TTC技術レポート
Technical Report

TR-M2M-0062v0.4.0

プライバシデータ保護規則をサポートするための機能拡張

oneM2M System Enhancement to Support Privacy Data Protection Regulations

2023 年 3 月 17 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TR-M2M-0062v0.4.0

プライバシデータ保護規則をサポートするための機能拡張 [oneM2M System Enhancement to Support Privacy Data Protection Regulations]

＜参考＞ [Remarks]

１．国際勧告等の関連 [Relationship with international recommendations and standards]

本技術レポートは、oneM2M で作成された Technical Report TR-0062-V0.4.0 に準拠している。

[This Technical Report is transposed based on the Technical Report TR-0062-V0.4.0 developed by oneM2M.]

２．作成専門委員会 [Working Group]

oneM2M 専門委員会 [oneM2M Working Group]

oneM2M
Technical Report

Document Number	TR-0062-V-0.4.0
Document Name:	oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)
Date:	<2022-12-01>
Abstract:	The document is describing state of the art privacy related regulations and their features followed by gap analysis to find out what features are supported and not supported by the current oneM2M system. Based on the result of the technical report, it will identify possible enhancement features to support data protection regulations which the next oneM2M release(s) could support.

'Template Version: January 2019 (do not modify)

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

Copyright Notification

Notice of Disclaimer & Limitation of Liability

Contents

1 Scope

The document is describing state of the art privacy related regulations and their features followed by gap analysis to find out what features are supported and not supported by the current oneM2M system. Based on the result of the technical report, it will identify possible enhancement features to support data protection regulations which the next oneM2M release(s) could support.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references,only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules (http://member.onem2m.org/Static_pages/Others/Rules_Pages/oneM2M-Drafting-Rules-V1_0.doc)

[i.2] GDPR website, https://gdpr-info.eu

[i.3]

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply:

3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

3.3 Abbreviations

<GDPR> <General Data Protection Regulation>

<PIPA> <Personal Information Protect Act>

4 Conventions

The key words “Shall”, ”Shall not”, “May”, ”Need not”, “Should”, ”Should not” in this document are to be interpreted as described in the oneM2M Drafting Rules [i.1]

5 Introduction

Laws to protect personal information from systems handling data are being enacted in many countries around the world. IoT platforms used to produce and store a lot of data, such as smart cities, smart health, and smart homes, need to comply with these laws. Therefore, this technical report analyses laws such as EU’s General Data Protection Regulation (GDPR) and examines the impact of these laws on the IoT platform to derive the requirements for the oneM2M system.

6 State of the Art on Privacy related Regulations

6.1 General Data Protection Regulation from EU

6.1.1 Introduction to GDPR

The GDPRis the European Union’s General Data Protection Regulation. Its purpose is to “harmonize data privacy laws across Europe, to protect and empower all EU residents’ data privacy, and to reshape the way organizations across the region approach data privacy for EU residents wherever they work in the world.” The law applies to any organization conducting business in the EU as well as to organizations outside the EU that collect, process, or store information on EU citizens as well as on non-citizens while they reside in the EU.

Article 1 of this regulation defines the GDPR objectives as:

- Enact rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- Protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

The GDPR regulations, define *personal data* as any anonymous data that can be used to identify individual. Following the evolution of information and communication technologies, personal data can be data that are not associated with the name of a person but can easily be used to identify him or her and to know his/her habits and tastes.

According to Article 5 of the GDPR regulation, 6 main principles are imposed for processing personal data:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject *(‘lawfulness, fairness and transparency’);*

b) Collected only for specified, explicit and legitimate purposes (‘*purpose limitation*’);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘*data minimisation’*);

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay *(‘accuracy’);*

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘*storage limitation’*);

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘*integrity and confidentiality’*).

The European authorities which are officially responsible for the legislative process are: the European Commission, the European Parliament and the Council of the European Union. In each member state of EU, there exist a data protection authority that ensure the application of the regulations.

Key features of GDPR are as follows:

- Enact rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- **Explicit consent:** Organizations must obtain explicit permission to collect, process or store personal data using language that clearly describes how the data will be used. Organizations will no longer be able to cloak the terms of consent in hard-to-understand, technical language or to rely on consumers to opt-out of unwanted communications. Moreover, consent must be use-specific, meaning that data collected for one reason (downloading a white paper, for example) can't be used for another purpose (such as targeting marketing emails) and that organizations cannot collect more data than is necessary for the stated purpose. In addition, organizations must make it easy for EU residents to withdraw their consent at any time.
- **Breach notification:** Organizations must issue all required notifications within 72 hours of the time they become aware of a breach. Required notifications vary by jurisdiction but typically include regulatory authorities, consumers, credit reporting agencies, law enforcement, etc. Organizations must also provide credit monitoring to consumers whose data was compromised.
- **Right to access:** Citizens and current EU residents have the right to know what data is being collected, how it's being used, where it's being processed, and who has access to it. In a significant shift toward empowering consumers, organizations (upon request) must provide an electronic copy, in machine-readable format, of the collected data free of charge. Users have the right to request that any incorrect information about them be corrected.
- **Right to be forgotten:** In addition to the right to withdraw consent, consumers have the right to demand that their data be erased and that, in some situations, third parties cease any processing of their data.
- **Data portability:** This provision of the GDPR introduces the concept of portability, which means that consumers have the right to request their data in an electronic format and to then transfer that data to another processor.

Article 4 defines data controllers and data processors as below:

- Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Generally speaking, the GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc. A data subject who wishes to revoke consent for his or her personal data therefore have to contact the data controller to initiate the request.

6.1.2 Impact to IoT System

- GDPR Article 32 "Security of processing" states that "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

  ➔ the pseudonymization and encryption of personal data

  ➔ the ability to ensure the ongoing confidentiality, integrity

  ➔ the ability to restore data in the event of a physical or technical incident

  ➔ When it comes to analyzing sensible datasets, measures which are mentioned more in detail are pseudonymization and anonymization.

- GDPR Article 25 “Data protection by design and by default” states that pseudonymization can help to implement the data protection principle of “data minimisation” and thus protect the data of the people involved.

  ➔ However, a pseudonymised data record still allows the identification of individual persons.

  ➔ Pseudonymization involves replacing the data in personally identifying fields with a seemingly random number or text.

  ➔ Simply replacing the data in these fields however does not make it impossible to re-identify individuals in a pseudonymized data set.

- The GDPR Recital 26 therefore states: “The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. […] The principles of data protection should therefore not apply to anonymous information, including for statistical or research purposes.”

- In its detailed documentation “Opinion 05/2014 on Anonymization Techniques”, the European Article 29 Data Protection Working Party has gone more into detail on how anonymization works in the context of the GDPR: “Accordingly, the Working Party considers that anonymization as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymization process is such as to reliably produce anonymized information in the sense described in this paper.”

  ➔ The anonymization of data does not require the user’s consent if there was a justified reason for collecting the data beforehand.

Nowadays, the Internet of Things (IoT) is becoming an increasingly growing topic that interests various sector of application e-health, connected homes, factory 4.0 agriculture, aquaculture etc. The IoT is partly responsible for an exponential increase in the volume of data generated on the network, at the origin of big data. This data has to be transmitted, processed in some way, and then potentially stored somewhere.

With 26 billion sensors planned for 2020, much of the produced data may be personal and some may be sensitive. This brings data privacy and personal data protection questions to the forefront. The question here is how are GPDR obligations are applied in a such context?

An important step towards GPDR compliance is about analyzing the dataflow in the existent system. Figure 1 details main dataflow steps in a generic IoT environment.

