International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3055

(09/2020)

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

Future networks

Framework for trust-based personal data management

Recommendation ITU-T Y.3055

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
Network control architectures and protocols	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.3055

Framework for trust-based personal data management

Summary

Data has become more important for various industries, and data stakeholders aggregate personal data from various data sources to find new values. To increase benefits from personal data utilization with the balance of privacy protection, it is important to support trust-based personal data management that considers the trust in personal data utilization processes. Thus, Recommendation ITU-T Y.3055 provides a framework for trust-based personal data management. It introduces the necessity of trust-based personal data management based on the analysis of personal data management. Then, it identifies various requirements for trust-based personal data management. After identifying the requirements, Recommendation ITU-T Y.3055 provides a framework architecture specifying related functional blocks and reference points with relevant information flows. Details of prospective technologies for personal data management and a trust evaluation model with a specific use case are described in informative appendices.

NOTE – In this Recommendation, some capabilities and applications may be related to regulation in some countries. In this case, non-functional aspects related to regulation are out of scope.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3055	2020-09-29	13	11.1002/1000/14393

Keywords

Personal data, trust-based personal data management.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T Y.3055

Framework for trust-based personal data management

1 Scope

To increase benefits from personal data utilization with the balance of privacy protection, it is important to support trust-based personal data management that considers trust in personal data utilization processes. Therefore, this Recommendation provides a framework for trust-based personal data management. More specifically, this Recommendation covers the following:

– The necessity of trust-based personal data management;

– Requirements considering personal data management comprising various stakeholders;

– Framework architecture specifying related functional blocks and reference points;

– Information flows describing interactions between/among functional blocks.

Details of prospective technologies for personal data management and a trust evaluation model with a specific use case are described in informative appendices.

NOTE – In this Recommendation, some capabilities and applications may be related to regulation in some countries. In this case, non-functional aspects related to regulation are out of scope.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.2 PII principal [b-ISO/IEC 29100]: Natural person to whom the personally identifiable information (PII) relates.

NOTE – Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ICT	Information and Communication Technology
TPDM	Trust-based Personal Data Management
PII	Personally Identifiable Information

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement needs not be present to claim conformance.

The term "personal data" in this Recommendation is equivalent to the term "personally identifiable information" in [b-ISO/IEC 29100] (see definition in clause 3.1.1).

6 Overview

6.1 Personal data stakeholders

As a result of the proliferation of connected technologies, an enormous amount of data is being generated. With emerging big data technologies, data has now become a key item for a data-driven environment. Particularly, personal data (or personally identifiable information) is drawing attention from various stakeholders because they can be used in value-added services and applications. There are complex value chains (from personal data creation to consumption) for various ecosystems utilizing personal data for new innovative services and applications. Figure 6-1 shows a generalized model for identifying personal data stakeholders in an information communication technology (ICT) environment.

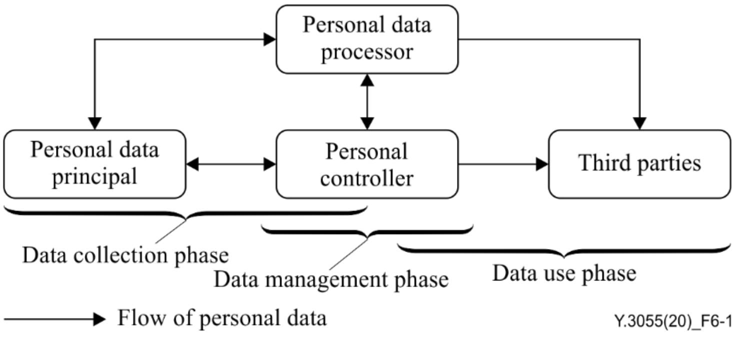


Figure 6-1 – A generalized model for personal data stakeholders in an ICT environment

NOTE 1 – Stakeholders and possible interactions between them are also described in [b-ISO/IEC 29100]

- **Personal data principal**: A person that is identified by personal data, which can be utilised by other stakeholders. As an individual who is the subject of personal data, a personal data principal may be inferable, directly or indirectly, through reference to one or more factors specific to his or her identities (e.g., physical, physiological, mental, economic, social or cultural identity).
- **Personal data controller**: A personal data stakeholder that collects and manages personal data by providing services/applications to personal data principals (e.g., personal data

principals create personal data when they utilise the services/applications from personal data controllers). A personal data controller determines the purposes and means for processing personal data other than personal data principal who uses it for personal purposes. The personal data controller instructs other types of stakeholders (e.g., personal data processors) to process personal data on its behalf while the responsibility for the processing remains with the personal data controller. That is, a personal data controller has overall responsibility for the why and how of personal data processing activities.

– **Personal data processor**: A personal data stakeholder that processes personal data and extracts information. A personal data processor processes personal data in accordance with the instructions of or on behalf of a personal data controller. The personal data processor must be able to provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that processing will comply with various requirements.

– **Third parties**: Any persons or groups that receive personal data from a personal data controller or a personal data processor. A third party will become a new personal data controller in its own right.

NOTE 2 – One entity can represent multiple stakeholders. For example, a single data broker can act as a personal data controller and a personal data processor at the same time.

Identifying whether a stakeholder is a personal data controller, a personal data processor, or a third party is not always straightforward. However, identifying the personal data stakeholders involved in a given personal data utilization situation can help them to decide what management processes are necessary and who should conduct them. Understanding various requirements in respect of personal data is important as it will help organisations to establish clearly their own and other stakeholders' responsibilities in the personal data management process.

With various personal data stakeholders, personal data flow has three main phases:

i) data collection phase,

ii) data management phase, and

iii) data use phase.

In the data collection phase, personal data are created by activities of personal data principals and are collected by personal data controllers and processors. In the data management phase, personal data controllers and processors handle collected personal data based on the agreement from the personal data principals. A personal data controller can also provide personal data to personal data processors if necessary. In the data use phase, a personal data processor processes and analyses collected personal data to find new information. Then, personal data consumers utilise the results of the personal data processors for their purposes. Since the personal data lifecycle covers various personal data stakeholders, it is needed to manage personal data by complying with various requirements regarding privacy issues. Therefore, the concept of personal data management is introduced.

6.2 Personal data management

Personal data management is activities that address the protection of privacy as potentially affected by an operation or set of operations performed upon personal data [b-ISO/IEC 27701] such as the collection, storage, alteration, retrieval, consultation, disclosure, de-identification, anonymization, pseudonymization, dissemination, or otherwise making available, deletion, or destruction of personal data [b-ISO/IEC 29100]. Any personal data stakeholders that handle personal data should have methods for personal data management based on the requirements to comply with various corresponding regulations. Since personal data management affects all phases of personal data flow, the following bullet items describe an application of personal data management for each phase of the personal data flow shown in Figure 6-1.

NOTE 1 – The detailed guidelines for personal data management are described in various existing ITU-T and ISO/IEC standards such as [b-ITU-T X.1058], [b-ISO/IEC 27701], and [b-ISO/IEC 29100].

- **Data collection phase**

One personal data management principle directly related to the data collection phase is that of data minimization. Each personal data controller or processor that is collecting the data needs to precisely define what personal data are actually needed (and what are not needed) for the purposes of the processing, including also the relevant data retention periods. In accordance with the consent or the agreement from personal data stakeholders, specific processes may be in place to comply with various requirements about personal data (e.g., exclude unnecessary personal data from collection, reduce data fields, provide automated deletion mechanisms, etc).

Another aspect is when aggregated information is used instead of personal data. Indeed, in certain cases (e.g., in statistical analysis from distributed sources), the personal data might not even need to be collected in the first place, and the collection of de-identified information might be sufficient.

- **Data management phase**

The data management phase is composed of data transformation and data retention phases. Data transformation encompasses a range of alterations for improving data utility and privacy, including aggregation, statistical disclosure limitation, encryption, etc. Data transformation may be applied at multiple stages, including directly after collection, directly prior to long term retention, after a substantial retention period, and prior to or integrated with access. The data transformation method choice should be made after careful considerations of the privacy guarantee that is required. The transformation decision should also consider the analysis that must be supported according to the purpose of data use, as the techniques employed for reducing disclosure risks can affect potential uses and analysis.

Data retention is described as to store data, including personal data, to any form of non-volatile storage by a personal data controller or a party acting under the personal data controller's direction. The information on security and privacy controls is common at the retention stage (e.g., access control, maintenance, security assessments, authentication procedures, incident monitoring and response, and audits). In particular, personal data stakeholders commonly implement data retention and decommissioning policies to ensure data are retained for no longer than necessary and data backups are destroyed after a certain length of time.

- **Data use phase**

The primary objective of personal data management is protecting the privacy of individuals in the process of collecting, storing, and sharing personal data for a range of purposes and applications. One of the main reasons for releasing personal data is to provide others with an opportunity to support specific services. Therefore, personal data management should also seek to preserve as much utility in the information as possible, while protecting the privacy of individuals. This dual purpose of personal data management makes it an important approach to consider for use in different contexts, including data release models.

NOTE 2 – Prospective technologies for personal data management are described in Appendix I.

6.3 The necessity of trust-based personal data management

Even if the concept of personal data management covers various issues regarding the processing of personal data, personal data can be compromised at various points and interfaces because the personal data ecosystem forms a very complex value chain. Objects in large-scale networks such as in the Internet of things possibly lack the knowledge to evaluate services' reliability as both untrustworthy and trustworthy objects can interact with each other. In addition, people (i.e., personal data principals) think they have no chance to control and to monitor their personal data utilisation by services and applications. Accordingly, mistrust about personal data stakeholders has sprouted over the years.

To overcome the current untrustworthy personal data ecosystem, trust becomes an essential element for value-added business models and personal data management in ICT environments. [ITU-T Y.3052] describes the concept of trust provisioning that provides a useful method for minimizing various risks through identifying trust characteristics. The objective of trust-based personal data management (TPDM) is to provide relevant trust information about the ability of personal data management to personal data stakeholders. Each stakeholder is able to refer to trust information for interacting with other stakeholders for various purposes. With a new trust-based personal data management concept, the balance of privacy protection and data utilization can be achieved not only by protecting the rights of the stakeholders but also by providing trust information to the stakeholders to encourage personal data utilisation. Therefore, this Recommendation describes a TPDM framework while considering characteristics of major personal data stakeholders.

7 Requirements for trust-based personal data management

The requirements for trust-based personal data management are identified as follows.

7.1 Requirements for personal data evaluation

Personal data evaluation is required to:

- monitor heterogeneous data types from various personal data sources (e.g., services or applications);
- filter and pre-process personal data from the monitored data (e.g., extract and identify personal data) before personal data transactions;
- verify privacy compliance of personal data to check whether personal data are transacted in accordance with established guidelines or specifications;
- evaluate the trust of personal data stakeholders utilizing personal data to check suitability for personal data transactions;
- manage the overall lifecycle (e.g., data collection, processing, storage, and destruction) associated with personal data.

NOTE – General requirements and guidelines for handling personal data are described in [b-ISO/IEC 29100] and [b-ISO/IEC 27701].

7.2 Requirements for personal data transaction management

Personal data transaction management is required to:

- apply proper methods to personal data (e.g., de-identifying personal data, checking consents of personal data principals, etc.) for satisfying privacy compliance before personal data transactions;
- safely transfer the personal data to personal data stakeholders;
- monitor and track the overall lifecycle about personal data transactions between/among personal data stakeholders (e.g., personal data principals, controllers, and processors) for internal compliance assessment and trust evaluation in the future.

7.3 Requirements for privacy compliance management

Privacy compliance management is required to:

- monitor privacy compliance guidelines from internal personal data stakeholders (e.g., rules, contracts, or consents/agreements between/among the personal data stakeholders, etc.) and external regulatory and standardisation bodies (e.g., privacy policies, regulations or standards related to personal data, etc.);

- perform privacy compliance assessment of personal data stakeholders based on the monitored guidelines;
- provide compliance information (including compliance guidelines and compliance assessment results) to personal data stakeholders;
- manage and track the overall lifecycle for keeping up to date compliance information.

