https://doi.org/10.33778/kcsa.2022.22.4.109

GDPR원칙을 고려한 PbD 적용 방안에 관한 연구★

유 영 천*, 권 순 범**, 이 환 수***

요 약

전 세계 국가들이 개인정보보호의 중요성을 인식하고 법률, 가이드라인, 지침 등의 다양한 형태로 정보주체의 권리 보호에 대해 논의해왔다. 개인정보보호를 위한 사전 예방적 차원에서 공통적으로 강조하고 있는 개념 중 하나가 PbD(Privacy by Design)이며 정보주체의 프라이버시 보호를 위해 필수적인 요소로 주목받기 시작하였다. 그러나 시스템 개발이나 서비스 운영에 있어서 사전에 개인의 프라이버시를 최우선적으로 고려하자는 PbD 개념이 아직은 선언적 차원에만 머물고 있어서 이를 실제로 구현하기 위한 구체적 방법에 대한 논의는 상대적으로 부족하다. 이에 본 연구에서는 GDPR의 기본 원칙과 정보주체의 권리를 기준으로 어떠한 원칙과 권리가 우선적으로 고려되어 PbD가 구현되어야 하는지를 논의하였다. 이를 통해 국내 환경에서 시스템이나 서비스 개발 시 우선 시 해야 할 프라이버시 고려사항을 제시하여 PbD의 적용을 위한 방안을 제시했다는 점에서 본 연구의 의의가 있다.

A study on the application of PbD considering the GDPR principle

Youngcheon Yoo*, Soonbeom Kwon**, Hwansoo Lee***

ABSTRACT

Countries around the world have recognized the importance of personal information protection and have discussed protecting the rights of data subjects in various forms such as laws, regulations, and guidelines. PbD (Privacy by Design) is one of the concepts that are commonly emphasized as a precautionary measure for the protection of personal information, and it is starting to attract attention as an essential element for protecting the privacy of information subjects. However, the concept of PbD to prioritize individual privacy in system development or service operation in advance is still only at the declarative level, so there is relatively little discussion on specific methods to implement it. Therefore, this study discusses which principles and rights should be prioritized to implement PbD based on the basic principles of GDPR and the rights of data subjects. This study is meaningful in that it suggests a plan for the practical implementation of PbD by presenting the privacy considerations that should be prioritized when developing systems or services in the domestic environment.

Key words : Privacy by design, GDPR, Borich Needs, The Locus for Focus Model

접수일(2022년 09월 03일), 수정일(2022년 10월 20일), 게재확정일(2022년 10월 29일)

★ 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행되었음(NRF-2018S1A5A8027174), 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2022년 산업혁신인재성장지원사업)

* 단국대학교 IT법학협동과정 석사과정(주저자)

** 단국대학교 IT법학협동과정 석사과정(공동저자)

*** 단국대학교 산업보안학과 조교수(교신저자)

1. 서론

오늘날 우리는 빅데이터를 비롯한 인공지능, 클라우드 등의 기술들을 손쉽게 이용할 수 있는 환경 속에서 살아가고 있다. 이러한 기술들은 방대하면서도 다양한 정보들을 수집하고 활용하는데 중요한 역할을 하고 있으나 그러한 정보들 중 민감한 개인정보들도 수집 및 활용의 예외는 아니다[1]. 인터넷 시대가 도래 하면서 개인정보는 무분별하게 수집 및 활용되었으나 초기 정보주체들이나 이를 이용하는 정보 관리자나 처리자들은 이에 대해 크게 문제의식을 갖고 있지 않았다. 하지만 개인정보를 이용한 사회적 문제들이 발생함에 따라 개인정보 및 이의 관리 중요성이 부각되기 시작하였고 세계 각국은 개인정보 보호를 위한 다양한 법 제도를 마련하여 관리해 왔다[2]. 미국, 영국, 프랑스 등은 개인정보보호를 위해 통합적 법률을 바탕으로 관리해왔고, 캐나다, 독일 등은 공공과 민간의 근거 규정을 달리하여 기준을 이원화하여 개인정보보호를 추진해 왔다. 유럽연합의 경우에는 GDPR이라는 개인정보의 처리와 이동에 관한 새로운 개인정보보호 틀을 마련하였다[3]. GDPR은 정보주체의 관점에서의 시스템 및 서비스 구축방향에 대해서 규정하고 있다.

전 세계 국가들이 개인정보보호의 중요성을 인식하고 법률, 가이드라인, 지침 등의 다양한 형태로 정보주체의 권리보호를 위한 노력들을 펼쳐왔다. 개인정보보호를 위한 사전 예방적 차원에서 공통적으로 강조하고 있는 개념 중 하나가 PbD(Privacy by Design)이며 정보주체의 프라이버시 보호를 위해 필수적인 요소로 주목받기 시작하였다. 그러나 시스템 개발이나 서비스 운영에 있어서 사전에 개인의 프라이버시를 최우선적으로 고려하자는 PbD 개념이 아직은 선언적 차원에만 머물고 있어서 이를 실제로 구현하기 위한 구체적 방법에 대한 논의는 상대적으로 부족하다. 최근 유진호[4]와 진상기[5]의 연구에서 블록체인 서비스 구현 과정에서 PbD 적용 방안을 보다 의미 있게 논의하고 있으나 아직은 법제도적 차원에서 PbD의 중요성을 강조하는 연구들이 대부분이다. 더욱이 국내 개인정보보호법은 정보주체의 관점에서 개인정보 사고의 사전방지 보다는 사고 발생 시 면책을 위한 내용들이 대부분이기 때문에 PbD의 구체화 방안에 대한 논의가 절실하다.

