.2 Data Ownership and Rights

The function and operation of TASMU Smart Services depends on the Processing of large quantities and varieties of data, and hence having clearly defined Data Rights within the TASMU Ecosystem is essential.

1. TASMU Service Operators SHALL ensure that if they are Processing data for any purpose other than the following, they disclose and obtain approval for that purpose from the TASMU Smart Nation Regulator:

   a. operation of the TASMU Smart Services
   b. improving TASMU Smart Services
   c. developing new functions
   d. enhancing user experience
   e. providing a more personalised service
   f. for measurement and analytics
   g. promoting safety, integrity and security
   h. for marketing communications with Subscribers
   i. for carrying out research and innovation for social good such as topic on general social welfare, technological advancement, public interest, health and well-being.

2. TASMU Service Operators SHALL seek the Consent of Data Owners and establish their Data Rights before Processing that data. Data Owners of TASMU Data are specified in the following table:

TASMU Data	**Data Owner**
Personal Data	Subscriber
Device Data	Various. See TASMU Smart Service specific policy
Service Data	TASMU Service Operators of TASMU Smart Services
Network Data	Network Service providers
Central Platform Analytic Data	MOTC
Sector Platform Analytic Data	Sector Platform Owner
Operations Data	MOTC
National Data	National Service Owner
Third Party Data	Third Party Partners

3. As part of the Consent process, TASMU Service Operators SHALL provide Data Owners with the following information:

   a. the purposes of Processing the data
   b. the Retention Period of the data
   c. data sharing plan
   d. data monetisation plan

4. Once Consent is obtained, TASMU Service Operators are liable for the security, safety and quality of the relevant TASMU Data, and SHALL comply with the TASMU Security Policy.

5. TASMU Service Operators SHALL have a documented process for recording Consent, and the Data Rights that they provide or have been granted.

2.3 Data Acquisition

1. TASMU Service Operators SHALL only acquire data that is relevant to operate their TASMU Systems and SHALL provide the TASMU Smart Nation Regulator with the following:

    a. a description of all data types, Data Sources, purposes and method of data acquisition, applicable to their TASMU System
    b. a description of all National Data types, Data Sources, purposes and method of data acquisition
    c. a description of all Third Party Data types, Data Sources, purposes and method of data acquisition

2. TASMU Service Operators SHOULD use the capabilities within the TASMU Ecosystem, where applicable, for data acquisition and aggregation.

3. TASMU Service Operators SHALL NOT refuse to provide their service even if a Subscriber revokes their Consent for information that does not form a core function of the TASMU Smart Service.

2.4 Data Use and Sharing

1. TASMU Service Operators SHALL conform to the following requirements for exchanging data with (J) National Platforms and Services:

    a. define a Data Sharing Agreement with the relevant Data Owner of (J) National Platforms and Services
    b. use formal, National Service Owner defined interfaces
    c. comply with the following national policies:

        - Open Data Policy
        - Data Management Policy

2. TASMU Service Operators SHALL have a suitable Data Sharing Agreement in line with this policy when sharing data with Third Party Partners.

3. Where applicable, TASMU Service Operators SHOULD adopt formal licensing arrangements where applicable to protect their Data Rights.

4. Data Sharing Agreements SHOULD cover, at a minimum, the following:

    a. purposes of data sharing
    b. description of data
    c. data security
    d. data Retention Period
    e. subsequent use of data
    f. conditions of the data use
    g. Service Level Agreements (SLAs)
    h. operational activities
    i. incident investigation process
    j. service improvement mechanisms
    k. any applicable sector specific requirements

5. TASMU Service Operators MAY share Anonymised TASMU Data outside of the TASMU Ecosystem, with the following Third Party Partners:

    a. partners providing measurement and analytics services
    b. advertisers
    c. partners offering goods and services as add-ons for the TASMU Smart Service
    d. TASMU Smart Service vendors and service providers
    e. researchers and academics

2.5 Data Access

1. TASMU Service Operators SHALL comply with TASMU Security Policy for accessing TASMU Data.

2. TASMU Service Operators SHOULD adopt the following good practices:

    a. define who can access data and the level of access permitted, especially for Subscribers and Third Party Partners
    b. define the list of legitimate and justifiable reasons for accessing different data types, including the level of authorisation
    c. define the approval process for data access

2.6 Data Retention

TASMU Service Operators SHALL govern the creation, storage, maintenance and usage of TASMU Data by ensuring, at a minimum, the following requirements for data storage and retention are met:

1. Identify the essential data to be retained, and define a Retention Schedule for it including the following elements:

    a. TASMU Data types
    b. Retention Period in line with business requirements and sector requirements
    c. Data Owners
    d. other relevant parties
    e. methods of data deletion

2. Retain TASMU Data for a minimum period of twelve (12) months.

3. Safeguard the TASMU Data during the defined Retention Period by using appropriate solutions or technology to prevent data loss, due to corruption or media failure, and data breaches due to inadequate data protection.

