석사학위 논문

EU-GDPR을 대비한 개인정보보호 인증제도의 개선방안

ISO/IEC 27701과 ISMS-P를 기준으로

A Way to Improve the Certification System to Protect Personal Information to Cope Properly with the EU-GDPR

Based on ISO/IEC 27701 and ISMS-P

2020년 12월

숭실대학교 정보과학대학원

핀테크융합학과

강 민 성

석사학위 논문

EU-GDPR을 대비한 개인정보보호 인증제도의 개선방안

ISO/IEC 27701과 ISMS-P를 기준으로

A Way to Improve the Certification System to Protect Personal Information to Cope Properly with the EU-GDPR

Based on ISO/IEC 27701 and ISMS-P

20년 12월

숭실대학교 정보과학대학원

핀테크융합학과

강 민 성

석사학위 논문

EU-GDPR을 대비한 개인정보보호 인증제도의 개선방안

지도교수 박 재 표

이 논문을 석사학위 논문으로 제출함

20년 12월

숭실대학교 정보과학대학원

핀테크융합학과

강 민 성

강 민 성의 석사학위 논문을 인준함

심 사 위 원 장 양 승 민 인

심 사 위 원 윤 준 성 인

심 사 위 원 박 재 표 인

20년 12월

숭실대학교 정보과학대학원

목 차

표 목 차

그 림 목 차

국문초록

EU-GDPR을 대비한 개인정보보호 인증제도의 개선방안

강민성

핀테크융합학과

숭실대학교 정보과학대학원

빅데이터를 기반으로 발전된 신기술들의 영향으로 개인정보를 활용한 영역과 규모는 증가하고 있으나, 개인정보를 보호하기 위한 체계 및 수단은 그만큼 개선되지 못해 매년 보안사고가 발생하고 있다. 이에 우리나라는 개인정보를 안전하게 보호하기 위한 제도적 장치인 개인정보 보호법 개정을 통해 보안수준을 강화하고자 했으며, EU에서는 회원국 국민의 개인정보보호와 현시대에 맞는 개인정보 거버넌스 체계 마련을 위해 GDPR을 제정하였다. GDPR의 적용 범위는 GDPR 제2, 3조에 따라 EU 회원국 국민을 대상으로 사업을 하는 국내기업들 역시 적용될 수 있어 이에 대한 주의 및 대비가 필요하다.

본 논문에서는 GDPR의 적용을 받는 국내기업들의 안전한 개인정보 처리와 GDPR을 효과적으로 대비하는 방안을 마련하기 위해, 개정된 개인정보 보호법을 기반으로 국내·외에서 시행되고 있는 개인정보보호에 관한 인증제도인 ISMS-P, ISO/IEC 27701을 분석하여 GDPR에서 요구되는 보안수준에 충족되는지 비교분석을 진행하였다. 개선이 필요한

ISMS-P의 경우 개선 필요항목에 대하여, ISO/IEC 27701 및 국내 환경 분석 결과를 기반으로 GDPR 평가항목을 대비한 ISMS-P 개선방안을 제시하였다.

ISMS-P 개선방안에 대한 정합성의 확인을 위해 개선방안에 대응되는 벌금 부과사례 4개를 기준으로 위반 조항, 위반 유형, 사건 내용 등을 분석하여 국내 환경에 맞게 기업이 취할 대응방안을 제시하여 ISMS-P 개선방안의 정합성을 확인하였다.

본 논문은 실제 벌금 부과사례들을 분석하여 국내기업이 우선적으로 대비해야 하는 GDPR 조항에 대해 식별 및 분석하고 그에 따른 개인정보보호 인증제도의 개선방안을 제시하였다. 이를 기반으로 GDPR의 적용을 받는 국내기업들이 기업에 맞는 최적화된 개인정보보호 관리체계를 수립하고, GDPR에 대한 지속적인 관심 및 연구가 계속된다면 GDPR을 대비하는 기반이 되는 데 도움이 될 것이라 기대한다.

ABSTRACT

A Way to Improve the Certification System to Protect Personal Information to Cope Properly with the EU-GDPR

KANG, MIN SEONG
Department of Information Security
Graduate School of Information Science,
Soongsil University

With the development of new technology based on big data, the scope of areas where personal information is used is rapidly expanding. But, as the means to protect personal information has not developed as fast as the expansion of the use of it, security accidents frequently take place. To strengthen security level, the Korean government revised the Personal Information Protection Law which is an institutional device to protect personal information. The EU established the General Data Protection Regulation (GDPR), to protect private information of citizens of member countries, and to prepare the governance system for private information. According to Articles 2 and 3 of the GDPR, the regulation is applied to the

foreign firms doing business with citizens of the EU member countries. Thus, Korean firms need to be well-aware of the contents of the GDPR.

To make domestic firms which deal with EU citizens treat personal information safely and cope properly with the GDPR, this study analyzed ISMS-P, ISO/IEC 27701, the certification system on protection of personal information based on the Personal Information Protection Law, which is implemented in Korea and overseas, and checked whether it satisfies the security requirements of the GDPR. For some items of the ISMS-P which need to be revised, this study suggested ways to revise them and improve the ISMS-P based on the results of the analysis of ISO/IEC 27701 and domestic environment, to respond to evaluation items of the GDPR.

To identify whether the ideas on revising the ISMS-P conform to the requirements of the GDPR, this study provides 4 cases where the actors were imposed fines by the EU authorities for violating the GDPR. This study analyzes the articles of the GDPR the actors violated, the types of violation, and contents of the accidents, etc. to let Korean firms respond properly to the requirements of the GDPR.

By analyzing real cases of fine imposition by the GDPR, this paper let the Korean firms recognize the GDPR articles they should be aware of, and suggested the ways of improving the personal information certification system. It is expected that, based on the findings of this paper, Korean firms affected by the GDPR will establish the optimal management system on personal information, and that there will be continuous attention to and researches on the GDPR.

제 1 장 서 론

1.1 연구의 배경

정보통신 기술의 융합으로 맞이한 제4차 산업 혁명은 인공지능(Artificial Intelligence), 블록체인(Blockchain), 사물인터넷(Internet of Things) 등과 같은 빅데이터를 통한 신기술의 발전을 통해 삶의 형태를 바꾸고 있다. 현시대를 영위하고 있는 대다수 사람은 휴대가 간편하고 통신이 가능한 스마트 기기 속 소셜 네트워크 서비스(Social Networking Service)를 통해 개인의 일상을 공유하고 국내·외 시사 정보 등을 손쉽게 접하는 것은 물론 유튜브(Youtube)를 포함한 다양한 플랫폼을 통해 불법과 합법의 중간경계에서 수많은 정보를 교환하며 살아가고 있다. 이처럼 개인정보를 활용하는 기술의 영역과 활용되는 개인정보의 그 규모는 방대해지고 있다. 그러나 개인정보를 처리하는 사람들의 개인정보보호 의식은 그만큼 확립되지 못하여, 매년 발생하는 보안사고 구글플러스 개인정보 유출 사고(5200만 명, 2018년 10월), 페이스북 개인정보 유출 사고(4억 2천만 명, 2019년 9월) 등의 사고사례로 알 수 있듯 개인정보 관련 사고는 점차 그 규모와 피해가 증가하고 있다. 이에 우리나라는 기존 데이터 3법(정보통신망법·개인정보 보호법·신용정보 보호법) 개정을 통해 앞서 언급한 신기술들을 활용한 안전한 데이터 이용 활성화를 촉진시키고자 하였다. 개인정보 보호법의 개정안은 기존 데이터 3법에서 각기 다루었던 개인정보와 관련된 내용을 정비, 일원화하여 2020년 8월 5일부터 시행하고 있다. 한편, EU(European Union, 유럽연합)는 회원국 국민의 기본권과 자유를 보호하고 개인정보의 자유로운 이동을 위해 GDPR(General Data Protection Regulation, 일반정보보호규정)를 2016년도에 제정하여 2년의 유예 기간을 거친 후 2018년 5월 25일부터 본격 적

용하고 있다[2]. GDPR은 법적 구속력을 가지는 규정으로 그 적용 범위는 유럽기업들뿐만 아니라, 국내기업들 또한 포함하고 있다. EU 회원국 국민에게 재화·용역을 제공하면서 그에 따른 개인정보를 처리하여 그 관련성이 인정될 경우 GDPR의 적용 범위에 포함되며, 이를 어길 때 최대 2,000만 유로 또는 전 세계 매출액의 4%에 해당하는 금액 중 더 큰 금액에 해당하는 과징금이 부과될 수 있다. 이런 측면에서 국내기업들 역시 GDPR에 대한 적용 범위 및 실제 사례 등의 분석을 통한 대비가 요구된다.

1.2 연구의 목적

본 논문에서는 개인정보 보호법과 GDPR 분석을 통해, 개정된 개인정보 보호법과 GDPR의 정의, 목적, 범위 등의 차이점을 식별하고, 실제 벌금 부과사례들을 기반으로 기존에 존재하는 국내 및 국외 인증제도에 GDPR 대응을 위해 항목을 추가하는 발전 방향성을 제시한다. 결과적으로 국내기업들이 정보보호 및 개인정보보호 관리체계(이하, ISMS-P) 인증 또는 ISO/IEC 27701 인증을 통해 매년 증가하는 보안사고를 대비하고자 하는 국내기업 및 EU GDPR의 적용을 받는 국내기업들이 개선된 개인정보보호 관리체계 수립 및 GDPR의 대비까지 함께하는 방안을 마련함에 연구의 목적이 있다.

