|  |
| --- |
|  |

|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SDS#46 |
| Title:\* | Pseuddonymization and anonymization of privacy data |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.kr  Minbyeong Lee, Hyundai Motors, [minbyeong.lee@hyundai.com](mailto:minbyeong.lee@hyundai.com) |
| Date:\* | 2020-07-07 |
| Input related to\* | WI-0095 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)  TR-0062 V 0.1.0 |
| Intended purpose of  document:\* | 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 key issue on pseudonymization and anonymization of privacy data for GDPR.

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

# 8 Proposed Solutions

*Editor’s Note: The section provides solutions to the required functions identified in the previous section.*

## 8.x Solution: Key Issue x – Pseudonymization and Anonymization of Privacy Data

Editor’s note: It is FFS how to move identified information and mechanisms into normative work. There are several possibilities. For example, results of this work can be used to define privacy handling policy, which complements oneM2M access control policy.

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** meansthe 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 | oneM2M annotated procedure |

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. 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 x: 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) |
| *privadyIndication* | 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) |

Editor’s note: It is FFS how to control the access of privacy data. For example, the owner of privacy data should have an access to the original data without any pseudonimization or anonymization.

Editor’s note: It is FFS how the proposed information can be provided more efficiently. 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.

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



Figure x2. 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.

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