개인정보 영향평가 사전진단도구 개발을 위한 평가 요소 분석

[1*]정영애

Analyzing Assessment Factors to Develop a Privacy Impact Assessment Pre-Diagnostic Tool

[1*]Young-Ae Jung

요 약

우리 나라의 개인정보 영향평가는 개인정보보호법 제33조 및 같은 법 시행령 제35조에 규정된 개인정보파일을 운용하는 기관이 필수적으로 수행하여야 하는 위험요인 분석과 개선사항 도출의 과정을 의미한다. 우리나라의 개인정보 영향평가 제도에는 크게 두가지의 한계가 존재한다고 볼 수 있다. 첫 번째 한계는 개인정보 영향평가를 받아야 하는 대상이 공공기관과 공공기관에 준하는 기관으로 한정되어 있다는 점이고, 두번째 한계는 적정한 인력과 설비 및 그 밖에 필요한 요건을 갖춘 기관만이 개인정보 영향평가를 수행할 수 있다는 점이다. 본 연구에서는 최근 들어 급속하게 발전하고 있는 데이터 시대에 민간기업 또는 중소벤처기업, 소상공인 등도 직접 수행할 수 있는 사전진단도구 개발을 위한 제안을 하고, 구체적인 평가 요소에 대한 분석을 제시한다. 본 연구의 결과는 셀프-체크리스트 형식의 제공되어, 일반 국민들이 손쉽게 접근할 수 있는 개인정보 영향평가 사전진단도구의 역할을 할 것으로 기대된다. 국가적으로도 개인정보 보호를 강화하고 관련한 법적 준수를 달성하는 데 기여할 것으로 예상된다.

Abstract

The Privacy Impact Assessment, PIPA in Korea refers to the process of analyzing risk factors and identifying improvements that must be carried out by organizations that operate personal information files as stipulated in Article 33 of the Personal Information Protection Act, PIPA and Article 35 of the Enforcement Decree of the PIPA. There are two main limitations of the PIA in Korea. The first limitation is that the targets of the PIA are limited to public institutions and organizations that are legally equivalent to public institutions, and the second limitation is that only organizations with adequate manpower, facilities, and other necessary requirements which are regulated upon the Enforcement Decree of the PIPA can conduct a PIA. This paper proposes to develop a preliminary diagnostic tool that can be performed by private companies, small and medium-sized venture companies, and small businesses in the era of rapidly developing data in recent years and presents an analysis of specific assessment factors. The results of this study are provided in the form of a self-checklist, which is expected to serve as a pre-diagnostic tool for the PIA that can be easily accessed by the general public. It is also expected to contribute to strengthening privacy protection and achieving legal compliance at the national level.

Keywords: *Privacy, Privacy Impact Assessment, Data Protection Impact Assessment, Privacy Threshold Assessment, Pre-PIA, Personal Data Protection*

[1*교신저자] *선문대학교 IT 교육학부 부교수 (yajung@sunmoon.ac.kr)*

Received: Feb. 07, 2024, Revised: Feb. 22, 2024, Accepted: Feb. 26, 2024

I. 서론

최근 디지털 환경에서의 개인정보 유출 사고 증가와 그로 인한 사회적, 경제적 피해가 확대되고 있어, 개인정보보호의 중요성이 더욱 강조되고 있다. 국내에서도 개인정보 보호의 중요성이 점점 더 강조되고 있는 가운데, 조직들은 개인정보 보호 법률 및 규정 준수를 위해 개인정보 영향평가(PIA, Privacy Impact Assessment)의 실시가 필수적이다[1].

그러나 기존의 평가 시스템은 대부분 복잡하고 시간이 많이 소요되며, 특히 소규모 기업이나 조직에서는 이러한 시스템을 적용하기 어렵다는 한계가 있다. 특히 중소기업 및 스타트업 기업은 자원의 제한으로 인해 전체 PIA 프로세스를 효율적으로 진행하기 어려운 경우가 많다.

본 연구는 간소화된 평가 프레임워크의 구현을 통해 개인정보 보호와 영향평가의 효율성을 높이는 동시에 조직의 규제 및 운영 부담을 완화하기 위한 전략을 모색하는 것을 목표로 한다. 본 연구에서는 경량화된 개인정보 보호 평가 시스템 개발에 중점을 두어 강력한 개인정보 보호에 대한 필요성과 오늘날 조직이 직면한 실제 현실 사이의 균형을 맞추는 실용적인 솔루션을 제공하고자 한다.

이러한 접근방식은 평가 프로세스를 간소화할 뿐만 아니라 개인정보 관리 및 보호의 지속적인 개선을 촉진할 것으로 예상된다. 이 연구는 최종적으로 개인정보 관리에 대한 정책 개발과 조직의 모범 사례 모두에 정보를 제공할 수 있는 통찰력을 제공하여 개인정보 보호에 대한 더 넓은 담론을 제공하는데 기여하고자 한다.

II. 관련 연구

2.1 우리 나라의 개인정보 영향평가

우리 나라의 개인정보 영향평가 제도는 「개인정보 보호법」(Personal Information Protection Act, PIPA)에 근거하여 운영되고 있다. 이 법은 2023 년에 중요한 개정을 거쳤으며, 개인정보를 다루는 모든 기관과 기업에 영향을 미친다. 개인정보 보호법은 개인정보를 취급하는 모든 개인정보처리자에게 적용되며, 개인정보처리자에는 정부기관, 공공기관, 법인, 단체, 개인 등이 포함된다[2].

