논문 19-44-12-25 The Journal of Korean Institute of Communications and Information Sciences '19-12 Vol.44 No.12
https://doi.org/10.7840/kics.2019.44.12.2352

개인정보 수집 및 활용을 위한 적극적 사용자 동의에 관한 연구 - EU GDPR이 규정하는 동의의 유형 및 조건을 바탕으로

박 효 주◆, 정 재 은*, 양 진 홍°

A Study on Active User Consent to Obtaining and Processing Personal Data - Based on the Types and Conditions of Consent in EU GDPR

Hyoju Park◆, Jae-eun Jung*, Jinhong Yang°

요 약

본 논문은 개인정보 수집 및 활용에 있어 정보주체인 사용자의 권리를 보호하면서 동시에 이를 정당하게 활용하기 위한 동의 획득 방안을 구체화 하는 것을 목적으로 하고 있다. 이를 위해 현재 개인정보 수집 및 활용과 관련해 세계적으로 가장 큰 영향력을 미치고 있는 EU GDPR 규정을 바탕으로 1) EU GDPR 원문 전체에 흩어져 있는 '사용자 동의 획득'과 관련한 내용을 분석, 재분류하고 2) 해당 내용의 구체화 및 활용을 위해 동의획득 과정에서 필수적으로 고려해야 할 사항에 대한 체크리스트를 구성하였으며 3) 체크리스트의 유용성을 확인하기 위해 현재 글로벌 시장을 대상으로 하고 GDPR 대응이 용이한 대기업으로 대표성을 갖는 국내 대기업(LG)의 동의 획득 수준을 체크리스트를 통해 분석하였다. 분석 결과, GDPR에서 요구하는 적극적 사용자 동의를 위한 조건은 4개 유형으로 분류할 수 있으며, 분류 항목에 따라 필수 고려 사항을 체크리스트로 구성한 결과 18개 항목이 도출되었다. 도출된 체크리스트로 국내 LG 스마트TV 약관을 분석한 결과, 미흡 및 불충족 항목이 절반 이상으로 나타나 국내 기업의 개인정보 수집 수준 파악 및 체크리스트의 유용성을 확인할 수 있었다. 마지막으로 적극적 사용자 동의 획득을 위한 두 가지 정책적 개선 사항이 제안 되었다.

Key Words : GDPR, User Consent, Personal Data, Privacy Policy, UI/UX

ABSTRACT

The purpose of this paper is to specify a method for obtaining consent to protect user's rights and to use them in order to collect and use personal data. To this end, based on the GDPR, 1) analysis and reclassification of contents related to 'acquiring user consent' scattered throughout the GDPR. 2) In order to materialize and utilize 'user consent' in GDPR, a checklist has been prepared that must be considered in the process of obtaining consent. 3) To check the usefulness of the checklist, we analyzed the level of acquiring consent from

※ 이 논문은 2019 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00261, IoT 환경에서 일반개인정보보호규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)
◆ First Author : Inje University Department of Computer Engineering, hjpark@inje.ac.kr, 정회원
° Corresponding Author : Inje University Department of Healthcare IT, jinhong@inje.ac.kr, 정회원
* Inje University Department of Healthcare IT, 20173287@oasis.inje.ac.kr
논문번호 : 201909-182-0-SE, Received September 2, 2019; Revised October 15, 2019; Accepted October 15, 2019

the representative domestic large enterprises(LG). The analysis shows that there are four types of conditions for active user consent. According to the classification, a checklist of essential considerations resulted in 18 items. As a result of analyzing the domestic LG Smart TV terms and conditions, more than half of the items were not satisfied. The usefulness of the checklist was confirmed as a starting point for identifying the level of personal data collection. Finally, two policy improvements were proposed.

Ⅰ. 서 론

데이터 경제(Data Economy)를 이끄는 핵심 원료는 데이터다. 그리고 이 데이터를 생산해내는 주체는 바로 IT서비스를 이용하는 사용자, 개개인이다. 이들이 눈부시게 발전하는 IT서비스의 수혜를 받고 편리함을 누리는 것은 이를 제공하는 각종 서비스들을 사용하겠다는 선택과, 지속적으로 서비스를 받기 위한 원료가 되는 정보를 자발적으로 모두 제공하겠다는 약속을 했기 때문이다. 만약 사용자가 더 이상 각종 서비스 및 편리함을 제공 받는 것을 원치 않는다고 하면 해당 서비스는 서비스의 원료가 되는 사용자의 모든 정보, 즉 기본 신원정보를 비롯한 행위 정보를 더 이상 수집 및 이용할 수 없으며 이것은 서비스 존재 자체와 직결되는 문제이다. 따라서 특정 서비스를 사용함으로써 자신의 정보를 서비스 제공자에게 제공하겠다는 개인의 의지, 즉 사용자의 서비스 이용 동의는 서비스 제공자 입장에서 매우 중요한 부분이며 이를 최대한 많이, 합법적으로 획득하는 것이 데이터 산업의 가장 기본이 되는 첫 단추이다.

