ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.4602 (03/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Internet of things and smart cities and communities – Services, applications, computation and data processing

---

Data processing and management framework for Internet of things and smart cities and communities

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	**Y.4550–Y.4699**
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4602

Data processing and management framework for Internet of things and smart cities and communities

Summary

Recommendation ITU-T Y.4602 describes the data processing and management (DPM) framework organized into five dimensions that are data lifecycle dimension, trust dimension, data commercialisation dimension, data ecosystem dimension, and data governance dimension. The DPM framework covers all the applications and services for Internet of things (IoT) and smart cities and communities. It provides a high-level view of the DPM capabilities required at each stage of the data lifecycle considering different inherent aspects of the data such as its source (personal data, legacy data, and public data) and external aspects that are actions needed to be applied to the data following data manipulation, sharing, security and governance requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4602	2023-03-28	20	11.1002/1000/15486

Keywords

Data processing and management (DPM), Internet of things, smart cities and communities.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4602

Data processing and management framework for Internet of things and smart cities and communities

1 Scope

This Recommendation covers the following:

– A high-level data processing and management (DPM) framework in Internet of things (IoT) and smart cities and communities (SC&C) from a capability perspective;

– Identification of related DPM concepts and their relationships;

– Common considerations of DPM in IoT and SC&C.

This Recommendation is intended to be used by:

– Those who are engaged in DPM activities;

– Those who are involved in data related standardization activities;

– DPM policy-makers and regulators;

– DPM information communication technology (ICT) city service users, developers, evaluators and auditors.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: Structured set of capabilities that provide value added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 capabilities [b-ITU-T X.1601]: Quality of being able to perform a given activity.

3.1.3 closed data [b-ITU-T FG-DPM TS D0.1]: Data that requires access control to be divulgated.

3.1.4 data [b-IEC 60050-831]: Representation of facts of objective reality in a formalized manner. Example: Data can be signs and symbols, and can be in analogue form, digital form or both.

NOTE – Data can be used for communication, interpretation or processing by human beings or automatic means.

3.1.5 data commercialization [b-ITU-T FG-DPM TS D0.1]: Process of creating commercial value from data.

NOTE – It may encompass various activities, including but not limited to, monetization, valuation, pricing, licensing, distribution, marketing and sales.

3.1.6 data exchange [b-ITU-T FG-DPM TS D0.1]: Accessing, transferring and archiving of data.

3.1.7 data governance [b-ITU-T FG-DPM TS D0.1]: Set of activities aimed to design, implement and monitor a strategic plan for data asset management.

3.1.8 data management [b-ISO/IEC TR 10032]: Activities of defining, creating, storing, maintaining and providing access to data and associated processes in one or more information systems.

3.1.9 data marketplace [b-ITU-T FG-DPM TS D0.1]: Electronic marketplace whose main product is the provisioning of data and/or related services around data.

3.1.10 data processing [b-ISO 5127]: Systematic performance of operations upon data.

3.1.11 data processing and management (DPM) [b-ITU-T FG-DPM TS D0.1]: The combination of all activities either directly performed on or indirectly influencing data.

NOTE 1 – Directly performed activities include among others [collecting/acquiring/capturing], exchanging, storing, securing, manipulating, reusing, aggregating, curating, disposing, monetizing and deleting data.

NOTE 2 – Indirectly influencing activities include among others policy and standards making, skills and innovation enhancement.

3.1.12 data sharing [b-ITU-T FG-DPM TS D0.1]: The process of data exchange among different parties with specified conditions.

3.1.13 ecosystem [b-ITU-T FG-DPM TS D0.1]: A set of organizations forming a distributed system with both technical and non-technical properties.

NOTE – In DPM, ecosystem refers to a data ecosystem, which is comprised of the technical and non-technical factors and mechanisms which directly or indirectly impact DPM activities in an ecosystem, based on various degrees of interoperability. Factors and mechanisms include, but are not limited to, data laws, regulations and policies, data standards, data skills, data research and development programmes, data entrepreneurship, data economy financial incentives and data platforms.

3.1.14 Internet of things [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.15 interoperability [b-ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.1.16 minimal interoperability [b-ITU-T FG-DPM TS D0.1]: The minimal sufficient degree needed to meet a certain requirement for data sharing, use and reuse.

NOTE – This is an approach to build a set of modular mechanisms, including information models, across multiple domains, locations and events. The definition aligns with the definition of "interoperability" in [b-ITU-T Y.101].

3.1.17 lifecycle [b-ISO/IEC TR 29110-5-3]: Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

3.1.18 open data [b-ITU-T FG-DPM TS D0.1]: Any information that has been made available for anyone under a legal framework to access, alter, and share without restrictions.

NOTE – It can be from a public source, e.g., government data, or from a business, e.g., company intelligence, and can be used for both commercial and non-commercial purposes.

3.1.19 personal data [b-PAS 185]: Data which relates to a living individual who can be identified: a) from those data; or b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.1.20 processed data [b-ISO 5127]: Data that have been transformed from raw data or from an earlier data stage into a more refined stage by data cleaning, sorting, linking, verifying and similar operations.