7.4 Requirements for trust information management

Trust information management is required to:

- monitor trust information from other third parties to gather information for trust evaluation and extract trust attributes for evaluating trust from numerous data sources;

NOTE 1 – Trust attributes are used as gradients to compute trust indicators, such as ability, benevolence, and integrity (see [ITU-T Y.3052] for the details of trust information).

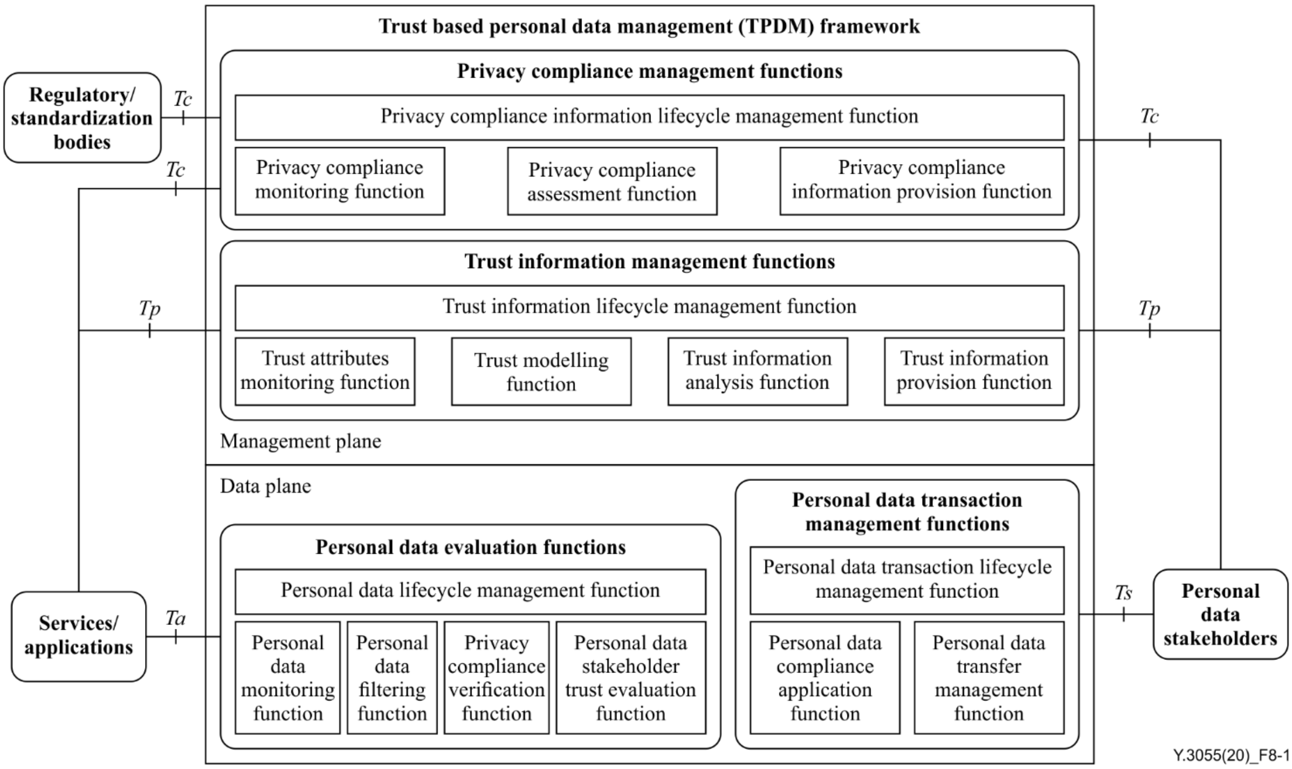
NOTE 2 – The target of trust evaluation is not limited to certain types of entities (e.g., personal data stakeholders, services and applications that provide personal data, etc.).

- model and evaluate trust based on trust information (e.g., trust attributes, indicators, etc.);

NOTE 3 – It is recommended to consider various factors for modelling and evaluating trust such as direct trust (e.g., trustworthiness or objective factors), indirect trust (e.g., experience, reputation, or subjective factors based on the relationships)

- manage trust information to be stored in a repository to keep track of trust over time and update trust information during the overall trust information lifecycle (e.g., created, updated, and destroyed);
- provide trust evaluation results and trust information (e.g., trust attributes and trust indicators) to personal data stakeholders.

8 Framework architecture for trust-based personal data management



Trust based personal data management (TPDM) framework
Privacy compliance management functions
Privacy compliance information lifecycle management function
Privacy compliance monitoring function
Privacy compliance assessment function
Privacy compliance information provision function
Trust information management functions
Trust information lifecycle management function
Trust attributes monitoring function
Trust modelling function
Trust information analysis function
Trust information provision function
Management plane
Data plane
Personal data evaluation functions
Personal data lifecycle management function
Personal data monitoring function
Personal data filtering function
Privacy compliance verification function
Personal data stakeholder trust evaluation function
Personal data transaction management functions
Personal data transaction lifecycle management function
Personal data compliance application function
Personal data transfer management function
Regulatory/ standardization bodies
Services/ applications
Personal data stakeholders
Tc
Tc
Tc
Tp
Tp
Ta
Ts
Y.3055(20)_F8-1

Figure 8-1 – A framework architecture for trust-based personal data management

A framework architecture for trust-based personal data management is shown in Figure 8-1. Each component provides functional modules aligning with specified requirements.

8.1 Trust-based personal data management framework

A trust-based personal data management (TPDM) framework has two major planes:

i) data plane; and

ii) management plane.

The data plane is directly related to personal data transactions between personal data stakeholders. It processes personal data from services and applications that have collected a personal dataset and decides whether personal data transactions should be performed or not based on the results of compliance verification and trust evaluation from the management plane. Based on the decision, personal data are properly processed for satisfying privacy compliance requirements and guidelines according to the level of trust and compliance of the target personal data stakeholder before transfer and transaction.

On the other hand, in the management plane, privacy compliance management is performed by assessing compliance guidelines from internal personal data stakeholders and external regulatory/standardisation bodies about personal data usage. Moreover, trust information is evaluated, and trust is assessed based on criteria related to personal data utilization. These assessment results are provided through trust provisioning functions to personal data stakeholders involved in the TPDM framework. The detailed explanations about each function are described in clauses 8.1.1 to 8.1.4.

8.1.1 Personal data evaluation functions

Personal data evaluation functions monitor and filter personal data from various data sources and check personal data compliance verification and trust evaluation of personal data stakeholders before actual personal data transactions.

– **Personal data monitoring function**: This function identifies personal data from an input dataset and extracts only personal data that should be handled in the TPDM framework for the transactions from various data sources of services and applications.

– **Personal data filtering function**: This function filters and categorizes personal data based on its importance (e.g., quasi-PII or PII) and sensitivity to privacy exposure.

NOTE 1 – A form of personal data is not limited to certain types of data. It can be texts, image, audio, video, etc. Based on services/applications or the scope of personal data form, the TPDM framework should support the relevant processing methods (i.e., monitoring and filtering personal data) before personal data transactions.

– **Privacy compliance verification function**: This function verifies privacy compliance of filtered personal data based on the results from privacy compliance management functions for personal data transactions. If the collected personal data are not privacy compliant (e.g., violation of either internal or external privacy compliance guidelines), the personal data should be discarded immediately, and the TPDM framework performs necessary actions to personal data stakeholders (e.g., notification, etc.).

– **Personal data stakeholder trust evaluation function**: This function evaluates the trust of the target personal data stakeholder (who receives personal data) for personal data transactions based on the results from trust information management functions.

NOTE 2 – Based on the results from personal data compliance verification function and personal data stakeholder trust evaluation function, the TPDM framework could inform the results to personal data providers (i.e., services applications) and decide whether it continues personal data transactions or not.

– **Personal data lifecycle management function**: This function manages the lifecycle of personal data and decides proper actions to handle personal data (e.g., analysis, usage, discard, etc.). Particularly, the expired personal data should be deleted from the TPDM framework.

8.1.2 Personal data transaction management functions

Personal data transaction management functions process personal data based on the requirements from privacy compliance management and transfer personal data to the target personal data stakeholder for personal data transactions. They also keep records of personal data transactions and consents to check the reliability of the transactions.

– **Personal data transaction lifecycle management function**: This function monitors personal data transactions and keeps their records for future trust evaluation and internal compliance assessment with a repository to store transactions and all the logs and contexts relevant to transactions. It also coordinates transactions across the TPDM framework (e.g., transaction lifecycle management, coordination of transactions across multiple resources, etc.).

– **Personal data compliance application function**: This function applies the proper processing methods to satisfy privacy compliance guidelines from the privacy compliance assessment function before personal data transfer based on the compliance assessment and trust evaluation results of the target personal data stakeholder.

– **Personal data transfer management function**: This function transfers the processed personal data to the target personal data stakeholder with proper security methods (e.g., end-to-end encryption, authentication mechanisms, etc.) based on the requirements/contracts or the trust of the stakeholders.

8.1.3 Trust information management functions

Trust information management functions model, analyse, and manage trust information of personal data stakeholders (e.g., trust attributes, trust indicators, trust index and the level of trust) associated with all related information for personal data utilizations and transactions.

– **Trust attributes monitoring function**: This function recognizes characteristics and factors influencing the trust of personal data stakeholders about personal data utilizations and transactions, and it determines proper trust attributes for trust modelling, analysis, and evaluation.

– **Trust modelling function**: This function is used to specify, annotate, and build trust relationships between/among personal data stakeholders to measure trust with obtained trust attributes.

– **Trust information analysis function**: This function analyses trust information by combining trust attributes and trust models for trust evaluation and trust information provision.

NOTE 1 – Methods for modelling and evaluating the trust with trust information are not limited to certain approaches. Various methods can be applied for handling trust information (e.g., simple rule-based decision mechanisms, complex artificial intelligence models, etc.).

– **Trust information lifecycle management function**: This function manages trust information by creating, updating, and destroying trust information in proper time and also manages the contexts for trust establishment, trust update, and trust revocation.

– **Trust information provision function**: This function provides trust information (e.g., a trust index as the benchmark measure for evaluating trust and trust indicators as criteria for measuring a trust index) from the trust management functions to each personal data stakeholder.

NOTE 2 – A form of trust provisioning results could be varied depending on environments (e.g., numerical value, dashboard, notification, etc.)

8.1.4 Privacy compliance management functions

Privacy compliance management functions monitor relevant compliance requirements from both internal personal data stakeholders and external regulatory or standardisation bodies and assess the level of compliance during the personal data evaluation process.

- **Privacy compliance monitoring function**: This function monitors privacy compliance requirements and guidelines from internal personal data stakeholders (e.g., rules, contracts, service level agreements, policies, etc.) and external regulatory/standardisation bodies (e.g., privacy policies, regulations or standards related to personal data, etc.). It periodically monitors the changes of privacy compliance requirements and guidelines and triggers privacy compliance assessment function for updating.
- **Privacy compliance assessment function**: This function assesses the level of privacy compliance based on the requirements for compliance verification during the personal data evaluation process and for compliance application during the personal data transaction.
- **Privacy compliance information provision function**: This function provides compliance assessment results from privacy compliance assessment functions to each personal data stakeholder.

NOTE – A form of compliance information could be varied depending on environments (e.g., numerical value, dashboard, notification, texts, etc.)

- **Privacy compliance information lifecycle management function**: This function manages the lifecycle of privacy compliance information (e.g., creation, usage, destruction, etc.) and maintains up to date privacy compliance information for verification of personal data transactions and personal data stakeholders.

8.2 Reference points

8.2.1 Reference point *Ta*

The reference point *Ta* enables the TPDM framework to monitor and evaluate personal data collected from services and applications for personal data evaluation functions.

