GDPR 개인정보 데이터 처리를 지원하는 oneM2M 표준

김효준 EGM 연구원
이민병 현대자동차 연구원
송재승 oneM2M SPG-13 의장, 세종대학교 정보보호학과 교수 (교신저자)

1. 머리말

유럽연합(EU, European Union)의 개인정보보호법인 일반데이터보호규정(General Data Protection Regulation, 이하 GDPR)이 2018년 5월 25일부로 시행되었다. EU 내 시민의 개인정보를 관리하는 광범위한 이 규정은, 유럽 내 법안이긴 하지만 EU 시민의 개인정보를 취급하는 모든 기업에 적용되므로 전 세계의 주목을 받고 있다. 특히 GDPR을 어기면 2천만 유로의 높은 과징금이 부과되기 때문에 전 세계 기업들이 발 빠르게 이에 대응하고 있다.

최근 사물인터넷(IoT)에 관한 연구가 세계 각국의 정부, 기업 등을 주축으로 활발히 진행되고 있다. IoT는 홈, 헬스케어, 스마트 팩토리, 자율 주행 등 산업 전반에 적용되며 그로 인해 생성된 데이터의 양이 기하급수적으로 늘어나고 있다. 2020년 IoT 디바이스에 연결된 센서의 수는 260억 개가 넘어서는데, IoT 디바이스에서 생성된 정보는 IoT 플랫폼을 장착한 게이트웨이 및 서버로 전송돼 처리, 저장, 분석된다.

센서로 수집된 정보는 개인정보나 민감한 정보를 포함할 수 있고, 직접적으로 개인정보를 포함하지 않더라도 이러한 단순 정보들이 모여 개인을 식별할 가능성이 있는 경우 위에서 언급한 GDPR과 우리나라의 개인정보보호법에 적용을 받는다. 따라서, IoT 디바이스에서 측정되는 각종 데이터를 수집하고 관리하는 IoT 서비스 공통 플랫폼은 법령을 준수하기 위해 개인정보 처리 메커니즘을 기본적으로 갖추어 제공해야 한다.

이에 따라, IoT 서비스 계층 플랫폼에 대한 사실상 국제 표준 단체인 oneM2M에서는 개인정보보호법을 준용하고[1], 개인정보를 다루는 서비스에 GDPR 등과 같은 법령에서 요구하고 있는 기능들을 공통기능의 일환으로 적용하는 데 필요한 신규 표준 개발 작업을 시작하였다[2](TR-0062). 해당 워크 아이템에서는 여러 국가에서 시행 중인 개인정보보호를 위한 법령 및 관련 기술을 살펴보고, IoT 서비스에서 GDPR을 준용하는 데 필요한 요구사항들을 도출하며, 이를 플랫폼에서 지원하는 데 필요한 핵심 이슈와 공통기능에 대한 표준 개발을 Release 5에서 진행할 계획이다. 특히, 해당 신규 워크 아이템은 한국 TTA의 멤버사인 현대자동차, 전자부품연구원, 한성대학교 등에서 주도적으로 발의했으며, IoT 글로벌 리더인 AT&T, Orange, British Telecom 등의 적극적인 지원을 받아서 2019년 12월 미국 워싱턴에서 개

최된 oneM2M Technical Plenary44회의에서 승인됐다.

본고의 구성은 다음과 같다. 2장에서는 개인정보의 중요성과 현재 유럽에서 시행 중인 유럽연합 GDPR과 한국의 개인정보보호법(PIPA)에 대해 서술한다. 3장에서는 GDPR 준용을 위한 oneM2M 플랫폼 요구사항과 eDPR (enhancement Data Protection Regulation)을 다룬다. 마지막으로 4장에서는 향후 표준화 방향과 결론을 맺는다.