개인정보 영향평가는 새롭게 도입하거나 변경되는 개인정보 파일에 대한 사전 조사, 분석 및 평가를 통해 위험 요소를 파악하고 개선하는 시스템이다. 이 평가는 개인정보 보호법 제 33 조에 의해 규정되어 있으며, 개인정보 파일을 설립하거나 운영하는 공공기관에 필수적으로 요구된다. 개인정보 영향평가는 원칙적으로 개인정보 파일 처리 시스템을 설계하거나 분석하는 단계에서 수행되며, 개인정보 보호 책임자, 개인정보 보호 담당자 등으로 구성된 평가 팀에 의해 이뤄진다. 평가의 결과는 필요한 경우 의견을 제공하기 위해 개인정보보호위원회에 제출된다. 다만, 기존에 운용 중이던 개인정보 파일이 요건 상 개인정보 영향평가의 대상이 아니었으나 개인정보의 수가 늘어나는 등의 주요한 변화에 의해서 개인정보 영향평가의 대상으로 전환되는 경우에는 개인정보 파일 처리 시스템이 운용되는 중에 수행되기도 한다[2].

개인정보 영향평가의 기준, 절차, 방법, 그리고 개인정보 영향평가 수행 인력 및 수행 기관 요건 등에 대하여는 개인정보 보호법 시행령[3]과 개인정보 영향평가에 관한 고시에 상세하게 규정되어 있다. 이러한 법령 및 고시 등은 국내에서 개인정보를 처리하는 모든 기관 및 기업이 개인정보 보호와 관련하여 준수해야 할 기준을 제공하는 것으로 볼 수 있지만, 사실은 일부 정하진 기관에만 의무적이며, 일반 민간 기업은 의무 수범자에 포함되지 않는다.

개인정보 영향평가를 수행하는 절차는 먼저 사전 준비 단계, 영향평가 수행 단계, 이행 단계로 구분된다[4].

1. 사전 준비 단계에서는 개인정보 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정한다.
2. 개인정보 영향평가 수행 단계에서는 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 개인정보 영향평가서를 작성한다.
3. 이행 단계에서는 개인정보 영향평가서의 침해요인에 대한 개선계획이 반영되는 가를 점검한다.

그림 1 은 이를 세분화하여 구분한 개인정보 영향평가 절차도를 보여주는 것이다.

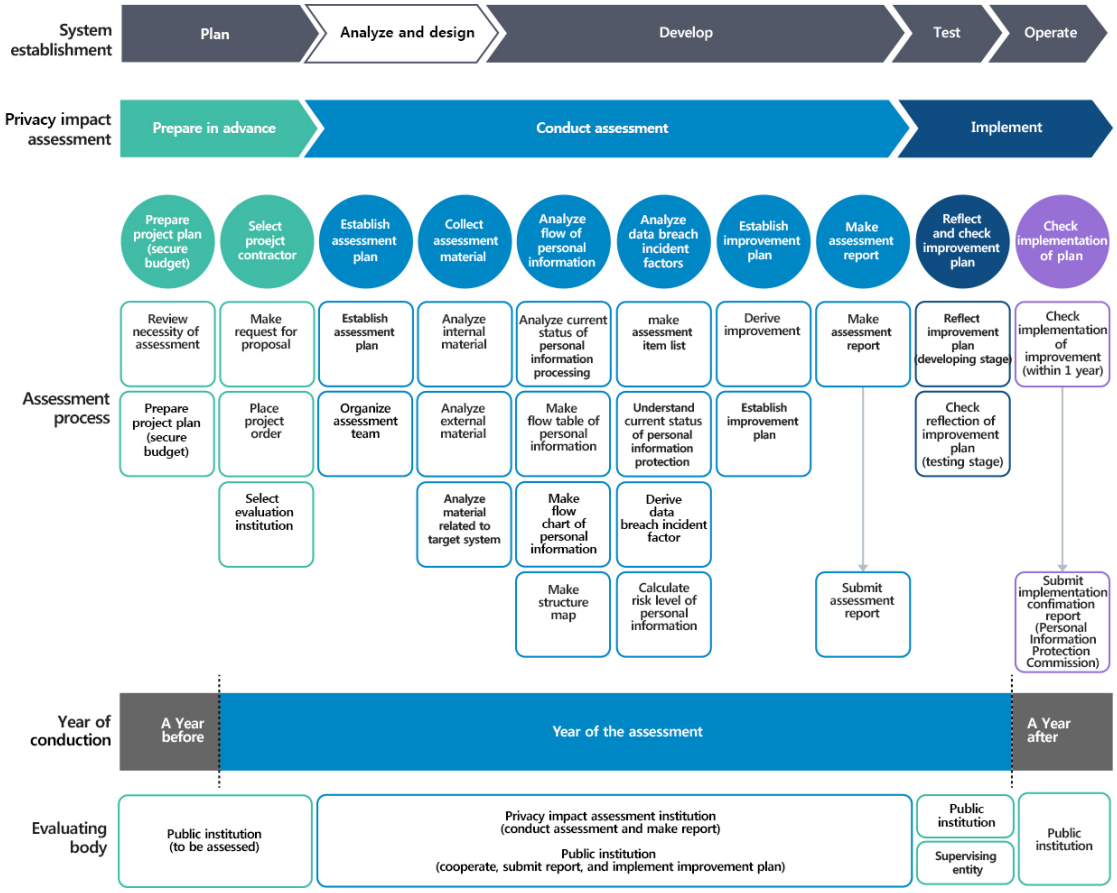

그림 1. PIA 의 상세 단계
Figure 1. Detailed steps for the PIA [5]

표 1 은 개인정보 영향평가에 관한 고시에서 규정하고 있는 개인정보 영향평가의 평가영역 및 평가분야, 세부 분야에 대한 것이다[4].