따라서 4차 산업혁명 시대를 이끌 새로운 기술, 빅데이터, AI, IoT, Cloud 등 미래 사회를 이끌 혁신적인 서비스 발전과 눈부신 미래를 이야기할 때 가장 먼저 논의되어야 할 것이 정보주체의 동의, 권리가 되어야 하는 것은 당연하다. 사용자, 정보주체로부터 데이터를 획득하고 활용하되 불이익을 입히지 않겠다는 약속, 이것에 대한 사회적 합의뿐 아니라 제도적 보장이 기본이 되어야 하는 것이다. 그러나 우리나라뿐 아니라 전 세계적으로도 '빅데이터'는 이미 주어진 것으로 보고, 이를 분석 및 활용하는 방안에 더욱 주목하여 가장 기본적인 부분에 대한 논의가 부족한 것이 사실이다.

유럽연합(EU)에서 시행한 개인정보보호 규제법 GDPR(General Data Protection Regulation)은 데이터 활용을 위한 전제조건으로서의 데이터 보호에 방점을 두고 있는 규율로서 그동안 간과되어온 정보주체의 권리에 관한 문제의식에 궤를 함께하고 있다[1] 2016년 5월 제정, 2년간의 유예기간을 거쳐 2018년 5월 본격적으로 시행된 이 법안은 EU 시민의 개인정보를 활용하여 서비스를 제공하는 기업을 대상으로 하고 있다. 그러나 이 법이 공포된 이래 전 세계적으로 기업의 무분별한 데이터 수집 및 활용을 경계하고 정보주체인 사용자의 권리에 집중하기 위한 논의가 확산되고 있다. 실제 GDPR이 시행된지 1년이 지난 현 시점에 정보수집에 대한 GDPR 규율을 위반하여 구글이 653억 과징금을 부과 받는 등 수억에서 많게는 수백억까지 벌금이 부과된 사례가 등장했다[2]. 이처럼 높은 수준의 규제조치는 향후 더욱더 정보주체의 권리와 이를 근거로 한 동의 획득, 정보수집 및 활용 방식에 있어서 적극적인 논의 및 기업의 대응을 이끌어 낼 것으로 보인다.

우리나라도 예외는 아니다. 기업 수준에서도 국내 기업 중 EU 시민을 대상으로 서비스하는 기업들은 정보주체로부터 동의를 획득하기 위한 절차상 GDPR 준수가 필수이므로 해당 내용에 대한 검토가 필수적이다. 또한, 국가적 차원에서도 향후 유럽과의 활발한 데이터 흐름 및 시장 발굴을 위한 적정성평가를 진행하고 있는 바[3], 국내 개인정보보호법의 개정 노력과 유관 학계의 논의가 진행되고 있다. 그러나 GDPR규정에서 정보주체의 동의와 관련된 부분은 축약된 형태의 원문 규정과 GDPR에 대한 해석을 제공하는 EU 정책 자문기구인 '제29조 작업반(WP29)'에서 발간한 가이드라인[4]에 산재되어 있어 파악 및 활용이 어려운 실정이다.

따라서 본 논문에서는 GDPR원문과 가이드라인을 통합적으로 분석하여 GDPR에서 규정하는 '합법적인 사용자 동의 획득'을 위해 고려해야 할 동의 요소들을 추출하여 유형화하고, 해당 내용의 구체화 및 활용을 위해 동의획득 과정에서 필수적으로 고려해야 할 사항에 대한 체크리스트를 구성하고자 하였다. 또한 체크리스트의 유용성을 확인하기 위해 현재 글로벌시장을 대상으로 하고 GDPR에 대응이 용이한 대기업으로 대표성을 가지는 국내 대기업(LG)의 동의 획득 수준을 체크리스트를 통해 분석하였다. 마지막으로 향후 정보주체의 권익을 보호하면서 동시에 이를 정당하게 활용하기 위한 정책적 개선방안을 제안하고자 한다.

Ⅱ. 기존 문헌

정보주체의 동의와 기본권 보장에 관한 논의는 그동안 법학계를 중심으로 이루어져 왔다. 법학계에서의 논의는 개인정보보호의 토대인 프라이버시권의 기원과 법적 근거 및 성질을 규명하고 IT기술의 발달에 따른 프라이버시의 침해유형을 새롭게 지적하면서 그 대응책으로 해외 입법사례들을 참조하여 새로운 보호영역을 모색하는 것이 일반적인 경향이었다[5]. 그중에서도 개인의 기본권으로서 개인정보, 이를 제공하는 정보주체의 동의 과정에 대한 문제의식을 드러내는 연구는 동의 절차상 문제점 및 동의제도 관련 법률 분석을 통한 개선방안 제시[6]나 '개인정보 수집이용 동의(국내 개인정보보호법 제15조)'개선의 시급성을 현장의 목소리를 들어 지적한 연구[7] 등이 대표적이다.

그러나 모바일과 인터넷 서비스의 사회적 영향력이 높아지면서 사물인터넷, AI 등 서비스의 영역이 확장됨에 따라 정보통신, 방송통신, 정책연구 등 프라이버시 및 정보주체와 관련한 연구 분야 또한 확장되고 있다. 새로운 온라인 서비스 환경에서 일어나는 개인정보 수집 및 활용, 이를 위한 사용자 동의 획득 관련 행위에 주목한 연구들은 공통으로 새로운 환경에 적합한 동의절차 개선, 고지 의무 강화, UI개선 등의 필요성을 주장하고 있다. 예를 들어, 최근 보편화된 온라인 서비스 소셜 로그인 서비스의 경우, 기존 가입 절차 대비 평균 더 많은 개인정보를 요구하고 수집하고 있음에도 이에 대한 소비자의 인식이 명확히 이루어지지 못한 점이 지적되고 있다[8]. 또한, 센서 기반의 자동화된 정보수집 등 사물인터넷 환경이 보편화함에 따라 기존의 선택권 보장 중심의 개인정보보호 정책은 그 실효성에 의문이 제기되고 있으며, 고지환경 및 고지수준, 내용 측면에서 개선이 필요하다는 점[9]을 주장하기도 하였다.

