韓國IT서비스學會誌
第18卷 第2號
2019年 6月, pp.55-73

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2019.18.2.055

ISMS-P와 GDPR의 개인정보보호 부문 연계 분석*

박민정** · 유지은*** · 채상미****

A Linkage Analysis of ISMS-P and GDPR; Focused on Personal Information Protection*

Minjung Park** · Jieun Yu*** · Sangmi Chai****

■ Abstract ■

The importance of the personal information has been increased, there have been a lot of efforts to establish a new policy, certification or law for administrating personal information more effectively and safely. Korean government has operated ISMS and PIMS certification system to assess whether an organization has established and managed appropriate information security system or not. However, it has been addressed the needs for revising and modifying of PIMS and ISMS. It is evaluated there are a few overlapped criteria to assess information management system in both ISMS and PIMS. ISMS-P certification, combining with ISMS and PIMS, is, finally, suggested, in the recent. GDPR is established having an aim of primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. This study compares GDPR and ISMS-P, focusing on "personal information". It can be expected to contribute as followings. This study can be a criterion for self-evaluation of possibility to violate of GDPR of a firm in preparation for ISMS-P. Second, this study also aims to increase the understanding of the role of ISMS-P and GDPR, among various certifications with the purpose of assessment of the information security management system, by reducing the costs required to obtain the unnecessary certification and alleviating the burden. Third, it contributes to diffusion of ISMS-P newly implemented in Korea.

Keyword : GDPR, ISMS, Information Security Certification, ISMS-P, Personal Information Protection, PIMS

Submitted : February 9, 2019 1st Revision : March 22, 2019 Accepted : June 3, 2019

* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A5A2A01039729).

** 이화여자대학교 일반대학원 경영학과 경영정보시스템 박사 수료

*** 이화여자대학교 일반대학원 빅데이터분석학 석사 과정

**** 이화여자대학교 경영학과 부교수, 교신저자

1. 서 론

기업이 보유한 개인정보를 비롯한 정보자산의 적절한 수립 · 관리 · 운영 여부에 대한 평가 필요성이 증가함에 따라, 이를 심사하기 위한 제도로 '정보보호 관리체계(ISMS, Information Security Management System)' 및 '개인정보보호 관리체계(PIMS, Personal Information Security Management System)'가 도입되었다. 이러한 인증제도는 각종 정보를 처리하는 기업의 정보보호 및 개인정보보호 관리체계를 객관적으로 평가하여 이에 대한 안전성을 담보하는 것에 주된 목적이 있다. 따라서 이러한 인증의 획득을 위한 기업의 노력은 기업의 정보보안 수준 향상을 유도하는 동시에 인증의 획득을 통하여 대외적으로 기업의 정보보안 수준을 보장 받을 수 있음에 따라, 기업 신뢰도 향상 및 경쟁력 확보를 도모한다. 그럼에도 불구하고, 정보보호 관리체계 인증제도를 획득한 기업이 대규모의 개인정보 유출 사고를 경험함에 따라, 기존 인증제도의 적절성 여부에 대한 논란이 지속적으로 제기되었다. 이에 2018년 11월, '정보보호 및 개인정보보호 관리체계 인증제도(ISMS-P)'가 새롭게 시행되어, 이에 대한 국내 보안 업계와, 기존의 관련 인증을 획득한 다수 기업의 관심이 증가하고 있다. 이는 각각 구분되어 운영된 기존의 ISMS와 PIMS 인증제도를 하나의 'ISMS-P' 인증제도로 통합한 것이다. ISMS와 PIMS는 심사 대상 항목이 유사함에도 불구하고 최근까지 분리되어 운영되어 온 탓에, 기업은 두 가지의 인증제도 획득을 위하여 중복 업무에 따른 효율성 저하, 높은 투자비용 등으로 인한 부담을 경험하였다. 이외에 과학기술정보통신부 소관의 ISMS와 행정안전부, 방송통신위원회 소관의 PIMS로 나뉘어 인증제도를 관리 및 심사함에 따라, 인증 심사기관의 재정 및 인력 낭비, 업무 연계 가능성을 저해 시켰다. 이에 따라, 정보보호와 개인정보보호 인증제도의 연계 필요성이 증가하는 동시에 점차 지능화, 고도화 되어가는 각종 정보 침해 위협에 대응하고자 ISMS와 PIMS의 통합이 추진되었고 그 결과, ISMS-P의 시행이 결정되었다. ISMS-P는 앞서 제시한 기존의 관련 인증제도가 가진 한계를 극복하여 기업의 재정 및 인력의 부담을 완화시켜 궁극적으로 기업의 전반적인 정보보안 수준을 향상시키고자 한다.

ISMS-P의 시행과 더불어 국내에서 주목받는 또 다른 정보보안 관련 제도는 ISMS-P와 유사한 시기에 도입된 유럽연합 일반개인정보보호법(GDPR, General Data Protection Regulation)이다. GDPR은 글로벌 ICT 기업의 데이터 독점에 대한 위험성을 완화시키고 디지털 시대에 적합한 새로운 개인정보보호 규제의 방향성을 제시한다는 점에서 전세계의 주목을 받고 있다(Park et al., 2018). 특히, GDPR은 28개의 유럽연합 회원국 전체에 대한 구속력을 갖는 법규인 동시에 역외 적용이 인정 된다. 또한 유럽연합의 모든 회원국이 의무적으로 준수하여야 하는 강행 규정이라는 점에서 권고 차원의 이전의 유럽연합 지침과는 구별된다. GDPR은 유럽연합 정보주체에게 서비스를 제공하거나 유럽 내 거주하는 정보 주체에 대한 모니터링을 실시하는 기업까지 GDPR의 적용 대상으로 규정하고 있음에 따라, 국내의 기업의 경우에도 유럽연합 회원국을 대상으로 비즈니스를 수행하는 경우, GDPR 준수 의무가 수반됨에 따라, 이에 대한 국내 기업의 관심은 지속적으로 증가하고 있다.

GDPR과 ISMS-P는 개인정보를 비롯하여 수집한 데이터를 적법한 보호 관리체계에 따라 처리 및 감독하기 위한 제도라는 점에서 도입 배경과 목적이 유사하다. GDPR과 ISMS-P는 개인정보 수집, 관리, 이용 및 파기의 개인정보 생명주기에 따라 개인정보 취급자가 준수하여야 하는 의무 및 개인정보 주체의 권리 방안 등에 대하여 공통적으로 다루고 있다. 이와 같이 ISMS-P의 심사 평가 주요 항목과 GDPR의 주요 원칙은 개인정보보호 관점에서 유사한 부분이 있는 동시에 차이를 보이는 경우도 존재한다. 예를 들어, ISMS-P의 인증제도는 국내 법률에 의거하여 인증제도 획득의 의무를 갖는 기업으로 하여금 관련 법령 준수와 더불어 해당

조직의 정보보호 관리체계에 대한 평균 수준을 보장 받을 수 있다. 이러한 인증 획득의 결과는 개인정보 처리자가 조직의 개인정보보호 수준 향상을 위하여 적극적으로 개인의 역할을 수행한 성과 즉, 개인정보 처리자의 의무 이행으로 인정받기 위한 심사 기준으로 고려할 수 있다. 그러나 GDPR은 보다 구체적으로 개인정보 처리자의 개인정보보호 활동에 대하여 제시함에 따라, 위와 같은 인증 획들을 위한 개인의 노력이 GDPR에 명시된 관련 사항을 모두 충족한 것으로는 판단하기 어렵다. 따라서, 두 제도 사이의 차이가 존재함을 추론할 수 있다. 이에 ISMS-P 인증을 획득한 국내 기업은 필요시, GDPR의 요건에 따라, 외국의 관련 인증을 별도로 취득해야 하는 부담이 발생할 수도 있다. 이에 두 제도에 대한 충분한 이해와 분석이 요구되는 시점이다.

본 연구에서는 두 제도에서 다루는 개인정보보호 평가 지표 및 조항에 주목하여 이에 대한 연계 분석을 수행하고자 개인정보 생명주기, 개인정보보호 특징 및 두 제도의 형성 목적 등을 바탕으로 기준 항목을 선정하여 분석 프레임워크를 구축하고자 한다. 이를 바탕으로 두 제도가 규제하는 개인정보보호에 대한 체계, 범위, 처리 절차에 대한 공통점 및 차이점의 매칭 분석 작업이 이루어질 예정이다.

본 연구의 주요 목적은 최근 새롭게 국내에 시행된 ISMS-P와 GDPR의 개인정보보호 부문에 대한 연계 가능성을 밝히는 것이다. 이를 통하여 본 연구는 다음과 같은 시사점을 갖는다. 첫째, 본 연구 결과는 ISMS 인증 의무 대상자가 ISMS-P 획득을 준비하는 과정에서 이와 동시에 기업의 GDPR 위반 가능성을 스스로 진단 및 평가할 수 있는 기준이 된다. 둘째, 본 연구는 개인정보보호 관리체계의 평가 목적을 갖는 다양한 제도 혹은 인증들 가운데 ISMS-P와 GDPR 의 역할에 대한 이해를 높여 기업의 불필요한 인증 획득에 요구되는 투자비용의 감소 및 업무 부담을 경감시키는데 기여한다. 셋째, 새롭게 시행되는 ISMS-P의 국내 정착과 확산에 본 연구가 기여하는 동시에 이는 ISMS-P 획득을 목표로 하는 국내 기업의 심사 대비를 지원한다. 더불어 국내 기업의 GDPR에 대한 이해와 효과적인 준수 방안 마련에 기여하고자 한다. 마지막으로, 본 연구는 향후 정보보호 및 개인정보보호 관리체계 관련 신규 인증 및 표준의 제정에 토대가 된다.