1.3 논문의 구성

본 논문은 본문 총 5장, 참고문헌, 부록으로 구성되며,

제 1 장에서는 본 연구의 배경 및 방향성을 제시한다.

제 2 장에서는 본 연구를 진행하기 위한 선행 연구로써 GDPR의 제정

배경과 체계, 항목연구와 개인정보 보호법의 개정 이유 및 의의, 마지막으로 ISMS-P와 ISO/IEC 27701의 통제항목들에 관한 연구를 진행한다.

제 3 장에서는 GDPR 평가항목을 도출하여 도출된 평가항목과 ISMS-P, ISO/IEC 27701간의 비교분석을 통해 개선 필요항목을 도출한다.

제 4 장에서는 GDPR의 대비를 위한 개인정보보호 인증제도의 개선방안을 도출하고 벌금 부과사례를 기반으로 한 대응방안을 제시한다.

제 5 장에서는 본문의 결론 및 본문에서 다루지 못한 향후 연구 과제에 관하여 서술하고 마무리한다.

제 2 장 관련 연구

2.1 EU-GDPR

2.1.1 EU-GDPR 개요

EU는 “1995년 10월 24일 개인정보의 처리와 자유로운 유통에 관한 개인정보보호 지침(Directive of the European Parliament of individuals with regard to the processing of personaldata and on the free movement of such data, 95/46/EC)”을 제시하였다. “회원국 국민의 기본권과 자유를 보호하고 개인정보 처리와 관련한 프라이버시권을 보호하며 EU 회원국 사이에서 개인정보의 자유로운 유통을 촉진”하기 위한 목적을 가졌으나, 지침(Directive)으로 제정되어 그 자체만으로는 법적 구속력을 가지지 못하는 한계를 가졌다[3]. 개인정보보호 지침은 각 회원국의 입법을 통해서만이 구속력을 가질 수 있었고, 이 때문에 EU 회원국의 적극적인 이행을 이끌어내는데 어려움이 존재하였다. 이에 개인정보보호에 관한 규율체계의 통일성 부재에 따라 EU 전역에 개인정보의 처리에 관한 법적 불확실성이 존재하는 상황이 지속되었으며, EU 개인정보보호 지침의 한계를 극복할 수 있는 회원국 전체에 공통으로 적용되는 규범의 필요성이 논의 요구되었다[10]. 이후 2011년 유럽의회에서 “유럽연합에서의 개인정보보호에 관한 종합적 접근”을 의결하면서 입법이 가시화되었으며, 개인정보보호 입법을 목표로 2012년 GDPR의 초안을 제안한 후 4년간 3천 건 이상의 수정안 이후, EU의 입법기관인 EU 이사회, 유럽의회, 유럽위원회의 3자 간 협의를 거쳐 2016년 5월 27일 GDPR이 채택되었으며, 2년의 유예 기간을 거쳐, 2018년 5월 25일부터 GDPR이 시행되었다[1][10].

2.1.2 EU-GDPR 구성

기존 EU 개인정보보호 지침이 총 7장 34개 조문으로 구성된 것에 비교하여 GDPR은 전문 총 173개 항, 본문 총 11장 99개 조문으로 구성되어 단순 조문 수만으로도 65개의 조항이 증가 되었으며[7], 그중 GDPR에서 정보주체의 권리를 보장하기 위한 신설 또는 강화된 조항은 다음 [표 2-1]과 같다[14].

[표 2-1] GDPR 정보주체의 권리보장을 위한 조항

정보를 제공받을 권리 [제12~14조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식
제13조 개인정보가 개인정보 주체로부터 수집되는 경우 제공되는 정보
제14조 개인정보가 개인정보 주체로부터 수집되지 않는 경우 제공되는 정보
정보주체의 열람권 [제12, 15조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식
제15조 개인정보 주체의 열람권 제16조 정정권
정정권 [제12, 16, 19조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식
제16조 정정권
제19조 개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무
***(신설) 삭제권(잊힐권리) [제12, 17, 19조]**
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식
제17조 삭제권('잊힐 권리')
제19조 개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무
***(신설) 처리 제한권 [제12, 18, 19조]**
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식
제18조 처리에 대한 제한권
제19조 개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무

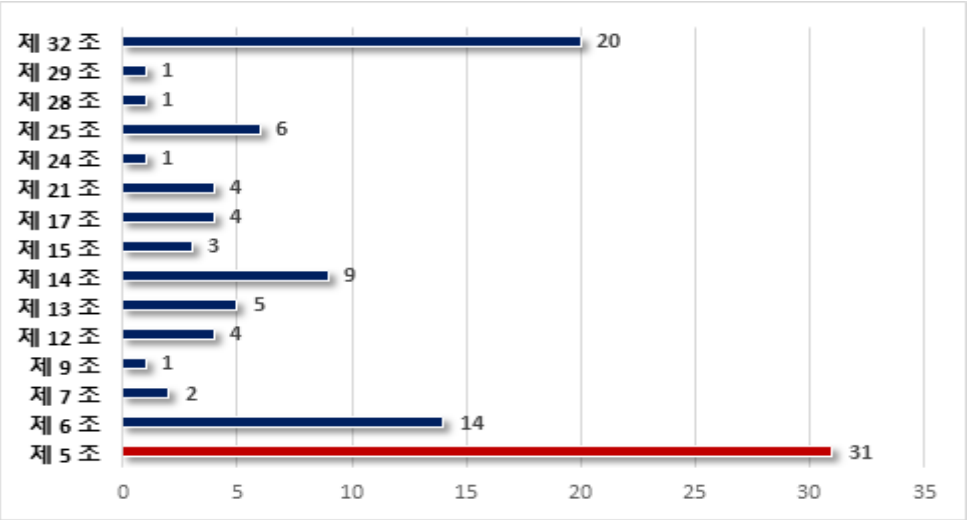
*(신설) 개인정보 이동권 [제12, 20조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 제20조 개인정보 이전권
반대권 [제12, 21조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 제21조 반대할 권리
*(신설) 프로파일링을 포함한 자동화된 의사결정 [제12, 22조]
제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 제22조 프로파일링 등 자동화된 개별 의사결정

GDPR은 권리, 의무, 범위, 책임 측면에서 EU 개인정보보호 지침보다 강화된 개인정보 보안수준을 요구하고 있으며, 개인정보 처리에 대한 기본원칙과 개인정보 처리의 적법성, 동의 조건, 그리고 아동의 동의에 적용되는 조건, 특수 범주의 개인정보 처리, 범죄에 관련된 개인정보 처리와 식별을 요구하지 않는 처리데이터 보호 즉 개인정보의 보호에 초점을 두고 있으며, EU 회원국이 준수해야 할 요구사항을 규정하고 있으며 이와 관련한 GDPR 전체 조문은 [부록 1]에 수록하였다[7].

2.1.3 EU-GDPR 벌금 통계

GDPR 제83조 행정 과태료 부과에 관한 일반 조건에 따라 EU GDPR이 시행된 2018년 5월 25일 이후부터 연구를 진행한 시점인 20년 11월까지 KISA GDPR 대응지원센터, PrivacyAffairs 사이트에 등록된 벌금부과 사례를 분석한 결과 총 부과횟수는 410번으로 1000€ 미만의 벌금은 33회, €5,000 미만의 벌금은 110회, €10,000 미만의 벌금은 60회, €50,000 미만의 벌금은 92회, €100,000 미만의 벌금은 50회, €100,000 이상의 벌

금은 54회로 그중 가장 큰 벌금은 2019년 1월 21일 프랑스의 개인정보 감독기구(Commission Nationale de l'Informatique et des Libertés, CNIL)이 GDPR의 투명성 원칙(제5조 1항), 개인정보 주체로의 정보 제공(제13조, 제14조), 처리의 적법성(제6조) 위반 혐의로 Google Inc에 약 5천만 유로(한화 약 673억 원)의 벌금을 부과된 것이며, 반대로 가장 작은 벌금은 2020년 8월 17일 에스토니아 경찰관이 개인정보 처리 원칙(제5조), 처리의 적법성(제6조)을 위반하여 부과된 48유로의 벌금이다[12][16]. 위 사례들을 포함한 벌금 부과사례들은 앞으로의 유럽연합 회원국의 감독 당국(Data Protection Agencies, 이하 DPAs)이 GDPR을 적용하는 그 기준이 되는 것에 있어 중요한 선례가 될 것이다. 다음의 통계 [그림 2-1] GDPR 항목별 위반 횟수는 위의 410개의 벌금부과 사례 중 영향도가 큰 €100,000 이상의 벌금 사례 54개를 기준으로 GDPR 위반 항목별 위반 횟수를 그래프로 나타낸 것이다.



[그림 2-1] GDPR 벌금 항목별 위반 횟수

GDPR에 근거한 벌금부과 항목은 제83조 4, 5에 따른 42개 조항이지만 위 그래프에서 알 수 있듯이 현재 실제 벌금이 부과된 항목은 15개 조항

으로 그중 제5조(개인정보 처리원칙)이 31번으로 가장 많은 비중을 차지하고 있다. 따라서 GDPR을 적용을 받는 기업들이 해당 항목들에 대해 우선적으로 대비하고 그에 따라 국내기업 역시 이를 분석하여 대비하는 자세가 요구된다.