4. TASMU Service Operators MAY jointly, with other TASMU Service Operators define the Retention Schedule, where necessary.

5. TASMU Service Operators SHOULD define a process to review all data on a regular basis, in order to decide whether to destroy or delete any data once the purpose for which that data was acquired and retained is no longer relevant, and update the Retention Schedule where necessary.

6. TASMU Service Operators SHALL:

    a. define a process for data destruction and processes to prevent the permanent loss of essential data as a result of malicious or unintentional actions
    b. destroy the data, at the end of the retention period, according to the Retention Schedule, on all Production systems
    c. obtain explicit permission from MOTC before deletion of any Analytics Data

7. As an exemption, Retention Periods MAY be prolonged in any of the following cases:

    a. where there is an ongoing investigation from other regulatory bodies or competent authorities
    b. when exercising their legal rights for court proceedings recognised under the laws of the State of Qatar

2.7 Data Quality

Establishing a standard of data quality is essential for the healthy operation of a TASMU System and the TASMU Ecosystem more generally.

1. In order to ensure the quality of data of a TASMU System, TASMU Service Operators SHALL select and develop a data management approach that will meet the following principles:
    - **Accuracy:** ensure the right data is collected, and present that data in a consistent and unambiguous form
    - **Completeness:** collected data reflects what is recorded based on a standard schema that defines completeness, including explanations and formulas for data derivation and calculation as part of the meta-data that defines and explains the raw data
    - **Timeliness:** ensure data availability and in case data sharing is required, release data as quickly as they are collected and processed, with priority given to data whose utility and value are time sensitive
    - **Machine Readable:** store data in a commonly used format that easily support machine readability, interpretation and processing
    - **Non-Duplication:** reuse data for multiple / generic purpose(s) to avoid data duplication
    - **Non-Proprietary:** make freely available alternative formats to prevent limits on consumption of data to specific, proprietary formats
2. TASMU Service Operators SHOULD adopt the following good practices as part of their data management approach:
    a. ensure that data capture, validation and Processing is automated wherever possible
    b. have processes and mechanisms in place to ensure all data can be validated and quality assured before being used
    c. adopt a collaborative approach for addressing data quality issues, maintaining data integrity and automated decision making, where applicable
    d. define and validate data quality rules based on the requirements of the TASMU Smart Service and this policy
    e. set up a data identification, remediation and reporting process for removing and recording any data that is subject to quality issues. Ensure a 'root cause' examination is conducted and analysis of why, where, and how the data defect originated
    f. conduct data profiling by reviewing and comparing Metadata and running statistical models to analyse data quality
    g. create a data repairing process

2.8 Data Standards

The sharing of data for the benefit of all TASMU Ecosystem stakeholders is at the heart of TASMU's aspirations. Data can be used in real time, from sensors and tracking devices, through to the use of data to develop longer term plans to improve the wellbeing of people and businesses. Having a common data standard will avoid using multiple data formats and vocabularies within the TASMU Ecosystem, which adds risk, cost and complexity.

1. TASMU Service Operators SHOULD use one of the following approaches for establishing data standards:
    a. adopt existing sector data standards, as applicable
    b. establish local TASMU Data standards based on the following international data standards, under the guidance of the TASMU Smart Nation Regulator:
        - PAS 182 Smart City Concept Model
        - PAS 180 Smart City Vocabulary
        - ISO 8000 Data Quality
        - ISO 15000-5 Electronic Business Extensible Markup Language (ebXML) Part 5: Core Components Specification (CCS)
        - ISO/IEC 11179-1 Metadata registries Part 1: Framework Registries and Classification
        - ISO/IEC 11179-2 Metadata registries Part 2: Classification
        - ISO/IEC 11179-3 Metadata registries Part 3: Registry Metamodel and basic attributes
        - ISO/IEC 11179-4 Metadata registries Part 4: Formulation of data definitions
        - ISO/IEC 11179-5 Metadata registries Part 5: Naming and identification principles