GDPR에서 강조하고 있는 PbD를 구현하고 보다 효과적으로 적용하기 위해서는 정보주체의 프라이버시 보호와 기업의 비즈니스 이익이라는 균형을 유지할 수 있는 지침을 제공할 필요가 있다[6]. 이에 본 연구에서는 GDPR의 기본 원칙과 정보주체의 권리를 기준으로 어떠한 원칙과 권리가 우선적으로 고려되어 PbD가 구현되어야 하는지를 논의한다. 이를 통해 국내 환경에서 시스템이나 서비스 개발 시 우선 시 해야 할 프라이버시 고려사항을 제시하여 PbD의 실체적 구현을 위한 방안을 제시한다는 점에서 본 연구의 의의가 있다.

2. 문헌연구

2.1 GDPR

General Data Protection Regulation(이하 “GDPR”)은 유럽연합의 일반 개인정보보호 규정이며, EU의 개인정보보호체계 구축 및 소비자와 기업의 경제적 이익과 혁신 보호를 목표로 제정되었다[7]. GDPR 이전의 유럽연합 개인정보보호지침(Data Protective Directive 95/46/EC)이 EU 회원국에게 직접적인 효력을 발휘하지 못한 것에 반해, GDPR은 EU 회원국들에게 직접적인 법적 구속력을 가진다는 점에서 차이가 있다[8].

GDPR의 적용대상은 식별되었거나 또는 식별 가능한 자연인과 관련된 모든 정보이다. 적용범위로는 유럽연합 내에 설립된 기관의 개인정보 처리 활동을 비롯하여 유럽연합 외에서 유럽연합 내에 있는 회원국 정보주체에게 재화 혹은 용역을 제공하는 경우, 더 나아가서는 유럽연합 내에 있는 정보주체가 수행하는 활동을 모니터링하고 있는 기관들이 포함되었다[9]. <표 1>과 같이, 개인정보를 처리하는 경우에는 GDPR의 7대 기본원칙을 모두 준수해야하며 이를 위반할 경우 과징금이 부과될 수 있다.

〈표 1〉 GDPR 7대 기본원칙

원칙	내용
합법성 공정성 투명성	정보주체의 개인정보는 합법적이고 공정하며 투명한 방식으로 처리해야 한다.
목적제한	개인정보는 특정되고 명시적이며, 적법한 목적으로 수집되어야 한다.
최소처리	개인정보는 처리되는 목적과 관련하여 적정하고 관련성 있으며 필요한 범위로 제한되어야 한다.
정확성	개인정보는 정확하고, 필요한 경우 최신 정보로 유지해야 한다.
보유기간 제한	개인정보는 처리목적을 위해 필요한 기간 안에 정보주체를 식별할 수 있는 형태로 보유해야 한다.
무결성 및 기밀성	적절한 기술·관리적 조치를 통해 개인정보의 적절한 보안이 보장되어야 한다.
책임성	컨트롤러는 개인정보보호원칙에 대하여 책임성을 갖추고 준수 여부에 대해서 증명할 수 있어야 한다.

GDPR은 유럽연합 회원국의 정보주체 권리 강화를 위하여 권리 행사와 강화에 대한 내용을 구체적으로 규정하고 있는데, 이와 관련된 내용은 <표 2>와 같다.

〈표 2〉 GDPR 정보주체 권리

권리	내용
정보를 제공받을 권리	정보주체는 자신의 개인정보를 처리한 정보에 대해서 간결하게 제공받을 권리가 있다.
정보주체 접근권	정보주체는 본인의 개인정보 처리 여부에 대해서 컨트롤러에게 확인 받을 수 있는 권리가 있다.
정정권	정보주체는 본인의 개인정보 중 정확하지 않은 부분에 대해서 수정할 수 있도록 컨트롤러에게 요구할 수 있다.
삭제권	정보주체는 본인의 개인정보 삭제를 요구할 수 있다.
처리제한권	정보주체는 본인 개인정보의 처리를 차단하거나 제한할 권리를 가진다.
개인정보 이동권	정보주체는 컨트롤러에게 본인의 개인정보를 다른 컨트롤러에게 전송하도록 요청할 수 있다.
반대권	정보주체는 컨트롤러에게 본인의 개인정보처리를 반대할 수 있는 권리가 있다.
프로파일링을 포함한 자동화된 의사결정	정보주체는 프로파일링 등이 포함되어 있는 자동화된 의사결정을 거부할 수 있다.