표 1. 우리나라의 개인정보 영향평가의 평가 영역
Table 1. PIA Assessment Categories regulated by the Personal Information Protection Act of South Korea

Assessment Categories	**Assessment Area**	**Detailed Field**
I. Target Organization Personal Information Protection Management System	1. Personal information protection organization	Designation of personal information protection officer
		Performance of the role of the personal information protection officer
	2. Personal information protection plan	Establishment of internal management plan
		Establishment of an annual plan for personal information protection

	3. Personal Information Infringement Response	How to report an infringement
		Response to leakage incidents
	4. Guarantee of information subject rights	Establishment of procedures to guarantee the rights of information subjects
		Guidance on how to guarantee the rights of information subjects
II.Personal information protection management system of the target system	5. Management of personal information handlers	Designation of personal information handlers
		Management and supervision of personal information handlers
	6. Management of personal information files	Management of personal information file ledger
		Registration of personal information files
	7. Privacy Policy	Disclosure of Privacy Policy
		Creation of Privacy Policy
III. Protection measures for each stage of personal information processing	8. Collection	Appropriateness of collecting personal information
		Appropriateness of Methods of Obtaining Consent
	9. Retention	Calculation of retention period
	10.Use and Provision	Appropriateness of providing personal information
		Restriction of use and provision for other purposes
		Securing safety when providing
	11. Entrustment	Disclosure of entrustment
		Entrustment contract
		Management and supervision on the person entrusted
	12. Destruction	Developing a destruction plan
		Establishment of a segregated storage plan
		Creation of a destruction register
IV. Technical Protection Measures for Target Systems	13. Access Authorization Management	Account Management
		Authentication Management
		Authorization Management
	14. Access Control	Access control measures
		Internet homepage protection measures
		Measures to protect business mobile devices
	15. Encryption of personal information	Encryption at storage
		Encryption during transmission
	16. Storage and inspection of access records	Storage of access records
		Inspection of access records
		Storage and backup of access records
	17. Prevention of malicious programs, etc.	Install and operate antivirus
		Applying security updates
	18. Physical access prevention	Establishment of access control procedures
		Establishment of import/export control procedures
	19. Destruction of personal information	Secure destruction
	20. other technical protection measures	Development environment control
		Security of personal information processing screen
		Protective measures when printing
	21.Protection of Personal Information Processing Area	Designation of protected areas
V. Protection of personal information when utilizing specific IT technologies	22. CCTV	Collecting opinions when installing CCTV
		CCTV Installation Guide
		Restrictions on the use of CCTV
		Consignment of CCTV Installation and Management
	23. RFID	RFID User Guide
		Attaching and removing RFID tags
	24. Biometric Information	Protection measures when storing original information
	25. Location Information	Consent to collect personal location information
		Guidelines for providing personal location information

국내에서는 개인정보 영향평가는 개인정보 보호법 및 시행령으로 정하는 기준에 해당하는 개인정보 파일의 운용으로 인하여 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선사항도출을 위한 평가를 의미한다. 이를 통해, 개인정보를 처리하기 전에 개인정보 보호와 관련한 위험을 평가하고 개선하여 안전한 개인정보 처리 과정 설계를 수행하는 것을 목표로 한다.

이런 사전 예방적 접근 방식은 데이터 처리 관행에 대한 포괄적인 검사를 특징으로 하며 사용자 동의, 데이터 최소화 및 보안 조치를 강조한다. 장점으로는 강화된 개인 정보 보호 및 법률 준수가 있으나, 단점으로는 PIA 수행의 복잡성과 리소스 요구 사항으로 인해 조직, 특히 중소기업에 잠재적인 관리 부담을 안겨 잠재적으로 혁신과 운영 효율성을 저해할 수 있다.

최근 우리나라 개인정보보호위원회는 개인정보 보호법 개전에 따라 도입된 '개인정보 영향평가 요약본 공개제도'를 본격적으로 진행한다고 밝혔고, 2024 년부터 개인정보 영향평가서 요약본을 통합해 공개할 예정이다 [6].

2.2 세계 각국의 개인정보 영향평가

미국은 2002 년 제정된 전자정부법 제 208 조에서 전자정부 구현 과정에서 프라이버시가 충분히 보호되도록 정부기관의 개인정보 영향평가를 의무화했다. 개인정보 영향평가 대상의 경우, 관리예산처(Office of Management and Budget) 지침으로 평가되는 정보체계의 규모, 정보의 민감성, 정보의 무단 공개로 초래되는 위험에 비례하여 영향평가를 수행토록 규정하고 있다. 특히, 신규시스템을 구축할 때는 개인정보를 수집・관리・배포하는 시스템 혹은 프로젝트의 개발, 10 인 이상의 개인정보를 온라인으로 수집하는 경우에 영향평가를 의무적으로 수행하며, 절차 및 시스템 변경 시에는 종이문서 기반 기록을 전자시스템으로 변형하거나 신기술 적용같은 IT 시스템의 신규 운용이 기존 개인정보에 중대한 변화를 야기하는 경우로 한국과 유사하게 규정하고 있다. 개인정보 영향평가의 이러한 프로세스는 법적 준수를 보장하는 장점이 있지만, 시스템 소유자와 개발자에게 추가적인 행정적 부담을 줄 수 있는 단점도 있다[7].

캐나다의 연방 개인정보 감독기관(Office of the Privacy Commissioner of Canada)의 개인정보 영향평가에 관한 가이드는 고위험 프로젝트의 경우 프로젝트 설계에 반영될 수 있도록 초반부 수행을 권장하는 적극적인 접근 방식을 강조한다. 이를 통해 프로세스 전반에 걸쳐 관련 이해관계자의 참여, 개인정보 보호법 준수 보장, OECD 개인정보 보호 원칙 준수를 권장한다. 이 가이드는 개인정보 보호 위험을 식별 및 완화하고, 개인정보 처리에 대한 법적 권한을 보장하며, 개인정보를 효과적으로 보호하기 위해 개인정보 보호 설계 원칙을 통합하는 것의 중요성을 강조한다. [8].

뉴질랜드는 개인정보 감독기관(Office of the Privacy Commissioner)을 93 년도에 개인정보 보호법의 제정과 함께 설립하였다. 뉴질랜드는 디지털 정부에서 프로젝트 개인 정보 보호 영향을 평가하기 위한 도구인 개인정보 보호 임계 값 평가(PTA) 및 PIA 에 대한 평가도구를 제공한다[9]. 이는 수집부터 폐기까지 개인정보 수명주기에 대한 개요를 제공하고 프로젝트 개인 정보 보호 위험을 식별하기 위한 프레임워크로 정보 개인 정보 보호 원칙(IPP)을 사용할 것을 명시하고 있다[10]. 3 장에서 자세히 다루는 호주의 Threshold Privacy Assessment 는 뉴질랜드와 유사하다.