2. 개인정보보호법 및 법령

우리나라의 개인정보보호법에서는 개인정보를 '살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보'로 정의한다. 오늘날 개인정보는 이름과 주민등록번호에 국한되지 않고 몸무게, 키, 경제 수준, 신용, 종교, 사상과 같은 개인 신상은 물론, 정보 사회의 도래로 새로운 유형으로 떠오른 생체정보, 유전정보, 위치 정보, 네트워크 정보(IP 주소)까지도 포괄한다. 이러한 정보 중 어느 하나만으로는 개인을 식별하기 어렵지만 두 가지 이상의 정보가 조합되는 경우 개인 식별 가능성이 높아지므로 모든 정보는 안전하게 보호돼야 한다.

특히 인터넷에 연결된 수많은 기기(웨어러블 디바이스처럼 생체정보, 또는 개인정보와 연관된 디바이스 포함)로 부터 수집되는 데이터들을 저장하고 처리하는 사물인터넷 플랫폼의 경우, 개인정보를 안전하게 보장하고 국가별 개인정보보호법을 준수하도록 하는 기능을 반드시 구현해야 하기에 관련 논의가 활발하게 이루어지고 있다. 본고에서는 유럽에서 시행되고 있는 GDPR과 한국의 개인정보보호법 두 가지를 심층적으로 분석하고 법령의 의의와 기대효과를 살펴본다.

2.1 GDPR

GDPR은 개인정보 처리에 대한 개인 보호 및 개인정보의 자유로운 이동에 관한 규정이다[3]. GDPR은 말 그대로 규칙(Regulation)이기 때문에 EU 회원국에 직접 적용되고 법적 구속력을 얻는다. 또한 GDPR은 유럽연합에 거주하는 시민을 보호하기 위해 유럽연합 역내에서 사업을 하는 모든 조직 및 기관뿐 아니라 유럽연합 시민의 정보를 수집, 처리, 저장하는 유럽연합 역외의 조직에도 적용된다. GDPR은 정보주체의 권리와 개인정보 처리자의 의무가 강조되었으며 이를 통해 기업의 책임을 강화하고, 위반 시 기업의 존폐를 결정할 만큼의 과징금이 부과된다. 이러한 이유로 인해 유럽에서 사업을 하고 있거나 계획 중인 전 세계 기업들이 GDPR에 주목하고 이에 대응하는 기능을 구현하는 데 힘쏟고 있다.

2.2 대한민국의 개인정보보호법(PIPA)

대한민국의 개인정보보호법(PIPA)은 2011년 9월 30일에 제정되었으며, GDPR과 마찬가지로 데이터 주체의 관점에서 개인정보보호 권한을 보호하며 대부분 조직, 정부 기관에 적용된다[4]. 이 법은 법적 구속력을 가진 엄격한 형사 규제로 벌금 및 징역을 포함한 처벌이 시행 중이다. 개인정보 보호법에서 개인정보는 이름, 주민등록번호, 또는 기타 유사한 정보와 같은 특정 개인을 식별하는 정보를 포함하는 살아있는 개인과 관련된 정보를 말한다.

GDPR과 PIPA의 경우 개인정보를 보호하기 위한 원론적인 부분은 대부분 동일하나, 실제 개인정보에 대한 처리 및 조치를 구체적으로 구현하는 부분과 개인정보를 가명화하는 부분이 상이하여 서로 호환이 완벽히 되지 않았다. 이를 보완하기 위해 국내에서는 데이터 3법을 2019년 11월에 발의하기도 하였다.

3. GDPR 준용 oneM2M 플랫폼

oneM2M은 사물인터넷 기기를 연결하고 관리하는 서비스 계층 플랫폼 표준을 개발하고 있다. 수많은 사물인터넷 기기에서 생성되는 데이터들이 oneM2M 표준을 참조하여 개발된 사물인터넷 플랫폼에 저장되고 처리된다. oneM2M 기반의 사물인터넷 플랫폼에 개인정보 관련 데이터가 저장될 경우, 반드시 GDPR 및 PIPA와 같은 개인정보를 보호하기 위한 국가 법령을 준수해야 한다. 특히, oneM2M 기반 사물인터넷 플랫폼의 경우 스마트시티의 주요 플랫폼으로 많은 국가에서 사용하므로 GDPR과 같은 법령을 준수하는 데 필요한 기능을 반드시 제공해야 한다.

