논문 18-43-02-28 The Journal of Korean Institute of Communications and Information Sciences '18-02 Vol.43 No.02
https://doi.org/10.7840/kics.2018.43.2.416

GDPR 환경에서 국내 개인정보보호 관련 인증제도 및 표준 발전방향에 대한 연구

최 보 미◆, 채 상 미°, 김 민 균*, 강 연 정**

A Study of Development Plan Regarding Personal Information Management System and International Standardization: GDPR Perspective

Bomi Choi◆, Sangmi Chai°, MinKyun Kim*, Yeonjeong Kang**

요 약

ICT의 비약적 발전으로 인해 글로벌화가 된 환경에서 개인정보보호는 더 이상 제한된 국가의 수준에서 이루어지기 어려워졌다. 정보의 유통이 국경을 초월하고 정보의 활용 범위가 갈수록 넓어지면서 전 세계적으로 기관과 기업은 어떻게 개인정보를 안전한 방법으로 활용할 수 있는가를 고민한다. 관련법과 정책, 기술적 방법 등 개인정보보호를 위한 방법들이 존재하지만 본 연구에서는 기업 및 기관의 측면에서 변화하는 개인정보보호의 국제 정세에 대비하기 위한 능동적인 대응 방안으로 개인정보보호의 표준 및 인증제도 획득의 중요성을 강조한다. 본 연구는 기업 및 기관의 개인정보보호에 선제적 대응 방안을 제시 하는데 있어서 첫째, 개인정보보호에 대한 국제적 환경변화에 대해 살펴보고, 둘째, 개인정보보호 관련 표준 및 인증제도에 대한 현황과 내용 분석을 진행하고자 한다. 또한 최근 개인정보보호의 국제적 변화가 반영된 표준의 내용을 분석 한다. 이를 통해 향후 글로벌화 되고 있는 국내기업을 위한 국내 표준의 발전방향에 대해 제시함으로써, 국내 기업 및 나가 가서는 국가 차원에서 개인정보보호에 대한 수준 제고에 기여 하는 데 그 목적이 있다.

Key Words : GDPR, Privacy Protection, Personal Information Security, Standards, Certification

ABSTRACT

As Information Communication and Technology has been developed very quickly worldwide, protecting personal information emerges as significant issues that organizations have to deal with all over the world. Organizations in the world need to consider solutions of using information safely while information is used in various ways and distributed without borders. Thus, this study emphasizes the importance of obtaining authentication of PIMS with international standards in order to react toward changes of international trend on protecting personal information although related laws, regulation, policy as well as technological methodologies exist. Our research investigates global environmental changes regarding protecting personal information and analyze the changes of national and Intranational Standards. Therefore, it contributes to providing future directions for organizations to manage information privacy and improves the level of protecting personal information in nation wide.

※ 본 연구는 한국인터넷진흥원 개인정보보호 관리체계 인증제도 운영 사업의 일환으로 수행되었습니다.
◆ First Author : (ORCID:0000-0002-3354-283X)Ewha Woman's University Department of Management Information System, bmchoi@ewhain.net, 정회원
° Corresponding Author : (ORCID:0000-0003-4889-7737)Ewha Woman's University School of Business, smchai@ewha.ac.kr, 정회원
* (ORCID:0000-0003-2993-4803)Sogang University Sogang Business School, minkyunkim@sogang.ac.kr
** (ORCID:0000-0002-9295-2628)Korea Internet & Security Agency, yjkang@kisa.or.kr
논문번호 : KICS2017-11-361, Received November 28, 2017; Revised January 11, 2018; Accepted January 22, 2018

Ⅰ. 서 론

정보통신기술 발전은 사회 전 영역에서의 편리한 삶의 방향의 순기능과 사이버 범죄나 관리소홀로 인한 개인정보 침해 사고 등 역기능이 동시에 존재한다. 개인정보 침해 사고는 개인정보 주체의 정신적 물질적 피해를 야기하며, 유출된 정보는 회수가 불가능하다는 특징을 가지면서 우리 사회에서 개인정보보호에 대한 관심이 높아지고 있다.

2016년 기준 공공·민간 구분 없이 접수된 개인정보 침해 신고·상담은 9만 8000건으로 지속적으로 개인정보 유출·침해사고가 나타나며[1], 한 보안 회사의 조사에 따르면 2015년에 전 세계적으로 전년 대비 38% 증가한 1조6900만개의 개인정보가 유출되었다고 발표한 바가 있다[2]. 국가적으로 개인정보보호를 위해 법제도 개선 및 거버넌스 체계 구축, 개인정보보호 정책 정비, 침해구제 방안 모색 등 다양한 방안으로 노력을 하고 있지만, 더불어 기업과 기관도 협조적이고 자발적인 개인정보보호를 위한 노력이 요구된다.

기업측면에서 개인정보보호는 직접적인 이익과 직결되는 문제다. 안전한 개인정보 관리는 고객의 신뢰와 기업의 이미지에 영향을 주며, 개인정보 유출 사고 시 손해배상금 등 실질적 비용 소요나 이에 따른 소송 등 송무 비용 소요를 고려하게 된다[3]. 이에 따라 기업과 기관 측면에서도 고객과 국민의 개인정보를 안전히 활용하기 위해 다양한 방법의 보호 조치에 관심을 가지고 있다. 실제로 기업 및 기관은 개인정보보호 관련 법 준수를 통한 개인정보를 보호하는 수준에 미친다. 2017년도 개인정보보호 연차보고서에 따르면 정보주체의 91.7%가 개인정보보호법을 인지하고 있으며 지난 2015년도와 비교했을 때 7.0%가 높아지는 것을 알 수 있다[4]. 마찬가지로 공공기관은 98.3%, 민간기업은 94.6%가 개인정보보호 관련 법률을 인지하고 있으며, 해당 관련 법률을 기반으로 내부 관리 계획의 수립 이행을 통해 개인정보보호의 안전한 관리 조치를 하는 것으로 밝혀졌다[4]. 특히 개인정보보호관련 법 제·개정 및 교육 활성화 등의 정부의 노력으로 정보주체와 개인정보처리자 모두에게 법 인지도는 높게 나타난 반면, 능동적인 보호활동은 다소 미흡한 것으로 조사되었다[4]. 이에 따라 기업 및 기관에게 법 이행 수준을 높이기 위한 자율규제 활동 강화에 대한 지원이 모색될 필요가 있다.

정보통신기술의 발달로 인해 기업과 기관은 글로벌화 되고, 국내 환경 뿐 만 아니라 다국적 환경의 이용자에게 정보통신 서비스를 제공하고 개인정보가 수집·활용되고 있다. 개인정보의 국외 이전이 가능해 짐에 따라 정보의 통제권 상실의 가능성이 커질 수 있으며, 이에 다양한 국가에서 자국민의 데이터를 보호하고자 하는 움직임이 나타나고 있다. 대표적인 예로 2018년도부터 시행되는 GDPR(General Data Protection Regulation) 법제도에 따른 기관 및 기업의 상황이 그러하다. 2018년도부터 시행하는 GDPR은 EU국가에 해당하지 않는 대부분의 기업 및 기관에서도 이 법률에 대해 주목하고 있다. EU 국가와 비즈니스 하는 기업 뿐 만 아니라 EU 국민의 데이터를 수집·관리하는 모든 기업까지 GDPR의 효력이 미치는 대상이 되며, GDPR의 규정을 어길 시, 세계 연매출 4% 또는 2000만유로 중 높은 과징금을 선택해 부과해야 한다[5]. 이렇게 EU 국가를 시작으로 GDPR과 같이 자국민을 보호하기 위한 개인정보보호를 위한 법적 강화 움직임이 전 세계적으로 나타나기 시작하는 오늘날 전 세계의 기업들은 이에 대한 적절한 대응책을 모색하고 있다.

