JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 29 No. 6, pp. 61-67, June 2024
https://doi.org/10.9708/jksci.2024.29.06.061

A Study on Strengthening Domestic Personal Information Impact Assessment(PIA)

Young-Bok Cho*

*Professor, Dept. of Computer Education, Andong National University, Andong, Korea

[Abstract]

In this paper, we presented a strengthening plan to prevent personal information leakage incidents by securing legal compliance for personal information impact assessment and suggesting measures to strengthen privacy during personal information impact assessment. Recently, as various services based on big data have been created, efforts are being made to protect personal information, focusing on the EU's GDPR and Korea's Personal Information Protection Act. In this society, companies entrust processing of personal information to provide customized services based on the latest technology, but at this time, the problem of personal information leakage through consignees is seriously occurring. Therefore, the use of personal information by trustees.

▸ **Key words**: Personal information, Privacy impact assessment(PIA), ISMS-P, Data protection, Trustee

[요 약]

본 논문에서는 개인정보 영향평가의 법적 준거성을 확보하고 개인정보 영향평가 시 프라이버시 강화 방안을 제시함으로써 개인정보 유출 사고를 방지할 수 있는 강화 방안을 제시하였다. 최근 빅데이터를 기반으로 한 다양한 서비스들이 생성되면서 EU의 GDPR, 국내는 개인정보 보호법을 중심으로 개인정보보호를 위해 노력하고 있다. 이런 사회 속에서 기업들은 최신기술을 기반으로 한 개인의 맞춤형 서비스를 제공하기 위해 개인정보를 위탁 처리하게 되는데, 이때 수탁사를 통해 개인정보 유출 문제가 심각하게 발생하고 있다. 따라서 수탁사들의 개인정보 사용에 따른 법적 준거성을 확보하면서 체계적으로 개인정보를 관리 할 수 있는 방안에 대해 고찰한다.

▸ **주제어**: 개인정보, 개인정보영향평가, 개인정보경영시스템, 데이터보호, 수탁사

• First Author: Young-Bok Cho, Corresponding Author: Young-Bok Cho
*Young-Bok Cho (ybcho@anu.ac.kr), Dept. of Computer Education, Andong National University
• Received: 2024. 05. 20, Revised: 2024. 06. 07, Accepted: 2024. 06. 07.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

4차 산업혁명으로 사회가 발전하고 인공지능과 빅데이터를 서비스하면서 사회는 디지털 대전환 시대를 맞이하고 있다. 디지털 대전환 시대를 맞이해 개인정보의 중요성이 주목받고 있다. 개인정보보호위원회의 개인정보 분쟁조정 제도는 개인정보 유출 등으로 피해가 발생했을 때, 침해 주체와 피해자 간에 소송 없이 신속하고 간편하게 문제를 해결하고 합의를 유도하는 제도이다. 이는 빅데이터 사회에서 중요한 역할을 한다[1][2]. 개인정보가 중요한 시대가 된 지금 개인정보 유출 사고는 꾸준히 발생하고 있다. 개인정보보호위원회 통계자료를 보면 2017년에는 해마다 10만 건 이상 개인정보 침해가 발생하고 있으며, 개인정보 침해 건수에 포함된 제3자 제공 관련 침해 건수는 2017년에는 3,881건(전년 대비 약 24% 증가), 2018년에는 6,457건(전년 대비 약 66% 증가), 2019년에는 6,055건(전년 대비 약 6% 감소), 2020년 가장 많았던 개인정보 침해유형은 '수집한 목적 외 이용 또는 제3자 제공'으로 개인정보위원회는 발표한 바 있다[3]. 2022년 분쟁 조정제도 운영성과 분석 결과에 따르면 개인정보유출 등 분쟁 사건처리가 전년 대비 12% 증가했으며 손해배상은 전년 대비 21% 증가한 것으로 보고되었다[4]. 그림 1은 2020년 분쟁조정 사건처리 통계로 개인정보보호위원회에서 발표된 개인정보 침해유형을 도식화하였다.