이러한 문제에 대처하기 위해 oneM2M에서는 현대자동차 및 전자부품연구원을 중심으로 각 국가에서 제정된 개인정보보호법을 분석하고, 이를 충족하는 데 필요한 기술을 oneM2M에 적용하기 위한 신규 워크 아이템(WI-0095, oneM2M System Enhancements to Support Data Protection Regulation-eDPR)이 제안, 승인되고 이를 기반으로 한 기술 보고서(TR-0062) 개발이 시작됐다. 해당 워크 아이템은 개인정보보호법이라는 중요한 이슈를 다루므로, 해당 아이템을 주도하는 우리나라 기업을 비롯하여 AT&T, BOE, Convida, Cisco, Gemalto, Huawei, Hitachi, Hyundai Motors, KETI, NEC Europe, Nokia, NTT, TIM 및 Qualcomm 등 전 세계 여러 선도 기업으로부터 지지를 받았다.

oneM2M TR-0062는 최신 개인정보보호 관련 규정(GDPR 및 PIPA)이 oneM2M 시스템에 미치는 영향 분석, 정보 보호와 관련해서 oneM2M이 지원하는 기능 및 미지원 기능에 대한 갭 분석, 개인정보보호 관련 규정을 처리하는 기능의 잠재적 유스케이스 및 요구사항 도출, oneM2M 시스템의 개인정보보호 관련 규정을 준수하는 솔루션 개발 등의 내용 등을 포함할 예정이다.

3.1 GDPR 관련 요구사항 및 구조

GDPR은 전문 총 173개 항, 본문 총 11장 99개 조항으로 이루어져 있다. 99개의 조항 중 oneM2M 플랫폼의 구조와 특징을 고려했을 때 시스템에 영향을 줄 수 있는 조항의 경우, 분석을 통해 oneM2M 표준에 필요한 요구사항이 도출되어야 한다. 예를 들어, GDPR에서는 다음과 같은 조항을 포함한다.

- **개인동의(Consent)**: GDPR의 40번째 조항에 따르면, 개인정보는 데이터를 소유하는 주체의 동의에 따라서 처리가 이루어져야 한다고 정의하고 있다.
- **잊혀질 권리(Right to be forgoten)**: GDPR의 17 및 19번 조항에 따르면 정보 주체는 프로세서에게 개인정보에 대한 삭제를 요청할 수 있고, 해당 데이터는 지체없이 삭제되어야 한다고 규정하고 있다.
- **비식별조치(Pseudonymization & Anonymization)**: 제4조 5항에서 가명처리, 즉 추가적인 정보의 사용 없이 개인을 특정할 수 없도록 개인정보를 처리하도록 정의하고 있다.

이러한 조항들은 시스템적으로 지원돼야 하므로 현재 oneM2M 표준에서 처리 가능한지 분석이 필요하다. 참고로, oneM2M에서는 접근 권한(ACP, Access Control Policy)을 사용하여 데이터에 대한 접근을 제어하는 기능과 데이터를 저장하는 리소스 주소에 대한 가명처리 기능을 제공하고 있을 뿐, 비식별 조치, 잊혀질 권리, 개인 동의 처리 등에 관한 내용은 이전 요구사항에 포함되어 있지 않다.

즉, 비식별 조치를 위해서는 사용자 또는 사물인터넷 기기로부터 수신되는 데이터가 개인정보 관련 데이터인지 식별해야 하며, 개인정보의 경우 시스템에서 데이터의 소유자로부터 처리에 대한 동의가 명시적으로 이루어질 수 있게 하는 것이 플랫폼의 한 기능으로 제공돼야만 한다. 이를 위해 oneM2M 표준에서는 기존 리소스에 대한 추가 속성에 대한 정의, 또는 GDPR과 같은 개인정보법령을 다루기 위한 신규 리소스 추가 논의가 앞으로 이루어질 계획이다.