2. 정보보호 및 개인정보보호 인증에 대한 선행 연구

2.1 정보보호 및 개인정보보호 인증

정보보호 및 개인정보보호는 각종 정보 및 개인정보를 비롯한 정보 시스템의 기밀성(Confidentiality), 가용성(Availability), 무결성(Integrity)을 보장하여 이를 안전하게 보호하는 것이다(Pfleeger and Pfleeger, 2006). 따라서, 이와 같은 정보보안의 상태를 위협하는 다양한 요인을 미리 발견하여 잠재적으로 발생 가능한 손실 및 피해를 예방하는 것이 정보보호 활동의 목적이며 이를 위한 한 가지 방안이 정보보호 및 개인정보보호 인증의 획득이다.

정보보호 및 개인정보보호 인증은 각 인증제도를 주관하는 인증기관의 심사 기준에 의거하여 이에 적합하다고 판단되는 경우, 기업에게 해당 인증을 부여하는 것이다. 구체적으로 조직이 보유한 정보 자산에 대한 안전성 및 신뢰성을 제고하기 위한 절차와 과정을 체계적으로 수립하여 이를 바탕으로 지속적으로 관리 및 운영함에 따라, 정보보호의 목표인 정보의 기밀성, 무결성, 가용성의 확보를 위한 활동이 정보보호 관리체계(ISMS) 이다(Jang and Lee, 2010; Park and Kim, 2015; Oh, 2018). 이에 따른 적합성을 기업이 인정받는 경우, 획득하는 것이 ISMS 인증제도이다. 즉, 정보보호/개인정보보호 관리체계 인증제도는 기업이 수립하여 운영하고 있는 정보보호/개인정보보호 관리체계가 일정한 인증 심사 기준에 적합한지 여부를 제3자인 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 판단하는 제도이다(Kang, 2014). 따라서, 정보보호/개인정보보호

인증 획득은 조직의 정보보안 수준을 객관적으로 평가하기 위한 절차로 조직의 정보 자산이 외부의 위협으로부터 적절히 보호되고 있으며, 이에 따라 안전하게 서비스를 제공할 수 있음을 대외적으로 입증한다(Park et al., 2016). 또한, 정보보안 인증은 조직의 정보보안 수준을 잠재적인 경쟁 기업 혹은 비즈니스 파트너와의 비교를 통하여 획득한 성과로 해당 인증의 취득을 통하여 고객의 신뢰를 확보할 수 있다(Von Solms, B., 2001).

2.2 해외 주요 개인정보보호 인증제도

개인정보보호 관련 인증제도를 가장 우선적으로 채택한 사례는 일본의 프라이버시마크 제도이다(Park et al., 2011). 이는 사업자의 개인정보 취급 방식과 운영의 적절성을 기준으로 하여 기업의 개인정보보호 체계가 적합하다고 판단되는 경우에 한하여 부여하는 인증제도이다. 현재는, 일본정보처리개발협회(JIPDEC)가 인정 및 인증기관의 역할을 병행하고 있으나 정부의 주도로 1998년 처음 도입되었다. 서류 심사 중심으로 이루어지며 심사 기준은 JIS Q 15001의 '개인정보보호 경영 시스템-요구 사항'기반으로 진행된다. 또한 해당 심사 요건에는 개인정보보호법 등 법령의 준수를 위한 사항도 평가 기준으로 다수 포함되어 있다. 따라서 프라이버시마크 제도의 취득은 기업의 개인정보 관리 체계가 적절히 운영되고 있음을 거래처나 소비자에게 입증할 수 있다는 인증제도의 본래 이점과 더불어 일본의 개인정보보호법령의 준수를 도모한다는 추가 이점이 있다.

미국의 BBB Online 프라이버시 인증은 사업자의 이용자에 대한 개인정보보호 의지와 실행 능력을 중점적으로 평가하기 위하여 형성된 인증제도이다. 공신력 있는 기관으로부터 주기적으로 개인정보 관리 상태에 대한 점검을 받고 이에 따른 인터넷 비즈니스를 사용하는 소비자의 신뢰를 확보하기 위하여 형성되었다 (Jang et al., 2011). 따라서 BBB Online 프라이버시 인증은 인터넷 비즈니스를 사용하는 사용자의 신뢰성을 제고하고자 미국 경영개선협회 이사회(Council of Better Business Bureaus)에 의하여 개설되었다. BBB Online 프라이버시 인증 심사 항목은 1) 개인정보보호 범위 및 이행, 2) 정보 수집, 3) 접속 및 수정 데이터 관리, 4) 행위 정보의 관리, 5) 정보의 통합 가능성 여부, 6) 예측 정보, 7) 정보 접근 제한, 8) 민감정보 처리 9) 아동 개인정보, 10) 개인정보의 공유 여부 등이다. 이외에 미국은 TRUSTe 인증제도를 추가적으로 운영하고 있다. 이는 Electronic Frontier와 CommerceNet가 설립하여 공동으로 운영하는 대표적인 온라인 인증 제도로 주로, 미국의 개인정보보호방침에 따라 사업자가 개인정보를 적절하게 수집 및 활용하고 있는지의 여부를 점검 한다. 따라서 해당 인증제도는 미국 상무부와 연방거래위원회 및 관련 업계의 자율규제안에 의하여 마련된 원칙인 1) 개인정보보호 대책의 채택과 이행, 2) 개인정보의 수집과 사용에 대한 통지와 공시, 3) 선택과 동의 (이용자가 자신의 정보를 통제할 수 있는가의 기회 부여), 4) 개인 식별 정보의 보안성과 정확성에 대한 보호 수단 강구의 항목으로 이루어져 있다.

영국은 영국왕립표준협회(BIS)에서 제안한 BS 10012 인증을 제정하여 개인정보보호 관리체계의 국가 표준으로 인정받았다. BS 10012는 조직 전체를 아우르는 정보 거버넌스 인프라의 일부분으로써, 데이터보호 요구사항을 준수하기 위한 프레임워크인 개인정보경영시스템(PIMS : Personal information management system)을 제대로 구축하고 올바르게 적용되는가를 주로 평가한다(Cha et al., 2012). 이는 개인정보의 효과적 관리체계를 평가하기 위한 것으로 영국의 개인정보보호법인 DPA (Data Protection Act)와 PDCA(Plan-Do-Check-Act) 프레임워크를 기반으로 심사한다는 점에서 일본의 프라이버시 마크 인증제도와 유사하게 자국의 개인정보보호법을 해당 인증제도의 심사 기준 요건으로 반영하고 있다. 최근에는 기존의 BS10012에 GDPR의 내용을 반영한 BS10012 : 2017을 발표하여 시행중이다(Choi et al., 2018).

3. ISMS-P 인증 및 GDPR

3.1 ISMS-P 인증

ISMS-P는 정보보호 관리체계 인증(ISMS)과 개인정보보호 관리체계(PIMS)를 통합한 인증제도로 ISMS, PIMS 인증기준의 유사 공통 항목을 통합하고 개인정보 특화 항목을 분리하였다.

ISMS-P는 융합화, 지능화 되고 있는 침해 위협에 효과적으로 대응하기 위하여 정보보호와 개인정보보호의 연계 필요성을 바탕으로 형성되었다. 또한 ISMS와 PIMS 인증 내용이 일정 부분 유사하거나 동일함에도 각각 인증을 받아야 하는 기업의 중복 부담을 완화하기 위하여 ISMS-P의 도입이 추진되었다. 기존의 ISMS 104개 인증기준 중, 82개 항목이 PIMS 인증기준과 동일하거나 유사하였으며, PIMS 86개 인증기준 중 58개 항목이 ISMS 인증 기준과 동일하거나 유사하다. 이에 ISMS-P는 ISMS와 PIMS의 관리과정 영역 및 보호대책 영역을 80개 인증기준으로 통합하였으며 (ISMS-P 內, 1. 관리체계 수립 및 운영, 2. 보호대책 요구사항), PIMS의 생명주기 영역을 22개 인증기준의 특화항목(ISMS-P 內, 3. 개인정보 처리단계별 요구사항)으로 포함시킴에 따라, 총 102개의 인증 기준 체계를 마련하였다. 또한 클라우드 서비스, 핀테크, 침해사고 탐지 강화 등과 같은 최신 기술 및 이슈 및 법 개정에 따른 요구사항을 반영하여, 1. 관리체계 수립 및 운영, 2. 보호대책 요구사항, 3. 개인정보 처리단계별 요구사항의 주요 지표로 심사하고 있다. ISMS-P의 상세 심사항목은 다음의 <Table 1>을 통하여 제시한다.