3.1.21 **raw data** [b-PAS 185]: Data that has not been processed for use.

3.1.22 **requirements** [b-ISO 8000-2]: Need or expectation that is stated, generally implied or obligatory.

3.1.23 **risk** [b-ISO 31000]: Effect of uncertainty on objects.

3.1.24 **safety** [b-ISO/IEC Guide 51]: Freedom from risk which is not tolerable.

3.1.25 **security** [b-IEC Guide 120]: Condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

3.1.26 **service** [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.27 **shared data** [b-PAS 185]: Data where the data owner has the legal authority to share it with one or more organizations, subject to a data or information sharing agreement which specifies that access is granted subject to specific restrictions and, where between different legal entities, is legally enforceable.

3.1.28 **Smart cities and communities** [b-ITU-T FG-DPM TS D0.1]: Effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens.

NOTE – This definition aligns with the definition of "Smart City" in [b-ISO/IEC 30182] and with the recommendation from the IEC/ISO/ITU Smart City terminology coordination task team [b-IEC/ISO/ITU draft white paper].

3.1.29 **stakeholders** [b-ISO Guide 73]: Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

3.1.30 **trust** [b-ITU-T X.1252]: The reliability and truth of information or the ability and disposition of an entity to act appropriately, within a specified context.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **active data**: Data streamed on a regular basis by the sensors.

3.3.2 **data category**: Data classification based on the corresponding security, privacy, quality, and governance rules.

3.3.3 **data types**: Categorization of data according to reception regularity of data at the databases and applications, and the way this data is retrieved either directly by the application or spontaneously by the sensors.

3.2.4 **data lifecycle**: Steps of data processing and management from its creation to its use and disposal.

3.2.5 **dynamic data**: Data generated by sophisticated sensors that are able to send and receive information to the applications directly.

3.2.6 **passive data**: Data that is not sent on a regular basis, it is obtained by the application explicitly requesting the sensor to send its data.

3.2.7 **time series data**: Data that is time stamped.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DPM Data Processing and Management

EIA Environmental Impact Assessment

GDP Gross Domestic Product

GHG	Greenhouse Gas
GVA	Gross Value Added
ICT	Information Communication Technology
IoT	Internet of Things
ITU	International Telecommunication Union
SC&C	Smart Cities and Communities
STI	Science and Technology Innovation

5 Conventions

None.

6 DPM framework concepts and high-level considerations

Data processing and management (DPM) framework proposes a multi-dimensional representation of the data related activities. It provides a high-level view of the DPM capabilities required at different stages of the data lifecycle considering different inherent aspects to the data such as its source (personal data, public data, etc.) and external aspects that are actions needed to be applied to the data following data manipulation, sharing, security and governance requirements and the commercialisation objectives. These actions require a set of DPM capabilities related to each identified dimension.

The unprecedented growth of cities and communities across the globe is bringing about significant challenges in housing, mobility, governance, environment, energy and water, safety, and economic and social welfare, among others.

On the other hand, advances in science and technology present enormous opportunities in addressing these challenges and building novel IoT-enabled services for smart cities and communities (SC&C).

Digital transformation and ICT initiatives together with the application of science and technology innovation (STI) have proliferated substantial data creation in cities. Public and private sector organizations have accumulated data that can be turned into practical use and benefit to address cities and communities challenges.

STI-based solutions, almost all, require data for problem solving. In this context, data acts as a strategic asset and enabler. Data allows problem identification, understanding, diagnostics and solution. It acts as a raw material, input and, also output depending on the problem and the innovation selected. It also helps determine cities and communities issues and challenges, shape appropriate solutions and validate outcomes. Hence, it acts as a highly critical ingredient in innovating solutions.

Utilizing data in cities and communities context poses its own data related challenges. It is important to identify data specific capabilities since they play a critical role throughout the lifecycle of data. It is also vital to ensure trust in data for accurate, ethical, and secure processing while preserving and respecting privacy. Additionally, appropriate commercialisation and monetization schemes might be needed to achieve tangible business benefits while contributing to the sustainability of data and the creation of a viable economy around it. Furthermore, it is also crucial to establish a prolific innovation ecosystem around data. This entails among others availing requisite data skills, potentially providing business support for data related innovation, conducting research and development (R&D) programmes, and formulating policies, regulations and standards where needed. It is also highly critical to establish an appropriate governance framework around DPM.

The DPM framework depicted in this Recommendation aims to address these data related challenges from a holistic perspective. This all-encompassing approach enables policy-makers as well as city service users to appreciate the broad scope inherent in data related activities and capabilities.

7 DPM framework

This clause presents a comprehensive DPM framework. The framework is composed of dimensions and capabilities for each dimension.