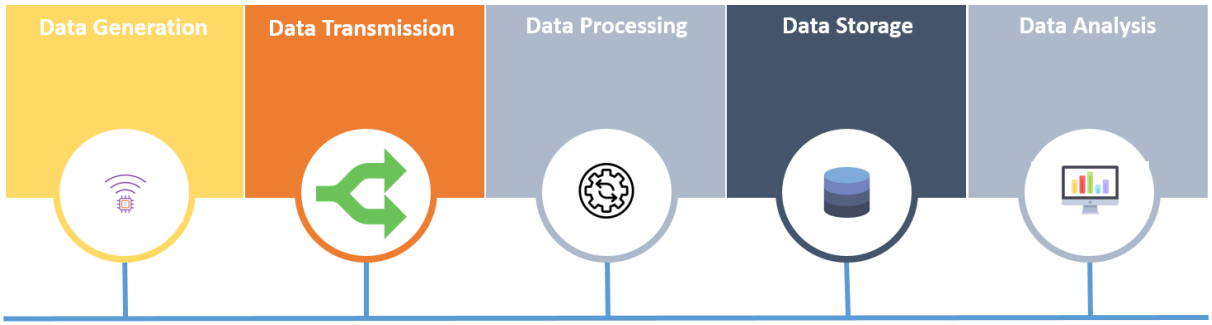


Figure 6.1.2-1: Data flow of a generic IoT environment

These steps are detailed below with some question about the GPDR obligations and potential impact to IoT platforms especially for the Article 5:

a. Data Generation:
   i. Is these data personal/sensitive? GPDR is-it applied in this context?
   ii. Did the user give his/her consent in the case of personal/sensitive data?
   iii. Is the collected data is only for specified, explicit and legitimate purposes?

b. Data Transmission

i. What is the transmission method? Is-it accessible for everyone (via the Web for example)?

ii. The used protocol for transmitting data is-it secured?

c. Data Processing

i. Is there an enough explication about this process to the concerned user?

ii. Which data is subject to pseudonimization and anonymization?

iii. Which algorithm has to be applied to which data?

d. Data Storage

i. Is data stored in the EU?

ii. User rights related to his/her personal data such as (rights: to access, of rectification, of opposition, of limitation, to data portability, to forget), are respected?

iii. What are the existing measure for protecting data bases (encrypting, archiving…)

e. Data Analysis

i. Did the user give his/her consent about analyzing his/her personal data?

6.2 Personal Information Protection Act from South Korea

6.2.1 Introduction to PIPA

South Korea's comprehensive Personal Information Protection Act (PIPA) was enacted Sept. 30, 2011. It is one of the world's strictest privacy regimes. Like the GDPR, it protects privacy rights from the perspective of the data subject and it is comprehensive, applying to most organizations, even government entities. It is not only applicable and strict, but its penalties — which include criminal and regulatory fines and even imprisonment — are enthusiastically enforced.

PIPA applies to personal information processing organizations, known as "data handlers," that are defined as a person, government entity, company, individual, or any other person that, directly or through a third party, handles personal information for work or business purposes. Personal information refers to information pertaining to a living individual, which contains information identifying a specific person, such as name, national identification number, images, or other similar information.

Under the Act on the Promotion of Information and Communication Network Utilization and Information Protection (the "Network Act"), which supplements PIPA, personal information includes name, national identification number, letter, voice, sound image, and all other information that makes it possible to identify a specific person. The Network Act provides measures for protecting the personal information of users collected and used by the telecommunications business operators.

In addition to regulating personal information, the Acts impose compliance measures to ensure proper collection, use, and transfer, among other things, of users' personal information. Technical and managerial protective measures must be taken in order to store personal information. Organizations must also inform data subjects of their rights and its obligations as a data handler.

7 Technologies for Handling of Privacy Information

This section introduces several well known algorithms and privacy models for protection of personal information.

7.1 Pseudonymisation Techniques

According to Article 4, paragraph 5 of the GDPR ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; Several pseudonymization techniques are introduced below.

7.1.1 Heuristic Pseudonymization

It is a method of hiding detailed personal information by replacing the values corresponding to identifiers with some predetermined rules or by processing them according to the judgment of the person.

For example, replace name information with a generalized name such as James or Sophia, or replace institution information with Korea, the United States, or Earth. This will be done by setting rules in advance. All data is processed in the same way, making it easy for users to use and understand.

7.1.2 Data Masking

The standard for pseudonymization is known as data masking. By replacing sensitive data with virtual but realistic data, it helps reduce data risks while preserving data utilities. Examples of data masking are shown in the table below.

Table 7.1.2-1: Example data masking

Before		**After**	
Last Name	**Credit Card**	**Last Name**	**Credit Card**
James	4234-5678-9128-4567	Schmidt	4876-5432-1987-6543
Davis	3213-4567-8901-2345	Fowler	3456-7890-1234-5678

Masked data shall not break application integrity. It shall meet the same business rules as real data(e.g., masked ages are still in the same age group. The zip code has the same geographic variance. Credit card checksums are correctly calculated to ensure that the application running for masked data is performed as if the masked data are real and that there is no limit to the user’s ability to use the application appropriately.

7.2 Anonymization Techniques

Anonymization is the processing of personal information into an unrecoverable state so that a particular individual is not identifiable. In IoT system that collects and analyzes large data and obtains useful information, in order to protect sensitive personal information, there is a need for anonymization technique that lowers personal identification of data.

Data anonymization is a method of protecting personal information and securing privacy through the aggregation of raw data. Since the concept of k-anonymity, the l-diversity and t-proximity -closeness, s-uniformity, and so on. Anonymization removes identifiers and anonymizes quasi-identifiers for privacy protection of sensitive attributes.

The following subsections present the privacy models and how to process anonymization.

7.2.1 Data Anonymization Algorithms

Data pseudonymization has the potential to be re-identifiable, therefore, data annonymization needs to be applied for data that should not be reidentifiable. In this sections, well known algorisms for data anonymization are introduced.

k-Anonymity: Basic model for privacy protection.

K-anonymity allows the same value to exist at least k in a given data set so that it is not easily combined with other information. A part of the data set is modified and all records have k-1 or more records that are identical to (not distinguished) themselves. Linking cannot be performed with confidence > 1/k. Sensitive attributes are not considered in this model. Normally k-anonymity can be implemented by generalization and suppression.

Original data		
Age	Gender	Zipcode
42	Female	53715
42	Female	55410
77	Male	90210
32	Male	02274
32	Male	02237

2-Anonymization			
	Birth	Gender	Zipcode
Group1	40-49	Female	5****
	40-49	Female	5****
Suppressed	77	Male	90210
Group2	30-39	Male	022**
	30-39	Male	022**

Figure 7.2.1-1: Example of k-Anonymity

The generalization technique is to replace attribute values with more generalized values. The k-anonymity condition can be achieved by converting the value of each attribute to a value on a more generalized domain. The greater the generalization, the more easily the k-anonymity will be met, but if the data table is modified too severely, no useful information will be available. Suppression means removing values from the information table completely; suppression removes all attribute of the cell, so more information is lost when compared to generalization. Remove all details, so only suppression is applied to major characteristics; data suppression does not result in a dangerous attack.It can be applied to row level column levels and to entire cells.

L-Diversity:

This privacy model is that records that are de-identified together in a given data set have at least l different sensitive information (in the same set). It defends attacks by homogeneity attacks and background knowledge, which are two attacks on k-anonymity. This model constitutes a equivalence class with sufficiently diverse (more than l) sensitive information in the de-identification process.

Original data

Non-Senstive			Senstive
Age	Gender	Zipcode	Disease
22	Female	02900	Diarrhea
20	Female	02274	Anemia
51	Female	53032	Diarrhea
41	Male	53001	Flu
39	Male	02150	Anemia
31	Female	02585	Flu

2-divirsity

Non-Senstive Data			Senstive Data
Age	Gender	Zipcode	Disease
0-40	*	02***	Diarrhea
0-40	*	02***	Anemia
40-80	*	53***	Diarrhea
40-80	*	53***	Flu
0-40	*	02***	Flu
0-40	*	02***	Anemia

Figure 7.2.1-2: Example of L-Diversity

The table above is an example of medical data that are de-identified by the 3-diversity model. Sensitivity information, the disease name is mixed enough to protect against attacks.

T-Closeness:

This privacy model can also be used to protect data from attribute disclosure. It requires that the distributions of values of a sensitive attribute within each equivalence class must have a distance of not more than t to the distribution of the attribute values in the input dataset.