나아가 ISMS-P는 인증체계, 인증기준, 인증·심사기관 등 인증제도 전반의 실질적인 통합을 이루어 기존의 ISMS와 PIMS의 심사기관이 구분되어 저하된 업무의 효율성 및 연계성을 향상 시키고자 한다. 따라서, ISMS-P는 과학기술정보통신부와 행정안전부, 방송통신위원회 3개 부처로 구성된 '협의회'를 통하여 인증기관 및 심사기관 지정, 심사원 관리 등 제도 전반에 관한 정책결정 및 관리를 공동으로 처리할 예정이다. ISMS-P의 시행은 '정보통신망 이용 촉진 및 정보보호등에 관한 법률' 제 47조 및 '개인정보보호법' 제 32조의 2에

〈Table 1〉 Certification Criteria of ISMS-P

Certification Criteria	
1. Establishment of Information Security Management System Policies and Implementation (16)	1.1 Establishment of Management System (6) 1.2 Risk Management (4) 1.3 Management System Operation (3) 1.4 Inspecting and Improving Management System (3)
2. Requirements of Protection Measurements (64)	2.1 Policies, Organizations, Asset Control (3) 2.2 Personnel Security (6) 2.3 Security of External Parties (4) 2.4 Physical Security (7) 2.5 Authentication and Authorization Management (6) 2.6 Access Control (7) 2.7 Cryptography Control (2) 2.8 System Development Security (6) 2.9 System Operation Security (7) 2.10 System and Service Security Management (9) 2.11 Accident Prevention and Response (5) 2.12 IT Disaster Recovery Planning (2)
3. Requirements of Personal Information Processing (22)	3.1 Protection Measures in Collecting Personal Information (7) 3.2 Protection of Personal Information and Use (5) 3.3 Protection Measures in Provision of Personal Information (3) 3.4 Protection Measures in Deletion of Personal Information (4) 3.5 Protection of Personal Information Subject Rights (3)

따른 법적 근거를 갖는다. 따라서 해당 법률에 의거하여, 기존에 ISMS 인증 의무대상자인 1) 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망 서비스를 제공하는 자, 2) 정보통신망법 제46조에 따른 집적정보통신시설 사업자, 및 다음 조건에 최소 하나라도 해당되는 경우로 3.1) 연간 매출액 또는 세입이 1,500억 원 이상인 자 중에서 「의료법」 제3조의4에 따른 상급종합병원 혹은 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교, 3.2) 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도 기준) 매출액이 100억 원 이상인 자, 3.3) 전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만 명 이상인 자의 경우 ISMS-P 혹은 ISMS를 의무적으로 획득하여야 한다.

3.2 GDPR 제정 목적 및 배경

GDPR은 유럽연합 회원국 28개에 일괄 적용되는 법률로 유럽연합의 모든 개인에 대한 데이터 보호를 강화함에 따라, 정보주체의 권리를 증진시키는 동시에 유럽연합 기업의 규제 비용 완화 및 유럽연합 내 전자상거래 활성화 촉진을 목표로 2018년, 공식적으로 시행되었다(Tikkinen-Piri et al., 2018). 이전의 유럽 개인정보보호 지침 수준의 규제와 달리 GDPR은 회원국 정부에서 따로 법률을 제정하지 않아도, 곧바로 구속력을 갖고 적용될 수 있다는 점에서 강력한 특징이 있다(Park et al., 2018). 또한 GDPR은 기존에 유럽연합 내에 다양하게 존재하던 각종 개인정보보호 관련 규제를 통합하여, 개인정보에 대한 통제권을 해당 개인에게 돌려주고 국제 비즈니스를 위한 개인정보보호 규제 환경을 단순화하고자 한다(Ryu, 2016).

3.3 GDPR 적용 대상 및 범위

GDPR은 유럽연합 거주자의 개인정보를 다루는 모든 기업이나 단체가 개인정보보호와 관련된 GDPR의 광범위한 규정들을 준수하도록 강제하는 것이 핵심이다(Cho, 2018). 특히, 본 규정의 이전의 관련 규제 및 지침과 구별되는 가장 큰 특징은 유럽연합 소속 거주민의 데이터를 취급하는 모든 외국 기업도 GDPR 준수 적용 대상이 된다는 점이다. 따라서 유럽연합 전반에 공통적인 규정을 적용하는 것을 넘어, 비유럽 기업들의 경우에도 GDPR 준수 의무가 수반되는 경우, 유럽연합 국가와 동일한 규정에 따라 데이터 보호 업무를 진행하게 된다. 따라서, GDPR의 적용 대상은 유럽연합 회원국과 더불어 1) 유럽연합 회원국에 사업장을 운영하는 기업, 2) 해당 국가에 사업장은 없지만, 인터넷 홈페이지를 통해 유럽연합 회원국에 거주하는 주민에게 상품 및 비스를 제공하는 기업, 3) 유럽연합 회원국에 거주하는 주민의 행동을 모니터 하는 기업이다. 즉, 데이터 관리 기관(Data Controller, 유럽연합 거주자로부터 데이터를 수집하는 조직이나 처리 기관), 데이터 처리 기관(Data Processor, 데이터 관리 기관을 대신하여 데이터를 처리하는 조직) 및 데이터 주체(개인)가 유럽연합 지역에 거점을 두는 경우이다(Kisa, 2018).

3.4 GDPR 주요 원칙 및 조항

3.4.1 개인정보 처리 원칙

GDPR은 처리의 적법성(Lawfulness of Processing)을 확보하기 위해서 '적법성, 공정성, 투명성의 원칙, 목적 제한의 원칙, 개인정보 처리의 최소화 원칙, 정확성의 원칙, 보관기간 제한의 원칙, 무결성 및 기밀성, 책임성'의 개인정보의 처리 원칙을 제시한다(GDPR 제 5조, 개인정보 처리 원칙). 즉, 개인정보의 주체와 관련해서 개인정보는 적법한 절차에 따라 공정하고 투명하게 처리되어야 하며, 타당한 목적에 따라 개인정보 수집은 이루어져야 하며, 특수한 경우를 제외하고는 해당 목적과 상충되는 방식으로 추가 처리가 이루어져서는 아니 된다는 것이다. 또한 개인정보 처리는 목적과 관련이 있고 적절해야 하며 필요한 범위에서

최소한으로 제한되어야 하며 부정확한 개인정보에 대해서는 즉각적인 삭제 또는 정정하는 등 타당한 조치를 취할 것을 규제한다. 나아가 개인정보 처리 목적에 필요한 기간이 지난 후에는 보관할 것을 금지하고 있으며 적절한 기술적·조직적인 조치를 활용하여 개인정보가 보호될 수 있음을 보장하여야 함에 따라, 데이터 관리 및 처리 기관은 상기 원칙을 준수할 의무와 이를 필요시 입증할 수 있어야 하는 책임이 있다.

3.4.2 동의(Consent)

GDPR은 이전의 개인정보보호 법규에 비하여 '동의' 방법의 적법성을 구체적으로 기술함에 따라, 이전에 비하여 요건이 강화되었다. 동의는 정보 주체가 진술(statement) 또는 적극적 행동(affirmative action)을 통하여 분명하게 의사 표시가 이루어져야 함에 따라, 모호하지 않아야 하고(unambiguous), 명확하고 적극적인 행위(clear affirmative action)에 따라 이루어져야 한다(GDPR 제 7조, 동의). 개인정보 처리가 동의에 근거한 경우, 데이터 관리 기관은 정보 주체가 자신의 개인 데이터 처리에 동의했음을 입증할 수 있어야 한다. 동의의 역할에 대하여 보다 자세히 살펴보면, GDPR은 동의는 적법한 개인정보 처리 근거 중 하나로서 명시적 동의는 민감 정보의 처리, 프로파일링을 포함한 자동화된 결정 또는 개인정보 역외 이전 관련 처리의 적법한 근거로 인정한다. 동의 의무 위반과 같은 중요한 사항에 대한 위법은 전 세계 연간 매출액의 4% 혹은 2천만 유로(약 250억 원) 이하의 과징금 중 더 큰 금액으로 기업에게 부가된다. 동의는 또한 정보 주체에게 본인의 개인정보 처리에 관해 실질적인 선택권과 통제권을 부여하는 것을 뜻하므로 개인에게 실질적인 선택권이 없다면 유효한 동의로 볼 수 없다. 따라서 동의 거부에 따른 불이익이 없어야 하고, 정보 주체는 언제든지 자신의 동의를 철회할 권리를 가진다. 철회에 대한 동의는 철회 전에 동의에 근거한 처리의 적법성에 영향을 미치지 않는다.

3.4.3 민감정보(Special Categories of Personal Data)

정보주체의 명시적 동의가 있는 경우, GDPR에 표기된 제한적인 경우 및 회원국 법률에 따른 경우를 제외하고는 GDPR은 민감정보의 처리를 원칙적으로 금지 한다(GDPR 제 9조, 민감정보의 처리). GDPR이 정의하는 민감정보는 개인의 정치적 견해, 인종·민족, 종교·철학적 신념, 노동조합 가입여부, 유전자 정보, 생체정보, 건강정보, 성적 취향 등에 관한 정보를 포함한다.