7.1 Dimensions of the DPM framework

The proposed DPM framework is composed of five dimensions, namely:

– Data lifecycle dimension;

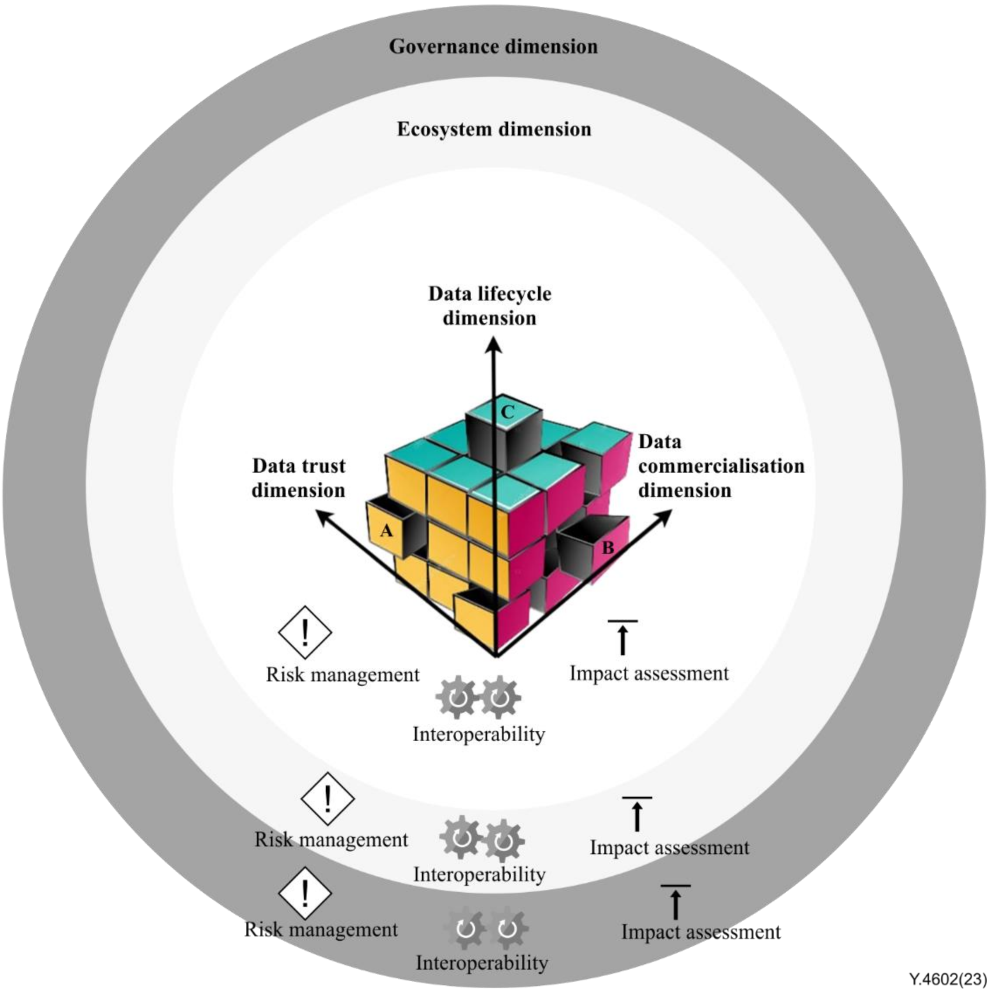
– Data trust dimension;

– Data commercialisation dimension;

– Ecosystem dimension;

– Governance dimension.

As depicted in Figure 1, the framework is designed flexibly to accommodate future expansion in terms of dimensions and capabilities.



Point A: Trusted, and processed data over the trust and data lifecycle dimensions, but not commercialised
Point B: Processed and commercialised data over the data lifecycle and commercialisation dimensions, but not trusted
Point C: Trusted, processed and commercialised data over the trust, the data lifecycle and commercialisation dimensions

Figure 1 – DPM framework [b-ITU-T FG-DPM TS D2.1]

Each dimension offers a particular perspective on DPM. In principle, they are independent, however taken together they complement each other.

The data lifecycle dimension concerns the processing and management activities conducted on the data from its creation to its use and disposal.

The data trust dimension includes various actions taken to safeguard the security, privacy and quality of data and to enhance trust for it.

The data commercialisation dimension includes all activities regarding the monetization and commercialisation of data.

The ecosystem dimension includes all factors and mechanisms that directly or indirectly impact DPM activities in the broader context.

The governance dimension covers all the policy related aspects that will be applied to each dimension.

In addition, there are three common considerations for the above dimensions:

– Interoperability;

– Risk management;

– Impact assessment.

The dimensions and their related capabilities as well as the common considerations for the dimensions will be explained in the following clauses.

7.2 Data lifecycle dimension

This dimension reflects all the steps and the related DPM capabilities followed by data from its creation to its use and disposal. From a data point of view, the listed capabilities might affect the state and structure of data, the location of the data, its combination with other data, its transformation, its use, exchange, storage, and its disposal.

A list of non-exhaustive and illustrative DPM capabilities is provided in Table 1 given below for the data lifecycle dimension.