아일랜드 개인정보 보호 위원회(Data Protection Commission)는 개인정보 보호법 2020 은 실제로 원칙을 기반으로 하며 다양한 상황에 적응하면서 조직의 자율성을 제공하는 것을 목표로 하는 유연성을 제공한다. PIA 와 관련하여 조직이 GDPR 준수 여부를 자가 평가할 수 있도록 체크리스트를 제공한다. 이 체크리스트는 개인 데이터, 정보주체 권리, 정확성 및 보존, 투명성 요구 사항, 기타 데이터 컨트롤러 의무, 데이터 보안, 데이터 침해, 국제 데이터 전송 등 다양한 분야에 대한 자세한 질문을 포함한다. 조직은 이 체크리스트를 사용하여 현재 보유 및 처리하는 개인 데이터, 데이터 수집의 법적 근거, 각 데이터 범주의 보존 기간을 매핑함으로써 GDPR(General Data Protection Regulation) 준수를 위해 필요한 즉각적인 개선 조치를 식별할 수 있다[11].

국내의 PIA 는 개인정보보호법(PIPA)에 의거하여 조직의 개인정보 처리 활동이 개인정보 보호에 미치는 영향을 사전에 평가하는 체계적인 방법을 제시한다. PIA 는 개인정보 보호 수준 강화, 법적 책임 명확화, 정보주체 권리 보호 등의 장점을 가지고 있지만, 높은 준수 비용, 복잡한 절차, 형식적인 평가 가능성, 부족한 전문 인력, 정부 지원 부족 등의 해결해야 할 과제를 가지고

있다. PIA 의 장점에도 불구하고, 높은 준수 비용과 복잡한 절차는 조직의 PIA 수행 참여를 저해하는 요인으로 작용할 수 있어 형식적인 평가 가능성, 전문 인력 부족, 정부 지원 부족은 PIA 의 효과성을 감소시키는 요인이 될 수 있다.

따라서, PIA 의 효과적 활성화를 위해 다음의 노력이 필요하다. 첫째, 준수 비용 절감 및 절차 간소화를 위해 PIA 수행 가이드라인 및 템플릿 제공, 온라인 PIA 시스템 개선이 필요하다. 둘째, 관련 분야의 전문 인력 양성을 위해 PIA 교육 프로그램 확대와 전문가 자격 제도 운영 등에 대한 제도 활성화가 필요하다. 마지막으로 PIA 수행 지원 사업 확대, 홍보 강화 등 정부 지원 확대가 필요하다.

표 2. PIA/개인정보보호법 특징 비교
Table 2. Comparison of PIA Characteristics

Country	Regulatory Framework	Scope	Approach	Characteristics	Pros	Cons
US	Sector-specific laws, Privacy Act of 1974	Varies by sector, federal agencies	Compliance-focused, varies by sector	Sector-specific regulations, federal agency guidance	- Expertise in specific sectors - Flexibility	- Complexity due to differences in sector-specific regulations - Focus on compliance only
Canada	PIPEDA, provincial laws	Private sector, federal institutions	Holistic, emphasizes accountability	PIPEDA, provincial laws	- Consistent approach - Clear organizational responsibility	- Limited scope of PIPEDA application - Need for coordination with provincial laws
New Zealand	Privacy Act 2020	Public and private sectors	Principles-based, flexible	Principle-based regulation, flexibility	- Organizational autonomy - Adaptable to various situations	- Lack of specific guidance - Difficulty in interpretation and application
Ireland	GDPR, Data Protection Act 2018	all sectors processing personal data	principles-based, ensuring flexibility and organizational autonomy	Emphasis on consent, rights protection, and organizational accountability.	comprehensive protection for individuals and adaptability for organizations	the complexity of compliance and potential ambiguity in interpretation
Australia	Privacy Act 1988, APP guidelines	Public and private sectors	Comprehensive, emphasizes open and transparent processes	Comprehensive, open, and transparent process	- High level of privacy protection - Transparency	- Complex process - High compliance costs
Japan	APPI	Public and private sectors	Focus on data subject consent, cross-border data flow	Data subject consent, cross -border data flow	- Strengthens data subject rights - Facilitates cross-border data flow	- Difficulty in obtaining consent - Need for coordination of cross-border regulations
EU	GDPR	Any entity processing EU residents' data	Extensive, rights of data subjects highlighted	Strong privacy regulation, facilitates market entry into the EU	- Strong privacy regulation - Facilitates market entry into the EU	- High compliance costs - Complex regulatory compliance
Korea	Personal Information Protection Act (PIPA)	Public and private sectors	Comprehensive, includes specific consent requirements	- High level of privacy protection - Provides specific guidance	- High compliance costs - Complex process	Comprehensive, specific consent requirements

III. 개인정보 영향평가 사전진단 도구 평가요소 분석

3.1 개인정보 영향평가 선진국의 PTA(Privacy Threshold Assessment) 분석

이 절에서는 간이 Pre-PIA 플랫폼(도구) 평가요소 도출을 위하여 기존에 PTA 를 선제적으로 활용하고 있는 호주, 뉴질랜드등 국가의 PTA 를 분석하였다.