3.4.5 정보주체의 권리

GDPR은 정보에 대한 열람권, 정정권, 삭제권, 처리 제한권, 개인정보 이동권, 반대권, 프로파일링 거부권 등을 통하여 정보주체의 권리를 보장하고 있다(GDPR 제12~22조, 정보주체의 권리 강화). 정보주체는 본인에 관한 개인정보의 삭제 및 이에 대한 처리의 제한 및 차단을 요구할 수 있는 권리가 있으며 본인의 개인정보를 본인 혹은 다른 사업자에게 전송할 수 있도록 스스로 결정할 권한을 보장 받는다. 그리고 본인에게 중대한 영향을 미치는 사항에 대하여 자동화된 처리에 의해서 결정되는 방식의 프로파일링을 거부할 수 있는 권리가 있으며 프로파일링의 프로세스가 어떻게 구현되는지 명확하고 간략하게 설명 받을 수 있는 정보 제공권이 정보주체의 권리로 함께 주어진다.

3.4.6 개인정보 역외이전

GDPR이 인정하는 역외 이전의 경우는 다음과 같이 제한되어 있다(GDPR, 제40-48조, 개인정보 역외 이전). 먼저, 적정성 결정(Adequacy Decision)을 통하여 개인정보보호 관련 법제가 적절한 수준의 보호를 보장하고 있다고 입증된 국가로 이전할 경우에는 개인정보의 역외 이전을 인정하고 있다. 또한 '적절한 보호조치(Appropriate Safeguards)'인 표준 개인정보보호 조항(Standard Data Protection Clauses), 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules), 승인된 행동규약(Codes

of Conduct) 및 인증(Certification) 등을 포함한 경우 역시 적법한 역외 이전이다. 이외의 특정 상황에 대한 예외(Derogations for specific situations)의 경우에 대해서는 명시적 동의(explicit consent)가 있거나, 계약의 이행 또는 정보주체의 요청으로 필요한 경우 및 공익의 중요한 이유 등과 같은 특정 상황에 해당하는 경우에 역외 이전이 가능한 것으로 간주 한다(GDPR, 제49조, 역외 이전 시 특정 상황에 대한 예외 조항). 이외에도 GDPR은 개인정보보호법과 관련 실무에 대한 전문적 지식과 업무 수행 능력을 보유한 전문가를 DPO(개인정보보호책임자)로 지정하도록 하여 기업의 개인정보 처리 활동의 기록, 개인정보 영향평가 등 기업의 책임성 강화를 위하여 노력할 것을 강제하고 있다(GDPR 제 37조, DPO의 지정).

4. ISMS-P 인증과 GDPR 개인정보 보호 연계 분석

4.1 ISMS-P와 GDPR 연계 분석 프레임워크 구축

본 연구에서는 ISMS-P와 GDPR의 연계 분석을 수행하기 위하여 개인정보 생명주기, 개인정보보호 특징, GDPR과 ISMS-P의 형성 목적을 각각 바탕으로 다음의 <Table 2>와 같은 분석 프레임워크를 구축하였다.

개인정보 생명주기는 개인정보의 수집-관리-이용/제공-파기의 흐름에 따라 개인정보보호가 이루어질 것을 권장하기 위하여 구축된 모델로 개인정보의 처리 과정을 모두 포함하였다는 장점이 있다(Jang et al, 2012). 적법한 원칙에 의거하여 개인정보를 물리적, 기술적 차원에서 관리하는 것도 중요하나, 점차 개인정보 보유 자체에 따라, 개인정보 처리 기업에게 요구되는 의무 사항이 증가하는 추세이다. 예를 들어, 개인정보 주체의 요구가 있을 경우, 개인정보 처리 담당자는 신속하게 처리하고 있는 개인정보 현황 및 상태를 주체에게 통지하여야 하는 의무 등이 존재한다. 이에 본 연구가 제시한 분석 프레임워크는 '개인정보 관리' 차원을 넘어 '개인정보 보유 및 이용'의 기준 항목을 포함하였다. 이외에 ISMS-P와 GDPR은 개인정보의 전처리 과정에 개인정보주체의 권리 보장 및 강화를 공통적으로 가장 우선시할 것을 권장함에 따라, '정보 주체의 권리 보호' 항목을 추가하여 본 연구의 분석 프레임워크를 구성하였다. 이렇게 구축된 프레임워크의 분석 기준 항목을 바탕으로 GDPR과 ISMS-P를 비교한다.

4.2 개인정보 수집

4.2.1 개인정보 수집 제한

'개인정보 수집'에 대한 항목을 살펴보면, ISMS-P와 GDPR은 모두 공통적으로 적법한 처리 원칙 혹은 법령에 근거한 처리의 기준을 바탕으로 필요한 범위 내에서 최소한으로 개인정보를 수집 할 것을 규정하고 있다. 하지만 GDPR은 개인정보의 수집, 저장, 변경, 삭제, 공개, 전송, 결합 등을 포함하는 개인정보를 이용한 모든 활동을 '개인정보 처리'로 통칭

〈Table 2〉 Framework for Analysis

Criteria for analysis	Definition
Collection	Collects the minimum personal information through legitimate consent process
Usage & Management	Manage and store personal information through legitimate procedures and methods
Provision	Provide no personal information to any third party without user's prior consent or legitimate process
Deletion	Deletion of personal information by the correct and legitimate principle of service provider
Protection of Personal Information Subject Rights	The right of the subject of personal information should be the highest priority in all processes related to personal information

하여 기술하는 반면에 ISMS-P는 개인정보의 수집, 처리, 관리 등을 별도의 기준 항목으로 각각 분류하여 심사 항목을 구성하였다는 점에서 차이를 보인다.

GDPR은 온라인에서 개인정보를 수집하는 시점에 개인정보보호 정책・고지에 대한 링크를 제공하거나, 개인정보를 수집하는 동일 페이지에서 해당 내용을 제시할 것을 강제 한다(GDPR 제29조 작업반). 이는 GDPR이 개인정보 수집 과정에서 정보주체에게 관련 사안에 대한 고지 의무를 수행함에 따라, 정보주체의 정보를 제공받을 권리(GDPR 제13-14조)의 보장을 시사한다. 그러나 ISMS-P의 경우, 개인정보 수집 시, 정보주체에 대한 고지를 통한 정보주체의 권리 확보가 아닌 동의를 위하여 요구되는 한 가지 절차로 관련 사안의 고지를 권고하고 있다. 즉, GDPR은 개인정보 수집 관련 정보를 고지 받은 후, 수집의 동의 여부를 결정하는 메커니즘이라면 ISMS-P는 정보주체가 동의에 대한 의사표시를 하기 위한 선행 요건의 하나로 개인정보 처리자의 고지 의무 이행이 이루어지는 것으로 해석 가능하다. 이는 GDPR과 ISMS-P가 개인정보 수집 과정에서 요구되는 '고지 의무'에 대한 역할과 이에 대한 비중의 차이를 추론할 수 있다.

GDPR과 ISMS-P는 공통적으로 정보주체가 수집 목적에 부합한 최소한의 정보에 제한되어 수집이 이루어질 것을 강력히 규정하고 있으며 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공 거부 등의 불이익을 정보주체가 입지 않도록 하여야 함을 제시한다.

4.2.2 개인정보 수집 동의

개인정보 수집을 위한 '동의'의 차원에서 ISMS-P와 GDPR은 모두 동의의 방법과 요건을 강조한다. ISMS-P는 개인정보 수집에 대한 동의가 적절한 방식과 절차에 따라 이루어졌는지를 평가하기 위하여 수집에 대한 동의 존재 여부, 동의 기록에 대한 보관 여부 등을 심사하고 있다. 이에 반하여 GDPR은 동의를 1) 자유롭게 부여된 동의, 2) 개별적으로 특정한 동의, 3) 사전 정보가 제공된 동의, 4) 정보주체의 명확한 의사표시로 나누어 유효한 동의의 종류를 세분화화고 있다는 점에서 포괄적으로 승낙 여부의 일종으로 동의를 다루는 ISMS-P과는 차이를 보인다. 또한 GDPR은 정보주체의 의사표시가 모호하지 않고(unambiguous), 명확하고 적극적인 행위(clear affirmative action)로 이루어져야 하는 것으로 동의를 정의함에 따라, ISMS-P에 비하여 동의의 방법을 정확하게 기술하고 있다. '동의의 철회'에 대해서도 GDPR은 '삭제권'을 바탕으로 개인이 동의를 철회한 경우 적용될 것을 인정하고 있으며(GDPR 제17조 1항b), 직접 마케팅 목적의 처리의 경우 예외적으로 정보주체는 데이터 처리에 '반대권'을 행사하여 동의를 철회할 수 있도록(GDPR 제 21조 1항) 동의 철회 방법과 보장의 경우를 기술하고 있는 반면에 ISMS- P는 동의 철회의 방법 등에 대해서는 구체적으로 언급하고 있지 않다.