Table 1 – Data lifecycle capabilities

Dimension capabilities	Capability description
Data source identification	The process of identifying the data source type (e.g., sensor, actuator), its location and potentially its owner.
Data categorization	The process of identifying the related security, privacy, trust, and governance level of the data which can for instance be private, open or public.
Data creation	The process of generating data (e.g., from an IoT device). For example, a sensor monitored environment phenomena generates data either when the phenomena changes (event data), or on a regular monitoring basis (time series data).
Data acquisition / retrieval / capture	The process used by an IoT application that runs a logic of requesting the data from the sensors and proceeds with the data acquisition.
Data collection	The process used by IoT applications to run business logic might need to collect data from different sources that might be sensors or the databases where datasets are stored.
Data masking	The process of making the data not possible to link with its owner. Techniques such as anonymization and pseudonymization are alternatives to enable the privacy of data during its lifecycle.

Table 1 – Data lifecycle capabilities

Dimension capabilities	Capability description
Data parsing	The process of acquiring data (image, etc.), parsing metadata from captured data, and generating new metadata with additional information, then acquiring new data by the registration of generated metadata and existing data.
Data organization	The process of enriching the data during its structuring with contextual information following a common metadata model.
Data transmission	The process of moving data from one location to another. It requires communication technologies between different entities.
Data storage	The process of accumulating data for future processing and use. The duration of storage depends on the application and the security, privacy, and governance rules.
Data monitoring	The process of monitoring service information (management information, etc.) after reconstruction of one precise large-scale image from sequential capturing of real-time data (image, etc.) with data coordination.
Data validation	The process of checking the quality and the correctness of the data.
Data cleaning	The process of removing or modifying incorrect data (e.g., data anomaly detection and fixing).
Data aggregation	The process of selecting data from different sources and combining them.
Data ingestion	The process of absorbing a bulk of data specified by the application(s) without losing the value of the original raw data.
Data processing	The process of handling data as input and applying different treatments that might modify the data or combine it without modifying it with other data in order to produce an output that is useful for a given application or service in the data lifecycle.
Data use, reuse and applications	The process of using, reusing, and applying data to different city services.
Data disposal	The process of getting rid of data (e.g., archiving or backing it up and deleting it or destroying it).

7.3 Data trust dimension

This dimension proposes a broad perspective of data trust which covers all the aspects of security, privacy, and quality among others in the DPM framework including relevant capabilities to enhance data trustworthiness.

Security and privacy capabilities refers to all the activities that allow identification, confidentiality, integrity, availability, and access control to the data. Examples are data encryption, data authentication, data integrity check, data masking, data access control, and so on.

Quality capabilities refers to all the activities that allow the assessment of the data quality from technical and non-technical perspectives. This enhances the confidence and the reliability of data in accordance with the data quality indicators such as completeness and uniqueness. An example of data quality capability is the fit for use check that ensures data is adequate for its intended purpose.

The following table provides the non-exhaustive capabilities needed in this trust dimension.

Table 2 – Data trust capabilities

Dimension capabilities	Capability description
Data confidentiality	Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Data integrity	Ensures the accuracy and completeness of data over its entire life cycle.
Data availability	Ensures accessibility and usability upon demand by an authorized entity.
Data unlinkability	Ensures that a user may make multiple uses of resources or services from data without others being able to link these uses together.
Data transparency	Ensures that an adequate level of clarity of the processes in privacy-relevant data processing is attained so that the collection, processing and use of the information can be understood and reconstructed at any time.

7.4 Data commercialisation dimension

Individuals (consumers) and organizations routinely provide and exchange information while interacting and consuming online. This collected massive amount of information is potentially commercially valuable and is enabling new business models to emerge.

Data can be sold and purchased (i.e., traded or commercially exchanged) just like raw materials in the form of goods and services. Data can also be directly or indirectly monetized; it can be an organization's main or a supplementary offering.

In this context, data commercialisation is the process of creating commercial value from data, and it encompasses a set of capabilities, including but not limited to, monetization, valuation, pricing, licensing, distribution, marketing and sales as briefly described in Table 3.

Table 3 – Data commercialisation capabilities

Dimension capabilities	Capability description
Data monetization	The process of generating incoming money flow with and out of data and data-derived information products and services.
Data valuation	The process of estimating the worth (or value) of data. NOTE – Contextualizing data to identify applicable use case(s) and to determine an appropriate valuation method are significant issues in data valuation.
Data pricing	The process of determining the price of data by an organization for selling it as a product / service.
Data licensing	The process of determining data related terms and conditions for the legally binding agreement between the data licensor and the data licensee.
Data distribution channel	The channel through which data will be sold (distributed) by a seller to the buyer(s).
Data marketing	The process of determining and conducting activities to create awareness for data and to incentivize its usage.
Data sales	The process of conducting activities to fulfil a data sales order, including the receiving, processing, and delivering of the order.

7.5 Data ecosystem dimension

DPM activities and more generally data economy exists in a broad context and are influenced by several factors which directly and indirectly shape or impact it. These factors may be considered peripheral; however, they tend to affect how various DPM activities are in reality conducted.

Hence, the term data ecosystem incorporates all other value adding peripheral and non-specific factors (in addition to the ones addressed by other dimensions).

Table 4 briefly describes some capabilities included in the data ecosystem dimension.