8.2.2 Reference point *Ts*

The reference point *Ts* enables the transfer of properly processed personal data (i.e., personal data originally monitored by *Ta*) to personal data stakeholders based on the privacy compliance assessment and trust evaluation.

8.2.3 Reference point *Tc*

The reference point *Tc* enables the monitoring of internal (from services/applications) and external (from regulatory/standardisation bodies) privacy compliance information for privacy compliance management functions and provides privacy compliance information to personal data stakeholders.

8.2.4 Reference point *Tp*

The reference point *Tp* enables the collection of trust related information from services/applications and provides trust evaluation results and trust information to personal data stakeholders.

9 Information flows

This clause specifies procedures for trust-based personal data management in accordance with the framework architecture identified in clause 8. This clause describes five major flows for the TPDM framework:

i) personal data transaction,

ii) trust information management,

iii) trust information provision,

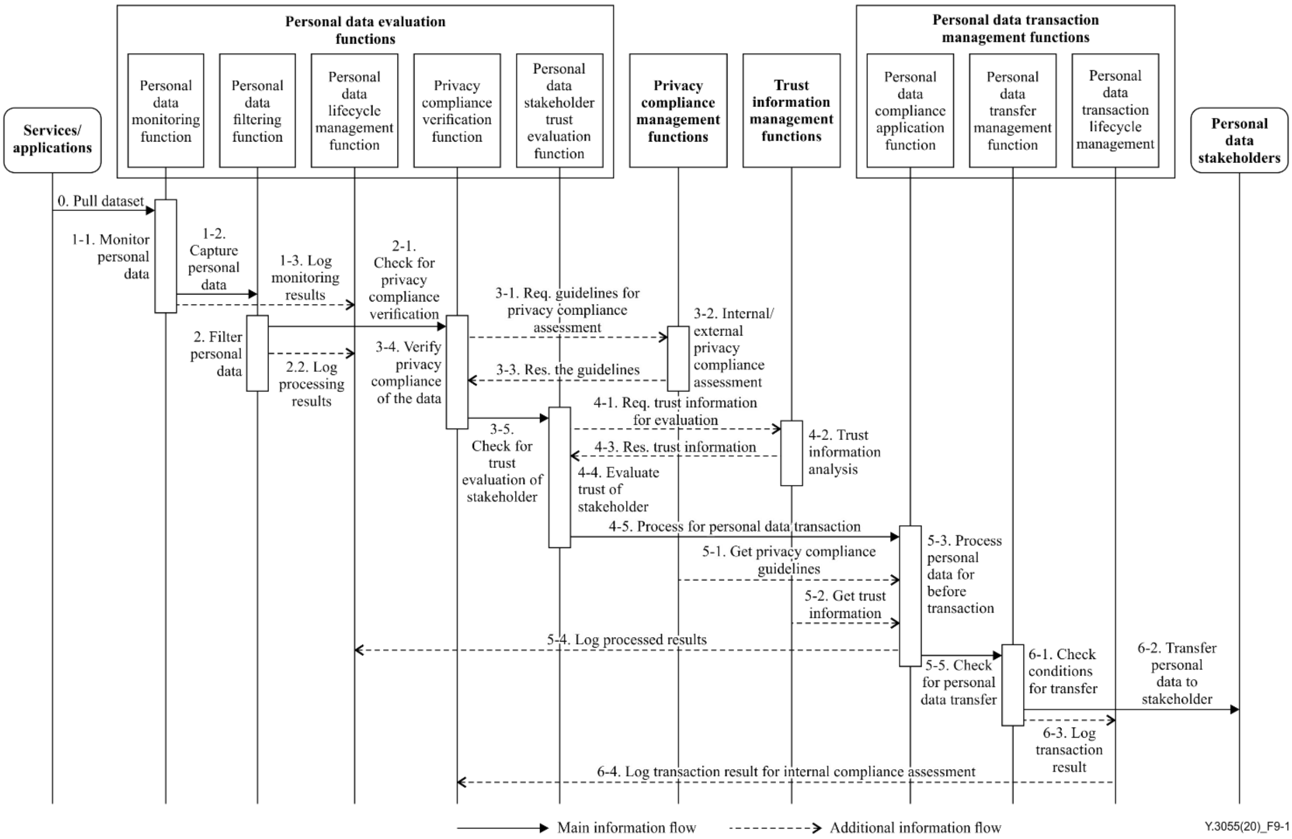
iv) privacy compliance management, and

v) privacy compliance information provision.

9.1 Personal data transaction flow

For the TPDM framework, one of the important information flows is supporting personal data transactions from services or applications that hold aggregated datasets (including personal data) to personal data stakeholders who need personal data for their own purposes. To support personal data transaction, datasets are pulled by the TPDM framework through personal data evaluation functions. Personal data evaluation functions monitor and filter personal data from the dataset, and then they verify privacy compliance of the personal data and evaluate the trust of the stakeholder for personal data transactions. If the verification and the evaluation succeed, then the personal data are handled by personal data transaction management functions. They process personal data to satisfy both privacy compliance requirements and trust requirements, and the processed personal data are transferred to the stakeholder in a safe manner.

The detailed information flow for personal data transactions is shown in Figure 9-1.



Personal data evaluation functions
Personal data monitoring function
Personal data filtering function
Personal data lifecycle management function
Privacy compliance verification function
Personal data stakeholder trust evaluation function
Privacy compliance management functions
Trust information management functions
Personal data transaction management functions
Personal data compliance application function
Personal data transfer management function
Personal data transaction lifecycle management
Services/ applications
Personal data stakeholders
0. Pull dataset
1-1. Monitor personal data
1-2. Capture personal data
1-3. Log monitoring results
2. Filter personal data
2.2. Log processing results
2-1. Check for privacy compliance verification
3-1. Req. guidelines for privacy compliance assessment
3-2. Internal/ external privacy compliance assessment
3-3. Res. the guidelines
3-4. Verify privacy compliance of the data
3-5. Check for trust evaluation of stakeholder
4-1. Req. trust information for evaluation
4-2. Trust information analysis
4-3. Res. trust information
4-4. Evaluate trust of stakeholder
4-5. Process for personal data transaction
5-1. Get privacy compliance guidelines
5-2. Get trust information
5-3. Process personal data for before transaction
5-4. Log processed results
5-5. Check for personal data transfer
6-1. Check conditions for transfer
6-2. Transfer personal data to stakeholder
6-3. Log transaction result
6-4. Log transaction result for internal compliance assessment
Main information flow
Additional information flow
Y.3055(20)_F9-1

Figure 9-1 – Personal data transaction procedure

0) Personal data monitoring function pulls a dataset from services or applications based on the request of a personal data stakeholder that needs personal data for its own purpose;

1) Personal data monitoring function monitors and captures personal data, which are sent to the personal data filtering function. In addition, it sends personal data monitoring results to the personal data lifecycle management function for further management;

2) Personal data filtering function applies pre-processing and filtering methods to personal data and sends the filtered personal data to the privacy compliance verification function. In

addition, it sends personal data filtering results to the personal data lifecycle management function for further management;

3) Privacy compliance verification function receives the filtered personal data and requests privacy compliance assessment guidelines to privacy compliance management functions. The privacy compliance assessment management functions perform internal and external privacy compliance assessment and return the guidelines to the privacy compliance verification function. The privacy compliance verification function verifies privacy compliance of the filtered personal data. If the verification fails, it stops the transaction. If the verification succeeds, it proceeds to the next step for evaluating the trust of the stakeholder;

NOTE 1 – Information flows for privacy compliance management functions are described in clause 9.2 and clause 9.3.

4) Personal data stakeholder trust evaluation function requests trust information for evaluating the trust of the stakeholder from the trust information management functions. The trust information management functions analyse and evaluate trust information and return the results to the personal data stakeholder trust evaluation function. With received trust information, the personal data stakeholder trust evaluation function evaluates trust of the stakeholder and proceeds to the personal data transaction stage if the evaluation satisfies certain criteria;

NOTE 2 – Information flows for trust information management functions are described in clause 9.4 and clause 9.5.

5) Personal data compliance application function applies proper methods to personal data for processing them based on the privacy compliance guidelines from the privacy compliance management functions and trust information from the trust information generation functions. Then, the processed results are sent to personal data lifecycle management function for further management, and it proceeds to the personal data transfer function;

6) Personal data transfer management function checks various conditions for personal data transfer to the personal data stakeholder, and it finally transfers personal data if the conditions are satisfied. The transaction results are sent to the personal data transaction management function and privacy compliance assessment management functions for further management (particularly, for future privacy compliance assessment).

9.2 Privacy compliance management flow

Privacy compliance monitoring functions monitor privacy compliance provided by both internal personal data stakeholders or services/applications and external regulatory/standardisation bodies related to trust-based personal data management. Since privacy compliance information can be dynamically changed or updated (e.g., changes in device permissions related to personal data in services/applications that can impact internal privacy compliance information), the flow for privacy compliance management is necessary to support trust-based personal data management. This flow describes basic procedures of privacy compliance management functions in the TPDM framework.

The detailed information flow for privacy compliance management is shown in Figure 9-2.

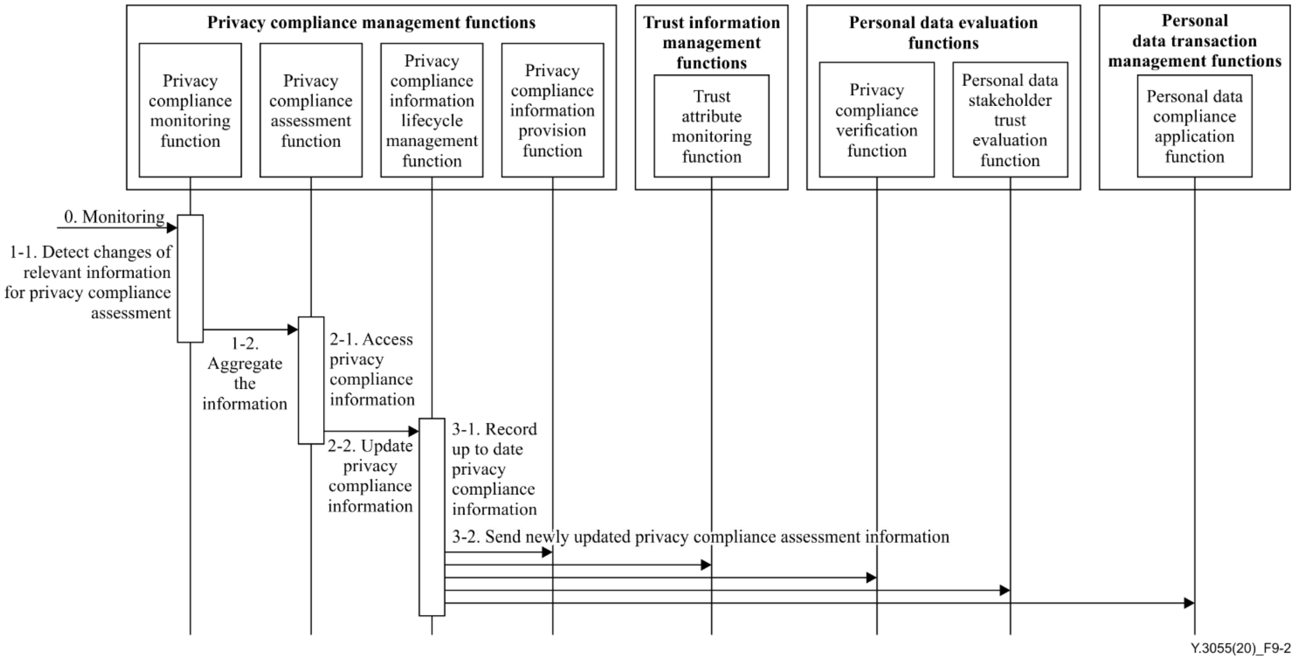

Privacy compliance management functions
Privacy compliance monitoring function
Privacy compliance assessment function
Privacy compliance information lifecycle management function
Privacy compliance information provision function
Trust information management functions
Trust attribute monitoring function
Personal data evaluation functions
Privacy compliance verification function
Personal data stakeholder trust evaluation function
Personal data transaction management functions
Personal data compliance application function
0. Monitoring
1-1. Detect changes of relevant information for privacy compliance assessment
1-2. Aggregate the information
2-1. Access privacy compliance information
2-2. Update privacy compliance information
3-1. Record up to date privacy compliance information
3-2. Send newly updated privacy compliance assessment information
Y.3055(20)_F9-2

Figure 9-2 – Privacy compliance management procedure

1) Privacy compliance monitoring function detects the changes in relevant information for privacy compliance assessment information and aggregates the detected privacy compliance information. Then, it provides the information to the privacy compliance assessment function;

2) Privacy compliance assessment function assesses privacy compliance information received from the privacy compliance monitoring function, and it transfers updated privacy compliance information to the privacy compliance information lifecycle management function;

3) Privacy compliance information lifecycle management function organises existing privacy compliance information and records up to date privacy compliance information including assessment results. It also sends newly updated privacy compliance information to other functional components (i.e., trust attribute monitoring function, privacy compliance verification function, personal data stakeholder trust evaluation function, and personal data compliance application function) in the TPDM framework.