3.1.1 뉴질랜드 Privacy Threshold Assessment

개인정보보호 임계 값 평가(PTA)에 대한 뉴질랜드의 접근 방식은 특히 개인 정보 보호법 2020 에 의해 뒷받침되는 포괄적인 개인정보 보호 프레임워크에 기반을 두고 있다. 이 입법 프레임워크는 원칙 기반 개인정보 보호를 강조하며 조직이 공정한 방식으로 개인정보를 처리하도록 보장하는 데 중점을 두고 있다. 뉴질랜드 개인정보보호위원회는 PTA 수행에 대한 지침을 제공하며, 이는 조직이 초기 단계에서 잠재적인 개인정보 보호 문제를 식별하여 전체 개인정보 영향 평가(PIA)가 필요한지 여부를 결정하는 데 도움을 주기 위해 고안되었다. 뉴질랜드의 PTA 항목을 분석하여 단순화된 Pre-PIA 플랫폼을 개발하는 데 주요 평가 요소를 도출하고자 한다.

다음은 뉴질랜드 PTA 의 핵심 요소이며, 각국의 PTA 와 비교분석 후 평가 요소 도출에 활용하고자 한다.

1) 개인 정보 식별: 첫 번째 단계에서는 프로젝트 또는 이니셔티브에 개인정보의 수집, 사용 또는 공개가 포함되는지 여부를 결정한다. 이는 프로세스 내에서 개인 데이터의 존재를 신속하게 확인하기 위한 Pre-PIA 도구의 필요성과 일치한다.

2) 개인정보 보호 위험 식별: 조직은 개인 정보 보호에 대한 잠재적인 위험을 식별해야 한다. 여기에는 정보가 수집, 저장, 액세스 및 폐기되는 방법과 데이터 위반 또는 무단 액세스 가능성에 대한 고려가 포함된다.

3) 개인 정보 보호 원칙 준수: PTA 는 제안된 활동이 뉴질랜드의 13 개 개인정보 보호 원칙에 얼마나 부합하는지 평가할 것을 요구한다. 이러한 원칙은 무엇보다도 수집 목적, 데이터 최소화, 데이터 품질, 보안, 액세스 및 수정 권한과 같은 측면을 다룬다. 단순화된 Pre-PIA 도구에는 이러한 원칙에 부합하는 체크리스트나 질문을 통합하여 빠른 평가를 촉진할 수 있다.

4) 참여 및 협의: 뉴질랜드의 접근 방식에는 개인정보가 처리될 개인을 포함한 이해관계자와의 적절한 협의가 있었는지에 대한 여부를 고려하여 평가 시 투명성과 참여의 중요성을 강조한다.

5) 전체 PIA 의 필요성에 대한 결정: 예비 평가를 기반으로 조직은 보다 자세한 PIA 가 필요한지 여부를 결정한다. 이 결정은 필요한 후속 조사 및 분석 수준을 결정하므로 매우 중요한 프로세스이다[10].

표 3. 호주 Threshold Privacy Assessment
Table 3. Threshold Privacy Assessment of Australia

Will the project involve:
"1. Collecting personal information or a new way of collecting personal information? (including from a new or existing source)"
"2. Using personal information to make decisions or take action against individuals in ways which can have a significant impact on them? (for example, whether to receive a service or benefit)"
"3. Collecting personal information in a way that might be perceived as being intrusive? (for example, camera surveillance, drones or biometric scans)"
4. Using personal information already held by the agency for a purpose other than how it is currently used?
5. Disclosing personal information to another agency, a contractor, the private sector or to the public?
6. An exchange of personal information between agencies?
7. Engaging a contracted service provider to deal with personal information in any way for the agency? Or will the contracted service provider transfer personal information to the agency or provide services to a third party for the agency?
8. Linking, matching or cross-referencing of personal information across or within the agency?
9. Using personal information for research or statistics?
10. A new or changed way of transferring personal information between agencies or between an agency and another entity?
11. New or changed legislative provisions that impact how the agency will collect, use or disclose personal information?
12. A new way or increased costs for individuals to access their own personal information?
"13. A change in the way personal information is stored or secured? (for example, a cloud-based storage system)"
14. A new or amended process for verifying an individual's identity?
"15. Transferring personal information outside Australia at any stage? (for example, publishing information to a website or through use of cloud-based services or online surveys)"
16. Using de-identified information that could be matched with another dataset (or publicly available information) and enable individuals to be identified?
17. Any other activity that could impact on the community's reasonable expectations of privacy? If yes, please detail:

3.1.2 호주 Threshold Privacy Assessment

호주의 임계치 개인정보 평가의 항목은 표 3 과 같다. 임계치 개인정보 평가의 항목을 기반으로 Pre-PIA 의 분류를 도출하였다. 그에 맞게 체크항목을 분류한 결과는 다음과 같다[12].

- 개인정보의 수집: 1, 3, 14
- 개인정보의 활용: 2, 4, 8, 9
- 개인정보의 공유, 이전: 5, 6, 7, 15
- 개인정보 처리, 보안 기술: 10, 12, 13, 16
- 개인정보의 법조항: 11
- 기타: 17

3.2 Pre-PIA 개발에 적용할 요소 도출

한국의 상황을 고려한 단순화된 Pre-PIA 플랫폼 개발을 위해 3 국의 PTA 접근 방식을 분석하면 다음과 같은 평가 요소와 함의를 얻을 수 있다.

- 단순성 및 유연성: 이 도구는 개인 정보가 관련되어 있는지, 즉각적인 개인 정보 보호 위험이 있는지 신속하게 식별하여 전체 PIA 의 필요성을 쉽게 결정할 수 있도록 설계되어야 한다.
- 원칙 기반 평가: 뉴질랜드에서 사용되는 것과 유사한 일련의 개인 정보 보호 원칙을 통합하면 조직이 체계적이면서도 유연한 방식으로 개인 정보 보호 요구 사항 준수를 평가하는 데 도움이 될 수 있다.
- 이해관계자 참여: Pre-PIA 프로세스에서 이해관계자 협의를 강조하면 잠재적인 개인 정보 보호 문제를 조기에 식별하고 투명성 문화를 조성하는 데 도움이 될 수 있다.
- 위험 기반 접근 방식: 이 도구는 조직이 위험의 우선순위를 지정하고 활동이 개인 정보 보호에 미치는 잠재적 영향을 이해하여 자세한 평가가 필요한지 여부에 대한 결정을 내리는 데 도움이 된다.