Table 4 – Data ecosystem capabilities

Dimension capabilities	Capability description
Data laws, regulations and policies	Includes all the laws, regulations and policies that directly impact or indirectly shape DPM activities. NOTE – Data laws and regulations can be thought of as data rules promulgated by legally authorized bodies such as a government agency or an appropriating agency. Data policies are a deliberate system of principles to guide decisions and achieve certain intended outcomes related to data.
Data standards	Includes all the commonly agreed norms, specifications and procedures related to data developed by the standards development organizations (SDOs).
Data skills	Refers to various DPM related skills and their availability, including but not limited to, problem solving by data, collecting and drawing insights from data, performing data analytics and quantitative reasoning.
Data R&D programmes	Includes all research and development programmes undertaken by government, private sector and academia related to data, various DPM capabilities and the requirements for it.
Data entrepreneurship	Includes all activities and support schemes to create a business environment that fosters DPM start-ups and the expansion of new firms.
Data economy financial incentives	Refers to monetary benefits to motivate or encourage data economy related activities.
Data platforms	Refers to readily available centralized systems for, among others, collecting, aggregating, analyzing, and processing large sets of data. NOTE – Data platforms provide connectivity and DPM capabilities by architecting and implementing DPM related ICT infrastructure, solutions, and services.

7.6 Governance dimension

Data governance refers to laws, regulations, policies, standards, and guidelines pertaining to how data is processed and managed in other dimensions as well as how the data ecosystem is established and governed. It indicates the scope of data under governance and sets the principles, direction, and unified ways of handling data (e.g., standards) for pertinent issues such as quality, security, privacy, commercialisation, and life-cycle management, among others.

It is important to identify the jurisdictional framework for the governance of DPM in IoT and SC&C. Figure 2 below depicts the sources of the drivers and influencers of the governance framework that need to be taken into consideration for the governance framework to be both legitimate and relevant [b-ITU-T FG-DPM TS D2.1].

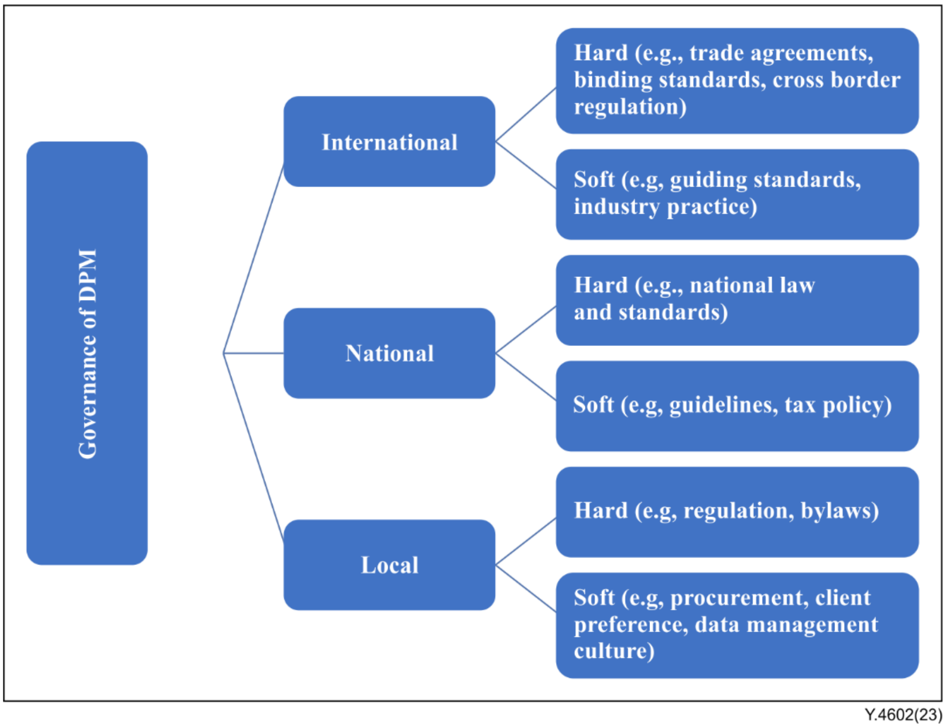


Figure 2 – Jurisdictional framework for the governance of DPM in IoT and SC&C [b-ITU-T FG-DPM TS D2.1]

Existing and applicable local, national, and international (e.g., supra-national, multilateral, regional) policies and agreements need to be taken into consideration during the development of governance for DPM in IoT and SC&C.

8 Common considerations for dimension

This clause includes three considerations that are applicable to all the five dimensions defined in this DPM framework namely, interoperability, risk management, and impact management.

8.1 Interoperability

Interoperability is a core concept for data processing and management (DPM) and it is important to recognise different types and degrees of interoperability. Interoperability refers to the ability of systems to provide services to and accept services from other systems, and to use the services so exchanged to enable them to operate effectively together [b-ISO 37100]. It may also refer to property permitting diverse systems or components to work together for a specified purpose. [b-IEC 60050-831].