- ISO/IEC 11179-6 Metadata registries Part 6: Registration
- ISO/IEC 11179-7 Metadata registries Part 7: Metamodel for data set registration
- ISO 29161 Data Structure Unique Identification For The IOT
- ISO 20802-1 Open Data Protocol (OData) Part 1: Core
- ISO 20802-2 Open Data Protocol (OData) Part 2: OData JSON Format
- IANA Registry Internet Assigned Numbers Authority Registry
- RFC2617 Hypertext Transfer Protocol Authentication: Basic and Digest Access Authentication
- RFC7159 The JSON Data Interchange Format
- RFC3986 Uniform Resource Identifier: Generic Syntax
- OData-Protocol OData Version 4.0 Part 1: Protocol
- OData-CSDL OData Version 4.0 Part 3: Common Schema Definition Language
- OData-ABNF OData Augmented BNF for Syntax Specifications Construction Rules Version 4.0
- OData-URL OData Version 4.0 Part 2: URI Conventions
- OData-CSDL OData Version 4.0 Part 3: Common Schema Definition Language
- W3C JSON-LD 1.0 A JSON-Based Serialization for Linked Data
- W3C JSON-LD 1.1 Processing Algorithms and Application Programming Interface
- W3C RDF Concepts Resource Description Framework 1.1 Concepts and Abstract Syntax
- W3C LD-DCAT W3C Linked-Data Data Catalog Vocabulary
- W3C WAP W3C Web Annotated Protocol standard

2. Where there is a requirement for establishing local TASMU Data standards, the standard SHOULD cover, at a minimum, the following:

   a. a roadmap for the design, development, testing, and implementation of a standard data architecture
   b. Service Oriented Architecture architecture design principles
   c. data architecture design, including the following:

      - data Processing capabilities
      - data profiles
      - data flow diagrams
      - data lifecycle model (general end to end data movement)
      - data security checkpoints
      - data quality checkpoints
      - reference to data dictionaries, data catalogues and business glossaries to ensure consistency during architecture development

   d. data architecture addresses the following core functions and systems:

      - Open Data management systems and services
      - Metadata repositories
      - data ingestion, transformation systems
      - data dictionary, data catalogue, and business glossary
      - document and content management systems
      - data analytic systems
      - data security systems & workflows

   e. accommodates the following data format types in the design for enabling Open Data:

      - XML and JSON data formats
      - fixed length data, record formats, fixed width file columns and records
      - proprietary formats from sectors

   f. establish a common data structure that covers the following, as a minimum:

      - general data concepts and models
      - common elements
      - identification scheme for IOT entity and IOT applications
      - format rules and specifications for JSON files and URL conversions
      - entity data models

- common schema definitions for XML data

g. define a Metadata Framework that covers:

- Metadata basic attributes
- Metadata and registry
- formulation of data definitions
- naming and identification principles
- Metadata registration
- data dictionaries
- data categories

2.9. Data Portability

The right for Data Portability gives Subscribers the right to retrieve Personal Data they have provided to a TASMU Service Operator in a structured, commonly used and machine readable format. It also gives them the right to request that a TASMU Service Operator transfers this data directly to another TASMU Service Operator. Hence TASMU Service Operators SHALL:

1. Respect a Subscriber's right to Data Portability by providing a capability for that Subscriber to receive a copy of their Personal Data, or/and have their Personal Data transmitted to another TASMU Service Operator, when requested by the Subscriber.
2. Complete the Data Portability request by using one of the following methods:
   a. directly transmit the requested data to the Subscriber
   b. provide access to an automated tool that allows the Subscriber to extract the requested data themselves
3. Ensure the transmission methods for Data Portability comply with the TASMU Security Policy.
4. Be responsible for the secure and accurate transmission, to the right quality, readable format and destination, of the Subscriber's data.
5. Permit portability of data related to minors, after obtaining permission from their legal guardian.
6. Limit the data transmission if it adversely affect the rights and freedoms of others when advised by the competent authorities.
7. Where there is a requirement for data retention, in national and/or sector policies, after data has been ported out, TASMU Service Operators SHALL NOT Process the relevant Personal Data during the remaining retention period.