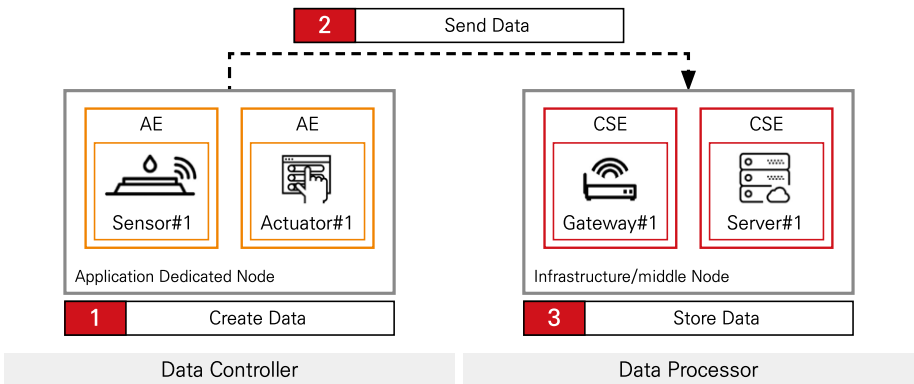
• oneM2M 시스템 내 컨트롤러와 프로세서의 배정과 역할 수행

GDPR은 개인정보를 처리함에 있어 컨트롤러와 프로세서를 정의하고 기술적·관리적 조치를 수행할 것을 요구한다. oneM2M 플랫폼 내에서 컨트롤러와 프로세서의 역할은 각각 Application Entity (AE)와 Common Service Entity (CSE)에 할당될 수 있다.

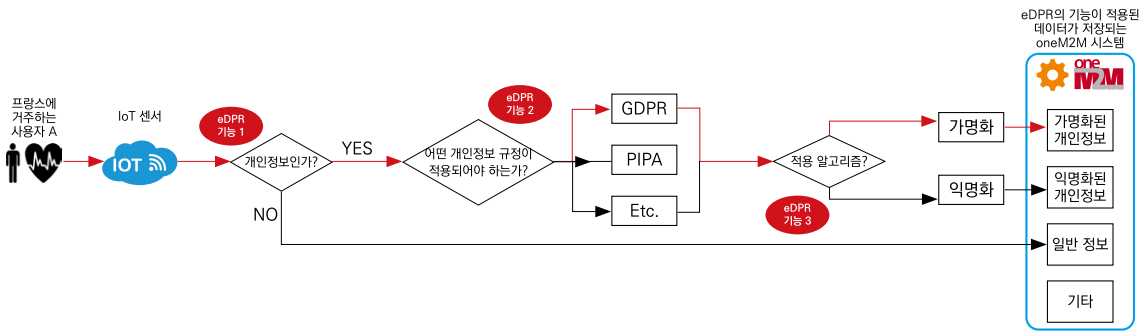
데이터 컨트롤러의 경우 개인 데이터 처리 방식 및 목적 등을 규정하는 주체로 정의되므로, oneM2M에서 플랫폼에 각종 데이터 처리를 요청하는 주체인 AE에 해당한다. 한편 GDPR에서 개인 데이터 기록을 유지관리하고 처리하는 데이터 프로세서의 경우, 사물인터넷 데이터를 실질적으로 저장하고 처리 및 관리를 담당하는 CSE에 해당된다. [그림 1]은 oneM2M 아키텍처 내부에서 데이터를 처리하고 제어하는 과정 중 AE와 CSE가 담당하는 GDPR 관련 역할을 보여준다.

