|  |
| --- |
|  |

|  |
| --- |
| Input Contribution |
| Meeting ID\* | SDS#46 |
| Title:\* | GDPR feature analysis and impact to oneM2M |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.krMinbyeong Lee, Hyundai Motors, minbyeong.lee@hyundai.com Ahmed ABID, EGM, ahmed.abid@eglobalmark.comFranck Le Gall, EGM, franck.le-gall@eglobalmark.comHyojun Kim, EGM, hyojun.kim@eglobalmark.com  |
| Date:\* | 2020-08-27 |
| Input related to\* | WI-0095 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)TR-0062 V 0.1.0 |
| Intended purpose ofdocument:\* | [x]  Decision[ ]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0062 |
| Template Version: January 2017 (Do not modify) |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# Introduction

This contribution provides input about analysis on GDPR features and oneM2M.

### -----------------------Start of change 1-------------------------------------------

# 7 Analysis on the Current oneM2M System

*Editor’s Note: The section provides an analysis of the current oneM2M system to see which features related to privacy related regulations are supported and not supported.*

## 7.1 Processing and Controlling activities in oneM2M

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

According to [Article 4](https://advisera.com/eugdpracademy/gdpr/definitions/%22%20%5Ct%20%22_blank) 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](https://advisera.com/eugdpracademy/gdpr/responsibility-of-the-controller/%22%20%5Ct%20%22_blank) 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 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.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 7.2 GDPR impact to oneM2M

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

The following tables list the key GDPR features that potentially have an impact to IoT platforms.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| GDPR Category | Feature No. | Key GDPR Features | Relevant Articles | GDPR statements[[1]](#footnote-1) |
| 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; |

## 7.3 Unsupported GDPR features and Key Privacy Issues

*Editor’s Note: This section describes unsupported key privacy issues related to privacy regulations.*

The following table lists up potential requirements that oneM2M may consider to support GDPR relevant features.

|  |  |  |
| --- | --- | --- |
| Feature(GF) No. | oneM2M support | GDPR relevant potential requirements |
| GF1 | Too broad | IoT system shall support management for further processing besides the purpose to minimize the processing of personal information. |
| GF2 | Too broad | IoT system shall support a mechanism providing the pruposes of data processing.  |
| GF3 | Out of scope | IoT system shall support 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 | IoT system shall support the deletion of data that have passed the retention period.🡪 oneM2M system support expiration timer.  |
| GF5 | Not supported | IoT system shall support a mechanism to demonstrate that the data subject has consented to processing of personal data. |
| GF6 | Not supported | IoT system shall support managing consents from user to process privacy data. |
| GF7 | Not supported | IoT system shall support mechanism that allows data subjects to easily revoke consent and stop processing. |
| GF8 | Out of scope | IoTsystem shall support verification the age of the data subject and obtain parental consent if under 16 years of age. |
| GF9 | Out of scope | IoT system shall support identification of sensitive information(racial, political, sexual, etc.) and restriction of processing. |
| GF10 | Supported | IoT system shall support provision of information about processing of personal information to data subjects. 🡪 Subscription/Notification can support this.  |
| GF11 | Supported | 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 | IoT system shall support identification of users and access history 🡪 partially supported via “Service Statistics Collection Recording” |
| GF13 | Supported | IoT system shall support access right to personal information. |
| GF14 | Supported | IoT system shall support modification of data based on the data subject’s rectification request. |
| GF15 | Partially supported | IoT system shall support the deletion of personal data based on the data subject’s delete request. |
| GF16 | Partially supported | IoT system shall support data subject identification and information deletion to the data subject’s restriction request. |
| GF17 | Out of scope | IoT system shall support provision of personal information in a machine-readable form (ex. CSV file..) when there is a movements of personal information by the data sujects request(either to the data subject or to anonther contoller). |
| GF18 | Out of scope | IoT system shall support processing interruption based on the objection from the subject of data. |
| GF19 | Out of scope | IoT system shall support regular self-test and assessments of the effectiveness of security technologies. |
| GF20 | Partially supported | IoT system shall support data anonymisation. |
| GF21 | Partially supported | IoT system shall support data pseudonymisation. |
| GF22 | Not supported | IoT system shall support means or information (e.g., log information) to be used by intrusion prevention and detection system. |
| GF23 | Out of scope | 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 to anonymise personal data? Which data need to be anonymised. What kinds of anonymization mechanism is used?
2. Key Issue #2 – GF21 (Support of data pseudonymization): How to pseudonimise personal data? Which data need to be pseudonymised. What kinds of psedunymisation mechanism is used?
3. Key Issue #3 – GF5, GF6, GF7 (Fine grained consent management): How to provide consent? What kinds of information should be kept and managed in consent?
4. Key Issue #4 – GF4, GF15, GF16 (Right to be deleted and forgotten): How to support various deletion and forgotten needs? For example, the deletion of all the personal data owned by a specific user.
5. Key Issue #5 – GF12, GF22 (Logging): How to support logging information? What kinds of logging information is needed to support GDPR?

### -----------------------End of change 1-------------------------------------------

1. <https://gdpr-info.eu/> [↑](#footnote-ref-1)