글로벌 시장에서 활동하는 기업과 기관은 개인정보를 최대한 효과적으로 활용하는 동시에 침해 사고 대응과 사고를 예방하기 위한 방안으로 표준 준수 및 인증제 취득을 중요시 한다. 예를 들어 글로벌 대표 기업인 아마존의 경우 미국, 유럽, 싱가폴, 캐나다, 호주 등의 다양한 국가의 개인정보보호 법제도 준수 사항과 함께 ISO 27001과 같은 약 34개의 국제 표준 및 인증제도 획득 등을 적극적으로 알리고 자율적인 규제 준수 활동에 노력하고 있다[6]. 기업 및 기관들은 빠르게 변화하는 기술 환경과 다양한 국가들의 관련 법률을 모두 파악하고 준수 여부를 확인하기 어려우며, 이에 기업들은 가장 효과적이고 안전한 개인정보보호의 예방 및 대응 방안 책으로 해당 목적에 규격과 표준을 만들어 이를 준수함으로써 합리적인 활동을 이끄는 표준과 평가 대상을 일정한 표준 기준과 규정이 적합하게 이행 되고 있는지 확인하여 안정성과 신뢰성을 인증하는 제도가 될 수 있다.

본 연구는 최근 중요성이 증가하고 있는 기업의 개인정보보호에 선제적 대응 방안을 제시 하는데 있어서 첫째, 개인정보보호에 대한 국제적 환경변화에 대해 살펴보고, 둘째, 기업들의 주요 대응방법의 하나인 개인정보보호 관련 표준 및 인증제도에 대한 분석을 진행하고자 한다. 또한 최근 개인정보보호의 국제적 변화가 반영된 표준의 내용을 분석 한다. 이를 통해 향후 글로벌화 되고 있는 국내기업을 위한 국내 표준의 발전방향에 대해 제시함으로써, 국내 기업 및 나가가서는 국가 차원에서 개인정보보호에 대한 수준 제

고에 기여 하는 데 그 목적이 있다.

Ⅱ. 개인정보보호의 표준 및 인증제도 조사 연구

2.1. 개인정보보호의 국제 환경 변화

한 국가에 국한하지 않고 인터넷이 되는 공간에서 다양한 정보 주체들이 정보통신서비스를 제공받으면서 정보가 수집되고 저장· 가공· 활용·이전 되면서 정보 통제가 어려워지고 있다. 이에 따라 EU 연합 국가의 GDPR 제정을 중심으로 다양한 국가에서 자국민의 데이터 보호를 위한 법률 및 정책적 제도의 변화가 나타나고 있다. 2016년 11월 중국은 최근 심각해지는 개인정보 침해 사고로 인해 강력한 데이터보호법인 네트워크 안전법이 제정되었다. 핵심 보안 인프라 운영자로 지정되는 기업은 중국 국민의 개인정보를 수집하거나 처리하는 서버를 중국에 설치함으로써 외국 기업에 대한 자국민의 정보 활용에 제한을 강하게 두는 법률이다. 또한 EU와 미국은 2013년 6월, 미국의 스노든 사건과 이에 영향을 받아 2000년 EU와 미국이 지난 맺은 개인정보전송 관련 협정인 세이프 하버(Safe Harbor)를 대체하여 새롭게 개인정보보호 쉴드(EU-US Privacy Shield) 협정을 체결하였으며[7], EU는 새 협정을 통해 미국 정부와 기업이 유럽 시민 데이터를 보다 엄격히 관리하도록 하였다. 이 협정은 구글, 페이스북, 아마존 등 EU 국가 시민들의 개인정보를 다수 보유한 미국의 IT 기업들에게 큰 영향을 미친다. 아시아 국가에서는 글로벌 서비스 확산으로 개인정보 국외 이전이 활발해 짐에 따라 우리나라를 포함한 APEC 회원국 간 개인정보보호 공동기준을 적용하고 법 집행 공조 등 협력 체계를 강화하기 위한 글로벌 개인정보보호 인증체계인 CBPR (Cross-Border Privacy Rules)를 구성하였으며, 회원국 간 법 집행 협력을 기반으로 운영한다[8]. 이와 같이 더 이상 개인정보보호는 단일 국가만의 노력으로 해결되지 않는 문제가 되었으며, 글로벌 환경에서의 개인정보보호 측면을 고려할 필요가 있다.

본 연구는 2018년부터 시행되는 EU국가의 공통적으로 적용되는 개인정보보호를 위한 법률인 GDPR에 주목한다. 1995년 10월 EU는 회원국들 간 정보의 자유로운 이전을 제한하고 EU의 공동시장의 발전을 위해 EU 수준의 통일된 개인정보보호법제인 EU 개인정보보호지침을 채택하였다. 2016년 5월 24일, EU는 최근 변화한 기술 환경과 개인정보보호 이슈를 반영하여 기존의 EU 개인정보보호지침의 한계를 대체한 법률인 GDPR을 발표하였다. GDPR은 발전하는 기술 환경에서 개인정보자기결정권을 보장하기 위해 새로운 정보주체의 권리를 발표하고 기업의 책임 강화를 위한 내용들이 포함된다. 이러한 개인정보보호 법의 최근 한계점을 보완했다는 측면 이외에도 GDPR를 범국가적 차원에서 주목하는 데 또 다른 이유가 존재한다. 앞서 언급했듯이 개인정보 침해 사고 시 GDPR의 적용대상에 EU 국가에 사업장을 보유한 기업 뿐만 아니라 EU 시민의 개인정보를 가진 모든 기업이 포함되기 때문이다. 심각한 위반 시에는 연간 매출액의 4% 또는 2000만 유로의 높은 과징금 부과로 인해, 글로벌 비즈니스를 추진하는 기업 뿐 만 아니라 EU에 정보통신서비스를 제공하는 소상공인에게도 영향을 미칠 수 있다. 이에 따라 GDPR 환경에 적절한 대응책이 시급하다.

2.2 개인정보보호 관련 국제 표준

국제 표준은 소비자들이 해당 제품이나 서비스가 안전하고 신뢰할 수 있으며 좋은 품질임을 확신 할 수 있도록 도우며, 이를 위해 국제 표준 기구에서 공통된 규격을 개발하고 제시한다[9]. 자국 내에 독립적인 규격 형태로 개발한 독자적인 시스템을 통해 정보보호를 이행했던 과거의 상황과 달리 국제 사이버범죄와 개인정보유출 사고 등이 증가하는 오늘날은 국가 간, 기관 간, 시스템 간에 공동 대응체계가 요구되고 있으며, 이에 따라 정보보호의 국제표준이 중요해졌다[10]. 특히 개인정보를 정보의 한 부분으로 봤던 과거와 달리 개인정보보호의 중요성을 강조하는 사회로 변화되면서 일반 데이터와 개인정보를 구분하고 이를 독립적인 개발 부분으로 인지하게 되었다. 국제표준기구(ISO)와 국제전기표준회의(IEC)가 정보기술 분야 국제 표준 작업을 관리하기 위해 설립한 공동 기술 위원회인 ISO/IEC 기구를 중심으로 개인정보보호 측면의 국제 표준 개발이 진행되었다. 개인정보보호와 신원관리 관련 국제표준 개발을 담당하는 ISO/IEC JTC 1/SC 27은 개인정보영향평가 (privacy impact assessment)의 가이드라인을 제공하는 ISO/IEC 29134: 2017, ICT 시스템의 개인정보를 보호하기 위한 상위 프레임워크를 제공하는 ISO/IEC 29100: 2011 등 다양한ISO/IEC 29k 개발로 개인정보보호 측면의 국제 표준을 발표했다. 또한 2011년도부터 ISO/IEC JTC 1/SC 27 회의에서 논의되어 추진되었으며, 국내의 개인정보보호 관리체계를 기반으로 개발된 ISO/IEC 29151가 2017년도 발표되었다[11]. 이러한 국제 표준은 공식 문서화 되면서 각 나라별로 인정기관 및 인증기관을 지정하여 표준 이행 및 준수 사항