3.2 eDPR 관련 유스케이스 및 주요 기능

[그림 2]는 oneM2M 기반의 플랫폼에서 개인정보를 처리하기 위해 eDPR 주요 기능이 적용되는 과정을 순서도로 보여주고 있다. 예를 들어, 프랑스에 거주하는 사용자 A가 체온 센서를 구매하고 측정된 온도를 개인정보와 함께 oneM2M 플랫폼에 저장했다고 가정해보자. oneM2M 플랫폼에 저장될 데이터는 A의 이름, ID, 체온 등의 개인정보가 포함되고 A가 프랑스 시민이므로 GDPR이 적용되어야 한다. IoT 시스템을 통해 개인정보로 식별된 데이터는 민감데이터로 표시하고 GDPR 또는 PIPA 규정에 맞게 가명화하거나 익명화하여 저장해야 한다. eDPR 기능은 이러한 처리 과정 전반에 걸쳐 개인정보 식별과 개인정보 규정 및 데이터 처리 기술에 대한 정보를 제공해



[그림 1] oneM2M 에서의 데이터 컨트롤러 및 프로세서



[그림 2] oneM2M에서의 개인정보 처리 절차의 예시

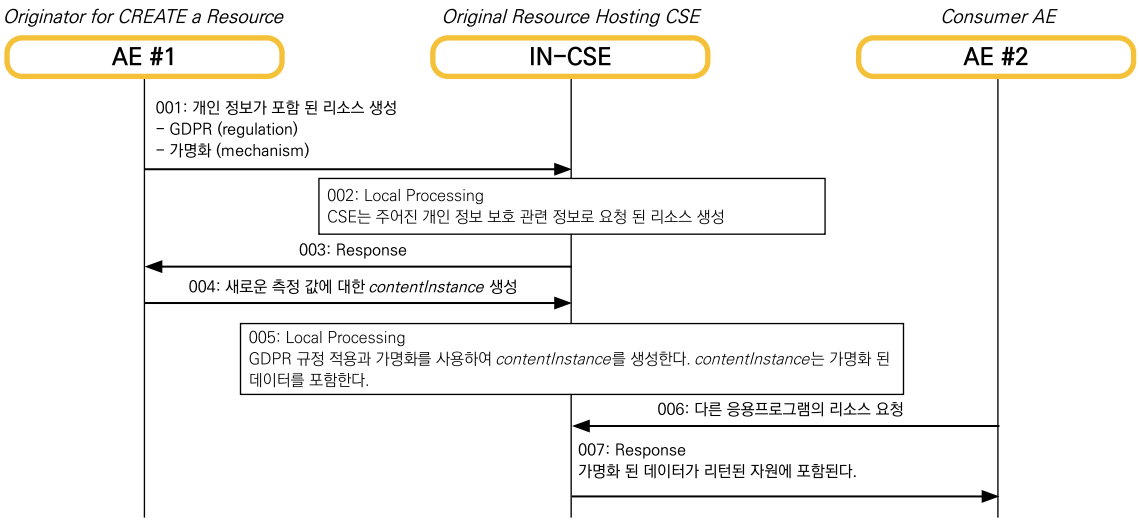
〈표 1〉 oneM2M에서 GDPR 처리를 위해 추가 가능한 속성 예제

Attribute Name	Description
privacyRegulation	데이터에 적용될 규정을 나타내는 데 사용된다. EU의 경우 GDPR 한국의 경우 PIPA가 적용될 수 있다.
privacyIndication	해당 데이터가 개인정보보호 규정의 적용을 받음을 나타내는 데 사용된다.
privacyProcessingRule	가명화 또는 익명화와 같이 사용될 기술을 언급하는 데 사용된다.
privacyTechniques	본 속성은 replacement, scrambling, masking, personalized anonymization, blurring과 같은 가명화 및 익명화와 관련된 세부 기술 정보를 언급하는 데 사용된다.
privacyBlock	데이터 일부에 개인정보 관련 데이터가 포함된 경우 이 속성을 사용하여 처리할 데이터의 정확한 부분을 식별할 수 있다. 예를 들어 Hyojun_info_3948272에는 익명화 해야 하는 데이터인 'Hyojun_info'가 포함되어 있다. 이 경우 Hyojun_info에 해당하는 11자리를 익명화해야 한다.
privacySubject	개인정보보호 규정의 적용을 받는 리소스 부분을 나타내는 데 사용된다.

야 한다. 이를 위해 IoT 시스템은 개인정보에 대한 식별 정보를 비롯하여 여러 추가 정보(법령 종류, 가명화 방법 등)와 이를 처리하고 저장하기 위한 리소스 관리가 필요하다.