GDPR은 개인정보 처리를 위한 EU 회원국들의 예방적 보호제도(PbD, DPIA 등) 운영을 구체적으로 명시하고 있는데, 이러한 GDPR의 예방적 보호제도에는 개인정보보호 적용설계(PbD), 개인정보보호 인증제도, 행동강령(CoP) 등이 포함되어 있다[10]. 법적구속력을 가지고 있는 EU의 GDPR 규정은 EU 회원국뿐만 아니라 비회원 국가들의 개인정보보호 정책과 법제수립에 많은 영향을 미치게 되었다. 이러한 이유로 국내에서는 GDPR의 적용범위[11]와 이를 토대로 한 법률적 적용 방안에 대한 연구[12] 및 GDPR 규정과 국내 개인정보보호법과의 비교에 대한 연구[1] 등이 활발히 진행되어 왔다. 해외에서도 GDPR에 근거한 개인정보 관리에 대한 연구들이 활발히 논의되고 있으며[13] 최근에는 개인정보 처리에 대한 사전적 예방조치가 중요해짐에 따라, GDPR의 예방적 보호제도 중의 하나인 PbD에 대한 논의가 이루어지고 있다.

2.2 PbD(Privacy by Design)

PbD는 Privacy by Design의 약자로 정보기술, 사업관행, 절차, 물리적 디자인, 네트워크 기반 등을 포함한 사용 단계에서 개인정보를 고려하는 것이 아닌 개인정보 사용이 예정된 최초 설계단계에서부터 사용자의 프라이버시를 고려해야 한다는 것이 PbD의 핵심 내용이다[14]. PbD는 2010년 10월 '정보보호와 프라이버시위원회(ICDPPC)' 국제 컨퍼런스를 기점으로 단순한 개념적 논의에 머무르지 않고 실행 단계로 발전하기 시작했다[15]. 초기에는 PBD의 개념을 정확하게 특정 하는데 한계가 있었고, 구체성 부족과 그 실행에 있어서 경제적 동기부여 및 법제도적 시스템 등이 미비하다는 지적이 있었다. 특히 PBD는 제시된 원칙들이 시스템 구축에 적용 시 많은 한계가 있다는 지적 또한 존재하였다[16]. 그러나 이후 GDP 제25조에 PbD 개념이 구체화되었으며, PbD의 이행은 정보주체의 개인정보 유출 및 침해와 관련된 위험을 최소화할 수 있어 개인정보보호 의무를 준수하는데 도움이 되고 있다.

PbD는 사생활 침해 위험을 최소화시키고 소비

자와의 신뢰성 향상을 위해 7대 원칙을 제시하고 있는데 이에 대한 내용은 <표 3>과 같다[17]. 이에 따라, PbD는 주요국들의 개인정보보호 정책과 법률의 기본 원칙으로 확대되고 있는 중이다. 이에 PbD에 대한 다양한 연구들이 논의되고 있는 중이며 PbD에 대한 국내 연구에는 PbD의 소개와 도입필요성에 대한 연구[18] 및 적용방안에 대한 연구[4]등이 진행된 바 있다.

〈표 3〉 PbD 7대 원칙

원칙	내용
사전예방책	프라이버시 침해 발생 후 조치를 취하는 것이 아니라 침해 발생 전 그 침해를 예상하고 방지한다.
프라이버시 기본설정	정보시스템 또는 비즈니스에서 자동적으로 개인정보보호 및 최대한의 프라이버시 보장
프라이버시 내재화	기본 설정과 개인정보보호 설계 항목 신설로 프라이버시 보호 가능
포지티브섬	프라이버시 대책과 보안 대책 모두 이익이 될 수 있는 win-win 관계 추구
End-to-End 보안	데이터의 생성부터 삭제까지 프라이버시 보호를 위한 강력한 보안조치 이행
가시성과 투명성	모든 이해관계인에게 명시하였던 원칙과 목적에 따른 사업 시행 또는 기술의 적용이 이루어지는 것을 보장하고 이와 관련된 요소들을 투명하게 공개
이용자의 프라이버시 존중	설계자를 비롯한 정보 처리자들이 강력한 프라이버시를 기본으로 설정하고 적절한 통지, 사용자 친화적 선택권 부여와 같은 조치를 제공하면서 개인의 이익을 우선적으로 보호

OAIC(Office of the Australian Information Commissioner)는 프라이버시의 관리와 침해의 위험 및 사용자의 효과적인 대응을 위한 프라이버시 관리 프레임워크를 제시하여 PbD를 내재화 하는 방안을 제시하였다(www.oaic.gov.au). KCG(Kleimann Communication Group)은 정보시스템 개발 라이프사이클 전 단계에 걸쳐서 PbD Checklist를 작성하여 세밀한 관리가 가능하다고 제안하였다(www.openlawlab.com). ENISA(European Union Agency For Network And Information Security)는 PbD를 실현하고 프라이버시 침해를 최소화하기 위한 8가지 전략을 제시하였다[14]. 데이터 중심 전략으로 최소화(Minimise), 숨기기(Hide), 분리(Separate), 추상화(Abstract) 전략, 프로세스 중심 전략으로 통지(Inform), 통제(Control), 집행(Enforce) 및 입증(Demonstrate) 전략으로 구성된다. 유럽 연합 지원 프로젝트인 PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in REsearch)은 시스템 설계단계에서 활용할 수 있는 26개 프라이버시 보호 디자인 패턴을 제안하기도 하였다. 그러나 이러한 가이드라인들은 시스템 개발 주체가 이의 구현을 위해서는 PbD에 대한 깊은 이해와 더불어 실제 개발을 위해서는 추가적인 비용 부담이 크다는 점에서 적극적으로 적용하기에는 어려움이 따른다.