ISMS-P는 정보주체의 동의를 받거나 관계 법령에 따라 적법하게 개인정보를 수집하여야 할 것을 밝히며 만 14세 미만 아동의 개인정보를 수집할 경우에는 법정대리인의 동의를 받아야 함을 명시하고 있다. GDPR 역시, 아동의 경우 개인정보 처리에 따른 특수한 위험성이 존재함을 인정함에 따라, 개인정보와 관련하여 특별한 보호가 필요함을인정한다(GDPR 제38조). 그러나 ISMS-P는 만 14세 미만의 아동의 개인정보를 수집하는 경우, 법정대리인의 동의를 받을 규정한 것에 반해, GDPR은 만 16세 미만의 '아동에게 직접' 정보사회서비스(information society services)를 제공할 때 부모 등 친권을 보유하는 자(holder of parental responsibility)의 동의를 받도록 요구하고 있어 GDPR과 ISMS-P가 규정하는 '아동'의 연령이 다르다. 특히, GDPR은 유럽연합 회원 국가의 개별 법률에 따라 친권자 동의를 요하는 아동의 연령 기준을 만 13세 미만까지 낮추어 규정할 수 있도록 하여 국가별 아동 규정의 폭을 넓게 인정하고 있다는 점을 알 수 있다.

4.2.3 주민등록번호 처리 제한

ISMS-P는 주민등록번호는 법적 근거가 있는 경우를

제외하고는 수집 · 이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체 수단을 제공하여야 함을 밝히고 있다. 그러나 주민등록번호의 경우, 국내 정보주체의 고유한 개인정보 유형으로 GDPR에서는 이를 동일하게 다루고 있지 않다. 단, 주민등록번호는 개인 고유식별번호의 한 종류임에 따라, 다음의 4.2.4절인 민감정보 처리 항목에서 추가적으로 분석하고자 한다.

4.2.4 민감정보 및 고유식별정보의 처리

ISMS-P는 민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아 수집 및 처리 하도록 한다. 그러나 GDPR은 민감정보를 처리하는 경우에 있어서 처리가 가능한 별도의 경우(GDPR 제9조 제2항)를 제외하고는 민감정보의 처리를 원칙적으로 금지하고 있다. 이에 GDPR과 ISMS-P는 '민감정보 처리 허용 범위'의 차이를 확인할 수 있다. GDPR은 해당 법령 내에 기술된 예외의 경우를 제외하고는 민감정보의 처리를 금지하고 있으나 ISMS-P는 정보주체의 동의가 있을 경우, 민감정보 처리의 일부를 인정한다는 점에서 다르다. GDPR이 예외적으로 인정하는 민감정보의 처리 가능 경우는, 정보주체의 명시적 동의가 수반된 경우, 공익을 위한 기록 보존 목적, 고용, 사회 안보나 사회보장 및 사회보호법 상의 의무 이행이 필요한 경우, 물리적 또는 법적으로 동의를 할 능력이 없는 정보주체의 중대한 이익을 보호하기 위하여 필요한 경우 등을 비롯하여 원문에 기재된 제한된 사례의 경우에 한하여 가능하다.

4.2.5 영상정보처리기기 설치 · 운영

ISMS-P는 영상정보에 대한 수집 시, 준수하여야 할 항목을 별도로 규정한다. 즉, 영상정보처리기기를 공개된 장소에 설치 · 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립 · 이행하여야 할 것을 제시하였다. 그러나 GDPR의 경우, 앞서 제시된 제5조, 개인정보 처리의 원칙에 개인에 대한 영상물을 개인정보로 명시하여 해당 조항에 따라 처리(수집, 보관, 파기 등)할 것으로 기술하였다. ISMS-P는 영상정보 처리를 위한 해당 물리보안 차원까지 다루는 것에 반하여, GDPR은 개인정보의 항목으로 영상정보를 포괄적으로 인정하여 이에 따른 적합한 처리 규정 원칙을 준수할 것을 강제한다. 이에 따라 각각 영상정보를 정의하는 방식에 있어 차이가 있음을 확인할 수 있다.

4.3 개인정보 보유 및 이용

4.3.1 개인정보 현황관리

ISMS-P는 수집 · 보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황의 정기적 관리 및 공공기관의 경우 법률에서 정한 관계기관의 장에게 등록할 것을 규정하고 있다. GDPR은 수집 및 보유한 개인정보의 관리 항목에 대하여 앞서 제시하였던 제5조 개인정보의 처리 원칙에 따라, 1) 적법성 · 공정성 · 투명성의 원칙, 2) 목적 제한의 원칙, 3) 개인정보 처리의 최소화, 4) 정확성의 원칙, 5) 보유 기간 제한의 원칙, 6) 무결성과 기밀성의 원칙, 7) 책임성의 원칙에 따라 가장 우선적으로 개인정보를 처리하도록 하고 있다. 추가적으로 GDPR은 제24조 및 제28조, 제29조를 통하여, 개인정보를 다루는 컨트롤러와 프로세서의 역할에 따른 의무를 제시하여 수집된 개인정보의 기술적 · 관리적 조치 방안에 대하여 구체적으로 기술하고 있다. 컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 주체를 의미하며 GDPR은 이러한 컨트롤러의 역할을 제시함에 따라 개인정보 처리의 성격 · 범위 · 목적 · 위험성 등을 고려하여 개인정보의 처리가 GDPR을 준수하여 수행되는 것을 보장하고, 이를 입증할 수 있는 적절한 기술적 · 관리적 조치를 이행할 것을 강제한다. 프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 자연인, 법인, 정부부처 및 관련기관, 기타 단체 등을 의미하며, 프로세서는 컨트롤러의 지시에 따라 개인정보를 처리한다. 특히, 프로세서의 개인정보 처리 과정에서 준수하여야 하는 의무사항과 원칙은 제28조

제3항의 '프로세서의 의무'를 통하여 8가지로 상세하게 제시한다는 점에서 ISMS-P에 비하여 구체적인 개인정보 관리 원칙을 기술하고 있다. 개인정보 처리자의 세부 심사 기준을 각각 살펴보면, ISMS-P의 경우, 대다수 공공기관의 개인정보 현황 관리를 중점적으로 평가하는 반면에, GDPR은 공공과 민간기업의 구분 없이 처리 현황을 감독하는 점은 서로 상이하다.

4.3.2 개인정보 품질보장

ISMS-P는 수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리 절차를 제공하도록 한다. 이는 GDPR의 제5조 개인정보 처리의 원칙에 따라, 개인정보의 처리는 정확하여야 하며, 필요 시 처리되는 정보는 최신으로 유지되어야 하는 것과 유사하다. 즉, 처리 목적에 비추어 부정확한 정보의 즉각적인 삭제 또는 정정을 보장하기 위한 모든 합리적 조치가 취해져야 한다는 1.4 정확성의 원칙 및 1.6 무결성과 기밀성의 원칙에 준수하여야 한다는 것이다.

4.3.3 개인정보 표시제한 및 이용 시 보호조치

ISMS-P가 제시한 개인정보 표시제한 및 이용의 보호조치는 인쇄, 화면표시, 파일생성 등의 개인정보 조회와 출력 과정에서 발생하는 개인정보 이용의 방법에 대하여 기술한다. 특히, 최근 빅데이터 분석의 적용 사례가 증가하는 시대적 상황에 따라, 이에 대한 과도한 개인정보의 이용을 방지하는 동시에 이에 따른 개인정보 식별의 가능성을 완화시키고자 하는 것으로 해석할 수 있다. 이와 유사하게 GDPR은 제22조 프로파일링을 포함한 자동화된 의사결정 조항과 제5조 제1항(c) 개인정보 처리의 최소화 원칙에 따라, 프로파일링에 활용되는 개인정보 수집 및 보유 사유를 명확히 입증할 수 있거나, 집합정보 또는 익명 처리된 정보를 사용 하여 적절한 보호조치를 보장하도록 하여 수집된 개인정보에 대한 식별 가능성을 방지하고 목적 이외의 개인정보에 대한 과도한 분석을 금지하고 있다. 또한 제5조제2항의 목적 제한의 원칙은 공익을 위한 기록보존 목적, 과학적·역사적 연구 목적 또는 통계 목적에 한해서만 추가 개인정보 처리가 가능함을 인정하고 있어 GDPR과 ISMS-P 모두 빅데이터 분석의 가능성을 인정한다. 또한 이 과정에서 발생할 수 있는 필요 이상의 과도한 개인정보의 분석을 두 제도 모두 동일하게 금지하고 있다.

4.3.4 개인정보 목적 외 이용 및 제공

개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립 및 이행하도록 ISMS-P는 정하고 있다. 이는 GDPR의 제7조의 '동의'에서 다루고 있는 사항과 맥을 같이한다. 이는 다음의 4.4절 '개인정보 제공'에서 보다 구체적으로 다루는 것으로 한다.

4.4 개인정보 제공

4.4.1 개인정보 제3자 제공

ISMS-P는 개인정보를 제3자에게 제공하기 위해서는 법적 근거에 의하거나 정보주체의 동의가 반드시 필요하며 개인정보 제공 과정에서 이를 안전하게 보호하기 위한 보호대책을 충분히 수립 및 이행하는가를 심사 기준으로 한다. GDPR은 이에 대하여 제5조 개인정보의 처리의 원칙에 따라 이루어질 것을 규제한다. 개인정보의 제공 역시, 개인정보의 수집, 이용 등의 '개인정보 처리 활동'으로 GDPR은 본다. 따라서 개인정보의 수집 및 이용과 같이 제5조가 제시하는 7가지 원칙에 따라 개인정보의 제공이 이루어져야 한다는 것이다. 따라서, 앞서 제시한 바와 같이, 제3자에 대한 개인정보 제공에 대해서 ISMS- P는 법적 근거가 존재하거나 정보주체의 동의가 수반된 제한된 경우에 한하여 인정하고 있으나 GDPR은 기업을 포함한 제3자의 타당한 이익 추구 목적을 위해 처리가 필요한 경우인 동시에 개인정보 처리의 원칙에 적법하게 따라 이루어지는 경우, 개인정보의 제3자 제공을 허용한다.