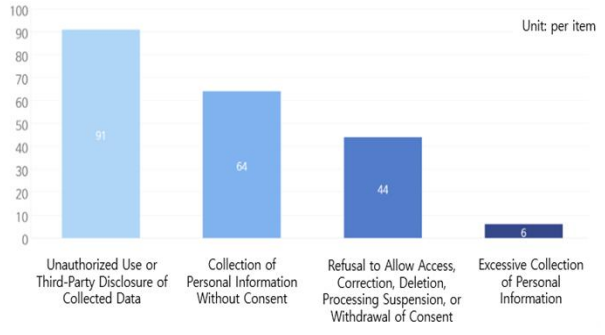

Fig. 1. 2020 Dispute Resolution Case Handling Statistics

우리나라는 4차 산업혁명 시대를 맞아 개인정보 보호 강화를 위해 '데이터 3법'이라 불리는 '개인정보 보호법', '정보통신망법','신용정보 보호법'을 동시에 개정하고 개인정보보호 체계를 일원화하면서 EU GDPR 적정성 결정이 최종 통과되어 개인정보 보호 우수국가로 인정받았다[5]. 그러나 여전히 개인정보 관리 소홀로 인한 사건은 지속해 발생하고 있다. 개인정보를 취급하는 개인정보처리자의 과실로 인한 대량의 개인정보가 유출되는 사고는 물론 개인정보 업무 담당자 등 개인정보 취급자에 의한 개인정보 유출 사고는 증가 추세에 있다[2][3]. 이는 개인정보보호법 제2조제5호에서 정의한 업무를 목적으로 개인정보 파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하도록 개인정보처리자를 지정하고 있는데 개인정보처리자의 부주의가 가장 높다고 밝히고 있다.

현재 기업의 경우 개인정보처리를 위해 개인정보 수탁자를 지정하고 있는데 개인정보 수탁업체의 94%가 개인정보처리 시스템 안정성 확보조치가 미흡하거나 위/수탁 계약이 미비하다는 문제들을 갖고 있다. 따라서 개인정보보호법 제26조에서 개인정보 안전성 확보조치 위반에 관한 조항을 통해 개인정보처리 시스템의 안전성 확보조치 기준을 마련하고 있으나 여전히 개인정보의 위탁 시 발생하는 문제는 지속되고 있다[6][7]. 최근에도 발생하는 위탁·수탁 문제를 현실적인 범주 내에서 강화하고 관리·감독이 필요하다. 따라서, 본 논문에서는 개인정보 위탁과 관련된 개인정보보호 법률들을 분석하고, 국내 개인정보 관리 구조들을 살펴보면서 문제점이 무엇인지 분석해 개인정보처리 표준안 개선안과 프라이버시 보호를 위한 강화 방안을 제시한다.

II. Preliminaries

1. Related works

최근 급격히 증가하고 있는 침해 사고로 앞으로는 AI, 블록체인 등 다양한 신기술 서비스 확대 및 이용자의 개인정보보호에 관한 관심 증가로 인해 새로운 분야에서 상담 및 신고가 증가할 것으로 예상되고, 데이터 3법 관련「개인정보 보호법」개정(안) 시행 등 개인정보 활용 범위가 확대되면서 개인정보 침해 원인 등이 다양해질 것으로 예측된다[8][9][10]]. 따라서 기업들은 침해 행위로부터 개인정보의 유출을 방지하기 위해 개인정보보호를 강화하고 다양한 보안 솔루션을 도입하기 위해 노력하고 있지만, 기업에서 시행하고 있는 개인정보 생명주기를 살펴보면 정보통신 서비스 제공자가 고객의 개인정보를 효율적으로 관리할 수 있도록 개인정보 생명 주기별 보안 관리 모델(TTA S.KO-12.0053)[11]을 표준으로 제시하면서 수집, 저장, 파기 부분에서의 보안 수준은 높아졌다. 그러나 개인정보 이용, 제공 부분에서 개인정보들의 침해 사고가 여전히 상승하면서 잠재된 보안 위협이 존재한다는 것을 알 수 있다.

1.1 Legal considerations to comply with when providing personal information

우리나라의 개인정보보호에 관한 대표적인 법률은 개인정보 보호법과 정보통신망법, 신용정보 보호법 즉 데이터 3법이 있다. 개인정보 보호법의 경우 일반법으로써 공공부문과 민간부문 전체에 적용되며, 정보통신망법의 경우 특별법으로써 정보통신 서비스 제공자를 적용 대상으로 신용정보 보호법은 신용정보의 효율적인 이용과 체계적 관리를 위해 정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호한다. 데이터3법에서는 개인정보 처리 업무 위탁 시 개인정보 라이프 사이클(수집 → 저장 → 이용 및 제공 → 파기) 별로 위탁사가 준수해야 할 법률 사항을 명시하고 있다[11][12].