2.3 GDPR과 PbD의 적용에 관한 논의

GDPR에 대한 기존 연구들은 GDPR 규정의 일부 조항을 분석하는 연구 혹은 국내 개인정보보호법과 비교·분석하는 연구가 대부분을 이루고 있다. 그 중에서도 국내 개인정보보호법과 비교·분석하는 연구를 보면 민감정보의 정의, 처리활동의 기록, 정보보호책임자(DPO), 개인정보의 역외 이전, 프로파일링 거부권 등에 관한 내용에서 차이가 있다는 것을 알 수 있다. 또한 GDPR의 정보통신발전에 맞춰 우리나라 법제에 필요한 범위 내에서 수용에 대한 고려가 필요하다는 주장들이 제시되어 왔다[12]. 실제 국내 개인정보보호법은 GDPR과 근본적으로 법적 성격이나 세부 규정에 있어서 많은 차이가 있으나 개인정보의 처리에 대한 이슈가 한 국가만의 이슈가 아니며, 정보통신기술의 발전은 국가 간의 경계를 허물게 됨으로써 글로벌 트렌드에 국내 개인정보보호법도 지속적으로 변화하고 있는 추세이며 최근 국내 데이터 3법의 개정 또한 GDPR의 고려한 변화로 볼 수 있다[19].

우리나라는 정보통신 강국으로써 인공지능, 블록체인, 스마트 시티 등 고도화된 시스템들이 선제적으로 활용되고 있고 개인정보보호에 대한 사회적 관심도 높아 PbD에 대한 논의도 이루어지기 시작하였다. 그러나 우리나라의 경우 아직은 PbD의 실질적 구현 방안이나 실무에서 참고할 수 있는 가이드라인들은 제한적인 실정이다. 주로 국외에서의 PbD 적용 사례를 언급하며 국내에서 도입의 필요성과 방향성에 대한 논의가 대부분으로 여전히 PbD의 적용과 활용에 대

한 연구는 부족한 상황이다[17]. 최근 연구가 진행되면서 개별시스템에 대한 PbD 가이드라인은 있으나 정보주체의 권리에 대한 PbD는 논의조차 이루어지지 않고 있다. 일례로 우리나라의 IoT 구축 정책에서 PbD와 유사한 Security by Design 개념이 활용되어 홈가전, 의료, 교통, 환경, 재난, 제조, 건설 등 다양한 분야에서 보안 내재화 정책을 추진해온 바 있다. 그러나 일반 개인정보보호에 대한 논의는 여전히 부족한 실정이다[15]. 더 나아가서는 공급자의 관점에서 개인정보보호에 관한 가이드라인은 배포되고 있으나, 정작 이를 이용하는 이용자 즉, 정보주체에 대한 가이드라인은 존재하고 있지 않다. 이에, 본 연구에서는 GDPR의 원칙을 중심으로 정보주체 관점에서의 PbD 적용 우선순위를 도출하고 국내 정보시스템 환경에서 PbD를 고려한 시스템이나 서비스 개발 시 어떠한 요소를 중심으로 고려한 개발이 효과적인지에 대해 제시한다.

3. 연구 방법

3.1 자료수집 및 분석방법

본 연구의 목적은 개인정보보호 영역에 대한 현재 수준과 개선 영역을 확인하여 PbD 적용을 위한 운선순위가 무엇인지를 분석하는데 있다. 이를 위해 온라인 설문조사 업체인 마크로밀엠브레인(https://embrain.com/)에서 보유한 조사 DB에서 무작위로 추출한 1,100명을 대상으로 설문조사를 진행하였다. 개인정보보호법에 대한 이해가 필요한 연구 주제의 특성 상 10대를 제외한 만 20세 이상의 일반인을 대상으로 설문조사를 진행하였으며 설문 문항에서 “개인정보보호법에 대해 알고 있습니까?”라는 설문에서 답변이 보통 미만(리커드 문항 1번, 2번, 3번 응답)인 154명을 제외한 총 946명의 데이터를 분석에 활용하였다.

본 연구의 설문문항은 GDPR에서 규정하고 있는 개인정보처리 7대 원칙과 정보주체의 8대 권리를 바탕으로 각각 10문항과 8문항으로 구성되었다. 측정문항의 구체적인 항목은 ① 합법성, ② 공정성, ③ 투명성, ④ 목적 제한, ⑤ 개인정보 최소처리, ⑥ 정확성, ⑦ 보유기간 제한, ⑧ 무결성, ⑨ 기밀성, ⑩ 책임성, ⑪ 처리중인 정보 제공, ⑫ 열람권, ⑬ 정정권, ⑭ 삭제 요청권, ⑮ 처리 제한 요청권, ⑯ 개인정보 이동권, ⑰ 처리 거부 요청권, ⑱ 자동화된 의사결정권 거부로 구성되었다. 측정문항들은 1-1. 개인정보는 적법하게 처리하는 것이 중요하다. 1-2. 기업들은 개인정보를 적법하게 처리하고 있다. 2-1 개인정보는 공정하게 처리하는 것이 중요하다. 2-2. 기업들은 개인정보를 공정하게 처리하고 있다. 등 항목별 중요성과 수준을 질의하는 한 문항씩 쌍으로 구성되었다. 모두 리커드 7점 척도로 응답이 수집되었으며, 수집된 데이터를 분석하기 위하여 SPSS 23과 Excel 2016을 활용하였다. 개인정보보호 영역에 대한 중요도와 현재 수준의 차이를 검증하기 위해 대응표본 t-검정을 실시하였고, PbD 적용을 위한 우선순위를 알아보기 위하여 Borich 요구도 분석과 The Locus for Focus 모델을 활용하였다.