2.2 개인정보 보호법

2.2.1 개인정보 보호법 개요

개인정보 보호법은 “정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있으나, 국가사회 전반을 규율하는 개인정보보호 원칙과 개인정보 처리기준이 마련되지 못해 개인정보 보호의 사각지대가 발생할 뿐만 아니라, 최근 개인정보의 유출·오용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있는바, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 적극화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장”하기 위해 제정되었다[4]. 또한, 개인정보 보호법은 개인정보에 관한 일반법으로 주민등록번호 처리의 제한에 관한 개정(2014.8), 개인정보 처리 시 안정성 확보 강화를 위한 개정(2016.9) 등 이후로도 여러 차례의 개정을 거쳤다. 2020년 8월부로 4차 산업혁명 시대로 전환되는 사회적 흐름을 반영하여 빅데이터, 클라우드, 블록체인, 사물인터넷 등 신기술을 활용한 데이터의 활성화를 위해 기존 개인정보 보호법과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등에서 분산되어 있던 개인정보 관련 법령 내용을 정비 일원화는 개정안이 시행되고 있으며, 정보 주체의 동의 없이 공익적 기록보존, 통

계작성, 과학적 연구 등의 목적으로 가명 정보를 처리할 수 있는 가명 정보에 관한 정의 및 근거마련, 가명 정보에 안전성 확보에 필요한 기술적·관리적·물리적 조치, 개인정보의 유출 등을 감독하는 행정안전부·방송통신위원회·개인정보보호위원회 등의 감독기구들의 역할을 개인정보보호위원회로 통합·이관하는 등의 내용을 담고 있다[4].

2.2.2 개인정보 보호법 주요 개정내용

개정된 개인정보 보호법은 총 10장에 걸쳐 76개의 조문으로 구성되어 있으며, 주요 개정된 내용은 [표 2-2]와 같다[4].

[표 2-2] 개인정보 보호법 주요 개정내용

조항	주요개정 내용
제2조 (정의) 제1호의 2	개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정개인을 알아볼 수 없도록 처리하는 것을 가명처리로 정의함
제7조 (개인정보보호위원회) 제7조 8 (보호위원회의 소관 사무)	개인정보보호위원회의 소속을 대통령 소속에서 국무총리 소속으로 변경하고, 「정부조직법」에 따른 중앙행정기관으로 보도록 하며, 현행 행정안전부와 방송통신위원회의 개인정보 관련 사무를 개인정보보호위원회로 이관하여 개인정보보호 컨트롤타워로서의 기능을 강화함
제15조 (개인정보의 수집·이용) 제3항 제17조 (개인정보의 제공) 제4항	개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보 주체에게 불이익이 발생하는지 여부, 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 정보 주체의 동의 없이 개인정보를 이용하거나 제공할 수 있도록 함
제28조의 2 (가명정보의 처리 등) 제 28조의3	개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하되, 서로 다른 개인정보처리자

(가명정보의 결합 제한)	간의 가명정보의 결합은 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행하도록 함
제28조의 4 (가명정보에 대한 안전조치의무 등)	개인정보처리자는 가명정보를 처리하는 경우 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 함
제28조의 5 (가명정보 처리 시 금지의무 등) 제 28조의6 (가명정보 처리에 대한 과징금 부과 등)	누구든지 특정개인을 알아보기 위한 목적으로 가명정보를 처리해서는 안 되고, 이를 위반한 개인정보처리자에 대해서는 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있도록 함
제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상의 개인정보 보호 관련 규정을 이 법으로 일원화함에 따라, 정보통신서비스 제공자 등의 개인정보 처리에 관한 특례 등을 규정함

2.3 국내·외 인증제도

2.3.1 ISO/IEC 27701

ISO/IEC 27701:2019(Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines)는 ISO(International Organization for Standardization: 국제 표준화 기구)에서 2019년 8월 발표한 국제 표준으로 정보보호관리체계(ISMS)의 요구사항을 규정한 국제 표준인 ISO/IEC 27001과 이를 기반으로 경영시스템을 구현하고 유지하기 위한 지침인 ISO/IEC 27002의 확장판이다[8]. ISO/IEC 27001에서 요구하는 ISMS를

유지하고 있는 조직에서 개인정보에 관련된 별도의 시스템을 구현하는 것이 아니라 부문별로 강화된 사항들에 대해 분석·적용하여 기존의 틀을 유지하면서 개인정보에 관련된 사항들을 강화할 수 있다. 또한, ISO/IEC 27701에서는 거의 모든 조직이 PII(Personally Identifiable Information : 개인식별정보)를 처리한다고 말하고 있으며 이에 따라 PII의 종류나 수는 이전과 비교할 수 없을 정도로 증가하고 있다[8]. ISO/IEC 27701에서는 PII와 관련하여 PII 컨트롤러에 대한 ISO/IEC 27002 추가지침, PII 프로세서에 대한 ISO/IEC 27002 추가지침을 추가하여 GDPR에서 요구 프로세서와 컨트롤러의 보안 사항에 대해서도 대비하고 있다. ISO/IEC 27701은 ISO/IEC 27001과 ISO/IEC 27002의 확장판인 만큼 해당 인증을 받기 위해서는 ISO/IEC 27001에 대한 인증이 필수적으로 선행되어야 하며 ISO/IEC 27701만 별도로 인증을 받을 수는 없다.

2.3.2 ISO/IEC 27701 구성

ISO/IEC 27701은 ISO/IEC 27001과 ISO/IEC 27002의 확장판인 만큼 초반 3장은 동일한 형식으로 구성돼있으며, 이후 4장부터 8장까지는 ISO/IEC 27701 제정 목적에 따라 개인식별정보와 관련된 내용 등이 확장 형식 구성으로 되어있으며, 이러한 ISO/IEC 27701에 대한 구성 및 항목은 [표 2-3]과 같다.

[표 2-3] ISO/IEC 27701 구성

ISO/IEC 27701 구성
1장 범위 (Scope)
2장 참고자료 (Normative references)
3장 용어, 정의 및 약어 (Terms, definitions and abbreviations)

4장 일반 규정 (General)
4.1 표준의 구조 (Structure of this document) 4.2 ISO/IEC 27001 요구사항 적용 (Application of ISO/IEC 27001:2013 requirements) 4.3 ISO/IEC 27002 지침 적용 (Application of ISO/IEC 27002:2013 guideline) 4.4 고객 (Customer)
5장 ISO/IEC 27001 관련 PIMS 요구사항 (5 PIMS-specific requirements related to ISO/IEC 27001)
5.1 일반 규정 (General) 5.2 조직 환경 (Context of the organization) 5.3 리더십 (Leadership) 5.4 계획 (Planning) 5.5 지원 (Support) 5.6 운영 (Operation) 5.7 성능 평가 (Performance evaluation) 5.8 개선 (Improvement)

6장 ISO/IEC 27002 관련 PIMS 지침
(PIMS-specific guidance related to ISO/IEC 27002)

6.1 일반 규정
(General)

6.2 정보보호 정책
(Information security policies)

6.3 정보보호 조직
(Organization of information security)

6.4 인적자원 보안
(Human resource security)

6.5 자산 관리
(Asset management)

6.6 접근 제어
(Access control)

6.7 암호화
(Cryptography)

6.8 물리적, 환경적 보안
(Physical and environmental security)

6.9 운영 보안
(Operations security)

6.10 통신 보안
(Communications security)

6.11 시스템 도입, 개발, 유지보수
(Systems acquisition, development and maintenance)

6.12 공급자 관계
(Supplier relationships)

6.13 정보보호 사고 관리

(Information security incident management) 6.14 업무 연속성 관리의 정보보호 측면 (Information security aspects of business continuity management) 6.15 준거성 (Compliance)
7장 PII 컨트롤러에 대한 추가지침 **(Additional ISO/IEC 27002 guidance for PII controllers)**
8장 PII 프로세서에 대한 추가지침 **(Additional ISO/IEC 27002 guidance for PII processors)**

ISO/IEC 27701은 1장 범위, 2장 참고문헌, 3장 용어, 정의 및 약어로 ISO/IEC 27001과 같은 구성을 가지며 4장 일반 규정부터는 ISO /IEC 27701에 대한 일반 규정들로 기존 ISO/IEC 27001과는 차이점을 가진다. 5장은 ISO/IEC 27001 관련 PIMS 요구사항, 6장은 ISO/IEC 27002 관련 PIMS 지침. 7장은 PII 컨트롤러에 대한 ISO/IEC 27002 추가지침, 8장은 PII 프로세서에 대한 ISO/IEC 27002 추가지침으로 구성된다. 이때 공통으로 적용된 변경사항은 ISO/IEC 27001 및 ISO/IEC 27002에서 언급되는 “정보보안”에 대한 요건들이 “정보보안 및 개인정보보호”로 확대된다는 사항이다.

2.3.3 ISMS-P

ISMS-P는 정보통신망법 제47조 (정보보호 관리체계의 인증)과 개인정보 보호법 제 32조의2(개인정보보호 인증)에 따라 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인증 기관(한국인터넷진흥원-KISA, 금융보안원-FSS)이 증명하는 제도로서, 정보보호를 위한 ISMS 인증과 정보보호 및 개인정보보호를 위한 ISMS-P 인증

으로 구분할 수 있다[11]. 이때 인증을 받기 위한 대상은 의무대상과 임의신청대상으로 구분되며, 의무대상은 보안사고가 발생 시 그에 따른 영향도가 사회·경제적으로 큰 파급력을 가지는 조직으로 정보통신망법 47조 제2항에 따라 다음 [표 2-4]가 해당한다.