서비스 제공자 입장에서 개선 사항 및 정보주체 권익 보호 측면 외에도 실제 정보주체의 입장에서 동의 행위에 따르는 이슈를 파악하고 해결방안 제시를 위한 논의도 일어나고 있다. 사용자의 '불성실한 동의 행동'은 주로 높은 연령대에서 나타나지만 전 연령대에서 인식 수준이 높지 않은 점, 그럼에도 개인정보 문제에 있어서는 높은 우려와 민감도, 권리 요구도를 나타내는 양면성을 파악한 연구[9] 및 이용약관 숙지 행위의 영향 요인으로 대처비용, 대안 효능감, 비차별성을 밝힌 연구[10] 등이 있다. 이와 같은 연구는 정보주체의 관점에서 적극적 동의, 선택적 동의를 표현하기에 제한된 환경에 대한 이해를 통해 이를 개선하는 방안을 모색하게 한다는 점에서 매우 주목할 만한 논의라고 할 수 있다.

이상에서 살펴본 바와 같이 개인정보를 수집 및 활용하는 환경은 변화하고 있으나 개인의 기본권으로서 개인정보, 이를 제공하는 정보주체의 동의 과정은 이를 충분히 반영하고 있지 못하고 있다는 문제가 공통으로 지적되고 있는 것을 볼 수 있다. 특히 현재 가장 진화한 개인정보보호법으로 평가받는 EU의 GDPR 시행 하에 정보주체의 권리에 관한 인식 수준이 점점 높아질수록 관련 이슈는 더욱더 증가할 수밖에 없다. 따라서 더 나은 사용자 동의 획득, 합법적이고 합리적인 개인정보 데이터수집 및 활용을 위해 해당 규정을 검토하고 필수 고려사항을 파악하는 일은 매우 중요한 일이 될 것이다.

Ⅲ. 연구 내용 및 결과

3.1 동의 관련 항 유형화

GDPR은 전문(Recital) 173항, 본문 11장(Chapter) 내 99개 조항(Article)으로 구성되어 있다. 그 중 전문은 제정 취지 및 배경을 설명하는 부분으로 그 자체로는 법적 구속력을 갖지 않으며 본문 11장에 걸쳐 제시된 99개 조항이 법적 구속력을 가지는 실제 법률 조항에 해당한다[11]. 본문 99개 조항 중 정보 주체의 동의에 관해 다루고 있는 항을 분석한 결과, 총 19개 항이 해당하였다. 가이드라인을 참조하여 각 항목을 특성별로 정리하면 크게 4개 유형으로 나뉘는데, 이는 1) 유효한 동의를 구성하는 요소 2) 유효한 동의를 위한 추가 조건 3) 특수한 개인정보처리 4) 특수사례이다.

첫 번째로 유효한 동의를 구성하는 요소는 본문 4조 11항에 정의된 정보주체의 동의를 준수하기 위해 필수적으로 요구되는 항목들이다. 해당 유형은 6개 세부 항목으로 구성되어 있는데 1) 동의 요청이 명확히 구분되어 제시되었는가에 관한 '동의 명확성', 2) 동의를 제공하는 것만큼 쉽게 철회가 가능한가에 대한 '동의 철회 가능성', 3) 정보처리 목적을 구체적으로 제시하였는지에 관한 '목적 구체성', 4) 서비스 이행에 필수적인 정보에 대해서만 동의를 요청, 끼워팔기나 엮음을 제한하는 '필수정보 동의', 5) 정보주체가 동의한 내용을 인지한 것으로 인정하기 위한 최소한의 조건을 제시한 '인지된 동의 조건준수', 6) 정보주체에게 정보처리자에 관한 정보 제공 의무를 제시한 '정보처리자 정보 제공'이 해당한다(총 7개 조항: 5~7조, 13~14조, 22조, 46조)

두 번째 유효한 동의를 위한 추가 조건은 정보 처

표 1. 동의 유형별 GDPR 항목 분류
Table 1. Classify GDPR by Consent Type

Category		Subclass	Article
Elements of valid consent		Clarity of consent	7.2
		Withdrawal of consent	7.3
		Purpose Specificity	5
		Consent of Essential Information	7.4
		Informed Consent Condition Compliance	5, 6, 22,49
		Provide controller's information	13, 14
Additional conditions for valid consent		Notification obligations	14
Processing of Special Personal Data		Request for a declaration of consent	7, 15-21
Specific case	Children	Age limit	9
		The proof of children's consent	22
		Informational method	49
	Scientific research	Specific	8.1
		Safeguards	8.2

리자(컨트롤러)가 획득한 유효한 동의를 유지 및 입증하기 위해서 준수해야 할 추가조건을 의미하며, 여기에는 정보주체가 자신이 제공한 개인정보에 대해서 열람, 정정, 삭제, 철회 및 수집된 정보를 수령, 이전요청에 관한 권리 등이 고지되어야 하는 고지의무가 해당한다(총 8개 조항: 7조, 15조~21조)

세 번째 유형인 특수한 개인정보처리는 별도의 명시적인 동의가 반드시 요청되어야 하는 경우이다. 이 유형은 민감 정보 수집 시 자유롭게 제공된 명시적 동의 여부 파악, 프로파일링에 대한 명시적 동의 획득, 제3국 이전에 대한 명시적 동의 획득 등의 사례가 해당한다.