〈표 1〉은 oneM2M에서 GDPR를 처리하기 위해 필요한 attributes와 내용을 보여준다. 해당 속성들은 현재 oneM2M 기술 보고서에 포함된 내용은 아니지만, GDPR 적용을 위해 기본적으로 필요한 정보를 리소스의 속성으로 만들 경우 추가 가능한 속성들을 보여준다.

[그림 3]은 oneM2M에 GDPR 관련 속성들이 추가되었을 경우 사물인터넷 센서에서 측정된 개인정보 관련 데이터가 어떤 절차를 거쳐서 oneM2M 플랫폼에서 처리·저장되는지와, 저장된 데이터에 대해 다른 응용 프로그램의 요청이 오면 어떻게 처리되는지 보여준다. 최초 AE가 개인정보를 포함하는 데이터를 저장하기 위해 관련 리소스를 CSE에 생성하며 필요한 정보를 리소스의 속성에 추가한다(스텝 001~003). 이후 생성되는 개인정보는 contentInstance에 저장되는데, 이때 저장되는 리소스의 개인정보 유무를 확인하고 익명화나 가명화 처리가 필요할 경우 속성에 명시된 방법에 따라서 데이터를 처리한다(스텝 004~005). 제3의 애플리케이션(AE#2)에서 개인정보에 대한 검색 요청이 올 경우, CSE는



[그림 3] 가명화 및 익명화 처리 절차

가명화 또는 익명화 처리된 데이터를 AE#2에 전달한다(스텝 006~007). 즉, 개인정보를 관리하는 리소스에 액세스할 수 있는 다른 IoT 응용 프로그램은 가명화하거나 익명화된 데이터만 볼 수 있다.

4. 결론 및 향후 표준 방향

4차산업혁명 시대를 맞아 다양한 산업들이 데이터 중심으로 이동함에 따라 사물인터넷 플랫폼에서 데이터의 중요성이 강조되고 있다. 특히, 유럽 및 한국을 중심으로 개인정보보호에 대한 인식이 강화되고 관련 법령이 발의됨에 따라 사물인터넷 표준에서도 이러한 법령을 준수하기 위한 노력이 시작되었다.

사물인터넷 플랫폼 관련 표준을 개발하는 국제 표준 단체인 oneM2M에서는 한국 업체들의 주도하에 선제적으로 개인정보보호 법령을 시스템적으로 지원할 수 있는 기능 관련 표준을 개발하기 위해 워크 아이템을 Release 5의 일환으로 제안하고 승인시킴으로써 개인정보보호 처리를 위한 기능 표준화를 국제적으로 선도하고 있다. 현재 개발 중인 기술 보고서에는 GDPR 지원을 위한 요구사항, 리소스 변경 및 속성 추가, 개인정보 처리를 위한 신규 절차 등에 대한 표준이 담길 계획이며, 이후 관련 내용들은 논의를 거쳐 정식 표준으로 진행된다.

개인정보법령을 지원하는 표준이 완성될 경우 oneM2M 표준은 데이터 처리의 보안성을 인정받아 스마트시티를 비롯하여 커넥티드카, 의료 등 좀 더 다양한 분야로 확산될 수 있을 것으로 기대된다. TTA

※ 본 연구는 현대자동차와 세종대학교의 산학연구 및 2019년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.(No. 2019-0-00426, IoT 기반 이식-침습형 고위험 의료장치를 위한 능동형 킬 스위치 및 바이오 마커활용 방어 시스템 개발)

참고문헌

[1] Swetina, J., Lu, G., Jacobs, P., Ennesser, F., & Song, J. (2014). Toward a standardized common M2M service layer platform: Introduction to oneM2M. IEEE Wireless Communications, 21(3), 20-26.

[2] oneM2M Technical Report, TR-0062, https://member.onem2m.org/static_Pages/others/WPM-pages/TR-TS_List.htm

[3] GDPR https://gdpr-info.eu/

[4] PIPA https://www.privacy.go.kr/