|  |
| --- |
|  |

|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | RDM#57 |
| Title:\* | Ownership of privacy data |
| Source:\* | JaeSeung Song, Sejong University, [jssong@sejong.ac.kr](mailto:jssong@sejong.ac.kr)  Franck Le Gall, EGM, [Franck.le-gall@egm.io](mailto:Franck.le-gall@egm.io) |
| Date:\* | 2022-11-29 |
| Input related to\* | TR-0062 V 0.3.0 |
| 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 proposes to include a new section addressing key issues 1 and 4.

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

## 9.x 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 |

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