마지막으로 네 번째 특수사례에 관한 유형은 아동을 대상으로 한 경우와 과학적 연구에 관한 동의를 획득할 경우의 조건이다. 아동을 대상으로 동의를 획득해야 할 경우의 나이 제한, 친권보호자 확인, 아동 배려 조건과 과학적 연구에 대한 동의 획득 시 연구목적 특정 및 안전조치 적용 여부 확인에 대한 항목이 포함되어 있다.

3.2 동의수집 유형별 체크리스트

동의수집 요건에 따른 체크리스트는 각 유형에 해당하는 개별 GDPR 조항을 중심으로 반드시 충족해야 할 내용에 대한 문항으로 구성한 것이다. 4개 유형 중 첫 번째, 유효한 동의를 구성하는 요소부터 살펴보면, 동의 명확성, 동의 철회 가능성 및 필수정보 동의는 원문 제7조 '동의의 조건'을 기반으로 하고 있다. 동의 명확성은 동의 요청이 기타의 사안과 구분되어 있는지, 관련 내용의 입수가 용이한지, 명확하고 평이한 문구를 사용하여 이해하기 쉽게 제시되었는지를 묻고 있다. 동의 철회 가능성은 동의 철회가 '동의를 제공하는 것만큼 쉽게' 가능한지를 묻는 문항으로 한 번의 클릭, 스크린 밀기, 한 번의 키 누름 등 동의 철회의 UI에 대한 검토를 요구하고 있다. 필수정보동의는 해당 계약이나 서비스 이행에 필수적인 정보에 대해서만 동의를 요청 하였는지를 묻고 있다. 소위 '끼워 팔기', '엮음' 등 해당 서비스를 이용하는데 필수적이지 않은 정보에 대한 동의를 요청하는 경우 이를 경고하는 것이다. 목적 구체성은 원문 제5조 개인정보처리 원칙을 근거로 동의 획득 시 개인정보의 처리 목적을 구체적(Specific)으로 제시하였는지에 관한 문항이다. 인지된 동의 조건은 원문 제 5조, 6조, 22조, 46조에 기반을 두고 있는데 정보주체가 '인지한 동의(informed consent)'를 제공하였는지 입증하기 위한 최소한의 조건을 준수하였는지를 묻는 것으로 가이드라인에서 6가지[1]로 제시하고 있다. 마지막으로 정보처리자의 정보 제공은 원문 제13조와 14조를 근거로 개인정보 주체로부터 개인정보를 직접 수집 또는 간접 수집할 경우 개인정보 처리자가 제공해야 할 정보를 충실히 제공하였는지 묻고 있다.

두 번째 유형인 유효한 동의를 위한 추가 조건에서는 원문 제7조, 15조부터 21조까지를 근거로 정보주체의 권리에 관해 충실히 고지하였는지를 묻고 있다. 정보주체의 권리는 수집된 개인정보에 대한 열람, 정정, 삭제, 처리제한뿐 아니라 동의 철회, 수집된 정보 수령 및 이전을 요청할 권리 등을 포함하고 있으며, 사용자는 동의에 앞서 이와 같은 권리에 관해 고지 받을 권리가 있음을 확인하는 것이다.

세 번째 유형인 특수한 개인정보처리 유형은 명시적 동의가 요청되는 세 가지 경우에 관한 확인 사항이다. 먼저 민감 정보를 수집하는 경우, 원문 제9조를 근거로 동의가 자유롭게(freely) 제공되었으며, 명시적으

1) '인지한 동의'를 위한 최소한의 조건: 1) 컨트롤러의 신원 2) 각 처리작업의 목적 3) 수집/사용될 데이터 유형 4) 동의 철회 권리의 존재 5) 자동화 의사결정과 관련한 데이터 사용에 대한 정보 6) 데이터 이전 시 발생 가능한 위험에 관한 정보가 제공되어야 함

로 요청되었음을 증명할 수 있는지에 관한 문항이다. 또한, 개인정보의 프로파일링(Profiling)을 비롯한 자동화된 처리가 발생하는 경우, 원문 22조에 따라 사용자는 이를 거부할 수 있으며 이에 대한 명시적인 동의를 요청하였는지가 주요 사항이 된다. 끝으로 제3국으로의 이전이 발생할 경우 원문 제49조에 의해 이에 대한 명시적인 동의 요청이 필수임을 묻고 있다. 이처럼 특수한 개인정보의 경우 GDPR은 향후 컨트롤러에게 유효한 명시적 동의를 획득하였음을 입증하는 것에 대한 중대 책임을 부과하고 있음을 확인할 수 있다.