[표 2-4] ISMS-P 의무대상자 기준

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조 제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다)
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당하는 자	1. 연간 매출액 또는 세입이 1,500억 원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의 4에 따른 상급종합병원 - 직전 연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교 2. 정보통신서비스 부문 전년도 매출액이 100억 원 이상인 자 3. 전년도 직전 3개월간의 일일 평균 이용자 수가 100만 명 이상인 자

2.3.4 ISMS-P 구성

ISMS-P 인증을 받기 위해서는 관리체계 수립 및 운영 16개, 보호대책 요구사항 64개, 개인정보 처리단계별 요구사항 22개로 총 102개로 구성되는 통제항목들을 충족해야 한다. ISMS-P 인증심사 시 102개, ISMS 인증심사 시 개인정보 처리단계별 요구사항 22개를 제외한 80개 통제항목을 기준으로 인증심사를 수행한다[6]. 상세항목은 다음[표 2-5]과 같다.

[표 2-5] ISMS-P 구성

영역	분야
1. 관리체계 수립 및 운영	1.1 관리체계 기반마련
	1.2 위험관리
	1.3 관리체계 운영
	1.4 관리체계 점검 및 개선
2. 보호대책 요구사항	2.1 정책, 조직, 자산 관리
	2.2 인적 보안
	2.3 외부자 보안
	2.4 물리 보안
	2.5 인증 및 권한 관리
	2.6 접근 통제
	2.7 암호화 적용
	2.8 정보시스템 도입 및 개발 보안
	2.9 시스템 및 서비스 운영관리
	2.10 시스템 및 서비스 보안관리
	2.11 사고 예방 및 대응
	2.12 재해복구
3. 개인정보 처리 단계별	3.1 개인정보 수집 시 보호조치

요구사항	3.2 개인정보 보유 및 이용 시 보호조치
	3.3 개인정보 제공 시 보호조치
	3.4 개인정보 파기 시 보호조치
	3.5 정보주체 권리 보호

또한, 앞서 언급한 인증 기관 중 금융보안원의 경우 위의 점검항목을 사용하는 것이 아닌 신용정보의 이용 및 보호에 관한 법령 및 규칙, 전자금융거래법에 관한 법령 및 규칙, 전자금융감독규정 및 시행세칙 등을 기반으로 금융권에 적합한 ISMS-P 인증 점검항목을 2016년에 개발하여 2017년부터 적용하고 있으며, 요구사항의 수는 102개로 일치하나 세부 점검항목의 수는 총 384개로 KISA에서 요구하는 325개의 점검항목에서 추가된 형태로 더욱 세부적인 사항을 포함하고 있다[9].

2.4 인증제도 분석 및 개선의 필요성

GDPR은 제2조 물적 범위와 제3조 지리적 범위에 규정되어 있는 근거에 따라 EU에 사업장을 가지고 있는 국내기업뿐만 아니라, 정보주체인 EU 회원국 국민에게 재화나 서비스를 제공하거나, 회원국 국민의 EU 내에서의 행동을 모니터링하는 국내기업 또한 적용 대상으로 규정하고 있다. 이는 현재 EU 회원국 국민을 대상으로 서비스를 제공하거나 앞으로 비즈니스를 계획하고 있는 국내기업들은 GDPR에서 요구되는 수준으로 정보주체의 권리를 보장하는 방법과 절차를 마련해야 하는 것으로, 기존 국내기업들은 정보주체 및 기업 내 정보를 보호하기 위해 국내에서 시행하고 있는 ISMS-P, 국외에서 시행하고 있는 ISO/IEC 27701등의 인증을 통해 정보보호 및 개인정보보호에 관한 관리체계를 수립하고 있다. 이때

ISMS-P의 문제점은 당초 목적 및 근거 그리고 요구항목은 국내 개인정보 보호법 및 정보통신망법을 기반으로 한 국내 환경에 맞게 수립된 인증인 만큼 EU GDPR에서 요구되는 항목과는 정의, 목적 등의 차이점으로 인한 보안요구사항 미흡 등으로 대비하지 못할 가능성이 있으며, ISO/IEC 27701의 경우 국외 인증 그리고 2019년 8월 시행된 만큼 국내 기업들에 있어 ISMS-P와 비교하면 ISO/IEC 27701의 인식 및 필요성이 낮으며 ISMS-P와 마찬가지로 GDPR에서 요구되는 항목에 미치지 못할 가능성이 있으므로 각각 ISMS-P와 ISO/IEC 27701을 분석하여, 공통으로 GDPR에서 요구되는 보안수준을 대비할 수 있는지, 부족하다면 부족한 항목에 대한 비교분석을 통해 개선항목을 도출하고 그에 따라 인증제도를 개선하여 GDPR을 대비할 필요성이 있다.

제 3 장 EU-GDPR 평가항목과 인증제도의 비교 및 개선

3.1 평가항목 도출

3.1.1 EU-GDPR 벌칙 기반 평가항목 도출

GDPR 벌칙을 기반으로 전체항목에서 평가항목 도출을 위해 다음과 [그림 3-1]과 같은 과정을 거친다.

[그림 3-1] GDPR 평가항목 도출과정

GDPR 전체 99개 조항 중 제83조 행정 과태료 부과에 관한 심각한 위반 조건의 근거하여 다음의 [표3-1]의 조항들을 도출한다.

[표 3-1] GDPR 심각한 위반 벌금조항

심각한 위반 : 2천만 유로 전 세계 연간 또는 매출액 4% 중 높은 금액	
구분	조항
동의의 조건을 포함한, 개인정보 처리원칙 위반	제5조, 제7조, 제9조
정보주체의 권리 보장 의무 위반	제12조, 제13조, 제14조, 제15조, 제16조, 제17조, 제18조, 제19조, 제20조, 제21조, 제22조
국제조직이나 제3국으로의	제44조, 제45조, 제46조, 제47조, 제48조,

개인정보 이전 시 준수 의무위반	제49조
감독기구가 내린 명령 또는 정보 처리의 제한 불복	제58조 제2항
개인정보 이동 중지 미준수 및 열람 기회 제공 의무 위반	제58조 제1항

GDPR 전체 99개 조항 중 제83조 행정 과태료 부과에 관한 일반 조건의 근거하여 다음의 [표3-2] 조항들을 도출한다.

[표 3-2] GDPR 일반 위반 벌금조항

일반 위반 : 1천만 유로 또는 전 세계 연간 매출액 2% 중 높은 금액	
구분	**조항**
프로세서 및 컨트롤러 의무위반	제8조, 제11조, 제25조, 제26조, 제27조, 제28조, 제29조, 제30조, 제31조, 제32조, 제33조, 제34조, 제35조, 제36조, 제37조, 제38조, 제39조, 제42조, 제43조
인증 기관의 의무위반	제42조, 제43조
행동규약 준수 모니터링 의무 위반	제41조 제4항

제83조에 근거하여 도출된 과태료 부과항목은 일반 위반 유형으로 22개, 심각한 위반 유형은 22개로 중복되는 항목들을 제외한 항목은 전체 99개 조항 중 42개 조항으로 도출되었다. 이 중 실제 벌금이 부과된 사례 410개를 기반으로 인증제도 개선을 위한 평가항목 14개를 다음[표 3-3]과 같이 도출하였다.

[표 3-3] GDPR 평가항목

조항	주요 내용	위반 횟수
제5조	개인정보 처리 원칙 (1) 데이터 최소화, (2) 정확성, (3) 목적제한, (4) 저장기간 제한, (5) 무결성과 기밀성, (6) 적법성, 공정성, 투명성 **- 적법한 데이터 처리에 관한 규정 미준수**	31
제6조	처리의 적법성 **- 개인정보 처리에 대한 법적근거 불충분**	14
제7조	동의의 조건 **- 동의를 위한 정확한 정보 미제공**	2
제9조	특정 범주의 개인정보의 처리 **- 처리가 금지된 개인정보의 처리**	1
제12조	개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 **- 정보주체의 권리를 보장하기 위한 정보 미제공**	4
제13조	개인정보가 개인정보 주체로부터 수집되는 경우 제공되는 정보 **- 정보주체의 개인정보 수집 시 정보 미제공**	5
제14조	개인정보가 개인정보 주체로부터 수집되지 않은 경우 제공되는 정보 **- 제 3자로부터 개인정보 수집 시 정보 미제공**	9
제15조	개인정보주체의 열람권 **- 개인정보주체의 열람권 미보장**	3
제17조	삭제권('잊힐 권리') **- 개인정보주체의 삭제권 미보장**	4
제21조	반대할 권리 **- 개인정보 처리에 관한 반대권리 미보장**	4
제25조	설계 및 기본설정에 의한 개인정보보호 **- 개인정보를 보호하기 위한 적절한 보안 조치 미고려**	6

제28조	프로세서 **- 불충분한 데이터 처리 계약**	1
제29조	컨트롤러 및 프로세서의 권한에 따른 처리 **- 제3자에 의한 개인정보 처리**	1
제32조	처리의 보안 **- 개인정보에 대한 적정한 기술 및 관리적 조치 미이행**	20

3.2 평가항목 기준 인증제도 비교

3.2.1 ISO/IEC 27701 분석

ISO/IEC 27701은 ISO/IEC 27001과 ISO/IEC 27002를 기반으로 개인정보보호에 관한 확장판이며, 조직의 개인식별정보를 보호하기 위한 컨트롤러 및 프로세서에 관한 지침도 제공하고 있다. 이때 컨트롤러와 프로세서의 용어는 국내 개인정보 보호법에서 정의되고 있는 위탁자 및 수탁자와는 분명 다른 것으로 다음과 같은 차이점을 보인다. GDPR 제4조 7항에서 정의하고 있는 컨트롤러는 개인정보의 처리, 수단, 목적을 단독 또는 공동으로 결정하는 자연인, 공공기관, 법인, 기타 단체 등을 의미한다[3]. 프로세서는 제4조 8항에 따라 컨트롤러를 대신하여 개인정보를 처리하는 자연인, 공공기관, 법인, 기타 단체 등을 의미한다. ISO/IEC 27001이나 ISO/IEC 27002에서는 프로세서 및 컨트롤러에 관한 용어 및 정의를 사용하고 있지 않으나 이에 대한 확장판인 ISO/IEC 27701에서는 컨트롤러와 프로세서의 용어를 사용하며 이에 따른 지침을 제공하고 있어 GDPR 대비하기 위한 적절한 기반이 된다[15].