요약하면, 개인정보 위험의 조기 식별과 개인정보 보호 원칙 준수에 초점을 맞춘 뉴질랜드의 PTA 항목은 단순화된 Pre-PIA 플랫폼 개발을 위한 귀중한 프레임워크를 제공한다. 이러한 요소를 통합함으로써 이러한 도구는 조직이 개인 정보 보호에 미치는 영향을 효율적으로 평가하고 전체 PIA 수행의 필요성을 결정하는 데 도움이 될 수 있다.

다음 표는 우리나라 개인정보 영향평가 대상이 되는 평가영역, 평가분야, 세부분야 중 Pre-PIA 에 들어가야 할 요소들을 확인하기 위하여, 세부분야별 Pre-PIA 분석을 위한 확인 질문들을 도출한 것으로서, 이 분석 결과는 국내 5 인의 전문가들의 자문을 거쳐 타당도를 높였다. 일부 항목은 실제 PIA 에서 확인할 수 있는 전문적인 항목으로 제외할 필요가 있다는 점이 도출되었다.

표 4. Pre-PIA 개발을 위한 PIA 세부분야에 대한 확인 질문 도출
Table 4. Deriving confirmation questions on the PIA assessment detail fields for pre-PIA development

Assessment Categories	Assessment Area	Derived questions on the detailed field
I. Target Organization Personal Information Protection Management System	1. Personal information protection organization	개인정보보호책임자가 지정되어 있습니까? Do you have a designated personal information protection manager?
		개인정보보호책임자가 있다면, 어떤 역할을 수행하고 있습니까? If you have designated a personal information protection officer, what role does he or she play?
	2. Personal information protection plan	개인정보보호 내부관리계획을 가지고 있습니까? Do you have an internal management plan for personal information protection?
		개인정보보호를 위한 연간 계획이 수립되었 있습니까? Has an annual plan for personal information protection been established?
	3. Personal Information Infringement Response	개인정보 침해 신고 절차가 마련되어 있습니까? Do you have procedures to report personal information infringement?
		개인정보 유출 사고 대응 절차가 마련되어 있습니까? Do you have procedures to respond to personal information leak incidents?
	4. Guarantee of information subject rights	정보주체의 권리보장 절차가 마련되어 있습니까? Do you have procedures to guarantee the rights of data subjects?
		정보주체의 권리보장 방법 안내는 어떻게 하고 있습니까? How do you provide information on how to protect the rights of data subjects?

II.Personal information protection management system of the target system	5. Management of personal information handlers	개인정보취급자 목록이 있습니까? Do you have a list of personal information handlers?
		개인정보취급자에 대한 관리·감독은 어떻게 하고 있습니까? How do you manage and supervise personal information handlers?
	6. Management of personal information files	개인정보파일 관리 대장이 있습니까? Do you have a personal information file management list?
		등록 의무 개인정보파일을 모두 등록했습니까? Have you registered all of your registration mandatory personal information files?
	7. Privacy Policy	개인정보처리방침 안내는 어떻게 하고 있습니까? How do you provide information on the personal information processing policy?
		개인정보처리방침이 있습니까? Do you have a privacy policy?
III. Protection measures for each stage of personal information processing	8. Collection	수집하는 개인정보에 대한 수집의 법적 근거를 확인했습니까? Have you confirmed the legal basis for collecting the personal information you collect?
		동의를 근거로 수집하는 경우, 동의 받는 방법은 정확합니까? If collection is based on consent, is the method of obtaining consent correct?
	9. Retention	적절한 개인정보를 보유 기간을 산정했습니까? Have you calculated the appropriate retention period for personal information?
	10.Use and Provision	개인정보를 제 3 자에게 제공하는 경우, 제공의 법적 근거를 확인했습니까? If you provide personal information to a third party, have you confirmed the legal basis for provision?
		개인정보의 수집 목적을 벗어나는 이용과 제공을 하지는 않습니까? Do you use or provide personal information beyond the purpose for which it was collected?
		개인정보를 제 3 자에게 제공하는 경우, 안전성 확보를 위해 어떤 조치가 마련되어 있습니까? When personal information is provided to a third party, what measures do you have to ensure safety?
	11. Entrustment	개인정보를 위탁하는 사실을 공개하고 있습니까? Are you disclosing the fact that you entrust your personal information?
		위탁계약을 체결했습니까? Have you signed a consignment contract?
		수탁사에 대한 관리·감독은 어떻게 하고 있습니까? How do you manage and supervise the person entrusted?
	12. Destruction	개인정보 파기 계획이 있습니까? Do you have any plans to destroy personal information?
		개인정보 분리보관 계획이 있습니까? Do you have a plan for separate storage of personal information?
		개인정보 파기 기록 대장이 있습니까? Do you have a record of personal information destruction?
IV. Technical Protection Measures for Target Systems	13. Access Authorization Management	개인정보에 접근하는 사용자에 대한 계정을 관리하고 있습니까? Do you manage accounts for users who access your personal information?
		사용자 계정에 대한 인증체계를 마련했습니까? Have you established an authentication system for user accounts?
		사용자별 개인정보 접근권한 설정을 하고 있습니까? Are you setting personal information access rights for each user?
	14. Access Control	개인정보파일에 대한 접근통제 조치가 마련되어 있습니까? Do you have access control measures for personal information files?
		인터넷 홈페이지에 대한 보호 조치가 마련되어 있습니까? Do you have protection measures for your Internet homepage?
		업무용 모바일기기에 대한 보호조치가 마련되어 있습니까? Dp you have protection measures for work mobile devices?