표 1. ISO/IEC JTC 1/SC 27에서 진행하는 개인정보보호 관련 표준 동향
Table 1. Privacy standards by ISO/IEC JTC 1/SC 27

표준 번호 및 제목	표준 개요	출간 시기
ISO/IEC 29134 Guidelines for privacy impact assessment	· 개인정보영향평가의 가이드라인 제공 목적 · 개인정보영향평가를 위해 요구되는 프로세스를 정의하고, 영향평가 보고서의 구조와 내용을 제시함 · 개인정보 영향평가의 법적 규제가 있는 조직이나 개인정보를 다루는 모든 유형과 규모의 조직 대상	2017-06
ISO/IEC 29100 Privacy framework	· 개인정보보호를 위한 시스템 설계, 조달, 개발, 테스트, 유지관리, 운영 등을 포함한 상위 프레임워크를 제공 목적 · 개인정보보호 프레임워크에서 요구되는 사항은 공통된 용어 지정과 개인정보 처리자의 역할 정의, 개인정보보호를 위한 요구사항의 설명, 원칙의 참조 사항의 내용을 포함함 · 개인정보를 다루는 ICT 시스템을 보유한 모든 조직 대상	2011-12
ISO/IEC 29190 Privacy capability assessment model	· 개인정보 관련 프로세스의 관리 능력 수준을 평가하는 방법의 가이드를 제공하는 것이 목적 · 조직에서 사용하는 개인정보 관련 프로세스의 능력 및 유효성을 평가하기 위한 접근법에 중점을 둠 · 조직의 개인정보를 감독, 관리 및 운영하는 책임자 또는 관련 이해관계자 그룹에 조언을 제공하는 담당자를 대상	2015-08
ISO/IEC 29101 Privacy architecture framework	· ICT 시스템에서 개인정보 처리를 위한 개인정보 제어 구현에 접근 방식을 제공하며, 개인정보 보안주체의 개인정보를 보호하는 ICT 시스템 아키텍처에 대한 지침을 제공함 · 개인정보를 처리하는 ICT 시스템의 지정, 조달, 설계, 설계, 테스트, 유지 관리, 운영 및 운영과 관련된 엔티티에 적용하며, 주로 개인정보의 주체와 상호작용하도록 설계된 ICT 시스템에 중점을 두어 개발됨 · 개인정보을 다루는 ICT 시스템을 보유한 모든 조직을 대상	2013-10
ISO/IEC 29151 Code of practice for personally identifiable information protection	· 개인정보보호와 관련된 위험 및 영향 평가로 식별 된 요구 사항을 충족시키고, 이를 위해 통제의 목적, 통제 지침을 수립하기 위한 목적 · ISO / IEC 27002에 기반한 정보보안 위험 환경의 맥락에서 적용 가능한 개인정보 처리 요구 사항을 고려하여 지침을 지정함 · 개인정보을 다루는 ICT 시스템을 보유한 모든 조직을 대상	2017-08

을 검증되며, 인증기관 내 인증위원회에서 인증결과를 심의하고 의결한다. 대표적인 국제 표준 기구인 ISO/IEC에서 제공하는 개인정보보호 관련 국제 표준 진행 현황을 확인하여 개인정보보호의 주요 시사점 파악이 필요하다.

2.2.1 ISO/IEC 29134: 2017

2012년 4월 스톡홀름 SC27 회의에서 신규워크아이템으로 채택되어 독일의 레인니스 매티어스 에디터와 한국의 염흥열 에디터의 주도로 개발된 국제표준이다[12]. ISO/IEC 29134: 2017은 개인정보영향평가(이하 PIA :privacy impact assessment)의 가이드라인을 제공하는 목적으로 개발된 표준으로 정보보호시스템의 관리수준을 위한 국제표준인 ISO / IEC 27001의 한 부분인 개인정보영향평가의 프로세스와 보고서를 구체화한 것이다[13]. PIA는 정보시스템, 프로그램, 소프트웨어모듈 디바이스 등 과정에서 나타날 수 있는 잠재적 프라이버시 관련 영향을 확인하고 개인식별정보를 처리하고 이해당사자들 간의 협의를 통해 개인정보보호를 하기 위한 조치이다. PIA 보고서는 정보 보안 관리 시스템의 사용으로 인해 발생하는 조치에 따른 ISO / IEC 27001 부분에 포함이 되어 있으나 개인정보보호의 중요성이 강조 되면서 PIA에서 요구되는 프로세스를 정의하고 보고서의 구조와 내용을 표준화 했다. PIA는 문화, 사회적 기대, 국가 등에 따라 규모와 영향에서 상이한 면을 보이기 때문에 이 표준이 규범으로 될 수는 없으나 이 문서가 개별 상황에 따라 해석하여 가이드라인을 제공할 수 있다. ISO/IEC 29134에서 개발될 프로세스와 보고서 구조는 국내 개인정보보호법에 의해 시행되는 공공부분의 개인정보영향평가의 방법론을 개선하기 위해 이용 가능하다 [11].

2.2.2 ISO/IEC 29100: 2011

ISO/IEC 29100: 2011은 ICT 시스템의 개인정보를 보호하기 위한 상위 프레임워크를 제공을 목적으로 개발된 표준이다[14]. ICT 환경에서 개인정보의 보호를 위한 조직, 기술, 절차 측면의 개인정보보호 프레임워크를 제공한다. 개인정보보호 프레임워크에서 요구되는 사항은 공통된 개인정보보호의 용어 지정과 개인정보 처리자의 역할 정의, 개인정보보호를 위한 요구사항의 설명, 개인정보보호 원칙의 참조 사항의 내용을 포함한다. ISO/IEC 29100는 개인정보를 다루고 보호하는 ICT 시스템의 설계, 구현, 운영 및 유지 보수를 지원하고, 혁신적인 솔루션 개발이 가능하며, 모

범 사례를 통한 조직의 개인 정보 보호 프로그램을 개선하는데 사용 될 수 있다. 또한 제공된 프라이버시프레임워크는 기술적 참고 아키텍처와 개인정보보호관리 구현 및 사용, 아웃소싱 된 데이터 프로세스에 대한 개인정보보호의 제어 방법, 특정 엔지니어링의 사양 등의 부분에서 개인정보보호 관련 표준 이니셔티브의 기반이 될 수 있다. 개인정보를 처리하는 ICT의 제공 범위가 넓어짐에 따라 공통된 이해를 통해 제공하는 국제 보안 표준이 필요하며, ISO/IEC 29100에서 제시하는 표준 프레임워크를 통해 개인정보보호의 법적 요구사항을 보완할 수 있다고 표준 문서에서 설명한다[14].