따라서 ISMS-P와 GDPR은 적법한 개인정보의 제3자 제공을 인정하는 사항에 있어서 차이를 보인다.

4.4.2 개인정보 국외 이전

ISMS-P는 국외 이전에 대한 정보주체의 동의여부와 관련 사항을 중점적으로 심사한다. 즉, 개인정보의 국외 이전을 위하여 정보주체에게 동의를 받았는지의 여부, 국외 이전 관한 계약 체결 여부 등의 방법을 통하여 이루어진다. 이에 반하여 사전에 GDPR에 기술된 적합성을 갖추지 않은 개인정보의 역외 이전은 원칙적으로 유효한 것으로 GDPR은 간주하지 않는다. GDPR은 개인정보를 역외로 이전하기 위해서는 이전하는 정보의 항목, 정보 제공자(Data exporter), 정보 수령인(Data importer), 이전받는 목적, 정보의 흐름, 적절한 안전 조치 등이 확인되어야 한다. 또한, 앞서 제시하였던 바와 같이, 적법한 역외 이전의 경우는, 1) 적정성 결정(Adequacy Decision)을 통하여 이전되는 국가의 개인정보보호 법제가 적절한 수준을 갖추었음이 입증되는 경우, 2) 표준 개인정보보호 조항(Standard Data Protection Clauses), 3) 구속력 있는 기업규칙(BCRs, Binding Corporate Rules), 4) 승인된 행동규약(Codes of Conduct) 및 인증제도(Certification Mechanism) 등을 확보한 경우 및, 5) 특정 상황에 대한 예외(Derogations for specific situations)로 제한하고 있다. 이를 통하여 개인정보 국외 이전을 인정하는 범위는 GDPR이 ISMS-P에 비하여 보다 엄격하다는 점을 확인할 수 있다. ISMS-P는 개인정보 주체의 입장에 차원에서 정보주체에게 충분한 동의가 적합하게 전달되었는지, 국외 이전에 관한 절차가 국내 개인정보보호 관련 법률을 준수하고 있는지를 주로 살펴보고 있다. 그러나 GDPR은 개인정보가 이전되는 국가가 개인정보를 보호하기 위한 표준 혹은 타당한 규약 및 인증의 취득 여부 혹은 해당 국가가 유럽이 평가하는 개인정보보호 관리체계를 확보하였는지 등을 기준으로 살펴본다는 점에서 ISMS-P보다 넓은 범위 즉, 국가의 차원에서 역외 이전을 통제하고 있다.

4.5 개인정보 파기

4.5.1 개인정보 파기

ISMS-P는 개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과 혹은 처리목적 달성 등의 파기 시점이 도달한 때에는 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 해당 개인정보를 파기하여야 하는 것을 원칙으로 제시한다. GDPR은 제5조 개인정보 처리 관련 원칙에서 수집, 제공 등을 포함하여 파기에 대하여 설명하고 있다. GDPR 역시, 법적 요건 등 처리 목적을 달성하거나 보유 기간이 만료된 경우에는 가능한 신속하게 개인정보를 파기하도록 규정화하였다. 또한 제28조제3항은 프로세서가 컨트롤러와의 관계를 종료하는 경우에는 컨트롤러의 선택에 따라 개인정보를 파기하여야 하는 프로세서의 의무를 밝히고 있다. 이는 ISMS-P는 단일한 주체의 개인정보 처리자가 처리 목적 달성 후 혹은 보유기간 경과 후, 개인정보를 파기하도록 하는 것만을 파기의 의무로 포함하고 있지만, GDPR은 이와 더불어 개인정보의 주요 처리자인 컨트롤러와 프로세서가 수반하는 개인정보 파기 의무를 각각 세부적으로 제시한다는 점에서 ISMS-P와 다르다.

4.6 정보주체 권리보호

4.6.1 정보주체 권리보장

ISMS-P는 정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회에 대한 요구를 쉽게 할 수 있도록 권리 행사와 관련된 방법 및 절차를 수립, 이행하고, 정보주체의 요구를 받은 경우 지체 없이 이를 처리하고 관련 기록을 남길 것을 인증 평가의 항목으로 제시한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립하여 이를 준수함에 따라 정보주체의 권리가 보장될 수 있는지를 ISMS-P는 평가한다. 이러한 정보주체 권리보장의 방법을 GDPR에서는 제13조, 제14조 정보를 제공받을 권리, 제15조 열람

권, 제16조 정정권, 제17조 삭제권, 제18조 처리 제한권, 제21조 반대권을 제시하여, 개인정보 수집, 이용, 제공 등의 기본 처리 과정과 더불어 프로파일링과 자동화된 의사결정 과정에서 정보주체의 권리 보장 방안을 구체적으로 기술하고 있다.

제13조, 제14조는 프로파일링의 프로세스가 어떻게 기능하는지 및 프로파일링을 포함한 자동화된 의사결정 발생 시 ① 프로파일링 사실, ② 프로파일링을 포함한 자동화된 의사 결정 사실에 대한 정보 제공을 전달받을 수 있는 정보주체의 권리를 표명한다. 제15조는 프로파일링 및 이에 활용된 정보에 대한 정보주체의 열람권을 보장하며 제16조는 프로파일링에 잘못된 개인정보를 활용 하는 경우 이에 사용된 정보 및 정보의 부정확성에 대하여 정정 및 이의를 제기할 수 있는 권리 보장을 의미한다. 제17조는 정보주체의 동의를 받은 프로파일링에 대하여 정보주체가 동의를 철회할 때, 법적 근거가 있지 않는 한 프로파일링에 사용된 개인정보 및 프로파일링 결과를 모두 삭제해야 하며, 제18조 처리 제한권에 대해서는 프로파일링 및 자동화된 의사 결정 과정의 모든 단계에 개인정보 처리를 차단하거나 제한할 권리를 적용하도록 하고 있다. 마지막으로, 제21조는 프로파일링에 대하여 반대권 제기 시 프로파일링 및 자동화된 의사 결정을 중단하고 필요할 경우 관련 정보를 삭제하여 정보주체의 권리를 보장한다. GDPR은 정보주체의 권리보장을 충분히 다하지 않는 경우, 이에 대한 의무 위반에 따른 과징금을 제12조에서 제22조에 걸쳐 제시한다. 이를 통하여 GDPR이 다루는 정보주체의 권리보장에 대한 중요성을 짐작할 수 있다. 그러나 ISMS-P는 ISMS 인증 의무 기업의 미취득의 경우를 제외하고는 GDPR과 같이 주요 원칙을 준수하지 않거나 관련 의무를 충분히 이행하지 않는 경우에 대한 별도의 과태료 및 법적 처분을 마련하지 않았다는 점에서 GDPR과 다르다.

GDPR과 ISMS-P의 개인정보보호 부문에 대한 연계 분석 결과인 매칭 표를 <Table 3>을 통하여 제시한다.

〈Table 3〉 ISMS-P and GDPR

ISMS-P	GDPR
Collection of Personal Information	
3.1.1 Restrictions on Collection of Personal Information	• Article 5 Principles relating to processing of personal data • Article 8 Conditions applicable to child's consent in relation to information society services • Article 22 Automated individual decision-making, including profiling
3.1.2 Personal Information Collection Agreement	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 8 Conditions applicable to child's consent in relation to information society services • Article 22 Automated individual decision-making, including profiling
3.1.3 Restrictions on Resident Registration Number Processing	• No similar provisions
3.1.4 Restrictions on Processing of Sensitive Information and Personally Identifiable Information	• Article 5 Principles relating to processing of personal data • Article 9 Processing of special categories of personal data • Article 18 Right to restriction of processing
3.1.5 Indirect Collection Protection Measures	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 22 Automated individual decision-making, including profiling
3.1.6 Installation of Video Information Processing Equipment · Operation	• No similar provisions
3.1.7 Measures to Take Advantage of PR and Marketing Purposes	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 21 Right to object

〈Table 3〉 ISMS-P and GDPR(Continued)