	15. Encryption of personal information	개인정보를 저장하는 경우 암호화를 하고 있습니까? When you store personal information, is it encrypted?
		개인정보를 전송하는 경우 암호화를 하고 있습니까? When you are transmitting personal information, is it encrypted?
	16. Storage and inspection of access records	개인정보 접속기록을 보관하고 있습니까? Do you keep personal information access records?
		개인정보 접속기록을 점검하고 있습니까? Are you checking personal information access records?
		개인정보 접속기록을 안전하게 보관하고 백업하고 있습니까? Are personal information access records safely stored and backed up?
	17. Prevention of malicious programs, etc.	백신 프로그램을 설치·운영하고 있습니까? Are you installing and operating an anti-virus program?
		보안업데이트 적용을 시의적절하게 하고 있습니까? Are you applying security updates in a timely manner?
	18. Physical access prevention	물리적 출입통제 절차가 마련되어 있습니까? Do you have physical access control procedures?
		개인정보를 반출·반입하는 절차가 마련되어 있습니까? Do you have procedures for exporting and importing personal information?
	19. Destruction of personal information	개인정보를 안전하게 파기하기 위한 방법이 마련되어 있습니까? Do you have methods to safely destroy personal information?
	20. other technical protection measures	개인정보 시스템을 개발하는 환경이 통제되고 있습니까? Do you have the environment in which personal information systems are developed controlled?
		개인정보처리화면에 대한 보안이 이루어지고 있습니까? Do you have security measures of the personal information processing screen?
		개인정보 출력시 보호조치가 마련되어 있습니까? Do you have protection measures when printing personal information?
	21.Protection of Personal Information Processing Area	개인정보처리를 위한 별도의 보호구역을 지정하고 있습니까? Do you designate a separate protection area for processing personal information?
V. Protection of personal information when utilizing specific IT technologies	22. CCTV	CCTV 설치시 의견수렴을 하였습니까? Did you collect opinions when installing CCTV?
		CCTV 안내문을 게시하고 있습니까? Are you posting CCTV notices?
		CCTV 사용 제한에 대한 사항을 준수하고 있습니까? Are you complying with restrictions on CCTV use?
		CCTV 설치 및 관리에 대한 위탁을 하는 경우 적절한 계약 및 관리 절차가 있습니까? When you outsource CCTV installation and management, do you have appropriate contract and management procedures?
	23. RFID	RFID 이용자에 대한 안내가 이루어지고 있습니까? Are you providing a guidance to RFID users?
		RFID 태그 부착 및 제거가 적절하게 이루어지고 있습니까? Are RFID tags being attached and removed properly?
	24. Biometric Information	바이오인식 원본정보 보관시 보호조치가 마련되어 있습니까? Do you have protective measures when storing original biometric information?
	25. Location Information	개인위치정보 수집에 대한 동의가 적절하게 이루어지고 있습니까? Are you properly obtaining consents to the collection of personal location information?
		개인위치정보를 제공하는 경우에 대한 안내가 적절하게 이루어지고 있습니까? Are you properly informing data subjects of providing personal location information?

3.3 Pre-PIA 구성 예시

본 연구에서는 3.2 절에서 연구결과로 제시한 Pre-PIA 개발에 도출된 요소들을 사용해 Pre-PIA 질문항목들을 구성 예시를 제시한다. 이 제안된 예시는 곧바로 사용할 수는 없으며, 향후 연구에서 추가적인 자문과 현장 실무자들의 의견을 반영하여 정리될 필요가 있으며, 종국에는 웹사이트 개발과 더불어 전국민이 사용할 수 있는 Pre-PIA 시스템으로의 구축이 필요하다.

표 5. Pre-PIA 구성 예시 제안
Table 5. Proposed Pre-PIA configuration example

개인정보의 수집 및 사용 관련 셀프 체크 리스트, Self-check list regarding collection and use of personal information
1. 프로젝트/시스템은 개인정보를 수집하나요? **Does the project/system collect personal information?**
2. 수집하는 개인정보는 민감한 정보(예: 건강정보, 금융정보)를 포함하나요? **Does the personal information you collect include sensitive information (e.g. health information, financial information)?**
3. 수집한 개인정보의 사용 목적이 명확하고 합법적인가요? Is the purpose of using the collected personal information clear and legal?
개인정보의 보관 및 파기 관련 셀프 체크 리스트, Self-check list regarding storage and destruction of personal information
1. 개인정보의 보관 기간이 명확하게 정의되어 있나요? **Is the storage period of personal information clearly defined?**
2. 보관 중인 개인정보는 안전하게 보호되나요? **Is stored personal information safely protected?**
3. 개인정보의 파기 절차가 안전하고 적절하게 이루어지나요? Do you have personal information destruction procedures carried out safely and appropriately?
개인정보의 전송 관련 셀프 체크 리스트, Self-check list regarding sharing and transmission of personal information
1. 개인정보를 제 3 자와 공유하거나 전송하나요? **Do you share or transfer personal information to third parties?**
2. 개인정보를 국외로 전송하는 경우가 있나요? **Is personal information ever transferred overseas?**
3. 개인정보의 공유 및 전송 과정에서 적절한 보호조치가 이루어지나요? Are appropriate protection measures taken during the sharing and transmission of personal information?
개인정보 침해 관련 셀프 체크 리스트, Self-check list regarding personal information infringement risks and responses
1. 프로젝트/시스템은 개인정보 침해 위험을 평가했나요? **Has the project/system assessed the risk of privacy infringement?**
2. 개인정보 침해 발생 시 대응 계획이 마련되어 있나요? Is there a response plan in place in case of a personal information breach?
정보주체 권리 보호 관련 셀프 체크 리스트, Self-check list for data subjects' rights protection
1. 프로젝트/시스템은 정보주체의 권리(접근, 정정, 삭제 등)를 보장하나요? **Does the project/system guarantee the rights of data subjects (access, correction, deletion, etc.)?**
2. 이해관계자(예: 정보주체, 관련 기관)의 의견을 수렴하는 과정이 포함되어 있나요? Does it include a process for collecting opinions from stakeholders (e.g. data subjects, relevant organizations)?
법적 및 규제 준수 관련 셀프 체크 리스트, Legal and compliance self-checklist
1. 프로젝트/시스템은 현행 개인정보 보호 법령과 규제를 준수하나요? Does the project/system comply with current personal information protection laws and regulations?
2. 필요한 경우, 개인정보 보호에 대한 법적 조언을 구했나요? If necessary, have you sought legal advice regarding privacy?