2.2.3 ISO/IEC 29190: 2015

ISO/IEC 29190: 2015는 개인정보보호 역량 평가 모델 (Privacy capability assessment model)을 제시하는 표준이다[15]. 조직의 개인정보를 감독, 관리 및 운영하는 책임자 또는 관련 이해 관계자 그룹에 조언을 제공하는 담당자를 대상으로 다양한 개인정보보호 이해 관계자 요구 사항을 고려하고 기업 전략에 의한 운영 및 LOB (Line-of-Business) 관리자에 이르기까지 여러 수준의 이해 관계자에게 개인정보보호를 위한 가이드를 제공한다. 개인정보 관련 프로세스의 관리 능력 수준을 평가하는 방법의 가이드를 제공하는 것이 목적으로 조직에서 사용하는 개인정보 관리 관련 프로세스의 능력 및 유효성을 평가하기 위한 접근법에 중점을 둔다. 개인정보보호 관리 가이드에서 나타나는 요구사항은 다양한 이해관계자가 존재함에 따라 다른 정책과 행동강령, 비즈니스 위험 평가, 감사 결과 등 차이가 있을 수 있고 다각도의 측면에서 이를 고려한다.

개인정보보호 역량 평가는 적정한 수준 (또는 관리의 수준)에서의 유용한 정보를 조직에게 제공하고 개인정보보호 역량이 각 이해관계자에 따른 상이한 영역(법률준수, 위험관리, 명성 등)에서 평가 되어야 한다는 주요 기준을 충족해야한다. 개인정보보호 역량 평가는 반복적이고 점진적인 과정을 통해 조직의 역량 향상 할 수 있으며, 이 표준을 통해 역량평가 모델의 전반적 점수 및 주요 성과에 평가를 확인하는 측정 지표, 특정 영역의 능력 향상을 위한 개인정보보호 프로세스 관리 감사 및 수행 방법에 대한 자세한 결과물 등 여러 가지 산출물을 도출할 수 있다.

점차 개인정보의 활용 범위가 확대됨에 따라 여러 이해관계자가 존재하며, 이와 같은 변화로 인해 ISO/IEC 29190: 2015는 다양한 이해관계가의 요구사항을 충족시키기 위해 광범위하고 실무적 맥락을 중심으로 개인정보 관련 프로세스의 관리 능력 수준을 평가하는 방법의 가이드를 제공한다는 점에서 주목할 필요가 있다.

2.2.4 ISO/IEC 29101: 2013

ISO/IEC 29101: 2013은 개인정보보호 아키텍처 프레임 워크 제공 (Privacy architecture framework)하는 국제표준이다[16]. ISO/IEC 29101는 개인정보를 처리하는 ICT 시스템의 지정, 조달, 설계, 설계, 테스트, 유지 관리, 운영 및 운영과 관련된 엔티티에 적용하며, 주로 개인정보의 주체와 상호작용하도록 설계된 ICT 시스템에 중점을 두어 개발되었다. ISO/IEC 29101는 ICT 시스템에서 개인정보 처리를 위한 개인 정보 제어 구현에 접근 방식을 제공하며, 개인 식별 정보의 처리, 액세스 및 전송을 제어하여 개인정보 보안 주체의 프라이버시를 보호하는 ICT 시스템 아키텍처의 계획, 설계 및 구축에 대한 지침을 제공하며 개인정보보호 아키텍처 프레임워크를 설명한다. 또한 개인정보보호 강화기술(PET)을 개인정보 제어로 사용하는 방법 제시한다.

계속해서 발전해 가는 기술 환경 변화에 따른 기술적 관리의 원활한 기준 확립하기 위해 개인정보를 다루는 ICT 시스템 구축의 프레임워크를 제공하는 국제표준인 ISO/IEC 29101를 상시 확인할 필요가 있다.

2.2.5 ISO/IEC 29151: 2017

ISO / IEC 29151 : 2017은 개인정보보호 관리체계에 있어 관련된 위험 및 영향 평가로 식별 된 요구 사항을 충족시키고, 이를 위해 통제의 목적, 통제 지침을 수립하는 국제표준이다. 2011년 10월 케냐 나이로비 WG5 회의에서 한국의 염흥열 에디터에 의해 국내의 개인정보보호 관리체계를 기반으로 국제표준화를 제안하였고, 2012년 로마 WG5에서 신규워크아이템으로 결정이 되었다[12]. ISO / IEC 27001의 정보 보안 관리 프로세스 및 관련 요구 사항과 ISO / IEC 27002의 조직의 정보 보안 위험 환경을 고려한 정보 보안 표준 및 정보 보안 관리 실무 지침, ISO / IEC 27018의 클라우드 서비스 환경에서 개인정보 처리 시 개인정보 프로세서 역할 등 SC27 표준에서 개인정보 처리의 맥락에 맞게 개인정보보호의 통제 관리를 위한 내용을 조정되어 개발하였다[12,17].

국내 개인정보보호 관리체계를 기반으로 개발되어 국제 표준인 ISO/IEC29151은 개인정보보호 관리체계의 전반적인 구조는 유사하나 부분적으로 상이한 특

징이 발견 된다. 특히 ISO/IEC29151은 국내의 관리 체계에서 다루고 있지 않은 신설 통제 항목에도 주목해야 한다. ISO/IEC 29151는 개인정보보호 조직의 체계적 책임이행을 보다 명확하게 알 수 있도록 책임(Accountability) 관련 표준화 기준으로 분류하고 해당 내용을 따로 한 항목에 명시하여[17] 개인정보를 다루는 관계자의 책임 소지를 보다 중요하게 다루고 있다. 또한 인적자원 관리 부문에 있어서는 고용 전 상태, 현재 고용 상태, 고용의 종료 및 변경 상태로 분류하여, 인력의 적격심사 및 고용조건을 구체화하고, 고용 종료 및 변경 단계의 인력 사후 관리 정책을 나타낸다[17].

많은 기관과 기업들은 다수의 공급업체와 협력하고 있다. 주체 기관 및 기업의 자체적 개인정보보호 강화뿐 만 아니라 공급업체의 상황을 함께 고려할 필요가 있으며, 공급업체의 개인정보보호 범위까지 이해하고 관리하는 가시성이 요구된다. 국내의 개인정보보호 관리체계는 위탁자에 대한 계약 및 관리 감독에 대한 기준이 명시 되어 있으나 공급업체와 관련한 관계 명시가 되어 있지 않으며, ISO 29151에서 공급업체관계(Supplier relationships)에 대해 분류 기준을 만들어 표준으로 명시함으로써[17] 기관 및 기업들이 공급업체와 정기적으로 협력해서 개인정보보호를 위한 방안을 선제적으로 구축하도록 한다. 정보보안 공급업체와 관계를 규정하기 위한 보안정책과 문제해결 방법, 정보 및 통신 기술의 공급망 기준을 제시하고, 공급자 서비스의 모니터링과 검토 방법, 서비스 변경 관리에 대해 구체적인 지침을 나타낸다.