Even if the k-anonymity and l-diversity are satisfied, if the sensitive information distribution of the combination is different from the distribution of the other combinations, the sensitive information is leaked due to the distribution difference. The idea is to make two distances less than the threshold t. In this case, the method used to calculate the distance between the two distributions uses the Earth Mover's Distance (EMD) used in statistics.

The table below shows anonymized data sets. The red areas show relatively similar salaries compared to the overall distribution (30-110): the attacker can infer an approximate salary and the disease properties indicate that everyone is vulnerable to the stomach disease. The T-closseness model defines excessive differences in the distribution between the equivalence class and the entire data set as a weakness of the l-diversity model and prevents similar values from pooling.

Non-Senstive Data			Senstive Data	
Age	Gender	Zipcode	Disease	Salary
0-40	*	02***	Gastric ulcer	30
0-40	*	02***	Chronic gastritis	50
40-80	*	53***	Acute gastritis	60
40-80	*	53***	Diarrhea	110
0-40	*	02***	Flu	90
0-40	*	02***	Chronic gastritis	100

t-closeness

Non-Senstive Data			Senstive Data	
Age	Gender	Zipcode	Disease	Salary
0-40	*	02***	Gastric ulcer	30
0-40	*	02***	Diarrhea	90
40-80	*	53***	Acute gastritis	60
40-80	*	53***	Diarrhea	110
0-40	*	02***	Chronic gastritis	50
0-40	*	02***	Chronic gastritis	100

Figure 7.2.1-3: Example of T-Closeness

The green part of the table above is a homogeneous set. Since the distribution of salaries is 30 to 90, there is no significant difference from the entire distribution of salaries(30-110). Diarrhea items also make it difficult to infer certain diseases.

δ-Disclosure privacy:

This privacy model can also be used to protect data against attribute disclosure. It also enforces a restriction on the distances between the distributions of sensitive values but uses a multiplicative definition which is stricter than the definition used by t-closeness.

β-Likeness:

This privacy model is related to t-closeness and δ-disclosure privacy and it can also be used to protect data against attribute disclosure. It aims to overcome limitations of prior models by restricting the relative maximal distance between distributions of sensitive attribute values, also considering positive and negative information gain.

δ-Presence:

This model can be used to protect data from membership disclosure. A dataset is (δmin, δmax)-present if the probability that an individual from the population is contained in the dataset lies between δmin and δmax. In order to be able to calculate these probabilities, users need to specify a population table.

	Public Data(P)				
	Name	Zipcode	Age	Nationality	Sen
1	Alia	47096	35	USA	0
2	Ben	47093	59	Canada	1
3	Catarina	47096	42	USA	1
4	David	47630	18	Brazil	0
5	Euria	47630	22	Brazil	0
6	Franck	47633	63	Peru	1
7	Gary	48973	33	Spain	0
8	Hailey	48972	47	Bulgaria	1
9	Ivan	48970	52	France	1

	Private Data(T)		
	Zipcode	Age	Nationality
2	47093	59	Canada
3	47096	42	USA
6	47633	63	Peru
8	48972	47	Bulgaria
9	48970	52	France

Figure 7.2.1-4: Example of δ-Presence

Given an external (public) background knowledge P, and a private table T; δ = (δmin , δmax)-presence holds for a generalization T* of T if δmin ≤ Pr(t Є T | T* ,P) ≤ δmax for every t Є P.

	Public Data(P)				
	Name	Zipcode	Age	Nationality	Sen
1	Alia	47096	35	USA	0
2	Ben	47093	59	Canada	1
3	Catarina	47096	42	USA	1
4	David	47630	18	Brazil	0
5	Euria	47630	22	Brazil	0
6	Franck	47633	63	Peru	1
7	Gary	48973	33	Spain	0
8	Hailey	48972	47	Bulgaria	1
9	Ivan	48970	52	France	1

	Private Data(T*)		
	Zipcode	Age	Nationality
2	47***	*	America
3	47***	*	America
6	47***	*	America
8	48***	*	Europe
9	48***	*	Europe

Figure 7.2.1-5: Generalized δ-Presence

δ-Presence can be generalized from the table above. A generalization T* of T is a nonoverlapping generalization with respect to P if – every tuple in P can be mapped onto at most one equivalence class in T* .

	Public Data(P*)				
	Name	Zipcode	Age	Nationality	Sen
1	Alia	47***	*	America	0
2	Ben	47***	*	America	1
3	Catarina	47***	*	America	1
4	David	47***	*	America	0
5	Euria	47***	*	America	0
6	Franck	47***	*	America	1
7	Gary	48***	*	Europe	0
8	Hailey	48***	*	Europe	1
9	Ivan	48***	*	Europe	1

	Private Data(T*)		
	Zipcode	Age	Nationality
2	47***	*	America
3	47***	*	America
6	47***	*	America
8	48***	*	Europe
9	48***	*	Europe

Figure 7.2.1-6: δ-Presence with an external background knowledge

Let T* be a non-overlapping generalization of T with respect to P. Then T* is δ-present, if for each equivalence class of the corresponding P*:

δmin ≤ (# of 1s in Sen.) / |ec| ≤ δmax

The values in the above tabel are Pr(t a Є T | T*) = 0.5 and Pr(t g Є T | T*) = 0.66.

8 Analysis on the Current oneM2M System

8.1 Privacy Features in oneM2M System

In GDPR, it is important to distinguish "Processor" and "Controller".

According to Article 4 of the EU GDPR, Controller and Processor are defined as follows:

- Controller – "*means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"
- Processor – "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

More specifically, according to Article 24 from the EU GDPR the main responsibility of Controller is ,"*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*"

On the other hand, according to Article 28 from the EU GDPR, the main responsibility of Processor is, "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*

The roles of Processor and Controller can be assigne to oneM2M entities.

In the oneM2M reference architecture, two basic types of entities are defined. One is an Application Entity (AE) and the other is a Common Services Entity (CSE):

- The AE is an embedded application hosted in the device with capabilities to monitor (sensor, actuator) and interact (sensor, actuator, consumer) with the gateway through specific oneM2M standards.
- The CSE is hosted in the cloud or server. A CSE is actually the entity that contains the collection of oneM2M-specified common service functions that AEs are able to use.

In order to clarify the different roles of AE and CES in processing and controlling data among the oneM2M architecture, the figure below proposes a simple scenario where data are produced by a sensor (or an actuator) then transferred to the gateway and server in the cloud to be finally consumed by a user via his device.

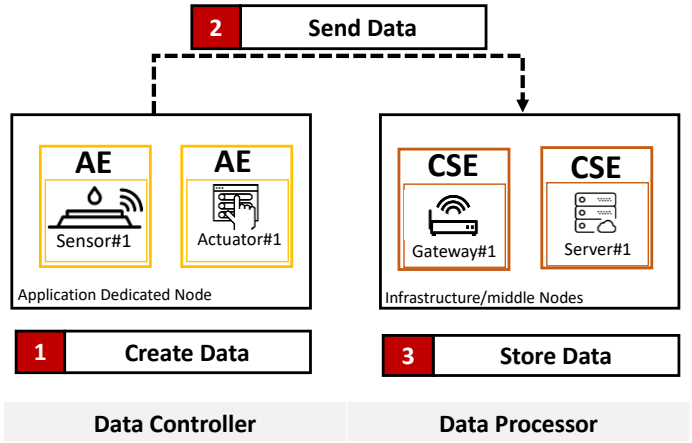


Figure 8.1-1: Processing and controlling activities in oneM2M

A data controller and a data processor have different roles and responsibilities. Also depending on a situation and configuration, the same entity can behave as a controller or processor. The concept of data controller and data processor between different oneM2M entities can be summarized according to the six steps shown in the Figure 1 and detailed here:

- **Step 1**: The AE (sensor or actuator) generates a piece of data; The AE decides whether the generated data is under the control of the GDPR regulation. In this case, the AE is considered as a Data controller.
    - A GDPR compliance needs to check at the first if the generated data can be used to identify a person. In addition, the process of generating this data should be authorized.
- **Step 2**: The AE sends the generated data to the CSE (gateway or server); As the AE indicates that the data is under the GDPR, the AE is still considered as a data controller.
    - A GDPR compliance needs to check if the manner of sending data if it is secured specially when using shared networks.
- **Step 3**: The CSE manages the data and stores it; As the CSE processes (e.g., annonymization and pseudonymization) the received data based on the GDPR regulation, it is considered as a data processor
    - A GDPR compliance needs to check the data is needed to be processed and stored in EU.