9.3 Privacy compliance information provision flow

The privacy compliance information function receives requests for privacy compliance information from personal data stakeholders and checks validity of the current privacy compliance information from privacy compliance information lifecycle management function. To update privacy compliance information, privacy compliance information lifecycle management function triggers privacy compliance monitoring function. Privacy compliance monitoring function collects relevant privacy compliance information and provides the information to privacy compliance assessment function. Based on the results from privacy compliance assessment function, the newly updated privacy compliance information is delivered to the personal data stakeholders.

Detailed information flow for privacy compliance information provision is shown in Figure 9-3.

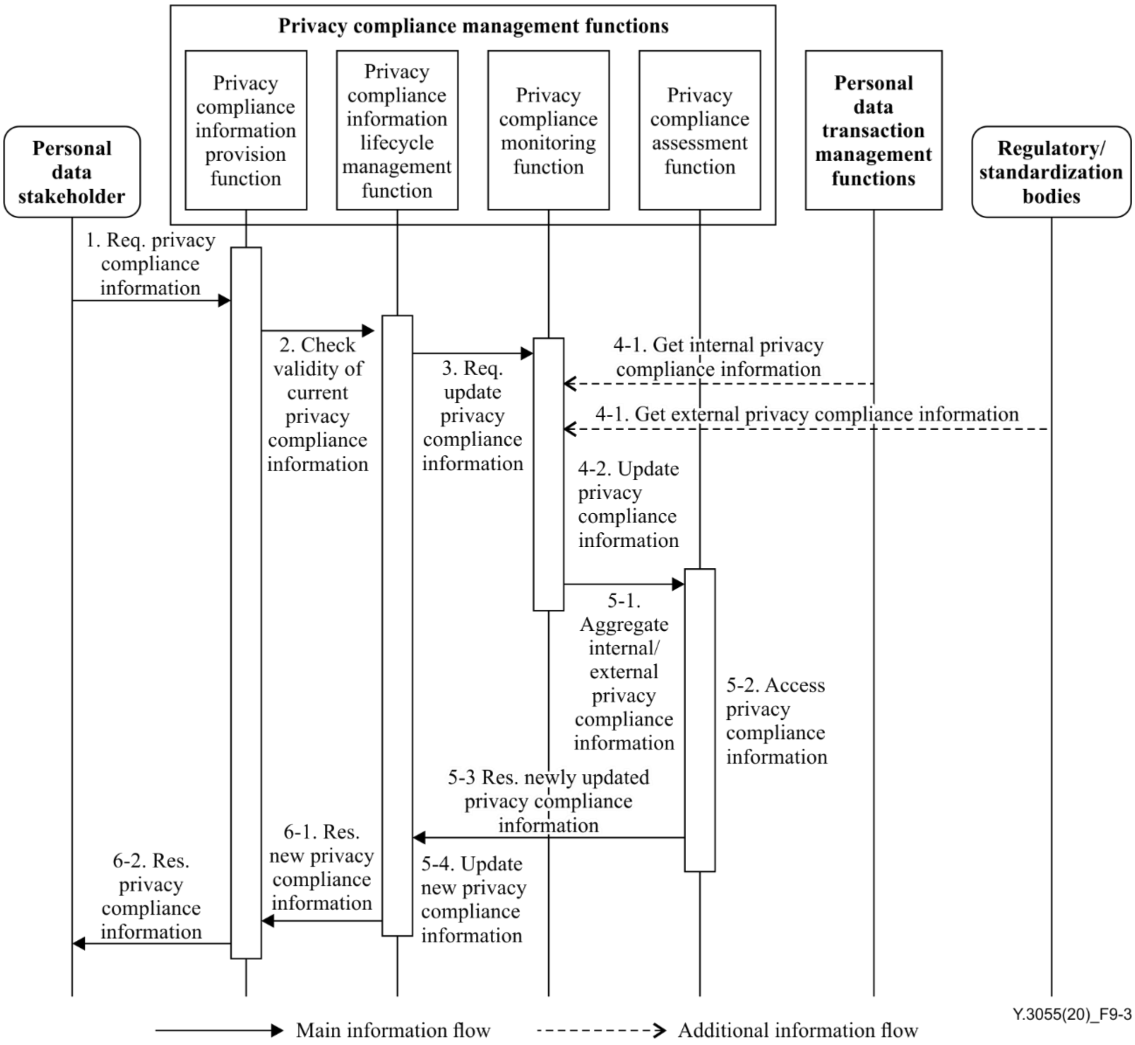

Privacy compliance management functions
Privacy compliance information provision function
Privacy compliance information lifecycle management function
Privacy compliance monitoring function
Privacy compliance assessment function
Personal data transaction management functions
Personal data stakeholder
Regulatory/ standardization bodies
1. Req. privacy compliance information
2. Check validity of current privacy compliance information
3. Req. update privacy compliance information
4-1. Get internal privacy compliance information
4-1. Get external privacy compliance information
4-2. Update privacy compliance information
5-1. Aggregate internal/ external privacy compliance information
5-2. Access privacy compliance information
5-3 Res. newly updated privacy compliance information
5-4. Update new privacy compliance information
6-1. Res. new privacy compliance information
6-2. Res. privacy compliance information
Main information flow
Additional information flow
Y.3055(20)_F9-3

Figure 9-3 – Privacy compliance information procedure

1) A personal data stakeholder requests privacy compliance assessment information from the privacy compliance assessment provision function;

2) Privacy compliance information provision function checks privacy compliance assessment information from its repository and requests the privacy compliance information lifecycle management function to check the validity of current privacy compliance assessment information;

3) Privacy compliance information management function triggers the privacy compliance monitoring function to update privacy compliance assessment information;

4) Privacy compliance monitoring function collects internal privacy compliance information from personal data transaction management functions regarding personal data stakeholders and external privacy compliance information from regulatory/standardisation bodies. Then, it updates new compliance information;

5) Privacy compliance assessment function aggregates internal and external privacy compliance information and assesses privacy compliance information (e.g., its impact on personal data handling, etc.). It sends newly updated privacy compliance information to the privacy compliance information lifecycle management function. Then, the privacy compliance information lifecycle function updates new compliance assessment information;

6) Finally, the newly updated privacy compliance assessment information is sent to the personal data stakeholder through the privacy compliance information provision function.

9.4 Trust information management flow

The trust attribute monitoring function monitors trust attributes and evaluates trust to generate trust information about various targets (e.g., personal data stakeholders, services/applications, persona data, etc.) by applying the proper trust modelling function and trust information analysis function. Then, the trust information lifecycle management function manages trust information created or updated by the previous functions since trust information can be dynamically changed or updated (e.g., the updates in services/applications that handles personal data or the behaviour of personal data stakeholders that can impact trust information). Therefore, the flow for trust information management is necessary to support trust-based personal data management.

Detailed information flow for trust information management is shown in Figure 9-4.

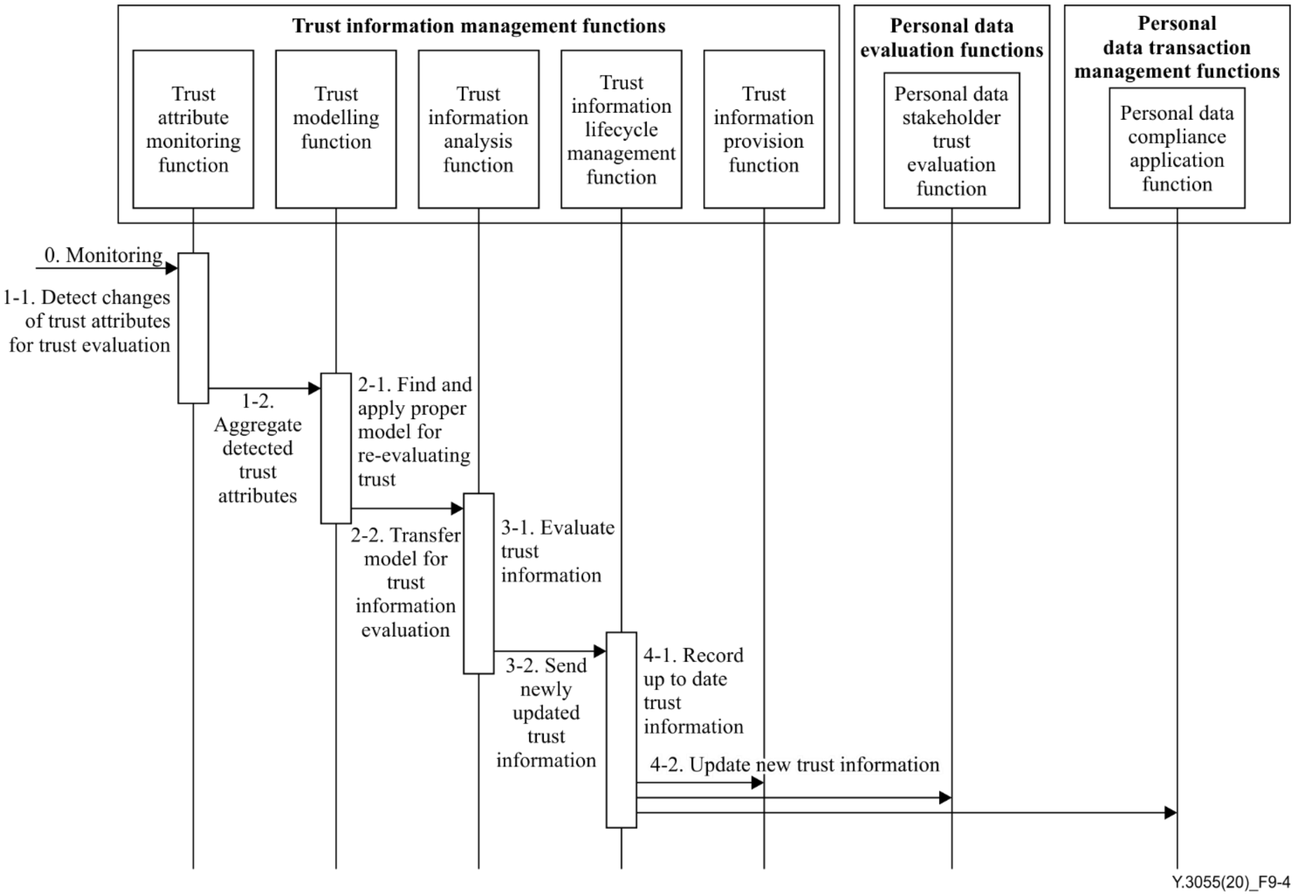

Trust information management functions
Trust attribute monitoring function
Trust modelling function
Trust information analysis function
Trust information lifecycle management function
Trust information provision function
Personal data evaluation functions
Personal data stakeholder trust evaluation function
Personal data transaction management functions
Personal data compliance application function
0. Monitoring
1-1. Detect changes of trust attributes for trust evaluation
1-2. Aggregate detected trust attributes
2-1. Find and apply proper model for re-evaluating trust
2-2. Transfer model for trust information evaluation
3-1. Evaluate trust information
3-2. Send newly updated trust information
4-1. Record up to date trust information
4-2. Update new trust information
Y.3055(20)_F9-4

Figure 9-4 – Trust information management procedure

1) Trust attribute monitoring function detects the changes in trust attributes regarding trust evaluation and aggregates detected changes. Then, it provides the attributes to the trust modelling function;

2) Trust modelling function finds and applies a proper trust model for re-evaluating trust based on the changed trust attribute, and it transfers the trust model for trust information evaluation to the trust information analysis function;

3) Trust information analysis function evaluates trust information and sends newly updated trust information to the trust information lifecycle management function;

4) Trust information lifecycle management function organises existing trust information (e.g., delete expired trust information, etc.) and records up to date trust information. It also sends newly updated trust information to other functional components (i.e., personal data stakeholder trust evaluation function and personal data compliance application function) in the TPDM framework.