더불어 ISO/IEC29151은 비지니스 연속성 관리 측면의 정보보안 통제항목을 새롭게 신설하였다 기관 및 기업에게 각종 재해 및 사고로 인한 개인정보 침해 사례의 위기대응 및 복구 관리체계의 중요성이 강조되면서, 계획과 매뉴얼에 따라 업무와 주요 인프라를 신속하게 복구할 수 있는 시스템을 구축하고자 하는 노력이 강구 되고 있다. 이에 따라 ISO29151은 사고예방, 위기대응체제의 구축과 정보처리 관련 인프라의 가용성을 확인하는 표준 항목을 추가적으로 제시한다.

2.3 개인정보보호의 국제 환경 변화에 따른 표준 변화 분석 (BS10012:2017)

본 연구는 GDPR의 환경에 기업의 대응책 마련의 측면에서 고려할 수 있는 개인정보보호를 위한 주요 표준을 분석하여 향후 글로벌화 되고 있는 기업 및 기관을 위한 국내 개인정보보호 관련 표준 및 인증 사업의 발전방향에 대해 제시하고자 한다. BS10012:2017의 경우, GDPR의 제정으로 인해 새로운 내용을 반영하여 2017년도 개정본이 발표되었으며, 이와 같은 변경은 GDPR의 요구사항에 맞춰 해당 표준의 이행이 가능하고 GDPR 불이행 및 미준수로 인한 기업의 피해에 대응하는 중요한 대응책이 될 수 있다.

BS10012는 영국 주도의 국가표준제정기구인 BSI에서 진행하는 세계 최초의 개인정보보호 관리체계의 국가 표준이다. BSI는 ISO/IEC 27001 표준과 같이 정보보안, 제조업, 에너지, 식품 표준을 개발하여 세계 표준 시간을 주도하는 대표적 기구중 하나이다. 실제 2009년 처음 발표된 개인정보보호 관리체계의 인증제인 BS10012:2009은 국내의 개인정보보호 관리체계 개발 시 주요하게 참고 되어 국내 환경에 적합하게 개선하여 개발한 바가 있다. EU 개인정보보호 지침과 영국의 데이터보호법을 기반으로 구성된 2009년도 버전의 BS10012:2009와 달리 GDPR의 제정으로 인해 새로운 내용을 반영하여 2017년도 개정본인 BS 10012:2017를 발표하였다. 개선된 주요 내용을 중심으로 국내의 개인정보보호의 표준 및 인증제도의 발전 방향의 시사점을 분석한다.

지속적인 개인정보보호 관리체계의 운영을 위해 관련 조직을 구성해야한다. BS10012:2017은 GDPR 제4장 37조의 법적 근거를 기반으로 DPO (Data protection officer)를 의무로 지정한다. GDPR에서 데이터보호를 위한 독립적인 감독자를 고용하도록 명시함에 따라 BS10012:2017에서도 DPO의 지정과 업무에 대한 내용을 포함하고 있다.

DPO는 GDPR 제38조의 DPO의 지위를 상세히 기술하면서 개인정보보호를 위해서 방해 받지 않는 독립된 지위를 부여하고 정보보호를 위한 권리 행사를 보장하는 전문적인 역할을 수행하는데 의미를 둔다[18,19]. DPO는 컨트롤러와 프로세스, 개인정보 처리 임직원에게 GDPR 및 EU국가의 개인정보 보호 규정 준수를 위한 실질적 업무를 진행하고 모니터링 및 감사를 진행하며 감독기관과 협력하여 의사소통의 창구로써의 책무를 다해야한다[18,19]. DPO는 개인정보보호 관련 업무 중 데이터 관련 법률 및 정책 준수 감사에 초점이 맞춰져 있다. 이에 따라 DPO는 GDPR과 같은 법률 및 정책의 전문성을 가지고 개인정보보호 업무의 독립적 위치를 보장하여 권리행사를 할 수 있도록 명시하고 있다. 현재 국내에는 DPO와 유사한 직무에 대한 기준이 존재하지 않는다.

처리를 위한 정보 주체의 동의에 있어 더 엄격해진 요구도 주목해야 한다. GDPR에서는 개인정보자기결정권을 가진 정보 주체의 권리 보호를 위해 EU 거주

표 2. BS10012:2017에서 명시하는 DPO 지정 요건 및 지위
Table 2. DPO designation requirements and status in BS10012:2017

DPO의 지정 (GDPR 제37조)	- DPO의 필수 지정이 필요한 요건 (1) 법원을 제외한 공공기관에 의해 데이터가 처리되는 경우 (2) 처리의 본질, 범위 및 목적에 따라 관리자 또는 처리자의 핵심활동이 정보주체의 정기적·체계적 모니터링을 요구하는 처리 경우 (3) 제9조에 따른 특별한 정보항목을 대규모로 처리하는 경우와 제10조에 규정된 형사기소 관련 특수한 개인정보를 처리하는 경우 - 공공기관이 관리자 또는 처리자인 경우, 그들의 조직과 구조와 규모를 고려하여 여러 기관을 위한 1명의 정보보호 담당관을 지정할 수 있음 - 제1항에 규정된 경우 외에 관리자 및 처리자, 또는 협회 그리고 그 밖에 관리자 및 처리자의 분류를 대표하는 기관들은 정보보호 담당관 지정 가능함 - 정보보호담당관은 전문적 자질, 특히, 정보보호 법령과 실무에 대한 전문 지식과 제39조에 규정된 임무를 수행할 수 있는 능력을 보유한 자이어야 함, 관리자 또는 처리자는 정보보호 담당관의 성명과 세부 연락처를 감독기관에 통지하고 공개하여야 함
DPO의 지위 (GDPR 제38조)	(2) DPO의 지위 (제38조) - 관리자 또는 처리자는 정보보호담당관이 개인정보의 보호와 관련된 모든 문제에 적절하고 신속한 방법으로 관여할 것을 보장하여야 함 - 관리자 또는 처리자는 정보보호 담당관에게 그들의 전문지식을 유지하고, 개인정보처리활동에 접근하고 그들의 임무수행을 위하여 필요한 자료들을 제공하여 제39조에 규정된 임무 수행 시 정보보호 담당관을 지원해야 함 - 관리자 또는 처리자는 담당관 임무행사 시 어떤 지시를 받지 않도록 보장하고, 담당관은 임무수행과 관련하여 징계나 해고되지 않아야 하며, 최고위층 관리자나 처리자에게 직접 보고하여야 함 - 정보주체는 개인정보처리 관련 모든 문제 및 이 규칙에 따른 자신의 권리행사에 관하여 정보보호담당관과 접촉할 수 있음 - 정보보호담당관은 유럽연합이나 회원국 법률에 따른 비밀유지의무 하에 있음

자에 대해 개인별로 식별 가능한 정보를 수집, 저장, 처리하는 조직은 정보 주체로부터 사전 동의를 받아야 하며, 이때 정보 주체가 이해 가능하고, 간단명료하며, 모든 법률적·전문적 용어가 아닌 평이한 언어 방식으로 동의를 구하라고 규정한다[17,18]. 또한 BS10012:2017은 정보 주체 동의 관련 인증기준에서 큰 차이는 동의에 대한 철회의 권리를 가진 다는 것이며, 이 철회 또한 쉽고 편리한 동의과정과 마찬가지로

표 3. BS10012:2017에서 명시하는 정보주체 동의 관련 내용
Table 3. Data subject' consent in BS10012:2017

BS10012:2017에서 명시하는 정보주체 동의 관련 내용
- 개인정보 처리가 동의에 근거한 경우, 컨트롤러(controller)는 정보 주체가 자신의 개인 데이터 처리에 동의했음을 입증할 수 있어야함 - 정보 주체의 동의가 다른 문제에 관한 서면 선언의 맥락에서 주어지는 경우, 동의 요청은 다른 사안과 명확하게 구별되는 방식이어야 하고 이해하기 무난해야하며 명확하고 쉬운 언어가 사용되어 접근하기 쉬운 형태로 제시되어야 함. 이 규정의 위반으로 구성된 선언의 일부는 구속력을 갖지 않음 - 정보 주체는 언제든지 자신의 동의를 철회할 권리를 가짐. 철회에 대한 동의는 철회 전에 동의에 근거한 처리의 적법성에 영향을 미치지 아니한다. 동의를 하기 전에, 정보 주체에 이를 통보해야한다. 동의를 하는 것만큼 철회하는 것은 쉬울 것임. - 동의가 자유롭게 주어 졌는지에 대한 여부를 평가할 때, 특히, 서비스 제공을 포함한 계약 이행이 그 계약 이행에 있어 필연적이지 않는 개인 정보 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 함.