1.2 The personal information management structure of domestic companies

국내기업에서는 개인정보 저장 데이터베이스를 기업의 개인정보관리 시스템에 의해 관리되며 사용자는 자신의 개인정보 이용 동의를 통해 관리 시스템에 저장된다. 이때 기업에서는 개인정보 관리 책임자에 의해 개인정보 관리 시스템이 운영되고 있다. 그림 2는 국내기업의 개인정보 관리체계를 도식화한 것이다. 개인정보를 취급하는 기업은 개인정보 활용을 위해 위탁기관을 선정하고 처리한다. 이때 개인정보 중에서 특정한 개인정보 파일을 취급하는 수탁자로 인해 발생하는 개인정보 침해 문제가 지속해서 증가하고 있다[13].

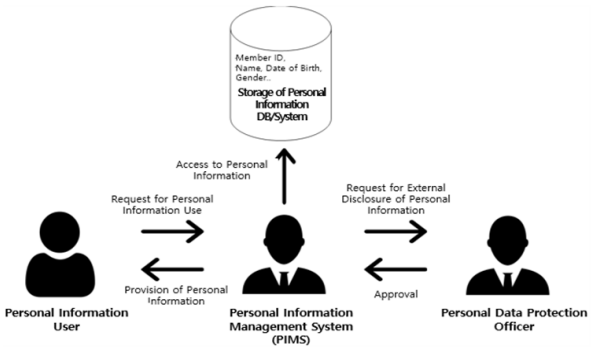

Fig. 2. Domestic Corporate Privacy Management Structure

1.3 Provision of personal information

개인정보의 "제공"이란, 개인정보가 저장된 매체나 출력물, 책자 등을 물리적으로 이전하는 것, 네트워크를 통해 개인정보를 전송하는 것, 제3자에게 개인정보에 대한 접근권한을 부여하는 것, 그리고 개인정보처리자와 제3자가 개인정보를 공유하는 등 개인정보의 이전이나 공동 이용을 발생시키는 모든 행위를 포함한다. 개인정보 보호법 제17조에서 "개인정보의 제공에서 제3자"는 정보 주체와 그에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 사람을 의미한다. 단, 정보 주체의 대리인(명확히 대리 범위 내에서 활동하는 경우)과 법 제26조 제2항에 따른 수탁자는 이에 포함되지 않는다[14]. 개인정보의 제공은 개인정보의 처리 업무 위탁과 제3자 제공으로 분류될 수 있다[15]. 위탁자는 업무 위탁으로 인해 정보 주체의 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 수탁자를 교육하고, 수탁자가 이를 준수하는지 감독해야 한다[2][9].

III. The Proposed Scheme

4차 산업혁명으로 빅데이터 시대가 도래하면서 개인이 가진 각종 개인정보가 중요해지게 되었다. 그에 따라 개인정보의 유출 사건, 사고들도 계속해서 증가하였고, 이를 방지하기 위해 공공기관에서는 개인정보 보호법 33조 제1항에 따라 영향평가 수행이 의무화가 되었다. 개인정보 영향평가는 공공기관에서 개인정보를 운영할 때 개인정보의 유출이나 침해가 의심되는 요인들을 분석하고 조사하면서 사고를 사전에 방지하기 위해 마련된 제도로 기업에서 개인정보 영향평가를 수행한 후 개인정보 유출 사고가 발생하게 되면 법적으로 관리적 책임을 다한 증거자료로 사용될 수 있는 유용한 제도이다. 그러나 각 기업에서는 평가를 통해 엄격한 주의와 감독을 받으며 개인정보 영향평가 항목들을 수행해야 한다.