Degrees of interoperability

To overcome the complexity and heterogeneity of IoT in SC&C, the DPM framework recognises the principle of minimal interoperability. Minimal interoperability refers to the minimal sufficient degree needed to meet a certain requirement for data sharing, processing and management. It is an approach for establishing a set of modular mechanisms across multiple application domains and geographic territories, without having to specify everything in complete detail, and without requiring complete implementation of and compliance with the entire framework. The principle of minimal interoperability can be applied to all types of interoperability, including, but not limited to, context information management (cross-domain information meta-model), shared data models (domain-specific information models), and ecosystem transaction management (conditions for exchange).

NOTE – The DPM framework does not directly establish such minimal interoperability mechanisms while recognising the need for further work in this regard.

Types of interoperability

The interoperability concept applies to all the five dimensions of the DPM framework. Data lifecycle interoperability is concerned more with technical issues such as controlling devices and communication technologies heterogeneity, multi-domain data aggregation and integration standards and metadata, and ontologies that are related to the semantic interoperability of data. However, interoperability can be equally extended to include trust dimension, commercialisation / economy dimension, ecosystem dimension and last but not the least the governance dimension. Interoperability pertaining to those dimensions will be concerned with technical as well as non-technical issues.

8.2 Risk management

DPM in IoT and SC&C can encounter or even create risks during its implementation. It is recommended that these risks are identified and managed through a risk management process to ensure a safe and secure development of SC&C.

To this purpose, a high-level four-step methodology is defined below: (definitions are adopted from ([b-ISO Guide 73]:2009 Risk management – Vocabulary):

– Risk identification: the process of finding, recognizing, and describing risk;

– Risk analysis: the process of identifying the nature of risk and determining its level;

– Risk evaluation: the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable;

– Risk treatment: the process of mitigating or modifying the risk.

Risks can be managed at "micro" and "macro" levels. The "micro" level manages risks at a project / initiative level whereas the "macro" level manages risks at the ecosystem or city / community level.

One important related capability is the ability to manage the city / community level risks related to the ecosystem such as systemic risks arising from the DPM. Another related capability is to determine the risk appetite and to make sure that the stakeholders accept the uncertainties and the potential adverse consequences generated by the DPM.

9 Guidance on using the DPM framework

This clause provides general guidance on how the DPM framework can be used. It is important for users of the DPM framework to define the scope of the DPM framework prior to its application.

9.1 Scoping boundaries for DPM framework

Boundaries for scoping purposes in this Recommendation consist of three types:

1) jurisdiction,

2) dimensions, and

3) common considerations for dimensions.

Boundaries determine what is "in" and "out" of the scope of the DPM framework as defined in this Recommendation.

9.1.1 Jurisdictional boundary

The DPM framework determines the jurisdictional boundary (e.g., city, community, nation, organization) for which it will be applied. DPM framework is flexible to accommodate well-defined jurisdictions with respect to geography, legal entity, and any other as deemed appropriate.

9.1.2 Dimensions boundary

The DPM framework needs to select one or more of the dimensions of the DPM framework during its application. In other words, the framework may opt to include one or more of the data lifecycle, data trust, data commercialisation, ecosystem and governance dimensions. The included dimensions comprise the scope in terms of the framework dimensions.

9.1.3 Common considerations for dimensions boundary

The DPM framework may opt to include one or more of the common considerations for dimensions, namely interoperability, risk management, and impact assessment. The included considerations comprise the scope in terms of the common considerations for the selected dimensions.

9.2 Revision of scoping boundaries

The boundaries assist users to determine the scope for applying the DPM framework. The framework is flexible to accommodate changes in scope in due course, whereby the DPM framework can modify the scoping boundaries to reflect the changing needs and concerns arising in practice.

Upon revision of scoping boundaries, the DPM framework can be reapplied with the new scoping boundaries taken into consideration. This flexibility allows the DPM framework to be attuned and revised as data maturity evolves over time.

Appendix I

Impact assessment

(This appendix does not form an integral part of this Recommendation.)

Data initiatives have a multitude of impacts. It is quite significant to identify and assess this impact. Identification and assessment of impact will allow better risk mitigation, DPM initiatives planning, setting and managing expectations with stakeholders, well-informed budgeting, and benefits realization among others. This will also help in communicating the DPM initiatives.

It is important to take a broad perspective and assess the impact of the DPM initiatives. The international association for impact assessment (IAIA) defines impact assessment as "the process of identifying the future consequences of a current or proposed action". Impact assessment can help owners of the DPM initiatives, as well as their stakeholders to determine the extent of the impact for their data initiatives. It can be used to identify and circumvent the adverse and unintended impacts while capitalizing on and enhancing the positive and sustainable impacts further.

Ex-ante impact assessment: Ex-ante impact assessment entails conducting a prospective analysis of what the impact of DPM initiatives might be. In general, it intends to inform DPM initiative owners of the potential future consequences.

Ex-post impact assessment: Ex-post impact assessment entails conducting a retrospective analysis of what the impact of DPM initiatives have been. It also permits evaluating whether intended consequences are attained or not.

In general, it would be beneficial to compare ex-ante and ex-post impact assessments to compare and contrast their results. Discrepancies would allow taking course correcting actions and also identification of the lessons learnt.