간단한 절차로 진행 되어야 함을 강조하고 있다[17,18].

GDPR 제정으로 인해 변화된 BS10012의 인증 기준 중 새로운 정보주체의 권리를 살펴볼 필요가 있다. 특히 국내법에 따라 정보주체의 권리에 명시되어 있지 않은 '개인정보 이동권', '반대할 권리', 자동화의 사결정 및 프로파일링 권리에 주목해야한다.

개인정보이동권리는 정보 주체가 자신의 정보를 이동할 수 있으며, 정보가 자동화된 방법으로 처리되고, 제 3자에게 정보를 전달할 수 있도록 하는 권리이다[18,19]. 국내에는 유사 관련 내용이 없다. 특정인에 의한 개인정보의 독점으로 사용되거나 정보주체의 동의 없는 무단 사용 등으로부터 정보 주체를 보호하기 위한 권리로 EU 시민들의 개인정보 보호를 강화를 위해 만들어졌다. 프로파일링 등 본인과 관련한 개인정보 처리를 언제나 반대할 수 있으며, 컨트롤러는 특별한 사유가 없는 한 이를 이행해야 하는 등 정보 주체가 자신의 정보에 대한 권리이행을 적극적으로 행사 할 수 있는 권리이다[18,19]. 국내법에는 아직 유사 규정이 없으나, 개인정보 처리정지를 요청 수준에서 인증기준이 존재한다. 마지막으로 자동화의사결정 및 프로파일링 권리는 최근 정보통신기술의 발달로 인해 중요하게 고려되는 권리 중 하나이다. 프로파일링(profiling)은 직업, 경제력, 건강, 취향, 관심사, 신뢰도, 행태, 위치, 이동 등 분석 또는 예측과 같은 정보주체에 관한 개인적 측면을 평가하기 위해 나타나는 자동화 처리의 모든 형태를 일컫는다. 이러한 프로파일링과 프로

파일링 된 정보로 자동화 의사결정이 맞춤형 마케팅과 같은 목적으로 활용되고 있다. 이에 프로파일링과 자동화의사결정에 대하여 정보주체는 자율적인 통제권을 행사할 수 있도록 하는 것이 중요하게 여겨지면서 만들어진 권리이다[18,19]. 정보주체가 자동화 정보처리의 상황을 인지하기 쉽지 않은 상태에서 진행되기 때문에 개인정보를 침해할 가능성이 높고, 경우에 따라서는 개인의 인격적 존엄성과 자율성을 위협할 우려도 있음을 고려해 만들어졌다. 국내는 아직 유사 법률이 없어 인증 기준이 존재하지 않는다.

마지막으로 BS10012의 개인정보보호의 대책 부문에 침해 사고 시 관리 방안관련 내용의 변경사항이다. 기업은 개인정보 침해사고 발생 시 정보주체와 관련 상부 기관에 사고에 대한 정보와 사고분석 후 발견된 취약점은 관련 정보를 보고할 필요가 있으며, 이는 유사 사고가 반복되지 않도록 재발방지 대책을 위함이다. 기존의 내용에는 개인정보보호 기준에는 감독 당국 및 정보 주체에게 참해 사고의 보고 관련 사항에 대해 언급은 되고 있으나 구체적인 이행 절차 및 내용은 기술되어 있지 않은 반면 변화된 내용에는 GDPR의 제33조-제34조에 따라 구체적으로 72시간 이라는 제한된 시간과 보고에 포함되어야 하는 내용과 보고 상황을 기술하고 있다[18,19].

표 4. BS10012:2017 침해 사고 시 관리 방안 관련 기준
Table 4. Managing security breaches in BS10012:2017

BS10012:2017에서 명시하는 침해 사고 시 관리 방안 관련 내용
- 개인정보 침해로 인한 피해를 복구하기 위한 절차를 포함하여 개인정보를 포함한 보안 침해사건을 평가, 관리하고 문서화함. - 정보 주체의 권리와 자유에 위험을 초래할 가능성이 있는 데이터 유출에 경우에 다음과 같은 내용을 포함하여 72 시간 이내에 감독 당국에 보고하는 것이 의무 (72 시간 통지 미행 시 이를 정당화할 사유를 함께 첨부하여 제출해야 함.) 1) 관련된 개인 정보에 대한 설명 2) 개인 정보의 범주 및 관련 기록의 대략적인 숫자 3) 조직 내의 DPO 또는 기타 연락처에 대한 연락처 세부 정보 4) 사고 발생 가능성에 대한 설명 5) 위반 사항을 해결하고 가능한 역효과를 최소화하기 위해 취하거나 제안한 조치에 대한 설명 - 정보주체에 위험을 처할 수 있는 사고에 대해 정보주체가 적절한 조치를 취할 수 있도록 다음과 같은 내용을 포함하여 해당 주체에게 즉각 모든 위반사항을 알려야 함. 1) 개인정보 침해 2) 침해 사고의 특성; 3) 침해 사고 조치에 관한 권고 사항 - 위반이 발생한 경위, 어떤 시정 조치를 취하는지, 위반 사항으로부터 파악할 수 있는지 등을 포함한 각 보안 위반 사항을 문서화 함.

Ⅲ. 결 론

본 연구는 국내의 기업 및 기관이 GDPR 환경과 같은 개인정보보호의 국제 환경 변화에 대응하기 위해서 선택할 수 있는 대응책 중 선택할 수 있는 개인정보보호의 국제 표준 및 인증 제도를 분석하였다. 기업 및 기관에게 표준 및 인증제도 획득은 개인정보보호를 위한 능동적인 보호 조치가 될 수 있으며 정보주체의 신뢰도 향상 및 조직의 이미지 향상에도 도움을 줄 수 있는 중요한 방법이다. 국내의 공공기관 및 대기업과 중소기업이 국내 표준 및 인증 제도를 획득하는 것은 해외 표준 및 국가 표준을 획득하는 것보다 효율적이고 용이하다. 하지만 ICT의 발전으로 개인정보 국외 이전 상황과 타 국민의 개인정보를 유통하는 기업들이 점차 늘어나면서 현재 기업이 국내의 표준 및 인증 제도를 획득이 국제 표준 및 해외 인증 제도를 획득하는 것 보다 나은 선택인지 의심할 수 있다. 특히 GDPR의 강력한 규제에 대한 우려로 인해 글로벌 기업들은 해당 법률을 기준으로 함께 고려할 필요가 있다.