1. Personal Data Impact Assessment

개인정보 영향평가는 개인정보 보호법 제2조 제6호에 따른 공공기관에서 운영하는 개인정보를 처리하는 시스템으로 의무 수행 대상자는 해당 개인정보 파일이 개인정보 보호법 시행령 제35조에 근거하는 경우, 개인정보 영향평가를 의무적으로 수행하여야 한다[12]. 표 1은 개인정보 영향평가 수행에 프라이버시 강화를 위한 기업 특성을 고려한 평가 항목이 추가되었다. 그러나 개인정보 위탁의 경우에는 원칙적으로 정보 주체에게 위탁할 것이라는 고지를 반드시 수행해야 하고 영향평가의 경우 모든 민간 기업에서 공통적인 기본사항을 제시하고 있으므로 수행하는 기업의 특성들을 고려해서 평가 항목들을 추가로 강화해야 할 필요가 있다. 국내의 경우 개인정보경영 시스템(ISPM-P)를 통해 개인정보 위탁사업자의 수탁자 교육 및

Table 1. The process flow of conducting a personal data impact assessment

Item	Value
Developing a Business Plan(Budget Allocation)	-Reviewing the Need for Impact Assessment -Writing a Business Plan (Budget Allocation)
Selection of Business Partners	-Writing a Proposal Request -Business Procurement -Selection of Impact Assessment Agencies
Evaluation Execution, Plan Establishment	-Composition of Evaluation Team
Collecting Evaluation Data	-Internal Data Analysis -External Data Analysis -Analysis of Relevant Data on Target Systems
Analysis of Personal Data Flow	-Analysis of Personal Data Processing Operations -Creation of Personal Data Flowcharts -Preparation of Personal Data Flow Diagrams -Development of System Architecture Diagrams
Analysis of Personal Data Breach Factors	-Writing Evaluation Criteria -Assessment of Current Personal Data Protection Measures -Identification of Factors Leading to Personal Data Breaches -Assessment of Personal Data Risk Level
Establishment of Improvement Plans	-Deriving Improvement Suggestions -Establishment of Improvement Plans
Writing Impact Assessment Report	-Writing Impact Assessment Reports -Submitting Impact Assessment Reports
Compliance Check	-Reviewing Implementation of Improvement Measures -Conducting Implementation Checks of Improvement Plans -Submitting Confirmation of Implementation Checks

감독 의무를 보증하고 있으나 기업별로 고객정보의 수집 이용관리에 대해서 외주용역을 통해 이루어지는 경우가 대부분으로 이때 개인정보 위탁사업자는 개인정보 보호법 시행령 제28조의 개인정보의 처리업무 위탁 시 조치에서 위탁자의 수탁자 교육 감독의 의무를 강조하고 있지만, 여전히 개인정보 유출 문제는 매년 증가하고 있다.

개인정보처리 업무 위탁 기업들은 ISMS-P의 개인정보 표시 제한 및 이용 시 보호조치에 대해서 개정 사항을 통해 개인정보의 처리 업무 위탁 조치를 강조하고 있지만, 개인정보처리 업무 수탁자가 개인정보처리 업무를 잘 수행하고 있는지는 개인정보처리 담당자가 지속적인 확인이 필요한 부분이다. 개인정보 처리를 위한 외부 위탁 시, 데이터의 안전과 개인정보 보호를 보장하기 위해 행정 및 기술적 조치를 모두 시행하는 것이 중요하기 때문에 추가로 '개인정보의 위탁에 관한 관리적·기술적 대책'이 제시될 필요가 있다. 따라서 어떤 행위가 개인정보의 제공에 해당하는지 아니면 처리 위탁에 해당하는지는 여러 요소를 종합적으로 고려하여 판단해야 한다. ① 개인정보의 취득 목적과 방법, ② 대가 수수 여부, ③ 수탁자에 대한 실질적인 관리·감독 여부, ④ 정보 주체 또는 이용자의 개인정보 보호 필요성에 미치는 영향, ⑤ 해당 개인정보가 있어야 하는 자가 실질적으로 누구인지 등 이러한 판단을 통해 대법원 판례[대법원 2017. 4. 7. 선고]를 참조해 법적 정당성을 확보할수 있다. 따라서, 개인정보 처리 위탁 시 수탁자는 위탁자로부터 위탁사무 처리에 대한 대가를 받는 것 이외에는 개인정보 처리와 관련하여 독립적인 이익을 가지지 않아야 하고 수탁자는 정보제공자의 관리와 감독 아래에서만 개인정보를 처리하며, 위탁된 범위 내에서만 활동함으로 개인정보 보호법 제17조와 정보통신망법 제24조의 2에 정의된 '제3자'에 해당하지 않음을 인식해야 합니다.