3.2 조사 대상자의 특성

조사 대상자의 인구통계학적 특성은 <표 4>와 같다. 먼저 응답자들의 성별을 살펴보면 남성 51.3%, 여성 48.3%로 구성되었으며 나이의 경우 20대 18.0%, 30대 19.5%, 40대 21.0%, 50대 20.8%, 60대 20.7%로 거의 유사한 비율로 응답이 수집되었다. 학력은 고졸 이하 16.9%, 대학 졸업(재학 포함) 71.2%, 대학원 졸업(재학 포함) 11.9%로 대학 졸업(재학 포함) 응답자 비율이 높은 것으로 나타났다. 소득은 월 100만원 미만 14.7%, 월 100-200만원 미만 12.9%, 월 200-300만원 미만 28.8%, 월 300-400만원 미만 26.7%, 월 500만원 이상 16.9%로 월 200-300만원 미만 응답자 비율이 높은 것으로 나타났다.

〈표 4〉 샘플의 특성

변수	구분	응답수(비율)
성별	남성	485(51.3%)
	여성	461(48.3%)
나이	20대	170(18.0%)
	30대	184(19.5%)
	40대	199(21.0%)
	50대	197(20.8%)
	60대	196(20.7%)
학력	고졸 이하	160(16.9%)
	대학 졸업(재학 포함)	674(71.2%)
	대학원 졸업(재학 포함)	112(11.9%)
소득	월 100만원 미만	139(14.7%)
	월 100-200만원 미만	122(12.9%)
	월 200-300만원 미만	272(28.8%)
	월 300-400만원 미만	253(26.7%)
	월 500만원 이상	160(16.9%)
합계		946(100%)

4. 분석 결과

4.1 t-검정 분석결과

Borich 요구도 분석에 앞서 개인정보보호에 대한 현재수준과 중요도의 차이를 확인하기 위해 대응표본 t-검정 분석을 수행하였다. 분석에서 t값과 p값은 중요도와 현재수준 차이의 통계적 유의성을 보여준다. <표 5>와 같이 개인정보보호 요소들의 중요도 대비 현재수준의 차이에 대한 t-검정 분석 결과에 따르면 모든 요소들의 현재수준과 중요도는 모두 유의미한 차이가 있는 것으로 나타났다. 측정항목들의 중요도 전체 평균은 6.43이었고, 현재수준의 평균은 3.99 정도로 약 2.44 정도의 차이가 있는 것으로 나타났다. 이는 응답자들이 개인정보처리원칙과 정보주체의 권리의 중요성을 높게 평가하고 있는 반면 기업들이 현재 이를 준수하는 수준은 보통 미만으로 차이가 크다고 인식하고 있는 것으로 나타났다. 즉, 응답자들은 기업들의 개인정보 처리에 대해 많은 부문에서 개선이 필요하다고 생각하고 있다는 것을 의미한다. 또한 중요도와 현재수준의 차이가 통계적으로 유의미하여 Borich 요구도 분석에 문제가 없음을 보여준다.

〈표 5〉 개인정보보호 중요도 대비 수준 t-검정 분석결과

항목	중요도 (RL)	현재수준 (PL)	t	p
①	6.50	3.93	44.14	0.00
②	6.52	3.89	48.12	0.00
③	6.43	3.77	44.92	0.00
④	6.52	3.86	46.63	0.00
⑤	6.47	3.73	49.98	0.00
⑥	6.57	3.73	55.32	0.00
⑦	6.53	3.89	48.12	0.00
⑧	6.61	3.82	53.14	0.00
⑨	6.56	3.75	49.72	0.00
⑩	6.55	3.72	54.02	0.00
⑪	5.80	4.21	24.70	0.00
⑫	6.34	4.10	40.14	0.00
⑬	6.36	4.39	38.12	0.00
⑭	6.53	4.26	43.26	0.00
⑮	6.52	4.19	44.21	0.00
⑯	6.28	4.13	40.58	0.00
⑰	6.36	4.12	43.36	0.00
⑱	6.23	4.29	38.88	0.00