3.2.2 ISMS-P 분석

ISMS-P는 정보통신망법 제47조, 개인정보 보호법 제32조의 2에 따라 인증심사를 신청한 조직이 정보보호 및 개인정보보호를 위한 일련의 조치와

활동이 인증기준에 적합함을 인증기관이 증명하는 제도이다.

2018년 11월 7일 정보보호 및 개인정보보호 관리체계 인증에 관한 고시가 시행되어 ISMS와 PIMS의 인증제도 통합 이후 연구가 진행된 현시점까지 한국인터넷진흥원을 통해 370개의 인증서가 발급되고 그중 368개의 인증서가 유지되고 있다. ISO/IEC 27001은 국내 한국인정지원센터에 등록된 국내 인증서 발급 현황이 63개로 ISMS-P와 비교하면 확연히 인증 기업의 수가 적다. ISO/IEC 27701의 경우 ISO/IEC 27001 인증이 선행되어야 하므로 국내 ISO/IEC 27701의 인증현황은 이보다 더욱 적을 것으로 판단된다. 이처럼 국내에는 ISO/IEC 27701보다 ISMS-P를 기반으로 한 보호대책을 수립하고 있는 기업의 수가 많으므로 GDPR에서 요구되는 항목들에 ISMS-P를 매핑하여 개선항목을 도출하여 개선방안을 제시하는 것이 GDPR을 대비하는 데 도움이 될 것이다.

3.2.3 GDPR 평가항목 기준 인증제도 매핑

GDPR 평가항목에 따른 ISO/IEC 27701과 ISMS-P의 인증항목별 매핑은 다음 [표 3-4]와 같다.

[표 3-4] 평가항목 기준 인증제도 매핑

평가항목	인증제도		비고
제5조 개인정보 처리원칙(1항, 2항)			
1항 (a) 개인정보 주체에 대해 적법하고, 공정하며, 투명하게 처리되어야 한다. (적법성, 공정성, 투명성)	ISO/IEC 27701	7.2.2 법률적 근거 파악 8.2.2 조직 목적	-
	ISMS-P	3.1.1 개인정보 수집 제한 3.2.5 개인정보 목적 외 이용 및 제공	-
1항 (b) 구체적이고 명시적이며 적법한	ISO/IEC	7.2.1 식별 및 문서화 목적	-

목적을 위해 수집되어야 한다. (목적 제한)	27701	7.4.1 수집 제한 8.2.2 조직 목적	
	ISMS-P	3.1.1 개인정보 수집 제한 3.2.5 개인정보 목적 외 이용 및 제공	-
1항 (c) 처리되는 목적과 관련하여 적절하고, 타당하며, 필요한 정도로만 제한되어야 한다. (데이터 최소화)	ISO/IEC 27701	7.4.1 수집 제한 7.4.4 PII 최소화 목표 7.4.5 처리 종료 시 PII 비식별화 및 삭제 8.4.1 임시 파일	-
	ISMS-P	3.1.1 개인정보 수집 제한	-
1항 (d) 정확해야 하고, 필요한 경우 최신의 것이어야 한다. (정확성)	ISO/IEC 27701	7.3.6 접근, 수정 및 삭제 7.4.3 정확도 및 품질	-
	ISMS-P	3.2.2 개인정보 품질 보장	-
1항 (e) 처리목적 달성에 필요한 기간에만 보관되어야 한다.	ISO/IEC 27701	7.4.4 PII 최소화 목표 7.4.5 처리 종료 시 PII 비식별화 및 삭제	-
	ISMS-P	3.4.1 개인정보의 파기	-
1항 (f) 개인정보의 적절한 보안을 보장하는 방식으로 처리해야 한다.	ISO/IEC 27701	6.3.2.1 모바일 기기 정책 6.5.2.1 정보 등급 분류 6.6.2.2 사용자 접근 권한 설정 6.8.2.7 장비 안전 폐기 및 재사용 6.9.3.1 정보 백업 6.10.2.1 정보 전송 정책 및 절차	-

		6.11.3.1 시험 데이터 보호 6.12.1.2 공급자 협약 내 보안 명시 6.13.1.1 책임 및 절차 6.15.1.1 적용 법규 및 계약 요구사항 식별	
	ISMS-P	2.10.6 업무용 단말기기 보안 2.1.3 정보자산 관리 2.5.2 사용자 식별 2.9.3 백업 및 복구관리 2.9.7 정보자산의 재사용 및 폐기 2.8.4 시험 데이터 보안 2.10.5 정보전송 보안 2.11.1 사고 예방 및 대응체계 구축	-
2항 컨트롤러는 제1항이 준수되도록 할 책임이 있다.	ISO/IEC 27701	6.15.1.3 기록 보호 7.2.6 PII 프로세서와의 계약 7.2.8 PII 처리 관련 기록	-
	ISMS-P	2.3.2 외부자 계약 시 보안 3.5.3 이용 내역 통지	-
제6조 처리의 적법성(1항, 4항)			
1항 개인정보 처리는 다음 각호의 하나에 해당되고 그 범위에서만 적법하다. (a) 개인정보 주체가 목적에 대해 개인	ISO/IEC 27701	7.2.2 법률적 근거 파악	-

정보 처리를 동의한 경우 (b) 계약을 이행하거나 개인정보 주체가 요청한 조치를 취하기 위해 처리가 필요한 경우 (c) 컨트롤러의 법적 의무를 준수하는데 개인정보 처리가 필요한 경우 (d) 개인정보 주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 개인정보 처리가 필요한 경우 (e) 공익을 위하거나 공식 권한을 행사하여 이루어지는 업무수행에 처리가 필요한 경우 (f) 컨트롤러 또는 제3자의 정당한 이익 목적을 위한 처리가 필요한 경우			
	ISMS-P	3.1.1 개인정보 수집 제한	-
4항 (e) 암호처리나 가명처리 등 적절한 안전조치의 존재	ISO/IEC 27701	7.4.5 처리 종료 시 PII 비식별화 및 삭제	-
	ISMS-P	2.7.1 암호정책 사용	-
제7조 동의의 조건(1항, 3항)			
1항 컨트롤러는 개인정보 주체가 본인의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.	ISO/IEC 27701	7.2.4 동의 및 동의기록	-
	ISMS-P	3.1.2 개인정보의 수집 동의	-
3항 개인정보 주체는 언제든지 본인의 동의를 철회할 권리를 가진다.	ISO/IEC 27701	7.3.4 동의를 수정하거나 철회할 수 있는 메커니즘 제공	-
	ISMS-P	3.5.2 정보주체 권리보장	-
제9조 특정 범주의 개인정보의 처리(1항)			

1항 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강정보, 성생활 또는 성적 취향에 관한 정보의 처리는 금지된다.	ISO/IEC 27701	7.2.2 법률적 근거 파악	-
	ISMS-P	3.1.1 개인정보 수집 제한	-
제12조 개인정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 (1항, 3항, 4항)			
1항 컨트롤러는 규정된 일체의 통지를 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 개인정보 주체에게 제공하기 위한 적절한 조치를 취해야 한다.	ISO/IEC 27701	7.3.3 PII 주체에게 정보 제공	-
	ISMS-P	3.5.3 이용내역 통지	**개선**
3항 컨트롤러는 요청을 접수한 후 한 달 이내에 부당한 지체 없이, 요청에 따라 취해진 조치를 개인정보 주체에게 전달해야 한다.	ISO/IEC 27701	7.3.9 처리 요청	-
	ISMS-P	3.5.2 정보주체 권리보장	-
4항 컨트롤러가 개인정보 주체의 요청에 대해 조치를 취하지 않는 경우, 개인정보 주체에게 지체 없이 통지해야 하고 조치를 취하지 않은 사유 및 민원을 제기하고 사법구제를 받을 수 있는 가능성 대해 개인정보 주체에게 고지해야 한다.	ISO/IEC 27701	7.3.9 처리 요청	-
	ISMS-P	3.5.2 정보주체 권리보장	**개선**
제13조 개인정보가 개인정보 주체로부터 수집되는 경우 제공되는 정보 (1항, 3항)			
1항 개인정보 주체에 관련된 개인정보	ISO/IEC	7.3.2 PII 주체에 대한	-

를 개인정보 주체로부터 수집되는 경우, 컨트롤러는 개인정보를 취득할 당시 개인정보 주체에게 다음 각 호의 정보 일체를 제공해야 한다. (c) 해당 개인정보의 예정된 처리의 목적뿐 아니라 처리의 법적 근거	27701	정보 결정	
	ISMS-P	3.1.2 개인정보 수집 동의	**개선**
3항 컨트롤러가 개인정보를 수집한 목적 외로 추가 처리할 예정인 경우, 컨트롤러는 추가 처리 이전에, 개인정보 주체에게 해당하는 기타 목적에 관한 정보와 제2항의 관련 추가 정보 일체를 제공해야 한다.	ISO/IEC 27701	7.3.2 PII 주체에 대한 정보 결정 7.3.3 PII 주체에게 정보 제공	-
	ISMS-P	3.2.5 개인정보 목적 외 이용 및 제공	-
제14조 개인정보가 개인정보 주체로부터 수집되는 않는 경우 제공되는 정보(1항)			
1항 개인정보가 개인정보주체로부터 수집되지 않은 경우, 컨트롤러는 다음 각 호의 정보를 개인정보주체에게 제공해야 한다. (c) 해당 개인정보의 예정된 처리 목적뿐 아니라 처리의 법적 근거	ISO/IEC 27701	7.3.2 PII 주체에 대한 정보 결정	-
	ISMS-P	3.1.5 간접 수집 보호조치	-
제15조 개인정보주체의 열람권(1항, 3항)			
1항 개인정보 주체는 개인정보 및 다음 각 호의 정보에 대한 열람권을 가진다. (a) 처리 목적 (b) 관련된 개인정보의 범주 (c) 개인정보를 제공받았거나 제공받을 수령인, 수령인의 범주	ISO/IEC 27701	7.3.2 PII 주체에 대한 정보 결정	-