9.5 Trust information provision flow

Trust information provision function gets requests for trust information from personal data stakeholders, and it checks trust information in its repository and requests the trust information lifecycle management function to check the validity of the trust information. Then, the trust information lifecycle management function triggers the trust attribute monitoring function for updating trust information. The triggered trust attribute monitoring function aggregates the relevant trust attributes and sends them to the trust modelling function to apply a proper model for the trust information analysis function. Based on the results from the trust information analysis function, the newly updated trust information is delivered to personal data stakeholders.

The detailed information flow for trust information provision is shown in Figure 9-5.

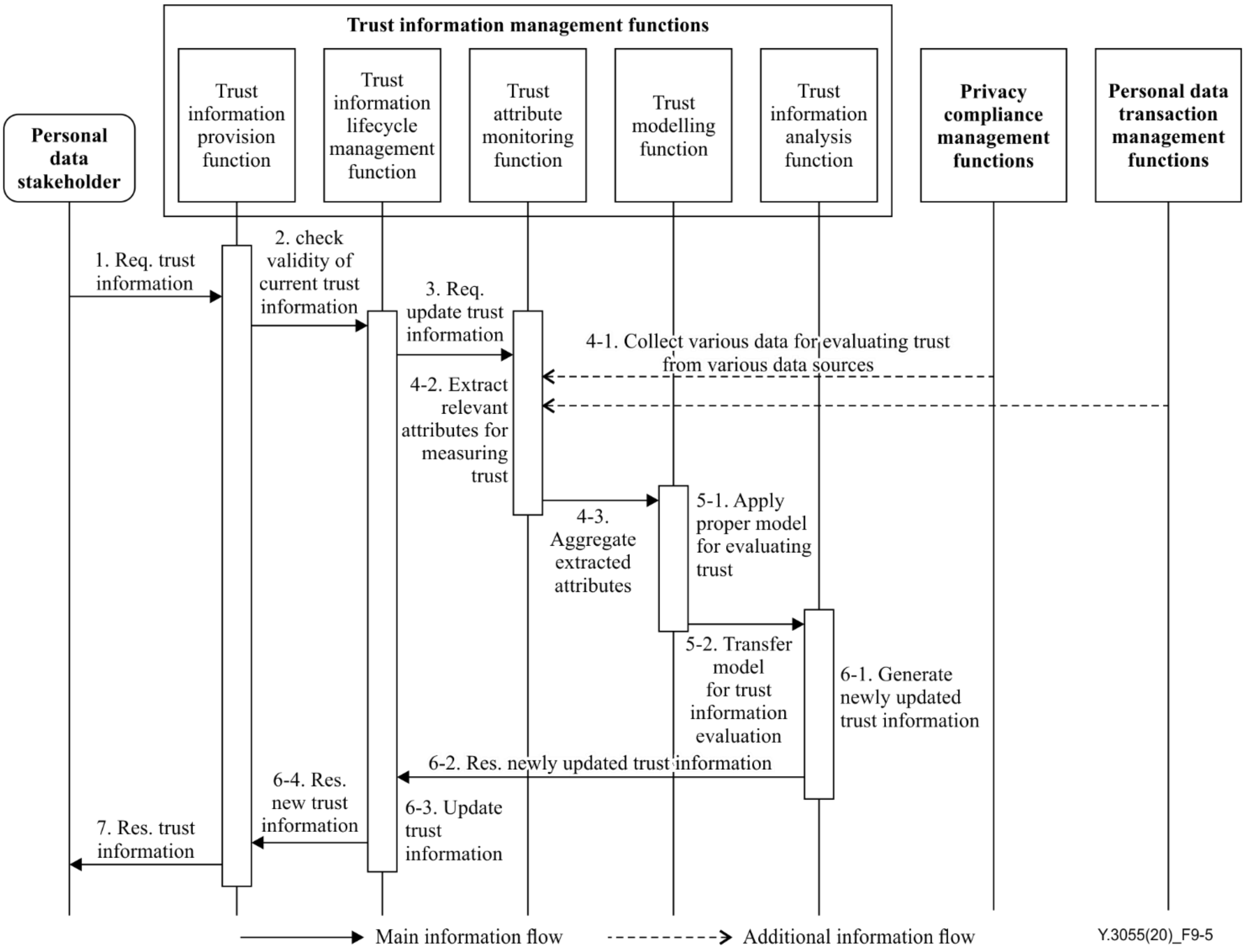

Trust information management functions
Personal data stakeholder
Trust information provision function
Trust information lifecycle management function
Trust attribute monitoring function
Trust modelling function
Trust information analysis function
Privacy compliance management functions
Personal data transaction management functions
1. Req. trust information
2. check validity of current trust information
3. Req. update trust information
4-1. Collect various data for evaluating trust from various data sources
4-2. Extract relevant attributes for measuring trust
4-3. Aggregate extracted attributes
5-1. Apply proper model for evaluating trust
5-2. Transfer model for trust information evaluation
6-1. Generate newly updated trust information
6-2. Res. newly updated trust information
6-3. Update trust information
6-4. Res. new trust information
7. Res. trust information
Main information flow
Additional information flow
Y.3055(20)_F9-5

Figure 9-5 – Trust information provision procedure

1) A personal data stakeholder requests for trust information about its target from the trust information provision function;

2) Trust information provision function checks trust information in its repository and requests the trust information lifecycle management function to check the validity of current trust information;

3) Trust information lifecycle management function checks whether the current trust information is valid or not, and triggers the trust attribute monitoring function to update trust information;

4) Based on the request, the trust attribute monitoring function collects data and information for evaluating the trust of stakeholders from various sources (e.g., privacy compliance management functions, and personal data transaction management functions) and extracts relevant attribute for evaluating trust. Then, it aggregates extracted attributes for the trust modelling function;

5) Trust modelling function applies proper models for evaluating trust based on the aggregated attributes and transfers the models for trust information analysis;

6) Trust information analysis function analyses and generates newly updated trust information. The newly updated trust information is recorded by the trust information lifecycle management function, and it is also sent to the trust information provision function;

7) Finally, the personal data stakeholder receives the newly updated trust information from the trust information provision function as a response on its request.

10 Security considerations

Trust-based personal data management is recommended to follow general guidelines about personal data management and handling from various ITU-T and ISO/IEC standards, such as [b-ITU-T X.1058], [b-ISO/IEC 29100], [b-ISO/IEC 27701], etc. Details of security technologies for personal data management are out of scope for this Recommendation.

Appendix I

Prospective technologies for personal data management

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

This appendix describes key items and prospective technologies for personal data management.

In personal data management, there are various processes that can take place including data collection, data storage, data usage/processing, data sharing, and data destruction. As all these processes are dealing with personal data, each process contains certain risks in terms of the privacy of the consumer or the user. Hence, it is important to place some personal data protection regulations in these processes to preserve the privacy of personal data principals (i.e., PII principals) from malicious threats which could be generated within or out of the system. The following key items for personal data management can be recognised as the most important rules that should be met before, during, and after processing personal data. Table I.1 shows associated processes and personal data lifecycle to ensure the key items about personal data management requirements.

- Lawfulness, fairness, and transparency

The lawfulness, fairness, and transparency principle emphasizes lawful, fair, transparent data management when it comes to personal data. When the data is collected, it must be clear as to why that data is being collected and how the data will be used including usages other than the primary purpose of the data.

- Purpose limitation, data minimization, and storage limitation

Purpose limitation emphasizes the purpose limitation in terms of data management especially with data collection, storage, processing, and sharing. In addition, the purpose limitation rule is closely associated with data minimization and storage limitation rules which instruct organizations to ensure the data they capture and store are adequate, relevant, and limited to the purpose.

- Accuracy

Accurate and up to date processing requires personal data controllers to make sure information remains accurate, valid, and fit for the purpose. To comply with this principle, the organization must have a process and policies in place to address how they will maintain the data that they are processing and storing.

On the other hand, an organization that is collecting and processing data is solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects under the integrity and confidentiality rule.

- Accountability principle and integrity and confidentiality (security)

The accountability and liability principle ensure that organizations have a strategy to audit all data flows specifically related to personal data to preserve privacy of personal data principals in the case of rule breaches. The organizations must be able to promptly remove that data if desired by the personal data principals. Organizations not only need to have a process in place to manage the request but also need to have a full audit trail to prove that they took the proper actions.

- Consent

In a network computing environment, consent mainly controls the access to user-specific information about his/her preferences on the collection, storage, processing, sharing, and deletion. Hence, having proper consent management mechanisms in place is one of the most critical factors to ensure all other rules mentioned in this appendix.

- Right to be informed and right of access

The right to be informed rule emphasizes that a personal data principal must be informed about the collection and purposes for processing their personal data, personal data processors retention periods for that personal data, and sharing of their personal data with other entities. On the other hand, individuals' right to request a copy of any personal data that the personal data processor holds on them and to request details regarding that data's use, retention, and any relevant sharing of the data are enforced by right of access rule.

- Right to rectification

An individual may have incomplete or inaccurate personal data. This may lead to issues with data management by the service providers in terms of providing a satisfactory service to their users. Hence, to regulate such issues, a right to rectification rule must be in place.

- Right to erasure, right to restrict processing, and right to object

The personal data principal should have the right to request the processing organizations to erase personal data without any delay and the processing organizations should obligate to such requests in cases such as when an individual is no longer a customer of the business, or when the individual has withdrawn his/her consent from the service to use the personal data. Moreover, right to restrict processing and right to object to rules are also associated with the right to erasure rule.

- Right to data portability

The right to data portability rule emphasizes the right of personal data principals to have their personal data in a structured, commonly used, and machine-readable format and to transmit those data to another organization. This right is applicable if: i) the data subject has provided the personal data to the controller, ii) the use or storage of the data is based on consents or contracts, or iii) the use of the data is carried out by automated means.

- Rights related to automated decision-making including profiling

The rights related to decision making including profiling rule highlights the right of personal data principals who are the subject of the decisions solely made by automated processing.

Even in cases where an individual consents for automated decision-making, he/she has the rights to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment, and to challenge the decision, etc.