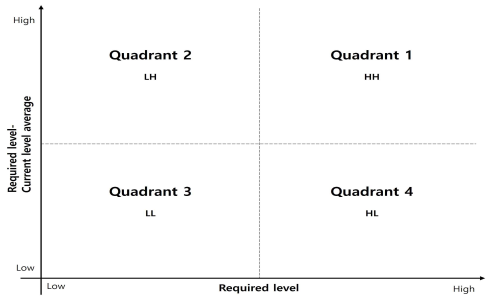
4.2 Borich 요구도 분석 결과

본 연구에서는 PbD 적용을 위한 개인정보보호 세부 요소의 우선순위를 분석하기 위해 Borich 요구도 분석과 The Locus for Focus 모델을 활용하였다. Borich 요구도는 주로 교육프로그램 개발 우선순위를 파악하기 위해 활용되는데, 현재 수준과 바람직한 수준(What should be)간의 차이를 분석하여 요구도를 도출할 수 있으며, 이는 특정 요소들의 우선순위를 결정하는데 활용할 수 있다고 제시하였다[20]. Borich 요구도 분석은 t-검정이 가지는 두 항목 간의 단순한 차이 비교의 한계를 극복하고 변별력을 가진다는 점에서 강점이 있다. 또한 IPA(Importance performance analysis)모델이 두 수준의 단순 차이 값을 활용하여 우선순위 도출에 한계가 있는 반면 Borich 요구도는 RL(필요수준 또는 중요도)과 PL(현재수준)의 차이에 RL의 평균을 곱하여서 가중치를 부여하는 방식으로 보다 정밀하게 우선순위를 도출할 수 있다. Borich 요구도를 계산하는 수식은 다음과 같다[21].

$$Borich\,요구도 = \frac{\sum(RL-PL)\times\overline{RL}}{N}$$

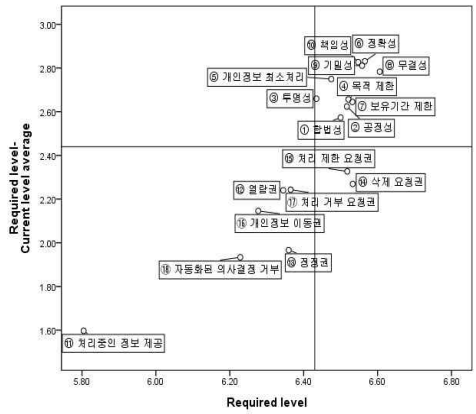
RL: 중요도수준
PL: 현재수준
$\overline{RL}$: 중요도평균
N: 전체사례수

(그림 1)과 같이 The Locus for Focus 모델은 X축과 Y축으로 구성된 좌표평면을 이용하여 우선순위를 결정하여 시각적으로 보여주는 방법으로 단순 좌표 숫자만 나타나는 Borich 요구도 분석의 한계를 보완하는데 활용된다[20]. 개인정보보호의 세부 요소들에 대한 Borich 요구도 분석결과를 바탕으로 X축에는 개인정보보호 처리원칙과 정보주체의 권리 항목의 중요도(RL), Y축에는 중요도 대비 현재수준(RL-PL)값을 설정한 Locus for Focus 모델을 설정하였다. 중요도와 중요도 대비 현재수준이 모두 높은 HH 영역, 중요도는 높으나 중요도 대비 현재수준은 낮은 HL 영역, 중요도는 낮고 중요도 대비 현재수준은 높은 LH 영역, 중요도와 중요도 대비 현재수준이 모두 낮은 LL 영역으로 구성된다.



(그림 1) The Locus for Focus 모델

(그림 2)와 같이 Locus for Focus 모델 분석결과 개인정보보호 요소들의 중요도(RL)의 평균값은 6.43, 중요도 대비 현재수준(RL-PL)의 평균값은 2.44로 나타나 축은 (6.43, 2.44)로 설정하고 4분면을 구성하였다. HH 영역에는 ① 합법성, ② 공정성, ③ 투명성, ④ 목적 제한, ⑤ 개인정보 최소처리, ⑥ 정확성, ⑦ 보유기간 제한, ⑧ 무결성, ⑨ 기밀성, ⑩ 책임성이 포함되었으며, LH 영역에 속하는 역량은 없는 것으로 나타났다. HL 영역에는 ⑭ 삭제 요청권과 ⑮ 처리 제한 요청권이 포함되었으며, LL 영역에는 ⑪ 처리중인 정보 제공, ⑫ 열람권, ⑮ 처리 제한 요청권, ⑯ 개인정보 이동권, ⑰ 처리 거부 요청권, ⑱ 자동화된 의사결정거부가 포함된 것으로 나타났다.



(그림 2) The Locus for Focus 분석결과

<표 6>과 같이 The Locus for Focus 모델을 사용하여 도출된 개인정보보호 역량에 대한 요소와 Borich 요구도 분석결과를 비교한 결과, 우선적으로 도입해야 하는 개인정보보호 원칙과 권리는 ① 합법성, ② 공정성, ③ 투명성, ④ 목적 제한, ⑤ 개인정보 최소처리, ⑥ 정확성, ⑦ 보유기간 제한, ⑧ 무결성, ⑨ 기밀성, ⑩ 책임성인 것으로 나타났다.

분석결과를 요약하면 응답자들은 기업들이 개인정보 처리 원칙을 준수해주기를 원하고 있는 반면에 그 원칙을 실제로 잘 지키고 있지 않다고 인식하고 있는 것으로 나타났다. 정보주체의 권리에 대해서는 상대적으로 요구수준이 높지 않으며 기업들이 어느 정도 지원하고 있다고 인식하는 것으로 나타났다. 즉, 응답자들은 기업들이 알아서 정보주체의 개인정보들을 정확하고 책임있게 안전하게 관리해 주기를 원하고 있으나 아직은 그렇지 못하다고 인식하는 것으로 이해할 수 있다.