(d) 개인정보의 예상 보관 기간 (e) 개인정보에 대한 정정, 삭제 또는 개인정보주체 본인에 관한 처리의 제한 및 반대를 요구할 권리 (f) 감독기관에 민원을 제기할 수 있는 권리	ISMS-P	3.5.2 정보주체 권리보장	-
3항 컨트롤러는 처리가 진행 중인 개인정보의 사본을 제공해야 한다.	ISO/IEC 27701	8.3.1 PII 주체에 대한 의무	-
	ISMS-P	3.5.3 이용 내역 통지	-
제17조 삭제권('잊힐 권리')(1항)			
1항 개인정보주체는 본인에 관한 개인정보의 삭제를 요청할 권리를 가지며, 컨트롤러는 다음 각 호가 적용되는 경우, 부당한 지체 없이 개인정보를 삭제할 의무를 가진다. (a) 개인정보가 수집, 처리된 목적에 더 이상 필요하지 않은 경우 (b) 개인정보 주체가 처리의 기반이 되는 동의를 철회하고 해당 처리의 대한 기타 법적 근거가 업는 경우 (c) 개인정보 주체가 처리에 반대하는 경우 (d) 개인정보가 불법적으로 처리된 경우 (e) 법적 의무를 준수하기 위해 개인정보가 삭제되어야 하는 경우 (f) 제8조 1항에 규정된 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우	ISO/IEC 27701	7.3.6 접근, 수정 및 삭제	-
	ISMS-P	3.5.2 정보주체 권리보장	-

제21조 반대할 권리(1항, 3항)			
1항 개인정보 주체는 본인의 특별한 상황에 따라 프로파일링 등, 본인과 관련한 개인정보의 처리에 대해 언제든지 반대할 권리를 가진다. 3항 개인정보 주체가 직접 마케팅을 위한 처리에 반대하는 경우, 해당 개인정보는 더 이상 그러한 목적으로 처리될 수 없다.	ISO/IEC 27701	7.3.5 접근, 수정 및 삭제	-
	ISMS-P	3.1.7 홍보 및 마케팅 목적 활용 시 조치	-
제25조 설계 및 기본설정에 의한 개인정보보호(1항)			
1항 컨트롤러는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 가명처리 등의 기술 및 관리적 조치를 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 이행해야 한다.	ISO/IEC 27701	6.11.2.1 개발 보안 정책 6.11.2.5 시스템 보안 공학 원칙	-
	ISMS-P	2.8.1 보안 요구사항 정의	-
제28조 프로세서(1항, 3항)			
1항 컨트롤러를 대신하여 처리가 이루어지는 경우, 컨트롤러는 적절한 기술 및 관리적 조치 이행을 통해 그 처리가 본 규정의 요건을 충족시키고, 개인정보주체의 권리를 보호하도록 충분한 보증을 제공하는 프로세서만 이용해야 한다.	ISO/IEC 27701	6.12.1.2 공급자 협약 내 보안 명시 6.15.1.1 적용 법규 및 계약 요구사항 식별	-
	ISMS-P	2.3.2 외부자 계약 시 보안 2.10.5 정보전송 보안	-

3항 프로세서의 처리는 컨트롤러와 관련하여 프로세서에게 구속력을 가지고, 처리의 주제와 지속기간, 처리의 성격과 목적, 개인정보의 유형과 개인정보 주체의 범주, 컨트롤러의 의무와 권리를 규정하는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 규제를 받는다.	ISO/IEC 27701	6.10.2.4 기밀유지 협약 6.12.1.2 공급자 협약 내 보안 명시 6.15.1.1 적용 법규 및 계약 요구사항 식별 8.2.1 고객 동의 8.2.2 조직 목적 8.2.4 침해 교육 8.2.5 고객 의무 8.5.4 PII 공개 요청 통지 8.5.7 PII 처리에 협력업체의 참여	-
	ISMS-P	2.2.3 보안 서약 2.3.2 외부자 계약 시 보안 2.10.5 정보전송 보안 3.1.2 개인정보의 수집 동의 3.5.2 정보주체 권리보장 3.4.1 개인정보의 파기	-
제29조 컨트롤러 및 프로세서의 권한에 따른 처리			
프로세서, 그리고 컨트롤러나 프로세서의 권한에 따라 행하는 자로서 개인정보를 열람할 수 있는 자는 유럽연합 또는 회원국 법률로 요구되는 경우가 아니라면 컨트롤러의 지시에 따른 경우를 제외하고 해당 개인정보를 처리해서는 안 된다.	ISO/IEC 27701	8.2.2 조직 목적	-
	ISMS-P	3.2.5 개인정보 목적 외 이용 및 제공	-
제32조 컨트롤러 및 프로세서의 권한에 따른 처리(1항, 2항)			

1항 (a) 개인정보의 가명처리 및 암호처리	ISO/IEC 27701	6.5.3.3 물리적 매체 이송 6.7.1.1 암호 통제 사용 정책 6.11.1.2 공중망 응용 서비스 보안 7.4.5 처리 종료 시 PII 비식별화 및 삭제	-
	ISMS-P	2.7.1 암호정책 사용	**개선**
1항 (b) 처리 시스템 및 서비스의 지속적인 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 역량	ISO/IEC 27701	5.4.1.2 정보보호 위험평가 5.4.1.3 정보보호 위험처리 6.11.1.2 공중망 응용 서비스	-
	ISMS-P	1.2.3 위험 평가 1.2.4 보호대책 선정 2.6.2 정보시스템 접근	-
1항 (c) 물리적 또는 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원 할 수 있는 역량	ISO/IEC 27701	6.9.3.1 정보 백업	-
	ISMS-P	2.9.3 백업 및 복구관리	-
1항 (d) 처리의 보안을 보장하는 기술 또는 관리적 조치의 효율성을 정기적으로 테스트 및 평가하기 위한 절차	ISO/IEC 27701	6.15.2.1 정보보호 독립적 검토 6.15.2.3 기술 준거성 검토	-
	ISMS-P	2.8.2 보안 요구사항 검토 및 시험	-
2항 보안의 적정 수준을 평가할 때는 처리로 인해 발생하는 위험성, 특히 이전, 저장 또는 다른 방식으로 처리된 개인정보에 대한 우발적 또는 불법적 파기, 유실, 변경, 무단 제공, 무단 열람에 대해 고려해야 한다.	ISO/IEC 27701	5.2.3 정보보호 경영시스템의 범위 결정 5.2.4 정보보호 경영시스템 5.4.1.2 정보보호 위험평가 5.4.1.3 정보보호 위험처리 6.5.2.1 정보 등급 분류 6.15.2.1 정보보호 독립적	-

		검토 6.15.2.3 기술 준거성 검토	
	ISMS-P	1.1.4 범위 설정 1.1.5 정책 수립 1.1.6 자원 할당 1.2.2 현황 및 흐름 분석 1.2.3 위험평가 1.2.4 보호대책 선정 2.1.3 정보자산 관리 2.8.2 보안 요구사항 검토 및 시험	-

3.3 평가항목 기준 분석 결과

GDPR 평가항목과 인증제도들을 매핑한 결과, ISO/IEC 27701의 경우 중복된 항목을 제외하면 5장. ISO/IEC 27001 관련 PIMS 요구사항에서 4개 통제항목, 6장. ISO/IEC 27002 관련 PIMS 지침에서 21개 통제항목, 7장. PII 컨트롤러에 대한 추가지침 16개 통제항목, 8장 PII 프로세서에 대한 추가지침 9개로 총 50개 통제항목에서 GDPR 평가항목과 빠짐없이 매핑되었으며, 이는 기업이 속한 국가의 법률을 근거하여 ISO/IEC 27701 통제항목들을 기반으로 한 보안체계를 수립한다면 GDPR을 부족함 없이 대비할 수 있다는 것을 의미한다. ISMS-P의 경우 중복된 항목을 제외하면 1. 관리체계 수립 및 운영 영역 7개 항목, 2. 보호대책 요구사항 영역 15개 항목, 3. 개인정보 처리단계별 요구사항 영역 10개로 총 32개 항목과 매핑되었으나, GDPR 제6조 (4항), 제12조 (1항, 4항), 제14조 (1항)에서 요구되는 항목에 미흡하여 국내기업들이 ISMS-P를 기반으로 한 GDPR 대응체계를 수립하기 위해서는 다음[표3-5]을 개선하는 것이 필요하다.