마지막 네 번째 특수사례 유형은 아동에 관한 동의 획득과 과학적 연구에서의 동의 획득이다. 아동에 관한 동의 획득은 서비스 제공 대상의 연령을 특정하고 있는지를 묻고 있는데(제8조), 최소 만 13세 이상일 경우 본인의 동의가 유효하나 이하의 나이는 친권보유자의 동의를 받을 것을 명시하고 있다. 이때, 데이터의 민감성에 따라 친권보호자에 대한 적절한 확인 절차를 거칠 것을 규정하고 있다. 또한, 원문 제12조

표 2. 동의 유형별 체크리스트
Table 2. Check List by Consent Type

Category		Subclass	Question	Article
Elements of valid consent		Clarity of consent	Did the request for consent be presented separately from other matters?	7.2
			Is it easy to get?	
			Is it provided in a way that is easy to understand using clear phrase?	
		Withdrawal of consent	Is it possible to withdraw consent at any time as easily as the user gives consent?	7.3
		Purpose Specificity	Have you specified the purpose of information processing?	5
		Consent of Essential Information	Did you request consent only for essential information to perform the contract or service?	7.4
		Informed Consent Condition Compliance	Did you comply with the minimum requirements for 'informed consent'?	5, 6, 22,49
		Provide controller's information	Did you comply with the requirements of providing controller information when personal data was collected from the user?	13
			Did you comply with the requirements of providing controller information when personal data was not collected from the user?	14
Additional conditions for valid consent		Notification obligations	Did you notify about the rights of the user?	7, 15-21
Processing of Special Personal Data		Request for a declaration of consent	When collecting sensitive data, was explicit consent required under Article 9, and could it be regarded as freely provided?	9
			If profiling of personal data(automated individual decisions) occurs, have you asked for explicit consent about profiling?	22
			Did you request explicit consent for the data transfer to a third country?	49
Specific case	Children	Age limit	Do you specify the age of the user?	8.1
		The proof of children's consent	When dealing with sensitive information, do you have an appropriate verification process to whom may hold parental responsibility?	8.2
		Informational method	Do you provide information in easier and more concise language when targeting children?	12
	Scientific research	Specific	Have you been given to user a clear and specific content about the research and data processing purposes?	7, 9
		Safeguards	Have appropriate safeguards been applied for the rights of user?	89

를 근거로 아동을 대상으로 할 때 보다 쉽고 간결한 언어로 정보를 제공하였는지 또한 확인해야 한다. 과학적 연구에서의 사용자 동의 획득에서 가장 중요한 것은 정보주체에게 연구 및 데이터 처리 목적에 대해 명확하게 제시하였는지를 확인하는 것이다(7조, 9조). 이와 더불어 과학적 연구에 활용하는 데이터의 경우 제89조를 근거로 정보주체의 권리를 보장하기 위하여 데이터 최소화, 익명처리, 가명처리, 데이터 보안, 분리조치 등 적정한 안전조치를 적용하였는지를 확인하고자 하였다.

Ⅳ. 사례분석 - LG 스마트TV

4.1 사례 개요

본 장에서는 현재 글로벌 시장을 대상으로 하는 기업, GDPR 등에 대응이 그나마 용이한 대기업으로 대표성을 가지는 대기업(LG)의 동의 획득 수준을 도출된 체크리스트를 통해 파악하고자 하였다. 이를 통해 국내 기업들의 정보주체 권리에 관한 대처 수준 파악 및 향후 기업들의 GDPR 대응을 위한 체크리스트의 유용성을 검증하고자 한 것이다.

스마트TV는 기존의 TV와 달리 인터넷에 연결되면서 IT기술의 발전을 가장 적극적으로 반영하고 발전하는 매체 중 하나다. 사용자들은 이제 단순히 TV를 시청할 뿐 아니라 홈쇼핑 등 전자상거래를 하고, 소셜아이디(Facebook, Google 등)로 로그인하여 애플리케이션을 설치, 이용하며 스마트폰을 연결하고 IPTV를 기반으로 각종 TV 콘텐츠 추천서비스 등을 받는다.

이렇듯 무궁무진한 스마트TV의 활용성이 확장되면 향후 스마트TV가 개인정보 침해 논란의 중심에 설 가능성 또한 높아진다는 것을 의미한다. 특히, 스마트TV의 이용약관 및 사용자 동의수집 절차는 리모컨을 활용, 최초 설치 시 1회 노출을 통해 이루어지는 등 스마트폰이나 PC보다 사용자의 접근성이 가능한 형태로 제공된다[2]. 이용약관은 필수 동의 사항 및 선택적 동의 형태로 제공되고 있으며, 본 논문에서는 11개 약관 전체를 대상으로 분석을 수행하였다.

4.2 분석 결과

각 체크리스트 문항별 이용약관의 충족 여부를 판단하기 위하여 먼저 단계 수준을 설정하였다. 정보주체의 입장에서 '충족'은 해당 정보가 쉽게 인지 가능한 형태로 존재하는 경우(별도 존재, 강조 등), '미흡함'은 해당 정보가 존재하나, 인지가 어려운 경우(추가 클릭 요구, 과도한 정보량 등), '불충족'은 해당 정보를 발견할 수 없는 경우, 해당 없음은 체크리스트 내용이 이용약관에 적용되지 않는 경우이다.