DPM initiatives impacts are assessed along the economic and environmental dimensions.

I.1 Economic impact assessment

Economic impact assessment identifies and analyses the economic effects and contributions of DPM initiatives. The economic impact can be viewed in terms of aggregate economic activity, gross value added (GVA)[1] or gross domestic product (GDP), productivity, wealth, personal income, jobs and labour force among others. DPM and data economy initiatives can qualitatively and quantitatively analyse economic impacts.

Top-down and bottom-up economic impact assessment

The economic impact can be assessed either through a top-down or a bottom-up approach. Top-down assessment looks at the overall changes in the economy and selected key economic variables (e.g., GDP, GVA, etc.) and seeks to understand the extent to which those economy-level changes can be attributed to DPM initiatives. Top-down economic impact assessment can be done through econometric modelling with a measure of the DPM initiatives as one explanatory variable, alongside a range of other variables that could explain the changes being observed in the selected key economic variables.

The bottom-up approach is based on a theory of change of how the inputs and activities associated with a DPM policy or initiative ultimately lead to end impacts in the economy. The relationships between impacts and the DPM policy or initiative are often complex, therefore describing the relationship between an input, activity, outputs / outcomes, and impacts is key. This approach in

1 GVA is defined as "the value of output less the value of intermediate consumption; it is a measure of the contribution to GDP made by an individual producer, industry or sector" [b-OECD].

general requires the collection of more data than an econometric modelling, top-down approach, and therefore can require greater resources to implement.

Bottom-up models estimate economic impacts at direct, indirect, and induced levels

– Direct impacts arise from direct expenditures associated with DPM initiatives (e.g., DPM related goods and services procurement and implementation, additional DPM skills needs, etc.).
– Indirect impacts arise from the suppliers of DPM initiatives procuring goods and services and recruiting new employees (i.e., creating new DPM related employment) to meet the DPM initiatives' demand.
– Last, but not the least, induced impacts include disbursements stemming from additional income in the DPM initiatives involving households (households that received extra earnings due to DPM initiatives and spend it on various other items). Induced impacts are spill-over impacts to various sectors of the economy.

The indirect and induced impacts are in general called secondary impacts.

I.2 Environmental impact assessment

Environmental impact assessment (EIA) is an analytical process that systematically examines the possible environmental consequences of the implementation of projects, programmes and policies [b-United Nations]. Hence, in this Recommendation environmental impact captures the anticipated effects and consequences of DPM initiatives on water, energy, emissions, air, land, waste and in general on the urban natural environment and resources (in a city). EIA allows a comprehensive impact assessment going beyond the social and economic impacts discussed in the previous sections.

Environmental impact intends to assess one or more of the following areas (depending on the selected DPM initiative):

• water – its usage and consumption and also potential loss (e.g., water supply leaks); planning for water sources, water availability, and also measuring and enhancing water quality;
• energy – its usage and consumption and also potential loss (e.g., energy transmission leaks); planning for energy sources (e.g., energy mix in terms of renewables) and energy availability;
• emissions – the extent to which greenhouse gas (GHG) emissions are affected and its impact on climate change;
• air quality – how DPM initiatives affect the particulate matters in the air and affect air pollution;
• waste – changes in waste collection, treatment, disposal, recycling, etc.;
• resilience – prevention or preparation for natural disasters (flooding, earthquakes, fires, landslides, etc.);
• land and soil – changes in land use and allocation, soil quality and quantity;
• biodiversity – the extent to which biological diversity is affected in terms of species, specifically on endangered and protected species, flora, fauna and landscape changes.

I.3 Scoping boundaries for impact assessment

This section is based on the scoping boundaries defined in ITU-T Recommendation "Smart sustainable cities impact assessment" [b-ITU-T Y.4905] and applied to the DPM context. This clause provides general guidance on how impact can be assessed for DPM initiatives. A number of DPM initiatives may be implemented with distinct scopes. It is important to determine the impact assessment boundaries and apply a well-defined process.

Initially, the time horizon for impact assessment should be determined prior to conducting impact assessment. More specifically, the impact assessment should clearly indicate the timeframe for assessment with a well-defined initial and completion time. Impacts should be identified for this timeframe.

Impact assessment boundaries in this Recommendation consist of three types:

– geographical,

– initiative, and

– impact.

Geographical boundary

Impact assessment should determine the geographical boundary (i.e., the actual physical or territorial boundary) for which the impact assessment will be conducted. For example, an entire community, city or a nation's boundaries may be used, or a different geographical boundary may be selected for impact assessment (e.g., a subset of administrative boundaries).

DPM initiatives may impact beyond their immediate location of implementation. Hence, it is important to consider suitable spatial boundary for identifying DPM initiatives impact.

DPM initiative(s) boundary

It is important to determine the scope of the DPM initiative(s) for which the impact assessment will be conducted.

One or more DPM initiative(s) may be included as part of the impact assessment or a portion of an initiative as well.

Various factors such as size, dependencies, complexity, and implementation timeframes may be used as possible factors to consider in selecting which DPM initiative(s) to incorporate in the data economy impact assessment.