Table I.1 – Associated processes and personal data lifecycle to ensure personal data management requirements

Personal data management requirement	Personal data management lifecycle (in Figure 6-1)	Associated processes
Lawfulness Fairness Transparency	• Data collection • Data management	• Consent/contract breach detection • Activity monitoring • Informed decision making (direct declaration, registry based)
Purpose limitation	• Data collection	• Time based restrictions on storage • Mandatory purpose specification before collection • Monitor any consent violations • Use purpose limitation protocols like Platform for Privacy preferences project • Sticky policies and privacy rights management

Table I.1 – Associated processes and personal data lifecycle to ensure personal data management requirements

Personal data management requirement	Personal data management lifecycle (in Figure 6-1)	Associated processes
		• Adaptive encryption depending on the requestor, the context, and purpose
Data minimization	• Data collection • Data management	• Define what data are needed before collection • Select before collect (Reduce data fields, delete unwanted information, etc.) • Strategic deletion
Accuracy	• Data collection • Data management	• Frequently update databases • Database cross checking • Standardize metadata • Keep track of data quality breaches
Storage limitation	• Data management	• Establish retention period for storage • Erase, anonymize, or pseudonymize the data • Separated or Distributed Storages • Process Data Locally • Table-specific pseudonyms
Integrity and confidentiality (security)	• Data collection • Data management • Data use	• Access control (Firewall, access lists, etc.) • Anonymity (e.g., k-anonymity, differential privacy) • Unlinkability • Undetectability • Pseudonym/Encryption
Accountability principle	• Data collection • Data management • Data use	• Auditing and punishing/rewarding systems such as based on reinforced learning mechanisms and trust evaluation • Follow the MAPE-K model
Consent	• Data collection	• Smart contracts • Consent management platform • Privacy policies, cookie notices and terms, and conditions • ticking an opt-in box on paper or electronically; • clicking an opt-in button or link online
Right to be informed	• Data collection • Data management • Data use	• Data flow audit mechanisms • Platform for privacy preferences protocol
Right of access	• Data management	• Database access control • Private information retrieval mechanisms
Right to rectification	• Data management	• Request scheduled updates from user • Dataset cross check • Statistical methods, filtering, maximum likelihood estimators, machine learning
Right to erasure	• Data management • Data use	• Database access control • Timestamp on data

Table I.1 – Associated processes and personal data lifecycle to ensure personal data management requirements

Personal data management requirement	Personal data management lifecycle (in Figure 6-1)	Associated processes
		• a form of digital request • privacy dashboards
Right to restrict processing	• Data management	• User consent • Cell/Row suppression in databases • Perturbative masking (noise addition, micro-aggregation, randomization) • Non-perturbative masking (sampling, generalization)
Right to data portability	• Data management • Data use	• Personal information management systems • Database access control • Impact assessment • Interoperable APIs
Right to object	• Data management	• User consent • Cell/Row suppression in databases • Perturbative masking (noise addition, micro-aggregation, randomization) • Non-perturbative masking (sampling, generalization)
Rights related to automated decision-making including profiling	• Data management • Data use	• User consent • Data pseudonymization, anonymization and encryption • Owner privacy preserving data mining • User-centric identity management • end-to-end encryption

Appendix II

A trust evaluation model and use case for trust information management functions

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

This appendix describes a trust evaluation model and use case for trust information management functions (described in clause 8) in the trust-based personal data management framework as an informative example. The trust evaluation model is based on the concept of trust provisioning described in [ITU-T Y.3052].

II.1 Trust evaluation on data privacy in trust by design concept

In order to balance the trade-off between data utilization and privacy protection, which cannot be easily quantified in numerical values to measure, the concept of "trust by design" has become important in personal data management. Nevertheless, the trust is not a simple concept that can be straightforwardly scaled as well. As shown in Figure II.1, each stakeholder in the personal data ecosystem should identify other stakeholders and measure their trust to decide whether they are trustful enough for handling personal data or not. Therefore, the trust evaluation requires to be processed in fine granularity.

On the other hand, [ITU-T Y.3052] introduced the concept of trust information (i.e., trust index and trust indicators) to measure and evaluate the trust of stakeholders and entities in ICT environment. Similarly, trust indicators and their characteristics are needed for trust-based personal data management. Detailed analysis for objective and subjective trust indicators and a trust evaluation model are described in clauses II.1.1 and II.1.2, respectively. Then, clause II.2 provides a use case on the trust evaluation of mobile applications.

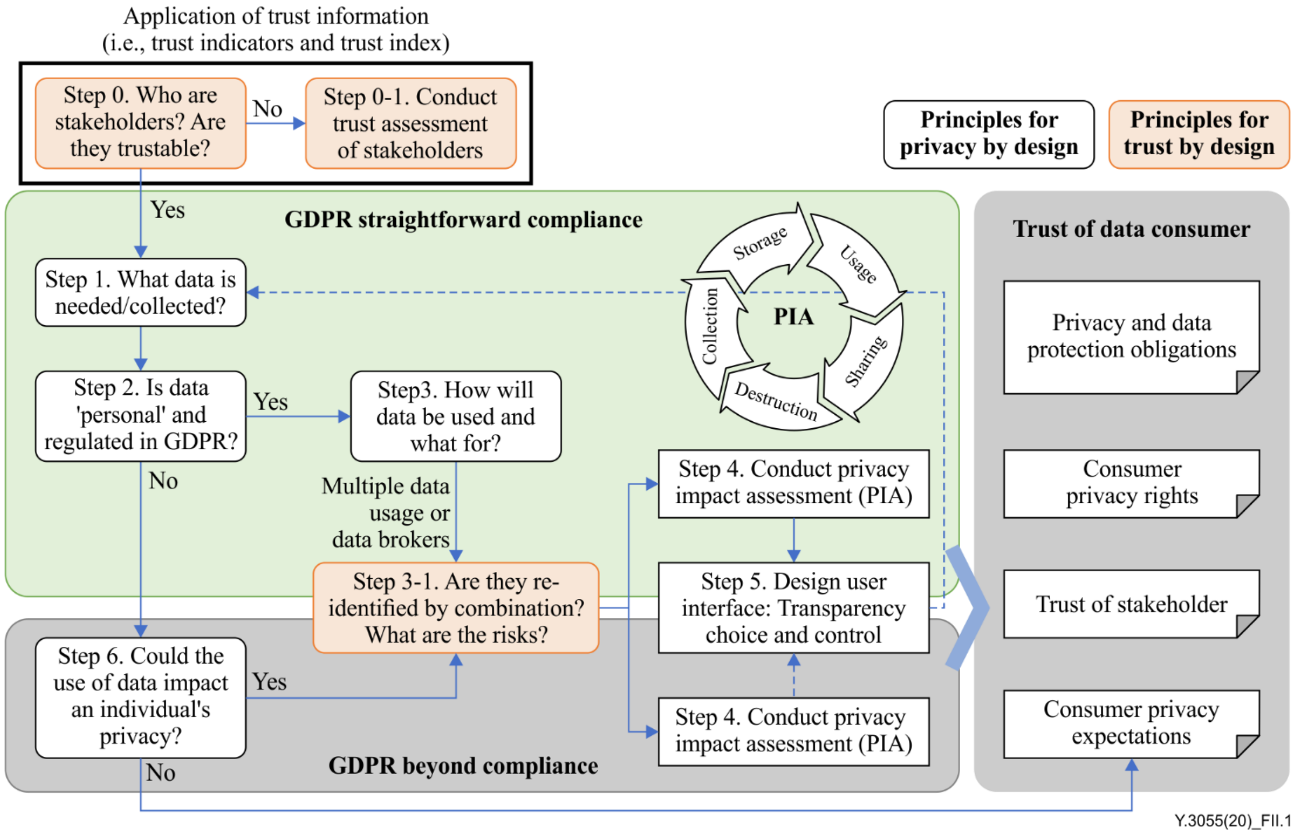

Application of trust information
(i.e., trust indicators and trust index)
Step 0. Who are stakeholders? Are they trustable?
No
Step 0-1. Conduct trust assessment of stakeholders
Principles for privacy by design
Principles for trust by design
Yes
GDPR straightforward compliance
Step 1. What data is needed/collected?
Storage
Usage
Collection
PIA
Sharing
Destruction
Step 2. Is data 'personal' and regulated in GDPR?
Yes
Step3. How will data be used and what for?
No
Multiple data usage or data brokers
Step 4. Conduct privacy impact assessment (PIA)
Step 3-1. Are they re-identified by combination? What are the risks?
Step 5. Design user interface: Transparency choice and control
Step 6. Could the use of data impact an individual's privacy?
Yes
Step 4. Conduct privacy impact assessment (PIA)
No
GDPR beyond compliance
Trust of data consumer
Privacy and data protection obligations
Consumer privacy rights
Trust of stakeholder
Consumer privacy expectations
Y.3055(20)_FII.1

Figure II.1 – Personal data utilization process based on privacy [b-GSMA-pbd] and trust by design with an application of trust information

II.1.1 Trust indicators for trust evaluation

The trust indicators can be categorized into two different types: objective and subjective (summarized in Table II.1). Objective trust indicators can be appraised only with unbiased factors, without the intervention of inclined opinions, views, and attitudes of the evaluator. Subjective trust indicators are influenced by the intrinsic perspectives and propensities of the evaluator. For the trust evaluation, the subject carrying out the evaluation is referred to as a trustor and the subject of the evaluation as a trustee.

II.1.1.1 Objective trust indicators

The objective trust indicators are related to the personal data exploitation of the subject which is being evaluated. For trust evaluation in a personal data management system, each indicator with distinct characteristics can be subdivided in the classified categories as listed but not limited to the following:

– **Ability** is characteristics that enable an entity to have influence within some specific contexts [ITU-T Y.3052]. In personal data management, it refers to the capability, reliability, stability, robustness, and other capacities to keep data secured and prevent it from being contaminated;

– **Integrity** is the quality of being honest and fair in the social world, the state of being complete in cyber and physical worlds, or intactness and consistency of information in terms of information [ITU-T Y.3052]. In personal data management, specifically, it means the consistency, compliance, validity, and legitimacy in personal data collection and usage overall;

– **Benevolence** refers to the desire to do well to others and willingness to work or act together for common purposes or benefits [ITU-T Y.3052]. In personal data management, it represents the amity, propriety and other good propensities to protect personal information aside from egocentric profit motives.

II.1.1.2 Subjective trust indicators

Subject trust indicators are related to the intrinsic perspectives and propensities of the evaluator. Especially in the personal data ecosystem, subjective trust indicators are closely related to the privacy paradox. The privacy paradox is a phenomenon where people that are aware of and care about privacy risk but willingly relinquish personal data easily when they are incentivized [b-Athey]. In other words, people weigh the value between protection of their privacy and incentives offered by providing their private information. Accordingly, subjective trust indicators need to capture personal opinions, perspectives, and attitudes. Therefore, subjective trust indicators need to be quantified by analysing the interaction between the evaluator and the subject of the evaluation. For trust evaluation in a personal data management system, the subjective indicators to capture preferences developed from subjective perspectives are described but not limited to the following:

- **Experience** represents the observation about the interactions between the evaluator and the subject of the evaluation, which is achieved by accumulating the state of interactions among entities over time [ITU-T Y.3052]. In personal data management, it refers to the accumulated interactions related to personal information between a data provider and a data stakeholder;
- **Reputation** indicates the accumulated experience of evaluator about the subject of the evaluation with respect to its prior behaviour and performance [ITU-T Y.3052]. In personal data management, it refers to the accumulated experience specifically related to personal information;
- **Inclination** indicates the subjective preferences of evaluators toward the subjects of the evaluation, which is accumulated from experience and reputation. In personal data management, it implies the personal information provider's preferences influence the appraisers of the data stakeholder.

Interaction accumulation and development are described in Figure II.2.