8.2 GDPR impact to oneM2M

The following Table 8.2-1 list the key GDPR features that potentially have an impact to IoT platforms.

Table 8.2-1: Identify GDPR statements that may have impact to oneM2M

GDPR Category	Feature No.	Key GDPR Features	Relevant Articles	GDPR statements
Data Processing	GF1	Further processing managements	5, 6, 7	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
	GF2	Data management based on purposes	5, 6	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
	GF3	Data accuration verification function	5, 6, 7	Personal data shall be accurate and, where necessary, kept up to date;
	GF4	Duration based data processing	5, 17	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
Consent Management	GF5	Consent checker	7	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
	GF6	Conesent-based data management	5 ,7, 17	Personal information processing shall be performed based on consent.
	GF7	Consent revoke function and stop processing function.	5 ,7, 17	The data subject shall have the right to withdraw his or her consent at any time.
Data Contents Management	GF8	Age checker	6, 8	The processing of the personal data of a child shall be lawful where the child is at least 16 years old.
	GF9	Sensitive information Identifier	5, 9, 10	Sensitive & criminal data processing shall be prohibited
Right to Data	GF10	Right to be informed	5,	Where personal data are collected information shall be provided to data subjects.
Data Access Management	GF11	System access mechanisms for users.	5, 15	A data subject should have the right of access to personal data which have been collected concerning him or her
	GF12	Account and logging	5, 15	A data subject should know where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing

	GF13	Identity verification	5, 15	The controller should use all reasonable measures to verify the identity of a data subject who requests access.
Right to Data	GF14	Right to rectification	16	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
Rigth to Data	GF15	Rigth to erasure	17	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data
Right to Data	GF16	Right to restriction of processing	18	The data subject shall have the right to obtain from the controller restriction of processing such as purpose of processing and the existence of right to request.
Right to Data	GF17	Right to data portability	20	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided
Right to Data	GF18	Right to object	21	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her including profiling based on those provisions.
Data protection impact assessment	GF19	Privacy assessment	32, 35	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data
Privacy Protection	GF20	Anonymisation	6, 24, 25, 32	Data rendered anonymous in such a way that the data subject is not or no longer identifiable.
	GF21	Pseudonymisation	5, 6, 24 25, 32	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.
	GF22	Risk detection function	25, 32	Technical and organisational measures should be taken to protect personal information.
	GF23	Background storage	5, 32	The Technical and organisational measures shall be taken to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

8.3 Unsupported GDPR features and Key Privacy Issues

The following Table 8.3-1 lists up potential requirements that oneM2M may consider to support GDPR relevant features.

Table 8.3-1: GDPR feature analysis

Feature(GF) No.	oneM2M support	Extracted potential requirements from GDPR statements
GF1	Too broad	The IoT system shall support management for further processing besides the purpose to minimize the processing of personal information.
GF2	Too broad	The IoT system shall support a mechanism providing the purposes of data processing.
GF3	Out of scope	The IoT system shall support an accurate and up-to-date verification function for collecting information. If it is not accurate or up-to-date, it shall be corrected or deleted by the function.
GF4	Partially supported	The IoT system shall support the deletion of data that have passed the retention period. → The oneM2M system already supports the expiration timer.
GF5	Not supported	The IoT system shall support a mechanism to demonstrate that the data subject has consented to the processing of personal data.
GF6	Not supported	The IoT system shall support managing consents from user to process privacy data.
GF7	Not supported	The IoT system shall support mechanism that allows data subjects to easily revoke consent and stop processing.
GF8	Out of scope	The IoT system shall support verification of the age of the data subject and obtain parental consent if under 16 years of age.
GF9	Out of scope	The IoT system shall support the identification of sensitive information (e.g., racial, political, sexual) and the restriction of the processing.
GF10	Supported	The IoT system shall support the provision of information about the processing of personal information to data subjects. → Subscription/Notification can support this.
GF11	Supported	The IoT system shall support proper access control policy to personal data. Access is supported by oneM2M. Access Control Policy (ACP) in oneM2M provides the means to access private data.
GF12	Partially supported	The IoT system shall support the identification of users and access history → This is partially supported via "Service Statistics Collection Recording".
GF13	Supported	The IoT system shall support access right to personal information.
GF14	Supported	The IoT system shall support the modification of data based on the data subject's rectification request.
GF15	Partially supported	The IoT system shall support the deletion of personal data based on the data subject's delete request.
GF16	Partially supported	The IoT system shall support data subject identification and information deletion to the data subject's restriction request.
GF17	Out of scope	The IoT system shall support the provision of personal information in a machine-readable form (e.g., CSV file) when there is a movement of personal information by the data suject's request (either to the data subject or to anonther controller).
GF18	Out of scope	The IoT system shall support processing interruption based on the objection from the subject of data.
GF19	Out of scope	The IoT system shall support regular self-test and assessments of the effectiveness of security technologies.
GF20	Partially supported	The IoT system shall support data anonymisation.
GF21	Partially supported	The IoT system shall support data pseudonymisation.
GF22	Not supported	The IoT system shall support means or information (e.g., log information) to be used by intrusion prevention and detection system.
GF23	Out of scope	The IoT system shall support information recovery and backup.

Based on the listed potential requirements for GDPR, the following key issues are identified.

1. Key Issue #1 – GF20 (Support of data anonymization):
   - How could the oneM2M system support the anonymisation of personal data stored in the resources?
   - Could the oneM2M system anonymise a portion of the data?
   - How could the oneM2M system support different types of anonymisation mechanism?

2. Key Issue #2 – GF21 (Support of data pseudonymization):
   - How could the oneM2M system support the pseudonymisation of personal data stored in the resources?
   - Could the oneM2M system pseudonymise a portion of the data?
   - How could the oneM2M system identify which data needs to be pseudonymized?
   - How could the oneM2M system support different types of pseudonymisation mechanism?
3. Key Issue #3 – GF5, GF6, GF7 (Fine grained consent management):
   - How could the oneM2M system provide consent from the owner of data?
   - What kinds of information should be stored and managed in the oneM2M system to support the consent from the user?
4. Key Issue #4 – GF4, GF15, GF16 (Right to be deleted and forgotten):
   - How could the oneM2M system support various deletion and forgotten needs defined in GDPR? For example, could the oneM2M system delete all the personal data owned by a specific user?
5. Key Issue #5 – GF12, GF22 (Logging):
   - Does the current oneM2M system support log various events such as access to a resource containing personal data?
   - What kinds of logging information or records should be supported by the oneM2M system to be compliant with GDPR?

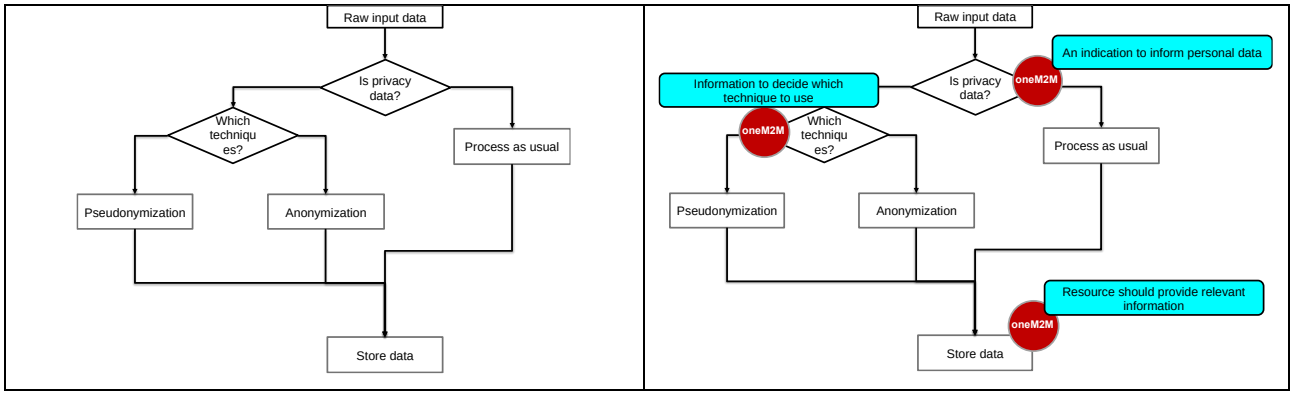
9 Proposed Solutions

9.1 Solution: Key Issue 1 & 2 - Pseudonymization and Anonymization of Privacy Data

Pseudonymization and anonymization can reduce the risk of data loss and assist a data processor in fulfilling their data compliance regulations. Therefore, pseudonymization and anonymization are considered key techniques to be used in IoT platforms to be compliant with GDPR. These two techniques are different and provide different results after processing. Therefore, the use of these techniques by an IoT platform may depend on the degree of risk and how the data will be processed. In addition, various algorithms and implementations are also available for each of the techniques.