〈표 6〉 Borich 요구도와 LF모델 분석

항목		Borich (순위)	LF 모델
개인정보 처리 원칙	① 합법성	16.72(10)	HH
	② 공정성	17.10(9)	HH
	③ 투명성	17.11(8)	HH
	④ 목적 제한	17.32(6)	HH
	⑤ 개인정보 최소처리	17.80(5)	HH
	⑥ 정확성	18.59(1)	HH
	⑦ 보유기간 제한	17.28(7)	HH
	⑧ 무결성	18.39(4)	HH
	⑨ 기밀성	18.43(3)	HH
	⑩ 책임성	18.51(2)	HH
정보주체의 권리	⑪ 처리중인 정보 제공	9.27(18)	LL
	⑫ 열람권	14.21(14)	LL
	⑬ 정정권	12.50(16)	LL
	⑭ 삭제 요청권	14.83(12)	HL
	⑮ 처리 제한 요청권	15.16(11)	HL
	⑯ 개인정보 이동권	13.47(15)	LL
	⑰ 처리 거부 요청권	14.28(13)	LL
	⑱ 자동화된 의사결정 거부	12.04(17)	LL

5. 논의 및 결론

본 연구는 Borich 요구도와 The Locus for Focus 모델을 적용하여, PbD 적용을 위한 우선순위가 무엇인지 분석하고자 하였다.

연구결과를 요약하면 다음과 같다. 첫째, 정보주체의 권리보다는 개인정보처리 원칙의 준수를 요구하는 것으로 나타났다. 이는 기업의 개인정보처리에 대한 불신과 불투명한 처리과정이 원인이 된 것으로 분석된다. 둘째, 개인정보처리 원칙 내에서는 정확성과 책임성, 기밀성에 대한 요구가 높은 것으로 나타났다. 즉, 시스템 오류나 비인가자의 접근에 의한 남용 등에 대한 개선 및 GDPR 기준 준수여부에 대한 객관적인 평가가 요구되고 있는 것으로 분석된다. 셋째, 정보주체의 권리에 대한 요구도는 상대적으로 높지 않은 것으로 나타났다. 그러나 정보 주체들은 정보주체들의 요구가 있을 시에는 처리가 제한되어야 한다는 것에 대한 필요를 인식하고 있었으며, 기업들의 개인정보 분석 및 활용에 대해서는 상대적으로 관대한 편인 것으로 나타났다.

위와 같은 분석 결과를 바탕으로 일반적인 개인정보보호의 영역에 PbD 적용방안을 제시한다면 다음과 같다. 먼저 국내 정보보호관리체계(ISMS-P) 인증에서 PbD 요건을 강화하여 적용을 유도하는 방안이다. 현재의 인증체계는 시스템과 관련한 보호대책과 개인정보에 대한 처리단계별 요구사항을 구분하여 제시하고 있어, 프라이버시 보호를 고려한 정보시스템 도입, 운영, 보안관리 방안에 대한 요구사항은 미비하다. 따라서 ISMS-P의 보호대책 요구사항 영역에서 정보시스템과 관련한 항목에 요구수준이 높은 개인정보 처리 원칙들을 기준으로 제시할 수 있다. 다른 방안으로는 PbD의 개념 자체가 소프트웨어 개발 라이프 사이클 전반에 걸쳐 개인정보보호를 고려하는 것이기 때문에 KCG의 Privacy check list처럼 소프트웨어 설계, 개발, 테스트, 배포, 평가 단계별로 개인정보처리 원칙이 지켜지고 있는지 매트릭스 형태로 관리하도록 가이드라인을 제시할 수 있을 것이다. CPO(Chief privacy officer) 존재하는 규모가 있는 기업일 경우에는 CPO가 조직의 정보시스템 개발 일련의 과정에서 앞선 분석 결과를 바탕으로 PbD가 고려되고 반영되고 있는지를 모니터링 하는 것도 한 방안이 될 수 있다.

본 연구는 학술적 및 실무적 기여는 다음과 같다. 먼저, 학술적 측면에서 선행연구들은 PbD 추진 방향에 대한 실증적 연구가 부족하였는데, 본 연구에서는 대규모 설문 데이터를 바탕으로 PbD 추진에 대한 방향성을 제공하였다. 실무적 측면에서는 기업의 시스템 개발 시 PbD 우선순위에 대한 참고사항을 제시하였다는 점과 이러한 연구 결과를 토대로 향후 개인정보보호 정책에 대한 방향성을 제시하였다는 점에서 의의가 있다. 그럼에도 불구하고 본 연구는 다음과 같은 한계가 있다. 가장 먼저 본 연구가 실증 분석을 통해 우선순위가 높은 적용 기준들을 제시하기는 하였으나 이의 적용을 위한 보다 구체적인 적용방안에 대한 논의는 다소 부족하다는 점에서는 한계가 있다. 앞서 제시한 인증체계의 기준이나 개발가이드라인에서의 검토 기준 등으로 기업들의 적용 가능성을 높일 수 있겠으나 보다 활발한 적용을 위해서는 더욱