IV. 결론

이 연구는 국제적인 개인정보 보호 법령들, 특히 유럽 연합의 GDPR, 캐나다 및 뉴질랜드에서 제시된 개인정보영향평제도, 즉 PIA 에 대한 다양한 접근방식을 비교 분석함으로써, 국내 일반 개인정보처리자들이 개인정보 보호 위험을 효과적으로 식별하고 완화할 수 있는 개인정보 영향평가 사전진단 도구, 즉 Pre-PIA 모델을 제안한다. 이 모델은 특히 중소기업 및 스타트업에

유용하며, 개인정보 보호를 강화하고 법적 준수를 달성하는 데 기여할 것으로 기대된다. 이 논문은 국내 개인정보 보호 환경에 적합한 간이 Pre-PIA 의 개발을 목표로 한다.

디지털 환경에서 개인정보 유출 사고가 증가함에 따라, 일반 국민들, 개인정보처리자들이 사용할 수 있는 효율적이고 실용적인 Pre-PIA 개발이 필수적이다. 특히 자원이 제한된 중소기업과 스타트업 기업에 도움이 될 Pre-PIA 모델의 필요성에 따른 평가요소를 제시하였다.

국제적인 개인정보 보호 규정 및 접근 방식의 비교 분석을 통해, 국내 개인정보 보호 환경에 적합한 Pre-PIA 모델의 예시를 제안하였다. 제안된 예시는 중소기업 및 스타트업 기업의 한계와 요구 사항을 고려하여 설계되었다. 이를 통해, 이러한 조직들이 개인정보 보호 위험을 효과적으로 관리하고 법적 준수를 달성할 수 있도록 지원한다. 이는 법적 준수뿐만 아니라, 개인정보 보호 수준을 강화하는 데 도움이 될 것이다. 실용적 관점에서 Pre-PIA 모델은 복잡성을 줄이고, 절차를 간소화하여, 조직이 개인정보 보호 위험을 효율적으로 식별하고 대응할 수 있도록 한다. 이는 개인정보 관리 및 보호의 지속적인 개선을 촉진할 것이다.

결론적으로 이 연구는 국내 개인정보 보호 환경에 적합한 간이 Pre-PIA 모델의 개발을 통해, 개인정보 보호를 강화하고 관련 법적 준수를 달성하는 데 기여할 실용적인 솔루션을 제시한다. 이 연구는 개인정보 보호에 대한 더 넓은 담론을 제공하고, 개인정보 관리에 대한 정책 개발과 조직의 모범 사례 모두에 유용한 정보를 제공함으로써 정책 개발 및 모범 사례에 기여할 것이다.

V. 감사의 글

이 연구는 2021 년도 선문대학교 교내학술연구비 지원에 의하여 이루어졌음.

VI. 참고문헌

[1] Y.-H.Choi, K.-H. Han, “Problems and Improvement of Privacy Impact Assessment,” Journal of The Korea Institute of Information Security & Cryptology, VOL.26, NO.4, pp.973-983, Aug. 2016.

[2] Korean Law Information Center, “Personal Information Protection Act, PIPA,” [Online] available : https://www.law.go.kr/LSW/eng/lawEngBodyCompareInfoP.do?lsNm=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95&lsId=011357&efYd=20230915&lsiSeq=248613&gubun=EngLs&ancYnChk=undefined

[3] Korean Law Information Center, “Enforcement Decree of the PIPA,” [Online] available : https://www.law.go.kr/LSW/eng/lawEngBodyCompareInfoP.do?lsNm=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95%20%EC%8B%9C%ED%96%89%EB%A0%B9&lsId=011468&efYd=20230915&lsiSeq=254693&gubun=EngLs&ancYnChk=undefined

[4] Korean Law Information Center, “Notification of Privacy Impact Assessment,” [Online] available : https://www.law.go.kr/행정규칙/개인정보영향평가에관한고시/(2023-10,20231016)

[5] Personal Information Protection Commission, “Privacy Impact Assessment procedure,” [Online] available : https://www.pipc.go.kr/eng/user/lgp/pbp/personalInformationImpactAssessment.do

[6] Public institutions handling personal information are required to disclose ‘personal information impact assessment’, Safe Times, [Online] available : https://www.safetimes.co.kr/news /article View.html? idxno=208966(Accessed: 23.12.30)

[7] S.-Y. Chang, “Comparison of the Domestic and International Status of the Privacy Impact Assessment System and Analysis of Implications,” ICT & Media Policy, VOL.30, NO.14, pp.1-13, 2018.

[8] Office of the Privacy Commissioner of Canada, “Expectations: OPC’s Guide to the Privacy Impact Assessment Process,” [Online] available : https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/#toc1(Accessed: 23.12.30)

[9] Privacy Commissioner, “Privacy Impact Assessment Toolkit,”[Online] available : https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-toolkit/(Accessed: 23.12.20)

[10] Digital New Zealand Government, “Privacy, security and risk,” [Online] available : https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/(Accessed: 23.12.20)
[11] Ireland Data Protection Commission, “Data Protection Impact Assessments,” [Online] available : https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments(Accessed: 23.12.20)
[12] The State of Queensland (Office of the Information Commissioner), “Threshold Privacy Assessment of Australia,” [Online] available : https://www.oic.qld.gov.au/__data/assets/word_doc/0007/37087/template-threshold-privacy-assessment.dotx (Accessed: 23.12.10)

저자소개

정영애(*Young-Ae Jung*)

2007 년 2 월 단국대학교 대학원 컴퓨터과학과 박사
2009 년 3 월~현재 선문대학교 IT 교육학부 교수

관심분야 : AI 소프트웨어공학 , 머신러닝, 프라이버시