- **Pseudonymization** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **Anonymization** means the data must be stripped of sufficient elements such that the data subject can no longer be identified. More precisely, that data must be processed in such a way that it can no longer be used to identify a natural person by using 'all the means likely reasonably to be used' by either the controller or a third party. An important factor is that the processing must be irreversible.

Specifically, the GDPR defines pseudonymization in Article 3, as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymise a data set, the "additional information" must be "kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person."



General procedure for handling privacy data	Possible place where oneM2M can be used to handle privacy data

Figure 9.1-1: Privacy data handling

In order to process privacy data in oneM2M based on regulations, the oneM2M system should provide a set of attributes to hold information to be used for data processing (see Figure 9.1-1). In particular, some necessary information for the processor to process privacy data are as follows:

- Which regulations to be applied?
- Is the data subject of private data?
- What kinds of rules have to be applied?
- What kinds of techniques or algorithms have to be used?
- Which parts of data are private data?

Such information can be modelled as attributes of oneM2M resources such as [contentInstance] and [container]. The definition of the attributes is explained in the table below.

Table 9.1-1: Attributes needed to support privacy data

Attributes	Multiplicity	RW/ RO/ WO	Description
privacyRegulation	1	RW	Used to indicate which regulation is to be applied. An example of this attribute is gdpr (for EU) or pipa (for KR)
privacyIndication	1	RW	Used to indicate that this data is subject to privacy regulation
privacyProcessingRule	1	RW	Used to mention a technique to be used, for example, pseudonymization or anonymization
privacyTechniques	1	RW	Optionally this attribute can be used to mention about detail information such as replacement, scrambling, masking, personalized anonymization, blurring.
privacyBlock	1	RW	If parts of data contain privacy-related data, this attribute can be used to identify the accurate parts of data to be handled. For example, Alice-info-3948272 contains 'Alice-info', which is data that should be anonymized. In this case, ten characters should be anonymized.
privacySubject	1	RW	Used to indicate which parts of a resource are subject for this privacy regulation (name or data)

The following figure shows how privacy data can be processed in oneM2M system.

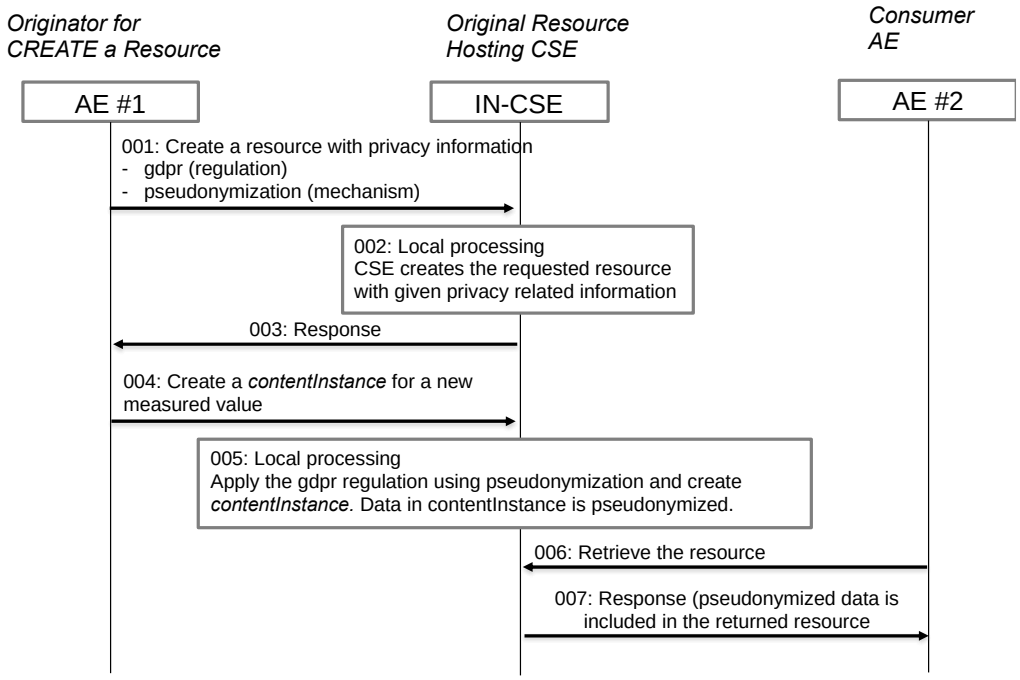


Figure 9.1-2: Privacy data handling procedure

- Step 1-3:
  A wearable sensor application that is associated with a person registers and creates corresponding resources on a IN-CSE. As the sensor application contains privacy data, the creation message contains attributes indicating which regulation to follow and the type of data processing mechanisms (e.g., pseudonimyzation).

- Step 4-5:
  When a new measurement from the sensor application creates a *contentInstance* resource, the data in the *contentInstance* is pseudonymized as indicated in the resource attribute.

- Step 6-7:
  AE2 tries to read the *contentInstance* resource to show the value to its user. As the resource is indicated as privacy data, the response includes pseudonymized data.

9.2 Solution: Key Issue 3 – Consent Management

Under GDPR, processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing by the owner of the data. According to GDPR, consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. Therefore, it is very important how to manage consent in IoT platforms.

oneM2M system supports access control policy (ACP) to handle the access right of the resources containing data. However, the current ACP is limited to support the concept consent management introduced by GDPR as it only defines the access right of the originator for the given operations (i.e., CRUDN).

In GDPR, Consent is defined in Article 4(11) as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". On the other hand, ACPs in oneM2M are used by the CSE to control access to the resources. This means that 'Consent' and 'ACPs' can complement each other as ACPs control the access of the resources, while consent further defines what kinds of processing are allowed on personal data within the resources.

In order to support the concept of consent management from GDPR, oneM2M system should answer the following two questions:

- How to provide consent from the users?

- How to manage consent information?

Consent is strictly related to data processing as it gives a clear indication about which is the purpose that the personal data of a user is processed for. Each processing purpose is associated with one or more processing activities. Basically, individuals who hold IoT data want to limit their consent. Assume that as an IoT service platform provider, a data holder wants to use collected IoT data for various purposes, including marketing purposes. Here are some examples of various consents.

- Customer A agrees to share personal bio data measured by wearable IoT devices to specific hospitals.
- Customer B agrees to use personal location data to be used by marketing companies after three months from now.
- Customer C agrees to forward personal data from IoT devices to 3rd party data analytics companies and receive recommendations.

Provisioning of consent:

As IoT platforms need to get users' consent for their data, there should be clear and easy ways to acquire consent from users. There exist three different ways to get it from IoT service platforms.

1. Pre-provisioning: When a user purchases an IoT device from a service provider, consent can be given and embedded to the IoT device. When the device is registered to an IoT platform, the pre-provisioned consent can be included in the registration procedures.
2. Post-provisioning: An IoT application is registered to an IoT platform without consent. Once the data of the IoT application is identified as personal data, a user can select its consent via, for example, a web interface IoT application.
3. Interactive-provisioning: When an IoT application is registered to an IoT platform, there should be an additional step acquiring users' consent.

Below Table 9.2-1 shows the differences between three consent provisioning mechanisms.