구체적인 학술적 논의가 진행되어야 할 것이다. 다음으로, 본 연구에서는 개인정보보호 역량의 중요도와 현재수준에 대하여 기업이나 관련 분야의 전문가들의 평가가 아닌 일반인들의 인식수준을 바탕으로 하였기 때문에, 연구 결과의 일반화와 정확한 검증을 위해서는 실제 개인정보보호의 중요도와 현재수준을 평가한 추가 연구가 필요하다. 또한 PbD를 모든 기술 및 상품에 적용하기에는 너무 광범위하여 세부적인 가이드라인을 제시하는데 한계가 있기 때문에, 이러한 점 역시 추후 연구를 통해 보완될 필요가 있다. 그럼에도 불구하고 본 연구는 그동안 공급자 관점에서만 논의되어 오던 PbD에 대한 접근을 정보주체의 관점에서 연구했다는 점에서 의의가 있고 PbD 추진 방향에 대한 실증적 연구가 매우 부족한 상황에서 대규모 설문데이터를 바탕으로 학술적 논의를 하였다는 점에서 의미가 크다.

참고문헌

[1] 김성현, 이창무, “EU GDPR과 국내 개인정보보호 법제 비교분석”, 융합보안논문지, 제18권, 제5호, pp.83-92, 2018.

[2] 권영준, “개인정보 자기결정권과 동의 제도에 대한 고찰”, 법학논총, 제36권, 제1호, pp.673-734, 2016.

[3] 손영화, 손수진, “EU 일반데이터보호규정(GDPR)에 대한 우리나라 기업의 대응방안” 비교사법, 제26권, 제1호, pp.413-452, 2019

[4] 유진호, "블록체인 서비스에서의 Privacy by Design 적용방안." 정보과학회지, 제38권 제7호, pp.32-39, 2020.

[5] 진상기, “스마트 도시(Smart City)의 데이터 경제 구현을 위한 개인정보보호 적용설계(PbD)의 도입 필요성 분석.” 정보화정책, 제26권, 제3호, pp.69-89, 2019.

[6] Ira S. Rubinstein, Nathaniel Good, “Privacy by Design: A Counterfactual Analysis of Google and Facevook Privacy Incidents”, Berkeley Technology Law journal, Vol. 28, pp.12-43, 2013.

[7] 홍선기, 고영미, “개인정보보호법의 GDPR 및 4차 산업혁명에 대한 대응방안 연구.” 법학논총, 제43권, 제1호, pp.313-337, 2019.

[8] 류승균, “EU 개인정보보호규칙(GDPR)의 제정과 시사점”, 경제규제와 법, 제9권, 제1호, pp.265-268, 2016.

[9] 오태현, 강민지, “EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안”, 대외경제정책연구원, 2018.

[10] 신영진, “개인정보의 예방적 보호방안 연구(PbD, DPIA를 중심으로)”, 개인정보보호위원회, 2018.

[11] 마광, 장교옥, "GDPR의 적용범위에 관한 연구." 과학기술과 법, 제12권, 제1호, pp.35-66, 2021.

[12] 조수영, “개인정보보호법과 EU의 GDPR에서의 프라이버스 보호에 관한 연구”, 법학논고, 제61권, pp.117-148, 2018.

[13] N. B. Truong, K. Sun, G. M. Lee and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 1746-1761, 2020.

[14] 유진호, 정상호, 김민정, 우재현, 정경오, 김용선, “블록체인에서의 Privacy by Design 적용방안 연구”, 한국인터넷진흥원, 2019.

[15] 김남심, 지성우, “Privacy by Design제도에 대한 규범적 고찰”, 성균관법학, 제30권, 제4호, pp.35-63, 2018.

[16] 차상육, “빅데이터 (Big Data) 환경과 프라이버시의 보호”, IT와 법 연구, 제8권, pp. 193-259, 2014.

[17] 김나루, “Privacy by Design의 도입과 그 적용에 관한 소고”, 성균관법학, 제29권, 제4호, pp.1-30, 2017.

[18] 최혜선, "개인정보보호의 신경향 -프라이버시 중심 디자인(Privacy by Design)을 중심으로-", 일감법학, 제24권, pp.305-340, 2013.

[19] 오정주, 이환수, “빅데이터 분석을 통한 데이터 3법 인식에 관한 연구”, 융합보안논문지, 제21권,

제2호, pp.19-28, 2021.

[20] G. Borich, “A needs assessment model for conducting follow-up studies”, Journal of Teacher Education Vol. 31, Issue 1, pp. 39-42. 1980.

[21] 이진구, 정일찬, 박민주, “DACUM 기법을 활용한 물리적방호 분야 일반보안 직무의 교육 요구 분석”, 한국콘텐츠학회논문지, 제21권, 제5호, pp. 234-246, 2021.

〔저 자 소 개〕

유 영 천 (Youngcheon Yoo)
2020년 2월 한세대학교 산업보안학과 학사
2020년 3월 ~ 단국대학교 IT법학협동과정 석사과정
email : y2c206@naver.com

권 순 범 (Soonbeom Kwon)
2022년 2월 단국대학교 법학과 학사
2022년 3월 ~ 단국대학교 IT법학협동과정 석사과정
email : kwonsb777@naver.com

이 환 수 (Hwansoo Lee)
2005년 2월 연세대학교 산업정보시스템 공학과 석사
2014년 2월 KAIST 기술경영학과 박사
2017년 ~ 단국대학교 산업보안학과 교수
email : hanslee992@gmail.com