따라서 국가적으로 글로벌 환경에서 기업들의 안전한 경영활동을 보장 하는 차원에서라도 국내의 개인정보보호의 표준 및 인증 제도를 국제 환경이 잘 반영하도록 보완 발전하는 것이 필요하다. 현재는 비즈니스 활동 범위에 따라 동일한 목적의 인증 제도를 중복해서 획득함으로써 발생되는 비용이 많다. 하지만 중소기업이나 영세 규모의 전자상거래 등 개인정보보호를 위한 투자에 한계를 가진 대상들에게 유사한 관련 표준 및 인증 제도를 여러 번 획득하는 것이 어렵다. 국내의 인증제도는 해외의 인증제도나 표준 보다 획득하는 것이 용이하고 획득으로 인해 국내 중소기업이 보호받는 환경에서 시장 경쟁력을 가지도록 도모할 필요성이 있으며, 이에 따라 GDPR과 같이 국가별로 자국민의 개인정보보호를 위한 법률이 강화되는 추세에 따라 글로벌 환경에서의 개인정보보호 인증 기준을 포함한 개인정보보호의 표준 및 인증제도로 개선이 필요하다.

첫째, 개인정보보호의 관리적 측면에 국제 환경에 적용되도록 개선이 필요하다. 본 연구는 개인정보보호 관련 국제 표준 조사를 통해 개인정보처리 관련 인력의 책임과 역할을 명확히 하는 기준을 나타내면서 전문성, 책임성, 독립성을 확보하는 개인정보보호 조직

관련 구성원을 요구한다. 국내도 개인정보보호 조직의 구성원 등 관련 인력의 적격심사 및 고용조건을 구체화하고, 고용 종료 및 변경 단계의 인력 사후 관리 정책 등 구체적인 대안을 고려해야 한다. 또한 GDPR에서 데이터 보호 관리자인 DPO의 의무 규정에 대한 국내의 대응방안 마련이 시급하다. 이는 GDPR의 법적 효력 대상이 국가적 제한이 무의미해짐에 따라 다른 국가의 법제도 및 정책의 영향을 충분히 받을 수 있는 다수의 기관과 기업이 DPO와 대응하는 담당자를 요구한다. 국내 개인정보보호의 표준 및 인증제도의 개인정보보호 조직 구성 측면에서도 DPO의 자격 및 업무, 책임에 대한 내용을 포함할 수 있는 기준 개발이 마련되어야 한다. 현재 우리나라는 국내 법률에 따라 국가 기관 및 공공기관에는 의무적으로 개인정보보호 책임자를 지정하게 되어 있으며, 기업은 CISO (Chief Information Security Officer), CPO (Chief Privacy Officer') 등의 직책으로 개인정보보호를 위한 담당자를 지정하고 있다. 우리나라의 DPO의 요구에 있어서 기존의 개인정보보호 책임자 및 담당자의 직무와 중복되는 범위를 고려해야하며, 기존의 직책과 이해 충돌을 피하기 위해 전문성에 따른 역할의 세분화가 필요한 시점이다. 국가 별 개인정보보호 관련 법률 및 정책적 지식을 충분히 가진 전문성을 증명하고, 기업의 개인정보보호를 위해 전적으로 담당하여 커뮤니케이션이 가능하며, 기업 내에서 독립된 위치를 보장하는 것이 DPO의 주요 특징 및 차이점으로 기존의 CISO, CPO와 상이한 부분을 충분히 고려하여 역할을 새로 지정하거나 추가적인 조건이 요구된다.

둘째. 변화하는 기업 환경에 따른 인증 기준 개선이 필요하다. 변화하는 개인정보보호의 기업 환경에 따라 다음과 같은 세 가지 측면에서 개선점을 요구한다. 첫 번째 측면은 개인정보보호 관점에서 비즈니스 프로세스의 보안 방향으로 개선하는 것이다. 기업 및 기관의 개인정보보호는 조직에게 신뢰와 연속성을 기반으로 하고 있어 단순히 보안 기술을 넘어 전사적 관점에서 비즈니스 프로세스를 이해하는 것이 필요하다. 신 ICT의 출현으로 인한 기업 환경 변화로 인해 정보 유출 사고가 늘고 개인정보처리 사고 시 다양한 이해관계자가 존재하며 책임 주체의 모호한 면을 나타내는 등 다양한 문제들이 나타나고 있다. 기업의 보안 관리 체계에 있어 과거에는 내부 기업 정보 등 정보보안에 초점을 두고 비즈니스 프로세스를 이해했지만 고객의 민감 정보를 대량으로 보유하는 전자상거래 기업 등 개인정보를 활용하는 기업 및 기관이 많아지면서 기업은 보유한 정보의 특성에 따라 개인정보보호 측면으로 비즈니스 프로세스 이해를 중요하게 고려해야한다. 두 번째는 비즈니스 연속성 (BCP: Business Continuity Plan) 측면에서의 개인정보보호의 관리 체계를 구축하는 것이다. 개인정보 침해 사고는 예방이 가장 기본이 되지만 동시에 사고 후 대처가 매우 중요하다. 개인정보 침해 사고는 정보 주체의 신체적 정신적 피해를 직간접적으로 줄 수 있으며, 이에 따라 신속하고 체계적인 대책 방안을 필요로 한다. 위험 관리와 피해 구제 등 비즈니스 연속성의 측면의 강조는 국제 표준을 중심으로 꾸준히 강조하는 부문으로 글로벌 기업을 중심으로 관련 국제표준 인증 취득이 늘어나고 있다. 개인정보 침해사고와 같은 리스크로 인해 정상적인 운용이 어려울 경우 주요 업무 기능을 복구해 조직과 정보 주체의 피해를 최소화하기 위한 핵심 실행 계획을 구성해 놓는 것이 중요하다. 개인정보보호 관련 재해 및 재난은 한 기업 뿐 만 아니라 국가 전체적으로 피해가 확산 될 수 있으므로, 기업은 개인정보보호 관리체계를 구축할 때, 국제 표준에 근거한 실무체계를 구축하는 것이 필요하다. 따라서 국내 개인정보보호 표준 및 인증제도는 비즈니스 연속성 측면에서 독립적인 인증 기준으로 구분하여 중요성을 강조해야 한다. 마지막 관점으로 공급자 관계에서의 정보보호를 상세하게 규정 하는 것이 필요하다. 기업이 보유한 데이터가 급증하면서 기업 및 기관이 자체적으로 이를 저장·처리·활용하는 것이 어려워졌다. 이에 따라 제 3자의 개인정보 처리자와 외주 용역, 위탁업체 등 다양한 개인정보 처리 주체가 존재하게 되고 이에 따라 기업과 기관은 관리해야 할 개인정보보호의 범위가 넓어지고 있다. 특히 최근 클라우드 서비스를 활용하는 기업이 많아지면서 개인정보보호의 관리적 범위가 확장되었지만 국내의 개인정보보호의 제도에서는 클라우드 서비스와 같은 공급자 관계는 명확히 규정해놓지 못한 상태다. 이에 따라 새로운 정보통신 기술에 따른 기업의 다양한 공급자 관계를 규정하고 구체적으로 공급자 관계에 대한 정보 보안 정책, 공급자 계약 내의 보안 문제 해결, 정보 및 통신 기술 공급망, 공급자 서비스 모니터링 및 검토, 공급자 서비스 변화를 단계적으로 확인하면서 변화하는 개인정보보호의 기업 환경을 고려해야 한다.