Table 9.2-1: Consent provisioning mechanisms

	Post-provisioning	Pre-provisioning	Interactive-provisioning
Who	User	User or Service Provider	User
When	After registration	At purchasing IoT device	During registration
How	Using UI (e.g., Web UI)	Using pre-configured message	Using enhanced registration procedures

9.2.1 Consent Management Solution #1

Consent management dedicated resource:

Consent should include various information to make the purpose and associated activities clearly. Such activities and information can be modeled as a resource called [*consentMgt*]. Each resource identified as personal data refers to associated consent resources. The following figure introduces a high-level concept of consent management.

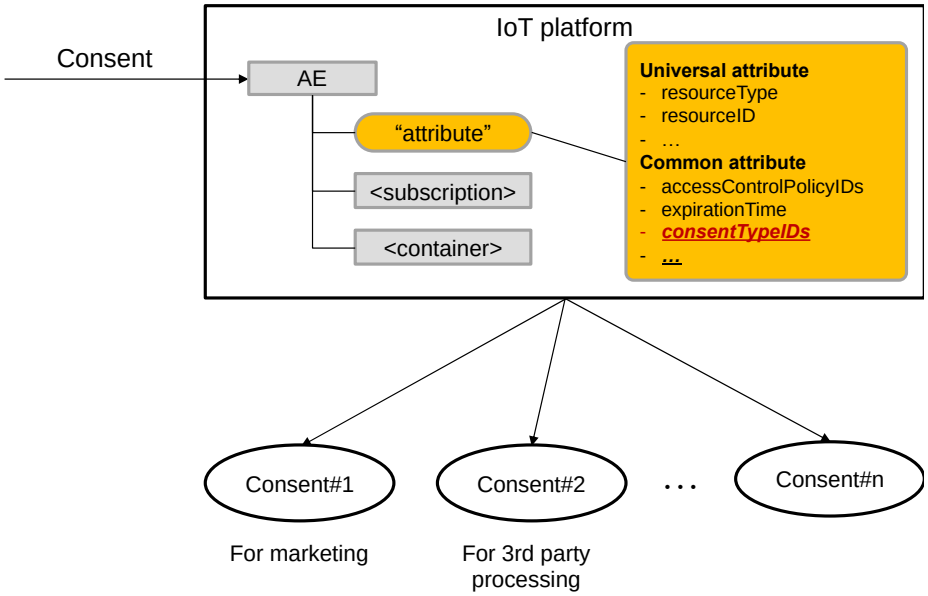


Figure 9.2.1-1. Consent management concept

The [*consentMgt*] resource is used to store consent purposes and relevant information.

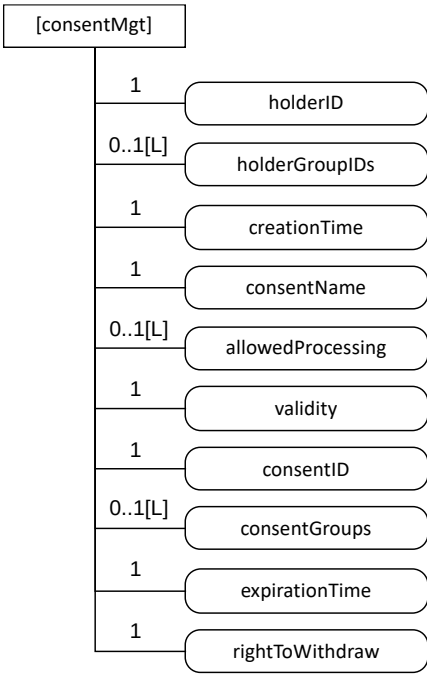


Figure 9.2.1-2: Structure of [*consentMgt*] resource

562 The *[consentMgt]* resource shall contain the attributes specified in the table below.

563 **Table 9.2.1-1: Attributes of [*consentMgt*] resource**

Attributes of *[consentMgt]*	Multiplicity	RW/ RO/ WO	Description
holderID	1	RO	The holder of the consent.
holderGroupIDs	0..1 (L)	RW	A list of groups that the holder of this consent belongs, for example, - Business - Consumer - Administrator - VIPs
creationTime	1	RO	Indicate when this consent is created.
consentName	1	WO	The name of this consent.
allowedProcessing	0..1 (L)	RW	A list containing allowed processing, for example, - Sharing with 3rd party - Marketing
validity	1	RW	Indicate the validity of this consent.
consentID	1	WO	The identifier of this consent.
consentGroups	0..1 (L)	RW	A list of consent groups that this consent belongs, for example, - Specific applications - Marketing campaigns - Cookie type of consents
expirationTime	1	RO	The expiration time of this consent.
rightToWithdraw	1	RW	Indicate whether the holder has a right to withdraw the consent at anytime.

564

565 9.2.2 Consent Management Solution #2

566 **ACP-based consent management:**

567 Consent can be considered as part of the access control policy as it handles a data holder's intention about data usage. If
568 contents of data are related to personally identifiable information, only contents with users' consent can be shared or
569 used by others except for the holder of data. Therefore, the consent can be considered as one of ACP. Therefore, in this
570 section, a solution enhancing the existing ACP mechanism to cover the consent management is introduced.

571 The existing <accessControlPolicy> resource is comprised of *privileges* and *selfPrivileges* attributes which represent a
572 set of access control rules defining which entities (defined as *accessControlOriginators*) have the privilege to perform
573 certain operations (defined as *accessContolOperations*) within specified contexts (defined as *accessControlContexts*)
574 and are used by the CSEs in making Access Decision to all or specific parts (i.e. child resources or attributes) of the
575 targeted resource (defined as *accessControlObjectDetails* and *accessControlAttributes*).

576 In the case of consent management, it is important to define what kinds of processings are allowed by the service
577 provider. Therefore, an additional attribute called *consentRules* can be introduced to define a set of consent
578 management rules that applies to resources referencing this <accessControlPolicy> resource.

579 For example, the following table that is copied from TS-0001 shows the attributes of <accessControlPolicy> resource.

580 **Table 9.1.2-1: Attributes of *<accessControlPolicy>* resource from TS-0001**

Attributes of *<accessControlPolicy>*	Multiplicity	RW/ RO/ WO	Description	*<accessControlPolicyAnnc>* Attributes
resourceType	1	RO	See clause 9.6.1.3.	NA
resourceID	1	RO	See clause 9.6.1.3.	NA
resourceName	1	WO	See clause 9.6.1.3.	NA
parentID	1	RO	See clause 9.6.1.3.	NA
expirationTime	1	RW	See clause 9.6.1.3.	MA
labels	0..1(L)	RW	See clause 9.6.1.3.	MA
creationTime	1	RO	See clause 9.6.1.3.	NA
lastModifiedTime	1	RO	See clause 9.6.1.3.	NA
announceTo	0..1 (L)	RW	See clause 9.6.1.3.	NA
announcedAttribute	0..1 (L)	RW	See clause 9.6.1.3.	NA
announceSyncType	0..1	RW	See clause 9.6.1.3.	MA
owner	0..1	RW	See clause 9.6.1.3	NA
privileges	1	RW	A set of access control rules that applies to resources referencing this <*accessControlPolicy*> resource using the *accessControlPolicyID* attribute.	MA
selfPrivileges	1	RW	A set of access control rules that apply to the <*accessControlPolicy*> resource itself and *accessControlPolicyIDs* attribute of any other resource which is linked to this <accessControlPolicy> resource.	MA
consentRules	1	RW	A set of consent management rules that applies to resources referencing this <accessControlPolicy> resource	NA
authorizationDecisionResourceIDs	0..1 (L)	RW	A list of addresses of <*authorizationDecision*> resources. See clause 9.6.41 for further details.	MA
authorizationPolicyResourceIDs	0..1 (L)	RW	A list of addresses of <*authorizationPolicy*> resources. See clause 9.6.42 for further details.	MA
authorizationInformationResourceIDs	0..1 (L)	RW	A list of addresses of <*authorizationInformation*> resources. See clause 9.6.43 for further details.	MA

581

582 The set of consent management rules represented in *consentRules* attributes are comprised of consent-management-rule-
583 tuples (*consentHolder*, *createdTime*, *consentName, allowedProcessing*, *consentValidity*, *expirationTime*,
584 *rightToWithdraw*) with parameters shown in Table 8.x.1-1 which are described in the previous clauses 8.x.1.