분석 결과, 총 18개 체크리스트 문항 중 LG 스마트TV 약관은 충족 7개, 미흡 5개, 불충족 3개, 해당 없음 3개로 GDPR 기준 정보주체의 동의를 받는 과정에서 필수적인 조건을 충분히 충족하고 있지 못한 것으로 나타났다.

첫 번째 유형인 유효한 동의를 구성하는 요소에서는 총 9개 문항 중 충족 4개 항, 미흡 3개 항, 불충족 1개 항, 해당 없음이 1개 항으로 분석되었다. 동의 명확성의 측면에서 동의 요청은 구분되어 제시되었고, 문구는 비교적 평이한 수준으로 제시되었으나 입수가 용의한가 여부에서는 사실상 TV 인터페이스를 통해서만 확인 가능한 점, 홈페이지 등에 고지되어있는 약관이 TV에서 제시되는 것과 다르고, 별도 요청을 통해서만 서면으로 확보할 수 있다는 점에서 미흡하다고 볼 수 있다. 동의 철회조건의 경우, 동의를 제공하는 것만큼 쉽게 철회가 가능해야 하는 GDPR 기준으로 이에 대한 명확한 인터페이스가 존재하지 않았다(동의함/하지 않음의 선택 항이 아닌 동의함, 향후 동의 등 인터페이스 모호함). 목적 구체성의 측면에서 정보처리 목적에 관해서는 상세하게 고지되었는데, 필수정보 동의의 경우 반드시 필요하지 않은 추가 서비스에 대한 동의(Pooq, 네이버 등)가 필수 동의 사항으

표 3. LG Smart TV 이용약관 구성
Table 3. Terms and conditions of LG Smart TV

No.	Title
1	Consent to collect of Personal Information
2	Agreement to provide personal information to third parties
3	Privacy policy
4	Collection agreement of Nuance voice information
5	Third party agreement of Nuance voice information
6	Customized advertising terms and conditions
7	Terms of smart TV service
8	Consent to collect of watching information
9	Agreement to provide watching information to third parties
10	Consent to collect of voice information
11	Agreement to provide voice information to third parties

2) 제조사 홈페이지 등을 통해 확인할 수 있는 이용 서비스 약관의 경우 TV에서 제공되는 것과 차이가 있으며, 제조사에 별도 요청을 통해 개별적으로 약관을 획득할 수 있다.

로 설정되어 끼워 팔기 금지 조항에 위배되는 것으로 나타났다. 인지한 동의를 위한 최소한의 조건의 경우 해당 정보가 제시되어 있기는 하나 과도한 정보량 및 정보 분산으로 인해 정보 주체자가 파악하기 매우 어렵다는 점에서 미흡하다고 볼 수 있다. 마지막으로 정보처리자의 정보 제공과 관련한 정보는 충분히 제공되고 있었다.

두 번째 유형인 유효한 동의를 위한 추가 조건으로서 정보주체자의 권리에 대한 고시 의무는 별도의 단락으로 제공되는 등 충족하고 있다. 그러나 세 번째 유형인 특수 개인정보처리를 위한 명시적 동의 요청에서는 미흡한 요소가 발견되었다. 음성정보 등 민감정보 및 프로파일링과 관련한 내용에 대한 동의는 구분되어 제시되어 있으나 제3국 이전에 관한 내용의 경우, 이전되는 다국적 기업의 정보 등은 존재하나 구체적으로 데이터가 처리되는 국가에 대한 정보는 부재 하는 등 충분한 정보가 제공되지 않았다는 측면에서 미흡하다고 볼 수 있다.

마지막 특수사례유형인 '아동'과 관련하여, 동의 절차상 나이를 특정하여 묻는 단계가 제시되지 않았다는 점에서 연령 제한 항은 위배되는 것으로 판단하였다. 물론 약관 내용 중 만 14세 미만인 경우 계약을 해지한다는 내용이 명시되었으나, 사용자의 나이를 파악하기 위한 별도의 절차 마련 등 관련 내용의 보완이 필수적인 것으로 보인다. 과학적 연구의 경우에도 해당 정보 수집 내용이 연구목적으로 활용됨을 명시하

표 4. 사례 분석 결과(LG Smart TV)
Table 4. Analysis result(LG Smart TV)

Category		Question	Compliance	Insufficient	noncompliance	N/A
Elements of valid consent		Did the request for consent be presented separately from other matters?	0			
		Is it easy to get?		0		
		Is it provided in a way that is easy to understand using clear phrase?	0			
		Is it possible to withdraw consent at any time as easily as the user gives consent?		0		
		Have you specified the purpose of information processing?			0	
		Did you request consent only for essential information to perform the contract or service?	0			
		Did you comply with the minimum requirements for 'informed consent'?		0		
		Did you comply with the requirements of providing controller information when personal data was collected from the user?	0			
		Did you comply with the requirements of providing controller information when personal data was not collected from the user?				0
Additional conditions for valid consent		Did you notify about the rights of the user?	0			
Processing of Special Personal Information		When collecting sensitive data, was explicit consent required under Article 9, and could it be regarded as freely provided?	0			
		If profiling of personal data(automated individual decisions) occurs, have you asked for explicit consent about profiling?		0		
		Did you request explicit consent for the data transfer to a third country?	0			
Specific areas	Children	Do you specify the age of the user?			0	
		When dealing with sensitive information, do you have an appropriate verification process to whom may hold parental responsibility?				0
		Do you provide information in easier and more concise language when targeting children?				0
	Scientific research	Have you been given to user a clear and specific content about the research and data processing purposes?		0		
		Have appropriate safeguards been applied for the rights of user?			0	

고 있으나 구체적인 연구 내용에 대한 정보가 충분치 않고, 이에 대한 별도의 동의를 받지 않는다는 점에서 모호하게 제시되었다고 하겠다. 마지막 정보주체의 권리와 자유를 위한 안전조치에 관해서는 명확히 제시되어 있지 않고, 수집된 정보로 재식별 가능성이 충분함에도 이에 대한 구체적 안내가 없어 불충분한 것으로 판단하였다.