[표 3-5] ISMS-P 개선항목

ISMS-P 개선 필요항목	GDPR 평가항목	판단근거
2.7.1 암호정책 사용	제32조 처리의 보안 1항 (a)	개인정보의 보호를 위한 보호조치 중 가명처리 방안 내용 미흡
3.1.2 개인정보 수집 동의	제13조 개인정보가 개인정보 주체로부터 수집되는 경우 제공되는 정보 1항 (c)	정보주체로부터 개인정보가 수집되는 경우 개인정보를 취득할 당시 처리의 목적뿐 아니라 법적근거를 정보주체에게 제공해야 한다는 내용 미흡
3.5.2 정보주체 권리보장	제12조 개인정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 4항	정보주체 요구에 불복하는 경우, 정보주체에게 관련 사유 등에 관한 내용을 지체없이 통지하여야 한다는 내용 미흡
3.5.3 이용내역 통지	제12조 개인정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 1항	정보주체가 관련 내용을 명확히 이해하기 쉬운 언어를 사용해야 한다는 내용 미흡

3.4 EU-GDPR 대응 개선방안

3.4.1 EU-GDPR 대응 개선방안 도출

GDPR 평가항목과 인증제도 간의 매핑을 통해 ISMS-P에서 개선이 필요한 항목들을 앞서 [표3-5]와 같이 도출하였다. 개선방안은 국내 환경에 준수될 수 있도록 개정된 개인정보 보호법을 기반으로 다음 [표 3-6]과 같이 도출하였다.

[표 3-6] ISMS-P 개선방안

코드	항목	인증기준
A-1	2.7.1 암호정책 사용	주요정보 보호 및 개인정보를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용, 가명처리 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호처리 및 가명처리를 통한 적절한 보호 대책을 적용해야 한다.
A-2	3.1.2 개인정보 수집 동의	개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 관련 정보 및 개인정보 처리에 관한 법적근거를 제공하고 그에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.
A-3	3.5.2 정보주체 권리보장	정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 만약 정보주체의 요청에 대해 불복할 경우 관련 내용을 지체 없이 통지하며, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
A-4	3.5.3 이용내역 통지	개인정보의 이용내역 등 정보주체(이용자)에게 통지하여야 할 사항을 파악하여 그 내용을 명확하고 평범한 언어를 사용하여 정확하고, 투명하며, 간결한 형식으로 주기적으로 통지하여야 한다.

4 장 인증제도 개선방안의 활용

4.1 개선방안을 활용한 보안사고 대응방안

4.1.1 (A-1) 독일 감독기구의 K사 벌금 부과사례

(위반 유형) 부적절한 기술적 또는 관리적 보안 조치

(위반 조항) 제32조 1항 (a)

(개요) 소셜미디어회사인 K사는 해킹의 공격으로 186만 개의 사용자 이름/비밀번호 조합과 80만 개 이상의 전자메일 주소가 유출됨. K사는 곧바로 GDPR 34조에 따라 포괄적이고 투명한 방법으로 공격에 대한 개인정보 유출 사실을 사용자들에게 통지하였다.

(사건 분석) 해당 사례에서는 해킹공격으로 인한 피해가 발생함에 따라 기업이 취해야 할 조치를 K사는 GDPR 제34조에 따라 올바르게 통지하였다. 문제는 독일 감독기구(Baden Württemberg DPA)는 조사 중 K사가 비밀번호를 일반 텍스트로 저장함으로써 개인정보를 처리할 때 정보보안을 보장할 의무를 고의로 위반한 사실과 비밀번호를 암호화하지 않은 형식으로 저장하여 공격을 용이하게 했다는 사실을 발견하여 이로 인해 €150,000 벌금을 부과하였다.

(조치 방안 예시) 해당 사례를 국내 환경에서 발생한 것으로 가정하여 국내기업이 취해야 할 대응방안으로는, 개선된 ISMS-P 2.7.1 암호 정책사용을 기반으로 기업은 법적 요구사항을 반영한 암호 및 가명처리에 관한 정책을 수립한다. 이때 암호처리는 국내 개인정보의 안전성 확보조치 기준 제7조 개인정보의 암호화 5항에 따라 안전한 암호알고리즘으로 암호화하며, 가명처리는 개인정보 보호법 제2조 1의 2에 따라 “개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록” 처리하며 추가적으로 해당 정책이 적용될 수

있도록 IT 보안 아키텍처를 개선하고, 정기적인 모의침투 테스트(Penetration Testing)를 통해 해킹에 대해 대비를 함으로써 위 벌금 부과 사례를 대비할 수 있다[5][4].

4.1.2 (A-2) 그리스 감독기구의 P사 벌금 부과사례

(위반 유형) 개인정보 처리에 대한 법적 근거 불충분

(위반 조항) 제13조 1항 (c)

(개요) P사의 직원들은 개인정보 이용 규정에 관한 동의 문서에 서명하도록 강제되었으며 그에 따른 "동의"가 자유롭게 이루어지지 못한다는 문제로 인해 그리스의 감독기구(Hellenic Data Protection Authority, 이하 HDPA)는 €150,000 벌금을 부과하였다.

(사건 분석) 해당 사례는 고용주와 직원 사이에 고용 관계에 있어 정보주체인 직원의 동의는 지위의 불균형으로 자유롭지 못한 측면이 있으며, GDPR 시행 이전에는 회사가 직원의 개인정보를 다룸에 있어 "직원의 동의"에 포괄적으로 의존하는 것을 적법하게 보았으나 GDPR 시행 이후 동의의 비자율성을 고려하여 직원의 개인정보를 다루는 것에는 사안마다 개별적인 법적 근거가 필요하며 사안별로 근거로 삼는 법적 근거를 직원에게 정보를 제공해야 함에도 이를 준수하지 못한 문제점이 벌금이 부과된 주요 쟁점 사항이다.

(조치 방안 예시) 해당 사례를 국내 환경에서 발생한 것으로 가정하여 국내기업이 취해야 할 대응방안으로는, 개선된 ISMS-P 3.1.2 개인정보 수집 동의를 기반으로 개인정보 수집 시 개인정보 보호법 제15조 2항에 따른 사항 1. 개인정보의 수집·이용 목적, 2. 수집하려는 개인정보의 항목, 3. 개인정보의 보유 및 이용기간, 4. 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우에는 그 불이익의 내용과 직원의 개인정보를 처리하는 사안별로 그에 따른 법적 근거를 직원에게 제공하여 동의를 받는 것으로 해당 벌금 부과사례를 대비할 수 있다.

4.1.3 (A-3) 이탈리아 감독기구의 M사 벌금 부과사례

(위반 유형) 데이터 처리원칙 미준수

(위반 조항) 제12조 4항

(개요) M사는 고용 관계가 종료된 직원의 이메일 계정을 활성 상태로 유지하였으며, 정보주체인 직원의 삭제 요청에도 불구하고 응답하지 않아, 이탈리아 감독기구(Garante)는 M사에게 €15,000 벌금을 부과하였다.

(사건 분석) 해당 사례는 고용 관계가 종료된 사항에 대해 정보주체의 정보가 담긴 이메일 계정을 삭제치 않고, 자동으로 공지되는 메일들을 정보 주체에게 전송한 것과 이에 대한 정보주체의 접근 및 삭제 요청에도 대응 및 관련 정보를 제공하지 않았다는 문제점이 있다. 이는 당초 개인정보 수집 목적에 따라 개인정보의 이용 목적이 종료된 시점의 관련 정보를 파기해야 하며, 이를 불복할 시 그에 따른 그 사유를 정보 주체에게 지체 없이 통지해야 하고, 그에 따라 민원 제기 방법 및 절차에 대해 고지해야 한다.

(조치 방안 예시) 해당 사례를 국내 환경에서 발생한 것으로 가정하여 국내기업이 취해야 할 대응방안으로는, ISMS-P 3.4.1 개인정보의 파기에 따라 파기 관련 내부 정책을 수립하고 그에 따라 안전성 및 완전성이 보장될 방법으로 지체 없이 파기하며, 또한 이를 이행할 수 없는 경우 개선된 ISMS-P 3.5.2 정보주체 권리보장을 기반으로 정보주체의 요구를 불복한 사유와 함께 개인정보보호위원회에 이의를 제기할 방법 및 절차에 대해 정보 주체에게 안내함으로써 해당 벌금 부과사례를 대비할 수 있다.

4.1.4 (A-4) 이탈리아 감독기구의 W사 벌금 부과사례

(위반 유형) 데이터 처리원칙 미준수 및 권리 행사를 위한 정보 미제공

(위반 조항) 제12조 1항

(개요) 이탈리아 W사는 사용자의 동의 없이 마케팅 캠페인을 목적으로 데이터를 불법적으로 처리함으로 이탈리아 감독기구(Garante)는 W사에 €16,700,000 벌금을 부과하였다.

(사건 분석) 해당 사례는 100명 이상의 고객이 개인의 동의 없이 원치 않는 문자, 이메일, 팩스 및 자동 전화를 통한 마케팅 전화를 받아 불만을 제기하였으며, 고객들은 해당 기업의 개인 정보보호 정책에서 필요한 정보를 제공하지 않아 기업이 처리하는 개인정보에 대해 GDPR 제17조 삭제권에 해당하는 권리를 행사할 수 없었다, 또한 정보 주체 중 일부는 직접적인 반대에도 불구하고 공중전화 목록에 게시되어 있다고 보고되었다.

(조치 방안 예시) 해당 사례를 국내 환경에서 발생한 것으로 가정하여 국내기업이 취해야 할 대응방안으로는, ISMS-P 3.1.7 홍보 및 마케팅 목적 활용 시 조치에 따라 그 목적을 분명 정보주체가 명확히 인지할 수 있도록 고지하여 동의를 받아 개인정보를 수집하며, 개선된 ISMS-P 3.5.3 이용내역 통지에 따라 개인정보 처리내용에 대해서는 정보주체가 알기 쉽게 정확하고 투명하게 정기적으로 제공하는 것으로 위 벌금 부과 사례를 대비할 수 있다.