585 The following Figure 8.x.2-2 shows a high-level concept of consent management using the <accessControlPolicy>
586 resource.

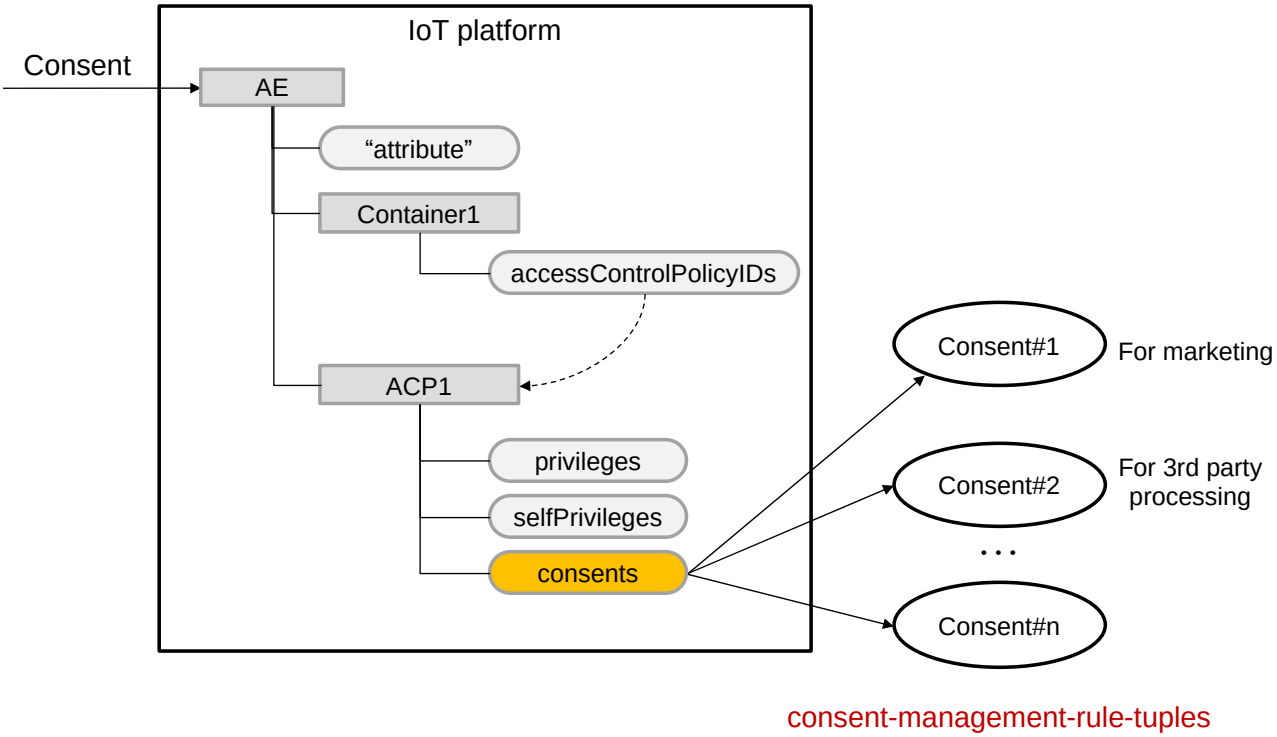


Figure 9.2.2-1: ACP-based consent management concept

9.3 Solution: Key Issue 5 - Logging

In GDPR, there are several articles that the processor has to monitor activities on data for various purposes. For example, the processor shall notify the controller without undue delay after becoming aware of a personal data breach. In addition, one of the principles of GDPR is 'integrity'. This means that the IoT platform playing as the processor should have to keep the data correct. Therefore, IoT platforms should have a logging feature at least recording the following information:

- Tracking access to IoT data: who accessed what and when. If access to data goes without proper access right, the system administrator can track all access to data and thus manifest that only the authorized personnel should be able to read the data.
- Tracking data modifications: one of the principles of GDPR is "integrity". The IoT platform should have to keep the data correct, therefore any modification should be logged.
- Logging GDPR-specific activities: e.g. when the data subject invokes their rights.
- Logging consent: – date, time, IP address, etc. Then any consent related activities, e.g., consent withdrawal, and the history of the consent of the data subject can be logged.

In order to support logging in oneM2M system, a resource that can support following information has to be defined:

- Enable/disable logging
- What to log
- When to log
- Types of log
- Format of log

Such information can be modeled into a resource called [*logMgtRule*]. The [*logMgtRule*] resource shall be used to define log rules and events that trigger logging. The [*logMgtRule*] resource shall contain the child resource specified in table below. The [*logMgtRule*] resource shall contain the attributes specified in the table below.

Table 9.3-1: Attributes of [logMgtRule] resource

Attributes of *[logMgtRule]*	Multiplicity	RW/ RO/ WO	Description
logStart	1	RW	When to start this log record
logEnd	1	RW	Wned to end this log record
logCriteria	1	RW	This si a property to provide which information should be logged. For example, if all the operations on the resource have to be logged, CRUDN have to be mentioned in this property.
logFormat	0..1 (L)	RW	This is a property to provide what kinds of log information have to be stored under which format. Default format could be <event time, Origin, operation, target resource, results> Additionally, ip address of Origin, binding protocols, etc. can be looged. Each item can be separated using a delimiter such as ';'.
logLevel	1	RW	Level of log information. Example values coule be store all information, store only successful events, store only failed events.
logResourceIDs	0..1 (L)	RW	A list of resource IDs to be logged.
logStorage	1	RW	A reference to a resource that actual log records are stored.

The [*logMgtRule*] resource can be created by an IoT application managing logging. In this case, the logging application indicates target resources to be logged, as well as other properties of the [*logMgtRule*] resource. If a user wants to record log information for a specific application, the application can be created with an indication activating the logging feature. In this case, existing [*logMgtRule*] has to be referred as a referencing log management rule to be used. The following two properties can be used to indicate log indication and referecing a log management rule:

- *logIndication*: This is a property to indicate a resource with this property is a subject for system log
- *eventLogID:* Which Log rules will be followed. A URI of referencing <logMgtRule> resource has to be added

The following figure shows the high-level resource structure of the proposed logging mechanism.

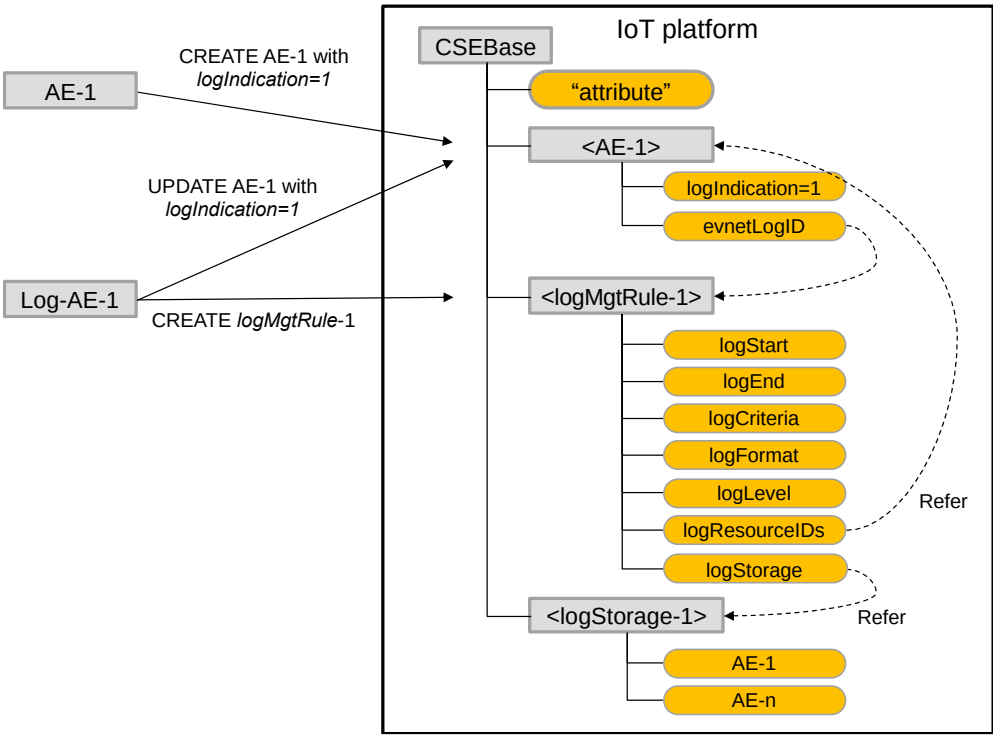


Figure 9.3-1: Logging resource structure

The following figure shows procedures that a logging application creates a logging management rule to oneM2M platform and an application uses the created logging rule to record any activities on it.