셋째, 급격한 ICT의 변화에 대응하는 개인정보보호 측면의 정보 주체의 권리가 고려된 인증기준 확립이 필요하다. 소셜네트워크서비스, 클라우드 컴퓨팅, 위치기반 서비스 등으로 개인정보처리가 늘어나고 빅데이터 분석 기법 및 인공지능 기술을 통해 대량의 개인정보가 실시간으로 사용되면서 다양한 가치 창출과

동시에 개인정보의 오남용으로 인한 정보주체의 피해 또한 늘고 있다. 선두로 EU GDPR은 이러한 기술 발전에 따른 정보 주체의 권리 강화를 위한 새로운 내용을 발표하였다. 정보주체의 개인정보자기결정권을 실질적으로 보장하기 위한 권리가 강화된 GDPR에 따라 개인정보 처리과정 시 내용을 고지하는 경우 정보주체가 쉽게 인지할 수 있도록 거듭 강조하고 있다. 또한 정보 주체가 자신의 정보를 이동할 수 있으며, 정보가 자동화된 방법으로 처리되고, 제3자에게 정보를 전달할 수 있도록 하는 개인정보이동권리를 통해 특정인에 의한 개인정보의 독점으로 사용되거나 정보주체의 동의 없는 무단 사용하는 것을 방지하였다. 또한 프로파일링 등 본인과 관련한 개인정보 처리를 언제나 반대할 수 있으며, 컨트롤러는 특별한 사유가 없는 한 이를 이행해야 하는 등 정보 주체가 자신의 정보에 대한 권리이행을 적극적으로 행사 할 수 있는 권리와 정보주체가 자동화 정보처리의 상황을 인지하기 쉽지 않은 상태에서 진행되기 때문에 개인정보를 침해할 가능성이 높고, 경우에 따라서는 개인의 인격적 존엄성과 자율성을 위협할 우려도 있음을 고려해 만들어진 권리를 포함하고 있다. 국내에는 이와 같은 정보 주체 권리가 존재하지 않는다. 하지만 해외 국가의 개인정보를 보유한 국내 기업 또한 GDPR과 같은 법의 적용 대상이 되면서 이를 포괄하는 국내의 표준 및 인증제도 기준 마련이 시급하다.

본 연구는 국내 기업이 국제적으로 급변하는 개인정보보호 환경에서 적절한 대응책의 한 방법으로 표준 및 인증제도 획득을 제시하고, 이를 위해 개인정보보호 관련 국제표준 및 인증제도의 분석과 개인정보보호의 국제적 환경 변화를 조사하여 국내 표준 및 인증제도의 발전 방향을 제시 하였다는 데 본 연구의 공헌도가 있다. 향후 이러한 국내 개인정보보호 관련 표준 사업 및 인증제도의 발전을 위해서는 정책적인 지지가 수반되어야 한다.

향후 연구에서는 본 연구에서 도출된 시사점을 반영하여 표준화 연구 이외에도 GDPR과 같은 국가 별 데이터보호법과 개인정보보호 국외이전의 환경에서의 기업의 개인정보 침해 사고의 예방 및 사후 문제 대처 방안을 개인정보보호의 거버넌스 측면에서 연구 될 필요가 있다. 또한 ICT 기술 발전으로 인한 새롭게 떠오르는 개인정보보호의 정보주체 주권 이슈 등을 국내 현황과 비교하여 추후 범국가적인 개인정보보호 기준을 고려한 방향 모색이 필요하다.

References

[1] J. W. Song, *Personal Information Leakage Incident ... Last year '40, 'near'* (2017), Retrieved Nov. 13, 2017, from http://www.ekn.kr/news/article.html?no=308336.

[2] G. B. Chun, *Personal information leakage accidents increase ... the importance of data security* (2017), Retrieved Nov. 13, 2017, from http://www.dt.co.kr/contents.html?article_no=2017051802100660049004

[3] *KISA Online Privacy Portal*, Retrieved Nov. 13, 2017, from https://www.i-privacy.kr/jsp/user4/intro/define3.jsp

[4] Personal Information Protection Committee, *2017 Annual Privacy Report* (2017), Retrieved Nov. 11, 2017, from http://www.privacy.go.kr/inf/rfr/selectBoardArticle.do?nttId=8086&bbsId=BBSMSTR_000000000044

[5] *EU GDPR*, Retrieved Oct. 18, 2017, from http://www.eugdpr.org/key-changes.html

[6] *Amazon Website Services*, Retrieved Oct. 18, 2017, from https://aws.amazon.com/ko/compliance/

[7] *Privacy Shield Framework*, Retrieved Nov. 10, 2017, from https://www.privacyshield.gov/welcome

[8] *CBPRs*, Retrieved Nov. 10, 2017, from http://www.cbprs.org/Agents/CBPRsRequirements.aspx

[9] *International Organization for Standardization*, Retrieved Nov. 20, 2017, from https://www.iso.org/benefits-of-standards.html

[10] H. R, Oh and Y. W. Kim, "ITU-T SG17 (Security) international standardization trend," in *Proc. KICS Winter Conf.,* pp. 1176-1177, 2016.

[11] H. Y. Yeom, "International privacy standardization trend analysis," *J. KIISC,* vol. 26, no. 4, pp. 6-10, 2016.

[12] H. Y. Yeom, "International privacy standardization trend analysis," *J. KIISC,* vol. 27, no. 5, pp. 43-48, 2017.

[13] ISO/IEC 29134:2017, Information technology — Security techniques — Guidelines for

privacy impact assessment.
[14] ISO/IEC 29100:2011. Information technology – Security techniques – Privacy framework.
[15] ISO/IEC 29190:2015, Information technology – Security techniques – Privacy capability assessment model.
[16] ISO/IEC 29101:2013, Information technology – Security techniques – Privacy architecture framework.
[17] ISO/IEC29151:2017, Information technology – Security techniques – Code of practice for personally identifiable information protection.
[18] BS 10012:2017, Data protection – Specification for a personal information management system.
[19] 'General Data Protection Regulation – European Commission.

최 보 미 (Bomi Choi)

2011년 8월 : 동국대학교 광고홍보학과 졸업
2014년 3월~현재 : 이화여자대학교 경영정보학과 석·박사 통합과정 (과정 수료)
<관심분야> 정보보호, 개인정보보호, 정보기술과 인간행동

채 상 미 (Sangmi Chai)

2003년 : 서울대학교 경영학과 석사
2009년 : The State University of New York at Buffalo, Ph.D in Management
2012년 3월~현재 : 이화여자대학교 경영학과 부교수 재직중
<관심분야> 정보기술과 인간행동, 정보보안과 조직, 빅데이터 분석

김 민 균 (Minkyun Kim)

2006년 : The State University of New York at Buffalo, Master of Science.
2010년 : The State University of New York at Buffalo, Ph.D in Management
2011~현재 : 서강대학교 경영학과 부교수 재직 중
<관심분야> 공급사슬관리, 정보기술의 활용, 리스크 재난위기관리

강 연 정 (Yeonjeong Kang)

2003년 2월 : 한양대학교 전자전기공학부 졸업
2006년 8월 : 한양대학교 수학과(암호학) 석사
2017년 2월 : 한양대학교 수학과(암호학) 박사과정 수료
<관심분야> 정보보호, 개인정보보호, 정보통신, 컴퓨터공학