5 장 결 론

본 논문에서는 GDPR의 적용을 받는 국내기업을 위한 국내·외 개인정보보호 인증의 실효성 및 개선방안을 도출하는 것을 목적으로 연구하였다. 그리고 실제 GDPR 벌금부과사례를 기반으로 도출된 평가항목을 기준으로 ISO/IEC 27701과 ISMS-P의 통제항목들을 분석하고 그에 따른 ISMS-P의 개선항목을 도출하고 제안하였다.

제안한 ISMS-P의 개선항목은 첫 번째 2.7.1 암호정책 사용은 개인정보 보호대책 수립 시 가명처리에 관한 개념을 추가하였으며, 두 번째 3.1.2 개인정보 수집 동의는 개인정보 동의를 받을 때 처리에 관한 법적 근거를 제공해야 한다는 내용을 추가하였으며, 세 번째 3.5.2 정보주체 권리보장은 정보주체 요청에 불복할 경우 불복한 사유 및 관련 내용을 통제하게끔 추가, 마지막 네 번째 3.5.3 이용내역 통지는 개인정보 이용내역에 대해 그 내용을 정보주체가 명확히 이해할 수 있도록 정확하며, 간결한 형식으로 통지해야 한다는 내용을 추가하였다. 이처럼 ISMS-P 개선항목은 정보주체의 개인정보를 보다 안전하게 보호하고 그 권리를 보장하기 위한 방향으로 제안되었다.

그러나 위와 같은 개선항목들은 그 자체만으로는 GDPR의 각 조항에 대한 각기 한가지들의 대응방안일 뿐이지만, 실제 기업이 변화하는 시대 속 정보보안 흐름, 최신 위협 동향 등을 분석하고, 직원들의 인식제고를 위한 정기적 교육, 경영진의 지속적인 관심 등과 함께 제안한 ISMS-P 개선방안을 활용한 기업에 맞는 최선의 개인정보보호 관리체계를 수립한다면 GDPR을 대비하는 기반이 되는 데 도움이 될 것이라 기대한다.

참고문헌

[1] 김성현. EU GDPR과 국내 개인정보보호 관련 법률의 비교분석 연구. 중앙대학교 대학원, 2019, 02.

[2] 고학수, 이창범, 안정민, 최경진. GDPR 등 EU와 우리나라의 온라인상 개인정보보호 법제 비교 연구. 가천대학교 산학협력단, 2016, 11.

[3] 최수용. GDPR에 대한 고찰과 ISMS-P 인증 기업들의 GDPR 대응에 관한 연구. 동국대학교 대학원, 2019, 02.

[4] 국가법령정보센터. 개인정보 보호법. 2020, 08.

[5] 한국인터넷진흥원. 개인정보의 안전성 확보조치 기준 해설서. 2018, 06.

[6] 한국인터넷진흥원. 정보보호 및 개인정보보호 관리체계 인증제도 안내서. 2019, 01

[7] 한국인터넷진흥원. 2020 EU 일반개인정보보호법(GDPR) 가이드북. 2020, 05.

[8] ISO/IEC. ISO/IEC 27701:2019(Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines). 2019, 08.

[9] 금융보안원, “금융권에 적합한 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증기준 점검항목. http://www.fsec.or.kr/user/bbs/fsec/148/319/bbsDataView/1359.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory= (Accessed 2020, 12, 09)

[10] 최경진, 유럽 일반정보보호규정(EU GDPR)의 분석 및 시사점. https://privacy.naver.com/download/EU_GDPR.pdf (Accessed 2020, 12, 09)

[11] 한국인터넷진흥원, ISMS-P 제도소개.

https://isms.kisa.or.kr/main/ispims/intro/ (Accessed 2020, 12, 09)
[12] 한국인터넷진흥원 GDPR 대응지원센터, 위반 및 과징금 부과사례.
https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000063 (Accessed 2020, 12, 09)
[13] 한국인터넷진흥원 GDPR 대응지원센터, GDPR 조문 번역문.
https://gdpr.kisa.or.kr/gdpr/static/gdprProvision.do (Accessed 2020, 12, 09)
[14] 한국인터넷진흥원 GDPR 대응지원센터, 정보주체의 권리.
https://gdpr.kisa.or.kr/gdpr/static/infoSubjectsRights.do (Accessed 2020, 12, 09)
[15] NAVER 개인정보보호 블로그, EU GDPR에서의
컨트롤러(Controller)와 프로세서(Processor).
https://m.blog.naver.com/n_privacy/221298526423 (Accessed 2020, 12, 09)
[16] PRIVACY Affairs, GDPR 벌금추적 및 통계.
https://www.privacyaffairs.com/gdpr-fines/ (Accessed 2020, 12, 09)

부 록

[부록 1] GDPR 전체조항

EU GDPR에 관한 전체조항 및 구성은 [표 6-1]과 같다.

[표 6-1] GDPR 전체조항 및 구성

구분	조항
제 I 장 일반 규정	제1조 주제 및 목적 제2조 물적 범위 제3조 영토의 범위 제4조 정의
제 II 장 원칙	제5조 개인정보 처리 원칙 제6조 처리의 적법성 제7조 동의의 조건 제8조 정보사회 서비스와 관련하여 아동의 동의에 적용되는 조건 제9조 특정 범주의 개인정보의 처리 제10조 범죄경력 및 범죄행위에 관한 개인정보의 처리 제11조 신원확인을 요하지 않는 개인정보의 처리
제 III 장 개인정보 주체의 권리	제12조 개인정보 주체의 권리 행사를 위한 투명한 정보, 통지 및 형식 제13조 개인정보가 개인정보 주체로부터 수집되는 경우 제공되는 정보 제14조 개인정보가 개인정보 주체로부터 수집되지 않는 경우 제공되는 정보 제15조 개인정보 주체의 열람권 제16조 정정권 제17조 삭제권('잊힐 권리')

	제18조 처리에 대한 제한권 제19조 개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무 제20조 개인정보 이전권 제21조 반대할 권리 제22조 프로파일링 등 자동화된 개별 의사결정 제23조 제한
제 IV 장 컨트롤러와 프로세서	제24조 컨트롤러의 책임 제25조 설계 및 기본설정에 의한 개인정보보호 제26조 공동 컨트롤러 제27조 유럽연합 내에 설립되지 않은 컨트롤러 또는 프로세서의 대리인 제28조 프로세서 제29조 컨트롤러 및 프로세서의 권한에 따른 처리 제30조 처리 활동의 기록 제31조 감독기관과의 협력 제32조 처리의 보안 제33조 감독기관에 대한 개인정보 침해 통지 제34조 개인정보 주체에 대한 개인정보 침해 통지 제35조 개인정보보호 영향평가 제36조 사전 자문 제37조 DPO의 지정 제38조 DPO의 지위 제39조 DPO의 업무 제40조 행동강령 제41조 승인된 행동강령의 모니터링 제42조 인증

	제43조 인증 기관 제44조 이전을 위한 통칙 제45조 적정성 결정에 따른 이전 제46조 적정한 안전조치에 의한 이전 제47조 의무적 기업 규칙 제48조 유럽연합 법률로 승인되지 않은 정보의 이전 또는 제공 제49조 특정 상황에 대한 적용의 일부 제외 제50조 개인정보보호를 위한 국제협력
제 VI 장 독립적인 감독기관	제51조 감독기관 제52조 독립성 제53조 감독기관 위원(들)의 일반 조건 제54조 감독기관 설립에 관한 규칙 제55조 법적 자격(competence) 제56조 선임 감독기관의 법적 자격 제57조 업무 제58조 권한 제59조 활동 보고서
제 VII 장 협력 및 일관성	제60조 선임 감독기관과 기타 관련 감독기관 간 협력 제61조 상호 지원 제62조 감독기관의 공동 작업 제63조 일관성 메커니즘 제64조 유럽정보보호이사회 의견 제65조 유럽정보보호이사회의 분쟁 해결 제66조 긴급성(시급성) 절차 제67조 정보의 교환 제68조 유럽정보보호이사회

	제69조 독립성 제70조 유럽정보보호이사회의 업무 제71조 보고서 제72조 절차 제73조 의장 제74조 의장의 역할 제75조 사무국 제76조 기밀성
제 VIII 장 구제책, 책임, 처벌	제77조 감독기관에 민원을 제기할 권리 제78조 감독기관에 대한 효과적인 사법구제권 제79조 컨트롤러나 프로세서를 상대로 한 효과적인 사법구제권 제80조 개인정보 주체의 대리 제81조 법적 절차 중지 제82조 보상 권리 및 책임 제83조 행정 과태료 부과에 관한 일반 조건 제84조 처벌
제 IX 장 특정 정보 처리 상황에 관한 규정	제85조 개인정보 처리 및 표현과 정보의 자유 제86조 개인정보 처리 및 공식 문서 공개 제87조 국가 식별번호의 처리 제88조 고용 환경에서의 정보 처리 제89조 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리와 관련한 안전조치 및 적용의 일부 제외 제90조 기밀유지의 의무 제91조 교회 및 종교 단체의 현행 정보보호 규정

제 X 장 위임법률 및 이행법률	제92조 위임의 행사 제93조 위원회(Committee) 절차
제 XI 장 최종 규정	제94조 지침 95/46/EC의 폐기 제95조 지침 2002/58/EC와의 관계 제96조 이전에 체결된 협정과의 관계 제97조 집행위원회 보고서 제98조 기타 유럽연합의 정보보호 법률에 대한 검토 제99조 발효 및 적용