ISMS-P	GDPR
Usage & Management of Personal Information	
3.2.1 Managing the Status of Personal Information	• Article 5 Principles relating to processing of personal data • Article 24 Responsibility of the controller • Article 28 Processor • Article 29 Processing under the authority of the controller or processor
3.2.2 Guarantee of Personal Information Quality	• Article 5 Principles relating to processing of personal data
3.2.3 Restrictions on Personal Information Display and Protection Measures	• Article 5 Principles relating to processing of personal data • Article 22 Automated individual decision-making, including profiling
3.2.4 User Terminal Access Protection	• No similar provisions
3.2.5 Use and Provision of Non-personal Information	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent
Provision of Personal Information	
3.3.1 Provided Personal Information to Third Parties	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent
3.3.2 Information Subject to Business Consignment Notice	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 33 Notification of a personal data breach to the supervisory authority • Article 34 Communication of a personal data breach to the data subject
3.3.3 Transfer of Personal Information according to the Transfer of Business	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent
3.3.4 Transfer of Personal Information	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 40 Codes of conduct • Article 42 Certification • Article 44 General principle for transfers • Article 45 Transfers on the basis of an adequacy decision • Article 46 Transfers subject to appropriate safeguards • Article 47 Binding corporate rules • Article 48 Transfers or disclosures not authorized by Union law • Article 49 Derogations for specific situations
Deletion of Personal Information	
3.4.1 Destruction of Personal Information	• Article 5 Principles relating to processing of personal data • Article 28 Processor
3.4.2 Maintenance of Treatment Objectives	• Article 5 Principles relating to processing of personal data
3.4.3 Inactive User Management	• No similar provisions
Protection of Personal Information Subject Rights	
3.5.1 Disclosuzre of Privacy Policy	• Article 5 Principles relating to processing of personal data • Article 7 Conditions for consent • Article 13 Information to be provided where personal data are collected from the data subject • Article 14 Information to be provided where personal data have not been obtained from the data subject
3.5.2 Rights of Personal Information Subject	• Article 5 Principles relating to processing of personal data • Article 13 Information to be provided where personal data are collected from the data subject • Article 14 Information to be provided where personal data have not been obtained from the data subject • Article 15 Right of access by the data subject • Article 16 Right to rectification • Article 17 Right to erasure ('right to be forgotten') • Article 18 Right to restriction of processing • Article 21 Right to object • Article 22 Automated individual decision-making, including profiling
3.5.3 Usage Notification	• Article 5 Principles relating to processing of personal data • Article 13 Information to be provided where personal data are collected from the data subject • Article 14 Information to be provided where personal data have not been obtained from the data subject

5. 결론 및 향후 계획

본 연구에서는 GDPR과 ISMS-P의 상세 분석 및 비교를 통하여 두 제도 사이의 주요 차이점과 유사점은 다음과 같이 요약될 수 있다.

첫째, GDPR은 개인정보의 수집, 제공, 이용, 보관 및 파기 등의 개인정보에 대한 전반적인 과정을 포괄적인 '개인정보 처리'의 개념으로 각각 분류하여 개인정보의 처리 활동을 평가한다. 이는 GDPR과 ISMS-P 모두 개인정보의 처리 방법 및 관리 활동에 대하여 살펴보고 있으나, GDPR은 포괄적인 개념의 '개인정보 처리'로 채택하여 상세 항목을 기술하고 있는 반면에 ISMS-P는 이를 별도의 수집, 제공, 이용 등의 세부 활동으로 다루고 있다는 점에서 차이를 보인다. 또한, 목적 외 개인정보의 과도한 수집 및 이용, 처리를 GDPR과 ISMS-P 모두 원칙적으로 금지하고 있으며 정보주체의 동의가 있는 경우 혹은 각 국의 법률이 사전에 인정하는 경우에 제한적으로 인정하고 있다는 점은 동일하다.

둘째, GDPR은 개인정보를 처리하는 개인을 컨트롤러와 프로세서로 구분하여 이들에 대한 의무와 역할을 각각 제시하고 있는 반면에, ISMS-P는 개인정보 처리자의 역할과 의무 이행 여부를 별도로 평가하기 위한 사항은 다루지 않고 있다. 따라서, ISMS-P에서 평가하는 항목은 주로 개인정보 처리자 혹은 개인정보 취급자 등의 개인 차원이 아닌 기관 혹은 기업의 전반적인 정책 수립 여부, 보호조치 의무의 마련 여부 등과 같은 조직적 차원에서 접근하고 있는 것으로 판단된다. 이를 통하여 ISMS-P는 조직의 개인정보보호 관리체계를 평가하고 있는 반면에, GDPR은 ISMS-P와 같은 조직의 개인정보보호 관리체계, 보호조치 여부 등의 제도적 차원과 더불어 컨트롤러 혹은 프로세서 등의 개인정보를 다루는 개인 차원의 두 가지 관점의 접근방식을 모두 채택하였다는 점에서 차이를 갖는다.

셋째, 빅데이터 분석을 통한 개인정보의 연계·결합 가능성을 ISMS-P와 GDPR 모두 중점적으로 다루고 있다. 이는 이전의 개인정보보호법 및 ISMS, PIMS에서는 간과되었던 부분이나, 빅데이터 시대의 등장에 따라, 대용량 개인정보의 수집 및 분석이 가능해졌기 때문에 GDPR과 ISMS-P 모두 정보주체의 동의 없는 프로파일링을 포함한 자동화된 의사결정의 가능성을 인정하고 이를 엄격히 금지하고 있다. 그러나 GDPR은 수집된 개인정보의 결합과 연계 작업을 통하여 식별 가능한 개인정보로의 인정 가능성, 이에 따른 익명, 가공처리 등의 개인정보 비식별 방안에 대하여 구체적으로 다룬다는 점에서 ISMS-P에 비하여 비교적 구체적으로 조직이 채택하여야 하는 보호조치를 기술한다. 또한 GDPR과 ISMS-P 모두 자동화된 프로파일링 기법을 이용한 홍보, 마케팅에 대해서도 평가 항목을 다루고 있으나 이로부터 정보주체의 권리 보장 방안의 경우, GDPR은 '동의권', '철회권'을 통하여 ISMS-P에 비하여 보다 구체적으로 평가하고 있다. 넷째, 빅데이터를 활용한 분석이 가능해짐과 동시에 최근 등장한 글로벌 ICT 환경의 형성은 개인정보가 국가 간의 경계 없이 수집 및 이전을 용이하게 하였다. 따라서 GDPR과 ISMS-P는 이러한 '개인정보의 국외이전'의 사항을 상세히 포함하고 있다. ISMS-P는 개인정보 국외 이전 과정에서 가장 우선시되는 요건은 정보주체의 동의 여부이며 이전 되는 국가의 개인정보보호 수준의 적합성을 평가하기 위한 항목은 이전 국가의 개인정보보호 관련 법률의 설치 여부이나 해당 요건은 고려의 대상만으로 권고한다. 즉, ISMS-P는 국내 개인정보보호법에 의거하여 개인정보의 국외 이전 적법성을 주로 평가한다. 이에 실제로 국외 이전의 대상이 되는 국가에 대한 고려는 간과되어 있다. 하지만 이와 다르게 GDPR은 국외 이전과 관련된 조항(적정성 결정, 표준 개인정보보호 조항, 구속력 있는 기업 규칙, 승인된 행동규약 및 인증제도 획득, 특정 상황에 대한 예외) 에서 열거하지 않은 경우에 대해서는 원칙적으로 개인정보의 국외 이전을 금지한다는 점에서

GDPR은 보다 엄격한 입장을 내세우고 있다. 따라서 ISMS-P의 심사 기준에 따라, 적법한 것으로 판단되는 개인정보 국외 이전 사례가 반드시 GDPR이 정의하는 유효한 개인정보 국외 이전으로 해석되기에는 어렵다.

앞서 제시한 바와 같이 본 연구를 수행함에 따라, 본 연구는 최종적으로 다음과 같은 공헌도를 기대할 수 있다.

첫째, 본 연구 결과는 GDPR 준수 혹은 ISMS-P인증 취득 의무가 있는 기업에게 상호 제도의 준수 여부를 스스로 평가할 수 있는 가이드라인을 제공한다. 즉, 본 연구의 결과를 바탕으로 기업은 ISMS-P 취득 혹은 GDPR 의무 이행을 위한 준비 과정에서 상호 제도의 준수 여부를 객관적으로 진단 가능하게 한다.

둘째, 기업의 효율적인 정보보호 및 개인정보보호 관리체계 방안의 마련을 도모한다. 개인정보보호 및 정보보호의 중요성이 증가함에 따라, 고객에게 신뢰를 제공하고 기업 이미지 제고를 위한 한 가지 방안으로 관련 인증제도 획득에 대한 기업의 관심이 증가하고 있다. 이에 개인정보보호 관리체계의 평가 목적을 갖는 다양한 제도 혹은 인증 역시 늘어나고 있다. 국내외 존재하는 다수의 정보보호/개인정보보호 인증 및 평가제도 가운데 본 연구는 ISMS-P 획득 혹은 GDPR 의 역할에 대한 기업의 이해를 증진시켜 불필요한 인증 획득에 요구되는 기업의 투자비용을 감소시킬 수 있다.

셋째, 최근 ISMS-P가 국내에 시행되기 시작함에 따라, ISMS와의 혼동, ISMS-P의 시행 여부에 대한 기업의 무관심 등으로 ISMS-P의 확산 및 국내 정착의 난항이 예상되는 시점이다. 이에 본 연구는 국내 기업의 ISMS-P 심사 준비를 지원할 수 있는 토대 자료를 제공함에 따라, 해당 인증제도에 대한 기업 및 대중의 관심을 증가시키고 이의 확산과 정착에 기여할 수 있을 것으로 판단된다.

