|  |
| --- |
| Input Contribution |
| Meeting ID\* | RDM #41 |
| Title:\* | Use case on data protection related regulations |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.kr Youngjin Na, Hyudai Motor, jkim@hyundai.com Min-Byeong Lee, Hyundai Motor, minbyeong.lee@hyundai.com  |
| Date:\* | 2019-07-08 |
| Input related to\* | TR-0026 (Rel-4) |
| Intended purpose ofdocument:\* | [x]  Decision[ ]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0026. |
| 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 new use case on data protection related regulations to Clause 6 “Vehicular Domain Use Cases” in TR-0026.

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

## 6.x Handling Data Protection-related Regulations

### 6.x.1 Description

Data protection (in particular personal data) is one of important issues to be managed by data handling systems including IoT service layer platforms. In order to protect privacy related data, many countries prepare and mandate personal data protection related regulations such as EU’s General Data Protection Regulation (GDPR) and Korea’s Personal Information Protection Act (PIPA).

* GDPR: The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using ***pseudonymization*** or full ***anonymization*** where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately.
* PIPA: The Personal Information Protection Act (PIPA) is a framework act on data protection both in the public sector and private sector in Korea. The act is applied to various areas as follows:
	+ the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc
	+ the Act on the Use and Protection of Credit Information
	+ the Act on the Protection, Use, etc. of Location Information
	+ the Act on the Development of Cloud Computing and the Protection of its Users
	+ and so on..

After GDPR is mandated, any web-based services handling privacy data (such as subscription based web-service, online banking) have applied techniques (getting users’ agreement and pseudonymization of privacy data) to their website to follow the GDPR.

Currently, oneM2M system supports pseudonymization technique on the address of oneM2M resources but not on data and name of resource. Therefore, oneM2M system needs to consider handling different countries’ data protection related regulations as a common function.

### 6.x.2 Source

RDM-2019-0066-Use\_case\_for\_privacy\_data\_protection\_related\_regulations

### 6.x.3 Actors

* Vehicle: An application sending various data generated from a vehicle and driver.
* Cloud Node: A node that handles and manages data from vehicles.

### 6.x.4 Pre-conditions

* A vehicle is equipped with various intenal sensors to collect data from vehicle and passengers (including the driver).
* Data stored in the Cloud IoT platform should be consumed by a designated application.
* The cloud IoT platform needs to be compliant to data protection related regulation such as GDPR.
* Personal data that falls under the data protection related regulation is indicated either via data administrator, or the owner of data or an automated algorithm detecting personal data.

### 6.x.5 Triggers

A vehicle measures various data from its internally equiped sensors, a driver and passengers. As data from the vehicle contains personal data from the driver or passengers, the IoT service cloud platform process these personal data based on a mandated regulation once it receives such data.

### 6.x.6 Normal Flow

Figure 6.x.6.1 illusrates the high-level flows of a use case showing how IoT service platforms process personal data based on a data protection related regulation (e.g., GDPR), which consists of the following steps:

* **Step 001**: IoT sensor (i.e., Application #1) in a car measuring personal data (e.g., driving patterns or health condition) sends measured personal data to the IoT platform, which should handle personal data in compliance to a proper data protection related regulation. The message fron the application includes which regulation need to be applied and a protection mechanism such as pseudonymization.
* **Step 002:** IoT service layer platform creates the requested resource with the information how to process personal data. The created resource is configured with the indication about data protection regulation and mechanism. For example, a regulation is ‘gdpr’ and a mechanism is pseudonymization.
* **Step 003:** IoT service layer platform returns response message to Application #1
* **Step 004:** Application #1 sends a request to create a resource which is a placeholder for new data measurement.
* **Step 005:** As the requested resource contains personal data that falls under GDPR IoT service layer platform process data with the specified mechanism (in this case pseudonymization). The created resource then contains pseudonymized data instead of raw input data.
* **Step 006:** IoT service layer returns response message to Application #1.
* **Step 007:** Application #2 tries to retrieve the created resource.
* **Step 008:** The pseudonymized data in the requested resource is returned to Application #2.



**Figure 6.x.x.6.1: Normal flow for managing privacy data that need to be handled based on a data protection regulation**

### 6.x.7 Alternative Flow

None

### 6.x.8 Post-conditions

None

### 6.x.9 High Level Illustration



Figure 6.x.9.1: High level illustration of privacy data protection management based on mandated regulation

### 6.x.10 Potential requirements

1. IoT systems consider regulations on handling privacy related data and applying proper data protection techniques (such as anonymization and pseudonymization) to personal identifiable information.

### -----------------------End of Change 1 ---------------------------------------------

Copy and paste the potential requirements to Section 7

# 7 Overview of Potential Requirements

Potential requirements from all vehicular domain use cases collected in this technical report are summarized as follows,

1. IoT systems consider regulations on handling privacy related data and applying proper data protection techniques (such as anonymization and pseudonymization) to personal identifiable information.

NOTE 1: This requirement addresses the use case 6.1.x