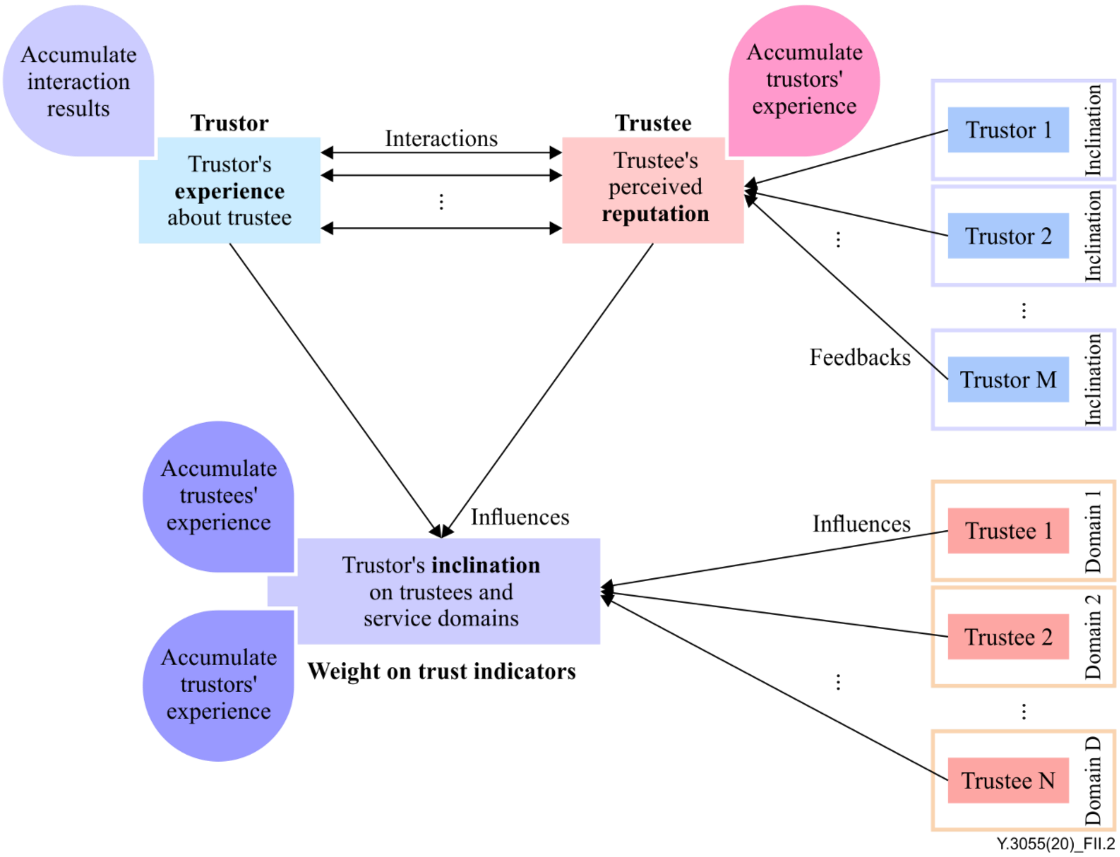

Accumulate interaction results
Trustor
Trustor's experience about trustee
Interactions
Trustee
Trustee's perceived reputation
Accumulate trustors' experience
Trustor 1
Inclination
Trustor 2
Inclination
Trustor M
Inclination
Feedbacks
Accumulate trustees' experience
Influences
Trustor's inclination on trustees and service domains
Weight on trust indicators
Accumulate trustors' experience
Influences
Trustee 1
Domain 1
Trustee 2
Domain 2
Trustee N
Domain D
Y.3055(20)_FII.2

Figure II.2 – Subjective trust indicators [ITU-T Y.3052]

Table II.1 – Summary of trust indicators in the personal data management context

Type	Indicator	Description
Objective	Ability	The indicator 'Ability' indicates the characteristics related to competency and ability in handling personal information, which may include the range and type of personal information collection, security features, etc.
	Benevolence	The indicator 'Benevolence' indicates the characteristics of the trustee's attitude to work or acts with the personal information provider, which may include whether and how to deliver the contents of the data subject's rights, such as the personal information processing/protection policy, etc.
	Integrity	The indicator 'Integrity' indicates the characteristics of the trustee's adherence to principles related to personal information, which may include the consistency of the personal information usage and the announced purpose, adequacy of the collection purpose, etc.
Subjective	Experience	The indicator 'Experience' indicates the accumulated interactions between the data provider and the trustee, which may include relationships such as the degree of service usage in the sense of frequency and duration.
	Reputation	The indicator 'Reputation' indicates the appraisals of the trustee's previous behaviour and performance, which may include the evaluation of not only the evaluation of the personal information provider but also other data subjects.
	Inclination	The indicator 'Inclination' implies the importance of the other trust indicators, and it is expressed as the weights of the indicators in the trust evaluation, which may differ according to the preferences of the personal data providers.

II.1.2 Trust evaluation for trust-based personal data management

To appraise the trustworthiness of a personal data stakeholder, the trust indicators need to be comprehensively considered in a trust evaluation model. The trust evaluation model shown in Figure II.3 calculates a trustee's trustworthiness as a weighted sum of the trust indicators. The inclination indicator specifies the weights of the other indicators.

Specifically, the trust evaluation model shown in Figure II.3 takes the cumulative values of the trust indicators, which are weighted by their defined importance to users. The evaluated trustworthiness of personal data stakeholders affects the interactions among the stakeholders. Through the interactions, the stakeholders update their behaviours or policies, which result in the accumulation in the values of objective and subjective indicators. In the process of repeating trust evaluations, interactions, updates, and accumulations, the trustworthiness of a personal data stakeholder is dynamically and adaptively evaluated.

The weights of the trust indicators are determined by the trustor's preferences or the trustee's domain-specific characteristics. The values of the other trust indicators are quantified by evaluating the trustee's behaviours and characteristics related to its personal information collection, usage or processing of collected personal information, grants on the rights of the data subjects, trustors' satisfaction, etc. The evaluation items to quantify the values of trust indicators and the possible methods for quantifying the items are categorized in Table II.2.

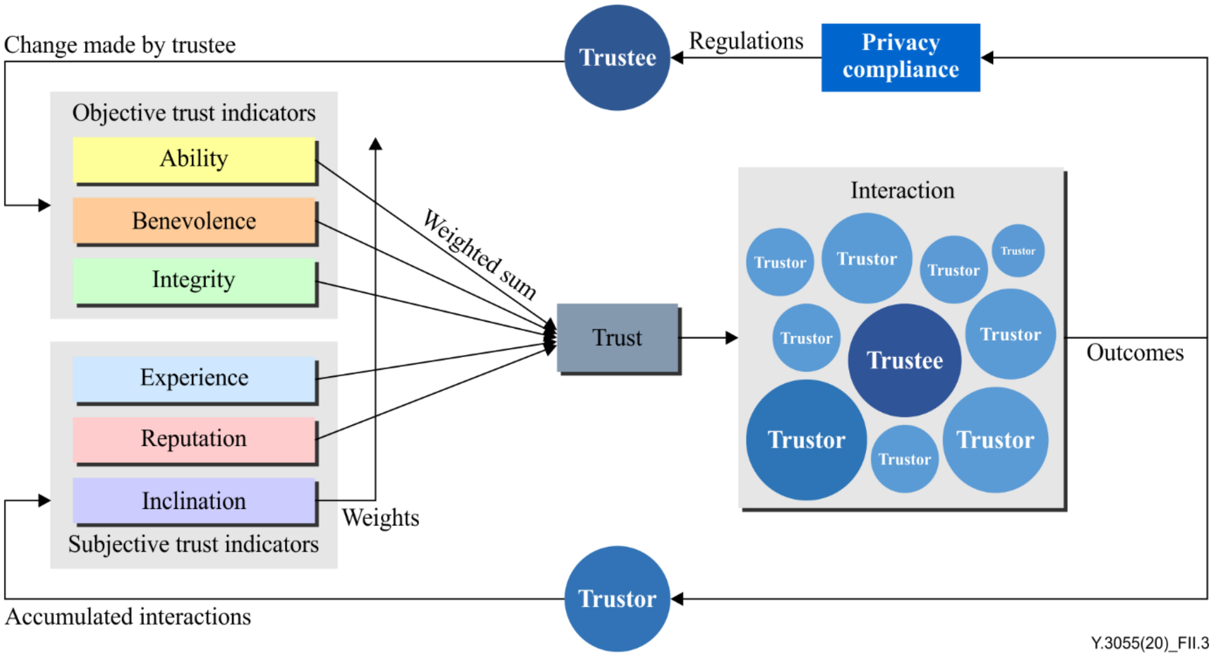


Figure II.3 – Trust evaluation model

Table II.2 – Evaluation items and possible methods to quantify the value of trust indicators

Trust indicator	Evaluation item	Quantifying method
Ability	A1. Collecting IP/device information and online access records	• Examining system loggings • Searching the contents in the agreement to collect personal information • Crowdsourcing by users • Analysing the contents of the agreement to collect personal information based on artificial intelligence • Analysing the contents of the agreement to collect personal information by law experts
	A2. Collecting of general personal information such as contact and name	
	A3. Collecting of sensitive personal information such as location or payment	
	A4. Providing security-related functions	
Benevolence	B1. Readability of privacy policy / agreement terms	• Applying readability calculation • Analysing the contents of the agreement to collect personal information by law experts
	B2. Granting the right to access and correct personal information	• Detailed analysis of information collecting system and service • Searching the contents in the agreement to collect personal information • Crowdsourcing by users • Analysing the contents of the agreement to collect personal information based on artificial intelligence • Analysing the contents of the agreement to collect personal information by law experts
	B3. Granting the right to choose and control personal information	
	B4. Providing contact information of the personal information manager	• Searching the contents in the agreement to collect personal information • Crowdsourcing by users • Analysing the contents of the agreement to collect personal information based on artificial intelligence • Analysing the contents of the agreement to collect personal information by law experts
Integrity	I1. Stating the purpose of the collection and the appropriateness of the purpose	
	I2. Sharing the collected personal	

Table II.2 – Evaluation items and possible methods to quantify the value of trust indicators

Trust indicator	Evaluation item	Quantifying method
	information with any third party	
	I3. Stating the type and purpose of personal information shared with any third party	• Requesting users' inputs • Acquiring the information from the users' devices • Acquiring the information from the rating service systems
	I4. Notifying any change in the privacy policy / agreement terms	
Experience	E1. Duration of service use	
	E2. Frequency of service use	
Reputation	R1. Rating of the service	• Requesting users' inputs • Acquiring the information from the rating service systems
	R2. Number of the users rated the service to ensure the credibility of the rating	
Inclination	W. User's preferences	• Requesting users' inputs

II.2 Use case

In this clause, a use case on the trust evaluation of mobile applications is studied to provide an informative example for a trust-based personal data evaluation. The use case demonstrates how the trust evaluation model described in clause II.1.2 evaluates a mobile application's trustworthiness in terms of the trust information management functions defined in clause 8. Specifically, the use case provides an example of how the trustworthiness of mobile applications can be evaluated by their users. Figure II.4 shows the trust evaluation model with evaluation methods for trust indicators.