넷째, 국내 정보보호 및 개인정보보호 관리체계인 ISMS-P와 GDPR을 비교, 분석함에 따라, 이는 향후, 관련 인증제도 및 정책 개발 작업의 기초가 된다. ISMS-P 또한 기존의 ISMS와 PIMS의 중복 평가 문항, 심사 기관의 분리 등에 따른 기존 제도의 취약점이 드러남에 따라 추진된 결과이다. 이에, ISMS-P와 GDPR의 연계 분석 결과는 향후, 개인정보보호 관련 국제 표준 및 국제 인증의 개발에 적용될 수 있을 것으로 기대된다. 최근, 기업의 블록체인의 도입과 확산이 늘어나는 동시에 암호화폐 거래소의 설립이 증가함에 따라, 이에 적합한 신규 정보보호/개인정보보호 관리체계의 마련이 시급한 시점이다. 따라서 본 연구는 이와 같은 신규 ICT 환경의 변화 및 신기술의 등장과 확산에 빠르게 대응할 수 있는 인증제도 및 관리체계를 확립하는데 기여할 것이다.

ISMS-P와 더불어 GDPR 모두 최근 시행 및 적용된 제도로 이에 대한 기업의 혼란은 지속적으로 증가할 것으로 예측된다. 그러나 이와 관련된 연구는 아직 미미하다. 따라서 본 연구는 두 제도를 함께 분석함에 따라, 관련 기업의 혼동을 줄여 기업 내 정보보호 및 개인정보보호 활동의 효율성을 증가시키는 동시에 관련 연구의 확장 필요성을 제기한다.

GDPR과 ISMS-P는 최근 형성되어 기업과 사회에 등장하였다. 이에 기업이 두 가지 제도를 도입 및 준수하기 위한 투자비용 혹은 도입과 준수에 따른 개인정보보호 수준의 향상 등을 측정하여 제도의 효과성을 실증적으로 검증하기 위해서는 아직 충분한 시간이 경과되지 않았다고 판단되어 본 연구에서는 정성적 연구 방법의 관점에서 비교, 분석 연구를 수행하였다. 이에 본 연구는 두 가지 제도가 수반하는 실효성을 정량적으로 수치화하여 제시할 수 없었으나, 향후 관련 실증 연구의 기반이 되는 탐색적 연구로서 개인정보보호 인증제도, 법률 연구 분야의 필요 및 확장에 기여한다.

References

Cha, G.S., H.Y. Han, and Y.T. Shin, “An Effective Personal Information Management System to Ensure Self-imposed Control on Per-

sonal Information Protection Act", *Journal of Computing Science and Engineering*, Vol.39, No.2, 2012, 276-281.

(차건상, 한호현, 신용태, "개인정보보호법의 자율규제 확보를 위한 효과적인 개인정보관리체계 인증제", *정보과학회논문지 : 정보통신*, 제39권, 제3호, 2012, 276-281.)

Cho, S.Y., "A Study on Privacy Protection in the EU's GDPR and Korea's Personal Information Protection Act", *Kyungpook National University Law Journal*, Vol.61, 2018, 117-148.

(조수영, "개인정보보호법과 EU 의 GDPR 에서의 프라이버시 보호에 관한 연구", *법학논고*, 제61집, 2018, 117-148.)

Choi, B.M., S.M. Chai, M.K. Kim, and Y.J. Kang, "A Study of Development Plan Regarding Personal Information Management System and International Standardization : GDPR Perspective", *The Journal of Korean Institute of Communications and Information Sciences*, Vol.43, No.2, 2018, 416-426.

(최보미, 채상미, 김민균, 강연정, "GDPR 환경에서 국내 개인정보보호 관련 인증제도 및 표준 발전방향에 대한 연구", *한국통신학회논문지*, 제43권, 제2호, 2018, 416-426.)

Jang, J.Y., T.H. Park, and B.S. Kim, "The life cycle model considering legal and technical", *Journal of Society for e-Business Studies*, Vol.17, No.3, 2012, 43-60.

(장재영, 박태환, 김범수, "개인정보의 법적·기술적 특성을 고려한 라이프 사이클(Life Cycle) 모델", *한국전자거래학회지*, 제17권, 제3호, 2012, 43-60.)

Jang, S.S. and H.S. Lee, "A Study on Analysis of Defects in Information Security Management System (ISMS) Certification Examination", *Journal of the Korea Institute of Information Security & Cryptology*, Vol.20, No.1, 2010, 31-38.

(장상수, 이호섭, "정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구", *정보보호학회지*, 제20권, 제1호, 2010, 31-38.)

Jang, S.S., H.B, Kim, and H.S. Lee, "Information Security Management System Certification System Introduction and Direction", *Journal of the Korea Institute of Information Security and Cryptology*, Vol.11, No.3, 2001, 1-15.

(장상수, 김학범, 이홍섭, "정보보호관리체계 인증제도 소개 및 추진 방향", *정보보호학회지*, 제11권, 제3호, 2001, 1-15.)

Kang, H.S., "An Analysis of Information Security Management System and Certification Standard for Information Security", *Journal of Security Engineering*, Vol.11, No.6, 2014, 455-468.

(강현선, "정보보안을 위한 정보보호 관리체계 및 인증체계 분석", *보안공학연구논문지*, 제11권, 제6호, 2014, 455-468.)

KISA, EU General Privacy Act(GDPR) Guidebook for Korean Companies, 2018.

(KISA, 우리 기업을 위한 EU 일반 개인정보보호법(GDPR) 가이드북.)

Moon, S.J., "An International Trends in On-line Individual Information Protection-Focusing on American System", *Journal of Comparative Law*, Vol.3, 2004, 57-81.

(문성제, "온라인상에서의 개인정보보호에 관한 국제 동향-미국의 제도를 중심으로", *비교법학연구*, 제3집, 2004, 57-81.)

Oh, K.H., "Information security management system according to international standards", *Journal of The Korea Institute of Information Security & Cryptology*, Vol.28, No.6, 2018, 96-102.

(오경희, "국제표준에 따른 정보보호관리체계 전문가 인증 방안", *정보보호학회지*, 제28권, 제6호, 2018, 96-102.)

Park, E.Y., J.W. Choi, and T.E. Cho, "Personal Information Protection Management System Certification System Case Study," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.21, No.5, 2011, 27-36.

(박은엽, 최진원, 조태희, "개인정보보호관리체계 인증제도 구축 사례 연구", *정보보호학회지*, 제21권, 제5호, 2011, 27-36.)

Park, J.Y., W.J. Jung, and B.S. Kim, "The Effect of Information Security Certification Announcement on the Market Value of Firms", *Journal of Information Technology Services*, Vol.15, No.3, 2016, 51-69.

(박재영, 정우진, 김범수, "기업의 정보보호 인증이 기업가치에 미치는 영향", *한국IT서비스학회지*, 제15권, 제3호, 2016, 51-69.)

Park, K.T. and S.H. Kim, "An Empirical Study on Expectation Factors and Certification Intention of ISMS", *Journal of The Korea Institute of Information Security & Cryptology*, Vol.25, No.2, 2015, 375-381.

(박경태, 김세헌, "ISMS 인증 기대 요인 및 인증 의도에 관한 연구", *정보보호학회논문지*, 제25권, 제2호, 2015, 375-381.)

Park, M.J., S.M. Chai, and M.J. Lee, "Legal Issues of Blockchain in Personal Information Protection : Based on GDPR and Personal Information Protection Act", *Journal of Information Technology Applications & Management*, Vol.25, No.2, 2018, 133-146.

(박민정, 채상미, 이명준, "개인정보보호법제 관점에서 본 블록체인의 법적 쟁점 : GDPR 및 국내 개인정보보호법을 바탕으로", *Journal of Information Technology Applications & Management*, 제25권, 제2호, 2018, 133-146.)

Pfleeger, S.L. and C.P. Pfleeger, "Harmonizing privacy with security principles and practices", *IBM Journal of Research and Development*, Vol.53, No.2, 2009, 6-11.

Ryu, S.K., "The Finally Agreed EU General Data Protection Regulation", *Journal of Law & Economic Regulation*, Vol.9, No.1, 2016, 265-268.

(류승균, "EU 개인정보보호규칙(GDPR)의 제정과 시사점", *경제규제와 법*, 제9권, 제1호, 2016, 265-268.)

Tikkinen-Piri, C., A. Rohunen, and J. Markkula, "EU general data protection regulation : Changes and implications for personal data collecting companies", *Computer Law and Security Rev*, Vol.34, No.1, 2017, 1-20.

Von Solms, B., "Information security—a multi-dimensional discipline", *Computers & Security*, Vol.20, No.6, 2001, 504-508.

About the Authors

Minjung Park (mjpark67@ewhain.net)

Minjung Park is Ph.D candidate of Ewha School of Business, Ewha Womans University. She received B.S from the college of Law in Sungshin Women's University and M.S in Data Analytics from Ewha Womans Univeristy. Her research interest is behavioral information security, information security management, Privacy and Blockchain.

Jieun Yu (ji-yu@ewhain.net)

Jieun Yu studies master's degree program in Big Data Analytics at Ewha Womans University. She received B.S. degree at Ewha Womans University. Her area of interests is Data Analytics, Blockchain, Information Security Management and Privacy.

Sangmi Chai (smchai@ewha.ac.kr)

Sangmi Chai is an Associate Professor in Ewha School of Business, Ewha Womans University. She received her PhD in MIS from School of Management, State University of New York at Buffalo. She was an Assistant Professor in College of Business, Information and Social Sciences, Slippery Rock University, PA, USA. She graduated from MBA in Seoul National University and received BS in the Ewha Womans University. Her research interests include information privacy and security, trust and knowledge management, and IT investment.