Impact type boundary

It is essential to decide which of the three main impact types will be incorporated in the data economy impact assessment, i.e., performance, operation, sustainability, social, economic and environmental.

In general, an all-encompassing approach can be adopted and all three aforementioned impact types can be included in the impact assessment. That is, social, economic and environmental perspectives can be included during the impact assessment.

Various stakeholders can be consulted to initially assess the potential impacts of the DPM initiatives. Consultation with government officials, related businesses, NGOs and selected individuals and community members might help identify which impact type(s) to include for impact assessment.

I.4 Impact evaluation and mitigation

Subsequent to conducting the impact assessment, potential impacts will be identified. It is also crucial to identify the relative importance of each potential impact to determine potential mitigation measures.

These measures may avoid, accept, reduce, or minimize undesirable and possibly adverse potential impacts while preserving and increasing desirable and favourable ones. The following measures can be considered for the mitigation of potential impacts:

i ***Accept impacts***: the potential impacts can be agreed upon and possibly tolerated in some cases. Hence the DPM initiative(s) can be implemented.

ii ***Reduce impacts***: the potential adverse impacts can in some cases be reduced by taking targeted actions. For example, policies and regulations may eliminate concerns of individuals, organizations and communities related to data in certain cases; training and reskilling programmes may boost the skills of the existing labour force and may also create new employment opportunities diminishing resistance to DPM initiatives (if any).

iii *Monitor impacts*: the potential impacts are closely watched and monitored during the implementation of the DPM initiative(s). Actual outcomes may necessitate taking further mitigation actions. Adverse impacts, if they occur, may trigger such actions.

vi *Avoid impacts*: in exceptional cases DPM initiative(s) may be abandoned due to the identified adverse impacts which critically obstruct their implementation. Prior to abandoning DPM initiative(s), various alternatives for reducing or monitoring impacts should be considered.

On the other hand, desirable (favourable) impacts act as a strong lever to highlight and convey the positive aspects of DPM initiatives to their stakeholders. They can facilitate easier funding for these stakeholders.

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure Terminology: Terms and definitions*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for Next Generation Networks*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4905] Recommendation ITU-T Y.4905 (2019), *Smart sustainable city impact assessment*.

[b-ITU-T FG-DPM TS D0.1] Technical Specification D0.1 (2019), *Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary*.

[b-ITU-T FG-DPM TS D2.1] Technical Specification D2.1 (2019), *Data processing and management framework for IoT and smart cities and communities*.

[b-IEC/ISO/ITU draft white paper] IEC/ISO/ITU Smart city coordination task group:2019, Draft white paper: *Suggested priority terms in need of common definitions to support standards activities for smart city*. Barcelona, World Smart City Forum, April 17, 2019.

[b-IEC 60050-831] IEC 60050-831 ED1 (2022), International Electrotechnical Vocabulary (IEV) – Part 831: *Smart city systems*. <https://bds-bg.org/en/project/show/iec:proj:102464>

[b-IEC Guide 120] IEC Guide 120:2018, *Security aspects – Guidelines for their inclusion in publications*. <https://webstore.iec.ch/publication/62122>

[b-ISO 5127] ISO 5127:2017, *Information and documentation — Foundation and vocabulary*. <https://www.iso.org/standard/59743.html>

[b-ISO 8000-2] ISO 8000-2:2022, *Data quality – Part 2: Vocabulary*. <https://www.iso.org/standard/85032.html>

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. <https://www.iso.org/standard/65694.html>

[b-ISO 37100] ISO 37100:2016, *Sustainable cities and communities – Vocabulary*. <https://www.iso.org/standard/71914.html>

[b-ISO Guide 73] ISO Guide 73:2009, *Risk management – Vocabulary*. <https://www.iso.org/standard/44651.html>

[b-ISO/IEC Guide 51] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*. <https://www.iso.org/standard/53940.html>

[b-ISO/IEC 30182] ISO/IEC 30182:2017, *Smart city concept model – Guidance for establishing a model for data interoperability*. <https://www.iso.org/standard/53302.html>

[b-ISO/IEC TR 10032] ISO/IEC TR 10032:2003 *Information technology – Reference Model of Data Management*. <https://www.iso.org/standard/38607.html>

[b-ISO/IEC TR 29110-5-3] ISO/IEC TR 29110-5-3:2018, *Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) – Part 5-3: Service delivery guidelines*. <https://www.iso.org/standard/69049.html>

[b-OECD] OECD (2007), Glossary of Statistical Terms. <https://crvssystems.ca/oecd-glossary-statistical-terms>

[b-PAS 185] PAS 185:2017, *Smart Cities. Specification for establishing and implementing a security-minded approach*. <https://www.en-standard.eu/pas-185-2017-smart-cities-specification-for-establishing-and-implementing-a-security-minded-approach/>

[b-United Nations] United Nations (1997), *Glossary of Environment Statistics, Studies in Methods*, Series F, No. 67. <https://unstats.un.org/unsd/publication/seriesf/seriesf_67e.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2023