2. The Legal Issues Regarding Outsourcing and Third-Party Data Disclosure

개인정보보호법에서 위탁과 제3자 제공은 나누어져 있으며, 위탁은 개인정보 보호법 제26조에서 정의되어 있고, 제3자 제공은 개인정보보호법 제17조, 18조에서 정의되어 있다. 이 두 제공을 구분하는 방법으로 첫 번째, 정보 주체가 사전에 예측이 가능한지의 유·무성이 있고, 두 번째, 이익을 위탁자가 보면 위탁, 제3자가 이익을 얻으면 제3자 제공으로 이익의 주체로 제공을 구분할 수 있고, 마지막으로 관리의 주체에 따라 위탁인지 제3자 제공인지 구분이 될 수 있다. 법적 판례(2018다223214)를[18] 살펴보면 위탁의 경우 법적 문제에서 시스템 개발 및 업그레이드를 목적으로 제공한 고객정보를 의도적으로 USB 메모리를 이용해 복사하고 대출 중개 영업 등에 활용함으로 손해배상 책임이 발생한 사례가 있다. 본 판례에서는 개인정보 보호

법 제26조 제2항에 규정된 수탁자에 해당하므로 제26조 제7항에 따라 준용되는 제24조 제1항, 제24조의2, 제1항, 제29조, 개인정보 보호법 시행령 제30조 제1항 각호의 위반에 따라 손해배상책임을 부담하도록 판시한 바 있다. 또한 개인정보처리 위탁이란, 원래의 개인정보 수집 및 이용 목적과 관련된 위탁자의 업무 처리와 이익을 위해 개인정보가 이전되는 경우를 의미한다. 이때 수탁자는 위탁자로부터 위탁 업무 처리에 따른 대가를 받지만, 개인정보 처리에 관하여 독자적인 이익을 가지지 않으며, 정보제공자의 관리와 감독하에 위탁받은 범위 내에서만 개인정보를 처리한다고 판시한 바 있다[19]. 개인정보 보호법의 경우 일반법으로써 공공부문과 민간부문 전체에 적용되며, 정보통신망법의 경우 특별법으로써 정보통신 서비스 제공자를 적용 대상으로 한다. 개인정보 처리 위탁의 경우, 제3자가 개인정보를 처리하더라도 그 이용 목적이 원래 개인정보를 수집한 위탁자를 위한 것이므로, 처리 과정에서 발생한 개인정보 침해에 대한 책임은 위탁자에게 있다.

IV. Enhancement Measures for Personal Data Protection During Outsourcing

1. Personal Data Processing Standard

개인정보를 수집·이용 및 제공하는 요건이 정보통신 서비스 제공자(온라인 사업자)와 공공기관·오프라인 등 개인정보처리자가 서로 다르게 규율되고 있어 개인정보 처리 요건을 일원화될 필요가 있다. 특히, 개인정보처리자가 개인정보를 수집, 이용, 제공하는 과정에서 정보 주체가 자유로운 의사에 따라 동의 여부를 결정할 수 없는 상황에서는 동의를 강제해서는 안 된다. 그러나 계약 이행 등 정보 주체가 충분히 예상할 수 있는 합리적인 범위 내에서는 개인정보를 수집하고 이용할 수 있도록 개선이 필요하다. 개인정보 침해 사고가 발생 시 위탁자가 재위탁한 사실을 알 수 없었다는 이유로 수탁자에게 책임을 전가하여 정보 주체의 피해구제가 관련한 사례가 발생하면 이에 대한 개선이 필요하다. 따라서 정보 주체와 위탁자, 수탁자 간의 관계에서 정보 주체에 대한 실질적인 책임은 위탁자가 부담해야 하며, 수탁자도 법 위반에 대해 일정 범위 내에서 책임을 지도록 개정이 필요하다. 현대 사회에서 증가하는 개인정보 침해와 기업에서 위탁과 수탁 시 계약이 미비하다는 통계적 분석을 기반으로 개인정보처리 위탁 시 준수사항을 강화할 필요가 있다. 표 2는 개인정보처리 위탁 계약서 체결히 필수사항을 정의한 것이다.

Table 2. Contents for Standard Personal Data Processing Outsourcing Agreement

No	Value
1	Purpose and scope of entrusted tasks.
2	Restrictions on re-entrustment.
3	Measures to ensure security, including limitations on access to personal information (administrative, technical, and physical safeguards for the protection of personal information).
4	Prohibition of processing personal information beyond the intended purpose.
5	Supervision and monitoring of the management status of personal information held.
6	Compensation for damages in case of breach of obligations.