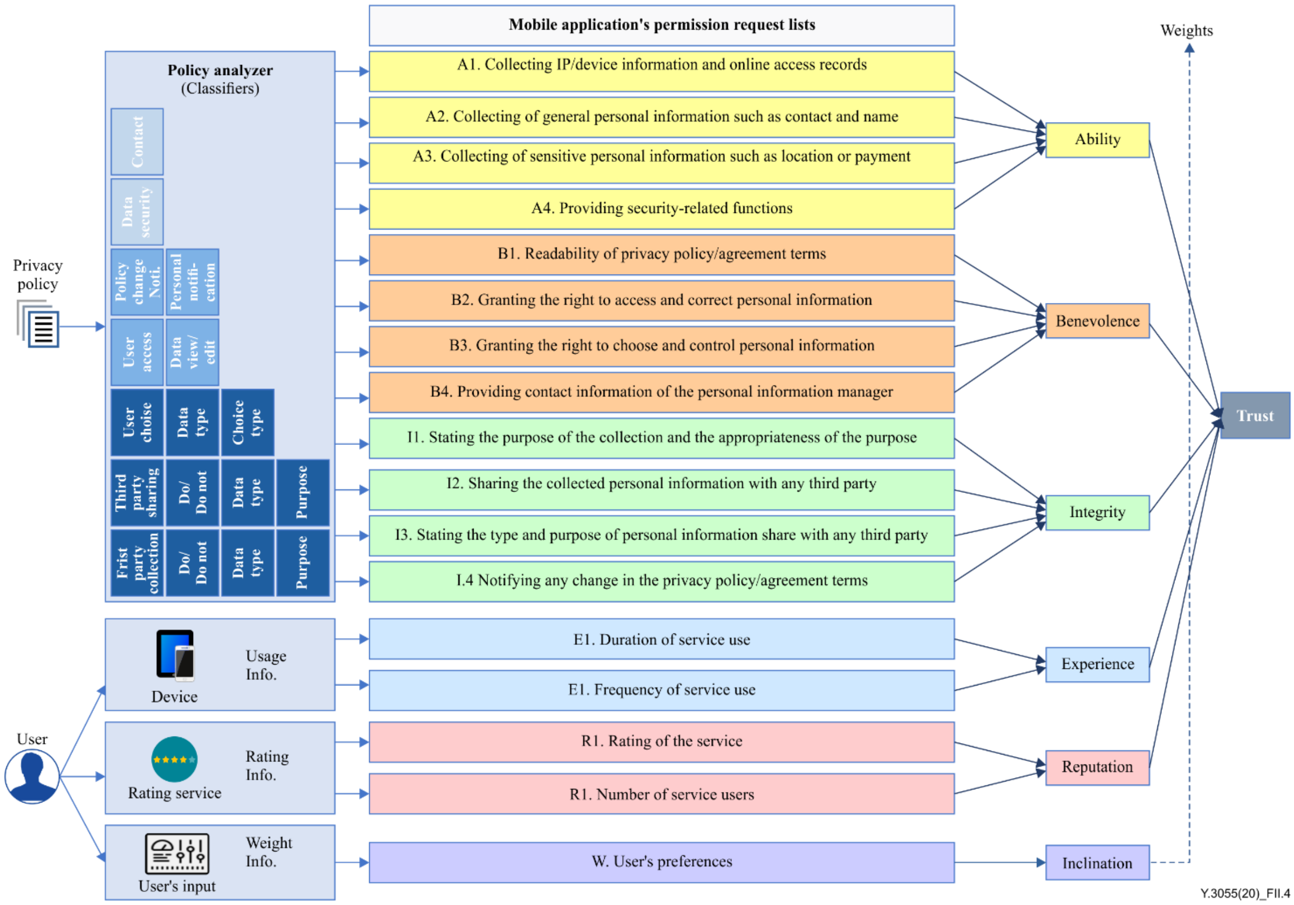

Mobile application's permission request lists
Weights
Policy analyzer
(Classifiers)
Contact
Data security
Policy change Noti.
Personal notifi-cation
User access
Data view/ edit
User choise
Data type
Choice type
Third party sharing
Do/ Do not
Data type
Purpose
Frist party collection
Do/ Do not
Data type
Purpose
Privacy policy
A1. Collecting IP/device information and online access records
A2. Collecting of general personal information such as contact and name
A3. Collecting of sensitive personal information such as location or payment
A4. Providing security-related functions
B1. Readability of privacy policy/agreement terms
B2. Granting the right to access and correct personal information
B3. Granting the right to choose and control personal information
B4. Providing contact information of the personal information manager
I1. Stating the purpose of the collection and the appropriateness of the purpose
I2. Sharing the collected personal information with any third party
I3. Stating the type and purpose of personal information share with any third party
I.4 Notifying any change in the privacy policy/agreement terms
Ability
Benevolence
Integrity
Trust
Device
Usage Info.
E1. Duration of service use
E1. Frequency of service use
Experience
User
Rating service
Rating Info.
R1. Rating of the service
R1. Number of service users
Reputation
User's input
Weight Info.
W. User's preferences
Inclination
Y.3055(20)_FII.4

Figure II.4 – Trust evaluation model with evaluation methods for trust indicators

- **Trust attributes monitoring function**

To recognize the characteristics of the objective trust indicators for mobile applications, the trust attributes monitoring function analyses the privacy policy of the mobile application based on artificial intelligence technologies. A set of hierarchically structured classifiers are applied to analyse the contents of a privacy policy. For the analysis, the privacy policies of the applications are pre-processed into segmented and polished sentences. Each segmented sentence is hierarchically classified to examine whether the sentences are correspondent to each evaluation item. In addition, the information on permissions requested by the application to access is utilized. From the application's permission request list, the trust attributes monitoring function checks whether the application has requested permissions related to the evaluation items. For the subjective indicators, the trust attributes monitoring function observes the information on the usage of the mobile application from the users' devices and users' inputs. The experience indicator implies accumulated interactions between the trustor and the trustee, which are respectively a user and an application in the use case study. Hence, the experience indicator can be quantified by measuring how often and long the user has used the service provided by the application. The usage information is obtainable from the user's device. In the case of the reputation indicator, it implies the accumulated experience of the user with the application, which represents the user's satisfaction with their experience. Accordingly, the reputation indicator is quantifiable based on the publicly shared ratings of the application.

- **Trust modelling function**

To measure the trust with the obtained trust attributes, the trust modelling function models the trust evaluation as a weighted sum of the trust attributes obtained from the trust attributes monitoring function as shown in Figure II.3. The importance of the trust attributes to the user is weighted as the inclination indicator specifies. The inclination indicator is represented as a vector of importance weights for the other indicators, of which the sum is 1. The trust modelling function requests and manages the users' inputs as values of the inclination indicator to specify the relationships of the other indicators. In addition, the trust modelling function applies the clustering technique to the applications' permission request information to form applications with similar characteristics into a set of groups, which share the weights set by the user.

- **Trust information analysis function**

To analyse the trust information by combining trust attributes and trust models, the trust information analysis function converts the data obtained from the trust attributes monitoring function into numeric values and applies the evaluation model specified by the trust modelling function. According to the evaluation items, the trust information analysis function quantifies the trust indicators. The trust indicators, excluding the inclination indicator, are quantified to have values between 0 and 1, which are referred to as the indicator scores. A higher indicator score implies more trustworthiness. For objective indicators, the sentences in the privacy policy and requested permissions related to each evaluation item are converted into the indicator scores. For subjective indicators, excluding the inclination indicator, the usage information and the ratings of the application are transformed into indicator scores. The trust attributes and trust models are combined as the indicator scores are aggregated as specified by the trust modelling function. As a result, the trust score of a mobile application is quantified as a numeric value between 0 and 1, where 0 implies low trustworthiness, and 1 implies high trustworthiness.

- **Trust information lifecycle management function**

To manage trust information, the trust information lifecycle management function ascribes an expiration time to each trust information when new trust information is created. According to the expiration time, the lifecycle management function periodically re-evaluates the trust attributes and trust information.

- **Trust information provision function**

To provide the trust information to the users, the provision function visualizes the trust information evaluated by the trust attributes monitoring, trust modelling, and trust information analysis functions. To ease the users' understanding and decision making, the trust information provision function utilizes graphs to show the scores of the mobile application in terms of trust indicators and the final trust score as shown in Figure II.5.

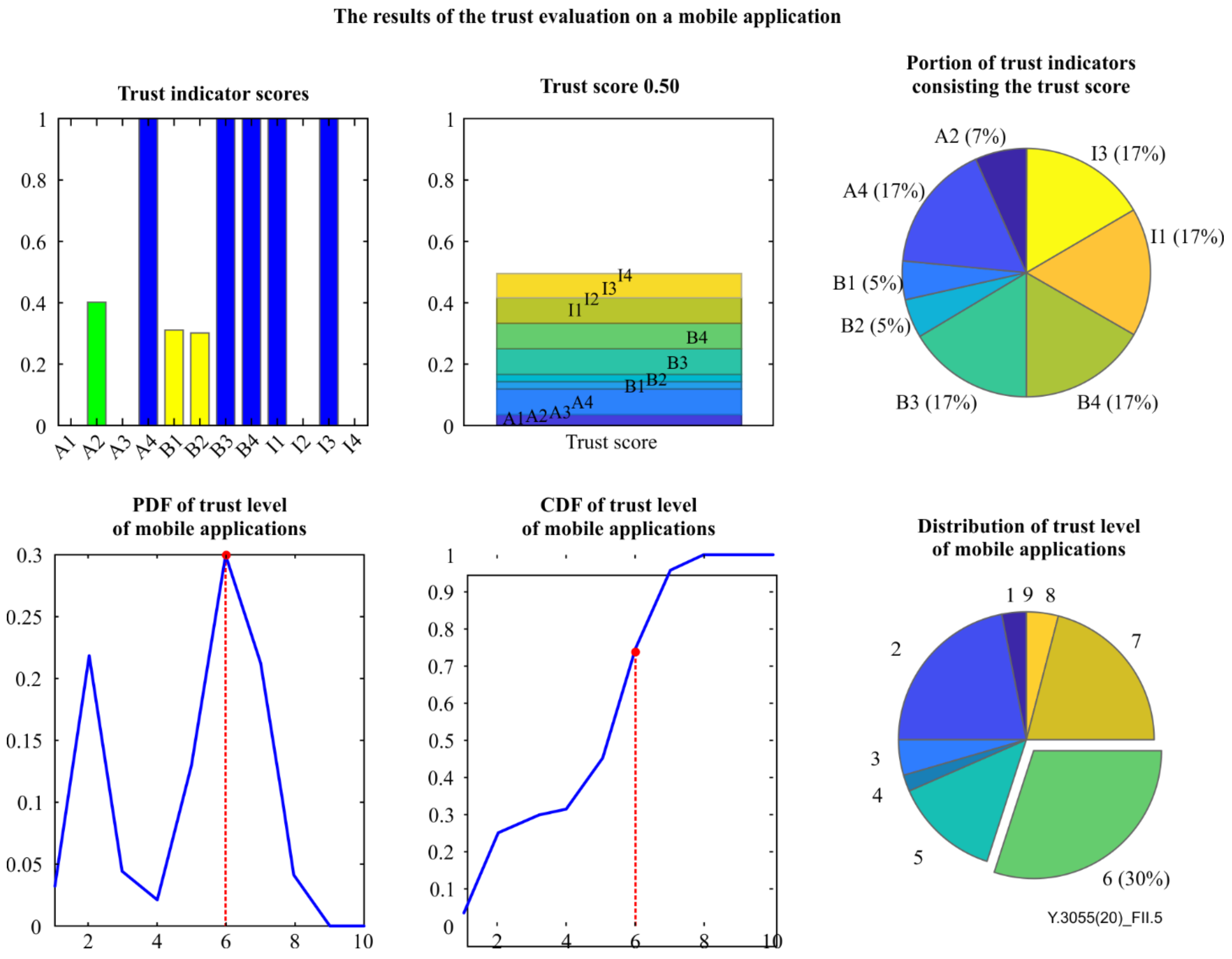


Figure II.5 – Example for visualization of the evaluated trust information

Bibliography

[b-ITU-T X.1058] Recommendation ITU-T X.1058 (2017), *Information technology – Security techniques – Code of practice for personally identifiable information protection*.

[b-ISO/IEC 27701] ISO/IEC 27701:2019, *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*.
https://www.iso.org/standard/71670.html

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.
https://www.iso.org/standard/73722.html

[b-GSMA-pbd] GSMA's IoT Privacy by Design Decision Tree, May 2015.
https://www.gsma.com/iot/iot-knowledgebase/iot-privacy-design-decision-tree/

[b-Athey] S. Athey et al., *The digital privacy paradox: small money, small costs, small talk* National Bureau of Economic Research, Working Paper 23488, Jun. 2017

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, 2020