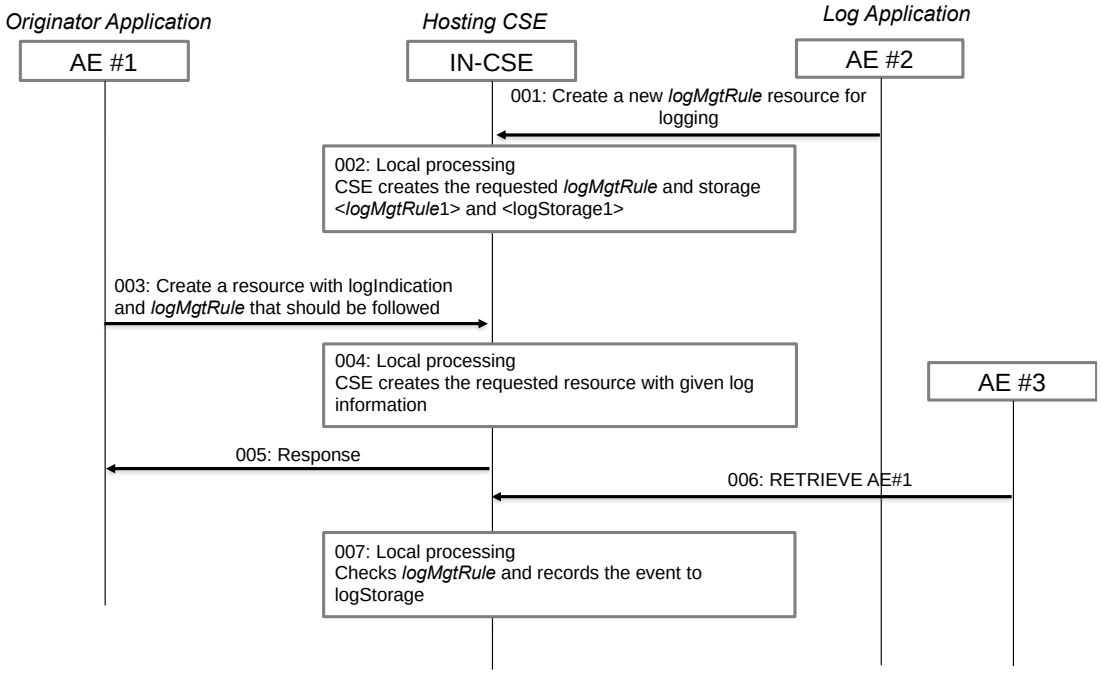


Figure 9.3-2: Procedure showing how log information can be created and started

- Step 1-2:
  A log management resource < *logMgtRule1*> was created at the IN-CSE by a log management application. Note that the < *logMgtRule* > can also be provisioned. When this resource is created, the application also have to create a resource to store actual log records. In this case, the <logStorage1> is created.
  For this specific use case, the < *logMgtRule1*> can be set as following: The logStorage attribute refers the address of < *logMgtRule*1> resource. The logFormat attribute is configured time;originator;operation;taget;status. The logResourceIDs attribute is configured AE#1. The logLevel attribute is configured to all request messages. The logCriteria attribute is configured CRUDN.

- Step 3-5:
  In this example, human body sensor application creates AE1 to IN-CSE with logIndication. The application also refer < *logMgtRule*1> as the logging rule to follow. The IN-CSE then add AE#1 to the logResourceID of < *logMgtRule*1> to start log for AE#1.

- Step 6-7:
  AE2 tries to read AE#1 resource to show the value to its user. When IN-CSE receives such request, it performs the operation. Then IN-CSE checks whether this message has to be recorded into its log resources. If AE#1 is subject to be loged, IN-CSE takes necessary information, which entity tries to read, when this message was received, which binding is used, what was the result of the request and stores the collected information to a proper resource. In this case, <logStorage1>/<AE#1> is the place to record the processed request.

9.4 Solution: Key Issue 1 & 4 – Ownership and Right to be deleted

In the case of GDPR-applied data, different data should be displayed depending on the user. For example, the owner of pseudonymized data can access the original contents regardless of the applied regulation. On the other hand, in the case of general users, they can access data containing personal information, but in the form of pseudonymization. Therefore, in the case of data specified as containing personal information, data ownership, not a simple access control policy, plays an important role.

In addition, in the case of data subject to the Personal Information Protection Act, upon request of the user who owns the data, it must be immediately deleted from the system (i.e., right to be deleted or forgotten). Therefore, if there is a

request to be forgotten from a user who has the ownership of privacy-related data, the IoT platform can process the request with two pieces of information, namely data ownership and whether or not GDPR is applied.

Such information (i.e., ownership and gdpr-applied) can be modelled as attributes of oneM2M resources such as <*contentInstance*> and <*container*>. The definition of the attributes is explained in the table below.

Table 9.1-1: Attributes needed to support privacy data

Attributes	Multiplicity	RW/ RO/ WO	Description
ownershipData	1	RW	Used to indicate the owner of data under a regulation
privacyActIndication	1	RW	Used to indicate that this data is subject to privacy regulation

10 Conclusions

This technical report analyses regulations related to personal data protection and privacy and looked at how these laws affect IoT platforms especially to the oneM2M IoT System. As a result of analysing the GDPR statements related to the IoT platform, this report derives the following five key issues:

- Key issue #1: support of data anonymization
- Key issue #2: support of data pseudonymization
- Key issue #3: Fine grained consent management
- Key issue #4: Right to be deleted and forgotten
- Key issue #5: Logging

The oneM2M system supports features that satisfy several GDPR-reated requirements, such as ACP and anonymization of URI, but consent management and advanced pseudonymization & anonymization are not currently supported. Therefore, the proposed high-level solutions need to be investigated further to be used to facilitate further normative work resulting in oneM2M technical specification. Especially, fine grained data pseudonymization & anonymization and consent management to be compliant with the personal data protection and privacy regulations around the world will be addressed in other oneM2M specifications.

NOTE 1. How to move identified information and mechanisms into normative work is for further study in future releases. There are several possibilities. For example, results of this work can be used to define privacy handling policy, which complements oneM2M access control policy.

NOTE 2. How to control the access of privacy data is for further study in future releases. For example, the holder of privacy data should have an access to the original data without any pseudonimization or anonymization.

NOTE 3. How the proposed information can be provided more efficiently if for further study in future releases. For example, such information can also be modelled as attributes of a resource representing a privacy rule. In this case, resources containing privacy data can refer to an appropriate privacy rule resource.

History

Publication history		
V1.1.1	<yyyy-mm-dd>	<Milestone>

Draft history (to be removed on publication)		
V0.0.1	<2019-10-10>	Skeleton of the TR.
V0.1.0	<2020-02-13>	Agreed contributions from TP #43 are added - SDS-2019-0634R01
V0.2.0	<2020-08-27>	Agreed contributions from TP #46 are added - SDS-2020-0046R01
V0.3.0	<2020-11-19>	Agreed contributions from TP#47 are added - SDS-2020-0134R03 - SDS-2020-0133R02 - SDS-2020-0132R06 - SDS-2020-0111R07
V0.4.0	<2022-12-01>	Agreed contributions from TP#57 are added - RDM-2022-0092R01 - RDM-2022-0093R01 - RDM-2022-0096