V. 결 론

본 논문은 개인정보 수집 및 활용에 있어 정보주체인 사용자의 권리를 보호하면서 동시에 이를 정당하게 활용하기 위한 동의를 얻기 위한 방안을 구체화 하는 것을 목적으로 하였다. 이를 위해 현재 개인정보수집 및 활용과 관련해 세계적으로 가장 큰 영향력을 미치고 있는 EU GDPR 규정을 바탕으로 1) EU GDPR 원문 전체에 흩어져 있는 '사용자 동의 획득'과 관련한 내용을 분석하여 재분류하고 2) 해당 내용의 구체화 및 활용을 위해 동의획득 과정에서 필수적으로 고려해야 할 사항에 대한 체크리스트를 구성하였으며 3) 체크리스트의 유용성을 확인하기 위해 현재 글로벌 시장을 대상으로 하고 GDPR에 대응이 용이한 대기업으로 대표성을 가지는 국내 대기업(LG)의 동의 획득 수준을 체크리스트를 통해 분석하였다.

분석 결과, EU GDPR에서 요구하는 적극적 사용자 동의를 위한 조건은 크게 4개 유형으로 1) 유효한 동의를 구성하는 요소 2) 유효한 동의를 위한 추가 조건 3) 특수한 개인정보 처리 4)특수사례로 분류할 수 있으며, 분류 항목에 따라 필수 고려 사항에 대한 체크리스트를 구성한 결과 18개 항목이 도출되었다. 도출된 체크리스트를 기반으로 국내 LG 스마트TV 약관을 분석한 결과, 미흡 및 불충족 항목이 절반 이상으로 나타나 국내 기업의 개인정보 수집 수준 파악 및 동의 획득 절차 관련 연구 활성화를 위한 시발점으로서 체크리스트의 유용성을 확인할 수 있었다.

개인정보의 정당하고 적극적인 활용은 향후 데이터 경제 활성화를 위해서 매우 중요한 사항이다. 그러나 이를 위해서는 먼저 정보주체의 권리보호를 위한 조치, 즉 적극적인 사용자 동의 획득을 위한 절차 확립이 반드시 전제되어야 한다. 그러나 LG의 사례에서도 알 수 있듯이 국내에서는 위법하지 않기 때문에 현재 글로벌 수준의 서비스를 운영하고 있는 대기업도 국내에서는 GDPR 수준의 사용자 동의 획득 절차를 확립하고 있지 않다는 것이 현실이다. 즉 소비자의 권리 보호에 대해 선제적으로 노력하는 것이 아니라, 법 규제에 따라 사후적으로 방어하는 수준에서 이루어지고 있는 것이다. 따라서 정보주체의 권리 보호를 위해서는 기업 수준에서 소비자 보호를 위한 글로벌 수준 파악 및 준수 노력 외에도 정책적인 개선노력이 동시에 이루어져야 할 것이다.

적극적 사용자 동의를 위한 정책적 개선방안은 두 가지가 있다. 먼저 첫 번째로, 국내 개인정보보호법 등 관련 규제 법제 개선이다. 우리나라는 GDPR이 시행된 EU와 유사한 수준으로 개인정보보호가 이루어지고 있어 데이터의 상호 교류 및 이전에 문제가 없다는 취지의 평가인 '적정성 평가'를 통과하기 위해 지속적으로 노력하고 있다. 그러나 본 연구의 사례연구에서도 드러났듯이 국내에서 아직 관련 규정이 모호하거나 부재하여 여전히 사용자의 인지 없이 개인정보가 무분별하게 수집되는 측면이 있다. 그러나 현재 관련 내용을 포함한 국내 개인정보보호법 개정안(인재근 의원 대표발의, 2018. 11. 15.)은 발의된 지 10개월째 국회처리가 계류 중이며, 이에 대한 합의가 충분히 이루어지지 못한 상황이다. 따라서 관련 논의 및 개정안 통과 등 정보주체 권리 보호를 위한 법적 개선 노력이 선행되어야 할 것이다.

두 번째는 정부 차원에서의 동의 절차 관련 UI/UX 가이드라인 설계 및 배포이다. 우리나라는 공공웹사이트에 대해 사용자 편의성 향상을 위한 UI/UX가이드라인을 이미 배포하고 있다[12]. 사용자가 정보 제공에 동의를 제공하는 것은 사실상 소비자의 권익의 관점에서 중요한 부분이기 때문에 정부 차원에서 이에 대한 논의를 진행하고 이를 가이드라인으로 하여 공공웹사이트부터 이를 적용, 활용한다면 민간 부분으로의 확장 또한 기대할 수 있을 것이다. 현재 정보 주체에게 제공되는 이용약관 및 동의 수집방식은 사실상 서비스 제공자 입장에서 과도한 정보량을 일률적으로 제시하고 있는 형태다. 이처럼 제공자 입장에서 법적 이슈를 피해가는 수준의 동의 절차는 사실상 제대로 된 정보보호라고 볼 수 없다는 주장이 제기되고 있다[13]. 현재와 같은 방식에서의 동의 획득은 사용자가 개인정보가 어떤 용도로 사용될지를 정확히 파악하기가 사실상 어렵기 때문에, 동의를 구하는 것 자체가 정보주체에게 모든 책임을 떠넘기는 불공평한 처사라는 것이다. 그러나 이용자의 포괄적 동의는 무용할지 몰라도 개인정보 제공에 대한 득실을 결정하는 것은 개인차가 있어 이용자들에게 권한을 주는 것이 필요하다는 반박 의견 또한 존재한다[13]. 따라서 이러한 이슈를 해결하기 위해서는 이용약관 제공 방식에 있어 UI/UX 적인 측면의 개선이 필수적이다.

European Commission의 2016년 보고서에 따르면, 소비자의 약관 주목률(readership)은 9.4%에 불과하지만, 약관의 노출 형태나 약관 형식에 따라 77.9%까지 높아질 수 있다[14]. 따라서 관련 논의를 활성화 하고, 이를 반영하여 정부 차원에서의 UI/UX 가이드라인을 설계 및 배포한다면 국내 서비스들의 소비자 권리 보호 수준을 전반적으로 높일 수 있을 것이다.

4차 산업혁명 시대의 데이터 경제를 견인할 데이터 생산 주체로서 소비자의 정보 주권 및 동의 제공, 프라이버시 침해 등 부정적 피해 방지에 대한 이슈 등 개인정보보호에 이슈는 향후 더욱 중요해질 것이다. 정보통신 강국으로 세계적 수준의 IT 기술을 선도하고자 애쓰고 있는 우리나라가 정보보안에 대한 수준 또한 세계적으로 높인다면 더욱 안정적인 발전을 이룰 수 있을 것이다.

References

[1] European Union, "Regulation(EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)", May 2016.

[2] Wonmo Yang, In the first year of the GDPR enforcement, five major violation cases, Retrieved Aug.30, 2019, from https://www.boannews.com/media/ view.asp?idx=79426.

[3] Hyo-ju Park, Jin-hong Yang, "Issues of adequacy decision of GDPR and policy responses", The Journal of Korean Institute of Communications and Information Sciences, vol. 44, no. 5, pp.983-991, May 2019.

[4] Article 29 Data Protection Working Party, "Guidelines on consent under regulation 2016/679", Nov. 2017.

[5] Jongcheol Kim, "An essay on the reorganization of personal information control as a basic constitutional right", Internet Laws, vol 4, p.24, Jan. 2001.

[6] Suyeong Jo, "A study on the guarantees of basic rights of data subject and consent by user in the law of personal data protection", Law Review, vol. 18, no. 1, pp.321-346, Mar. 2018.

[7] Inha Industry Academic Cooperation Foundation, "A study on the improvement of consent procedure · method according to collection of personal information and on the introduction of management grading system of personal information protection", Dec. 2014.

[8] YoungHoon Jung, "A study on consumers" problems and social log-in in online services", Policy Research Report, pp.1-222, Dec. 2017.

[9] Jeeyeon Sah, "A study on consumer rights to control personal data in the IoT Era", Policy Research Report, pp.1-347, Dec. 2017.

[10] Suwon Kim, Seongcheol Kim, "Factors affecting users behavior towards online privacy agreements", Journal of Broadcasting and Telecommunications Research, pp.9-37, Oct. 2018.

[11] Ilyeong Jung, et al., "GDPR and improvement of data system in South Korea", STEPI Insight, no. 227, Dec. 2018.

[12] Ministry of the Interior and Safety, https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000045&nttId=69451

[13] Eugene Baek, Personal consent process, not proper information protection, Retrieved Aug.30, 2019, from http://news.bizwatch.co.kr/article/mobile/2019/08/29/0019/naver

[14] European Commission, "Study on consumers' attitudes towards terms and conditions(T&Cs) Final report", p.9, Mar. 2016.

박 효 주 (Hyoju Park)

2016년 2월 : KAIST 기술경영학과 석사
2012년 8월~2014년 2월 : KAIST IT융합연구소 연구원
2016년 3월~2018년 8월 : 부산과학기술기획평가원 연구원
2018년 9월~현재 : 인제대 연구원
<관심분야> 과학기술정책, 개인정보보호, GDPR
[ORCID:0000-0002-7756-0263]

양 진 홍 (Jinhong Yang)

2017년 2월 : KAIST 정보통신공학 박사
2017년 2월~2018년 1월 : HECAS 최고기술책임(CTO)
2018년 3월~현재 : 인제대학교 헬스케어IT 학과 조교수
<관심분야> CPS, IoT 시스템, 프라이버시
[ORCID:0000-0002-5871-8387]

정 재 은 (Jae-eun Jung)

2017년 3월~현재 : 인제대학교 헬스케어IT 학과 재학 중
<관심분야> IoT, UI/UX, 개인정보보호, GDPR
[ORCID:0000-0002-6131-1027]