또한 위탁 내용 및 수탁자를 홈페이지에 공개 또는 직접 정보 주체에 고지하도록 의무화하고 정보 주체가 언제든지 쉽게 확인할 수 있도록 홈페이지 개인정보처리 방침 등에 공개함으로 개인정보 주체 및 개인정보 서비스 제공자들의 수탁자 관리를 필수화하고 수탁자도 개인정보처리자의 소속 직원으로 간주하여 위탁 업무 관련 법 위반으로 발생하는 손해배상책임을 수탁자 외 위탁자도 부담하도록 강화할 필요가 있다.

위탁사는 수탁사에게 제공한 개인정보를 보호할 책임이 있으므로 표 3과 같이 위탁 계약 시 용역업체 보안 관리 점검표를 통해 수탁사의 실태 점검, 개인정보보호 미이행에 따른 3진 아웃 제를 도입하고, 경고 이후에 보안 교육실시, 수탁사의 개인정보 책임자 재배정, 계약 파기를 추가함으로 더욱 안전한 개인정보 처리가 이루어질 수 있을 것이다. 이는 수탁자에 대한 관리·감독이 강화될 뿐만 아니라 개인정보 파기에 대한 시간이나 책임자 명시를 명확하게 하고 이후 개인정보 유출 문제가 발생 시 개인정보 책임자를 명확히 함으로 개인정보 취급 시 주의를 요할 수 있다.

2. Three-Strike Personal Data Protection Warning System

개인정보보호를 위해서는 위탁사·수탁사의 책임감을 강화해야 할 필요가 있다. 수탁사에 대한 실태 점검을 바탕으로 개인정보보호가 미흡할 시에는 경고를 누적하는 시스템을 도입하면서 위탁 계약을 해지하거나 강력하게 다음 계약에 불이익을 주는 등 책임감을 느끼게 해야 한다. 표 4는 수탁사의 실태 점검 결과 경고에 따른 제재 사항을 명시화함으로 법적 준거성을 확보한다.

Table 3. Subcontractor Security Management Inspection Checklist

Item	Sanction Details
Compliance with the contents of the outsourcing contract	Have the following items included in the standard personal information processing outsourcing contract been complied with? - Prohibition of processing personal information beyond the intended purpose. - Restrictions on re-entrustment. - Measures to ensure security, including limitations on access to personal information.
Implementation of personal information education	Has the subcontractor conducted its own personal information protection education for employees participating in the business?
	Is the content of the personal information protection education appropriate? - Provision of security special clauses in outsourcing contracts and regulations regarding penalties for violations of the Personal Information Protection Act. - Compliance with laws and regulations to prevent the loss, theft, leakage, alteration, or damage of personal information.
Adherence to security measures	Has a security pledge been drafted for individuals handling personal information?
	Have access controls and restrictions on access rights been implemented for personal information (e.g., PC, laptops)?
	Has encryption been applied to personal information files being held?
	Is antivirus software installed, operated, and kept up-to-date to prevent and treat malware?
	Are personal information files stored in a secure location with locking mechanisms? - Storage conditions for documents containing personal information, auxiliary storage media, etc. - Storage conditions for hard drives removed from PCs, etc.
Personal information destruction	Has personal information that has exceeded the retention period or achieved its procEssing purpose been destroyed? - Is personal information from unnecessary local education administrative institutions (schools) stored on PCs or laptops?
	Have measures been taken to ensure that personal information is destroyed in a way that cannot be recovered or regenerated?
Response procedures in case of exposure or leakage	Are subcontractors aware of the procedures for handling personal information exposure or leakage? - Immediate emergency measures to prevent further damage. - Reporting to the principal immediately in case of exposure or leakage (including details, timing, circumstances, methods to minimize damage, procedures for remediation, and contact information for reporting damage). - Formulation of measures to minimize damage and implementation of necessary actions.

Table 4. Sanctions imposed based on accumulated warnings

Item	Sanction Details
Personal Data Breach Incident Occurrence	Termination of Outsourcing Agreement and Compensation for Damages
3	Termination of Outsourcing Agreement
2	Reassignment of Personal Data Protection Officer
1	Conducting Security Training
0	None

V. Conclusions

개인정보 영향평가에 대해 다양한 시스템들을 살펴보면서 법적 준거성을 논리적으로 수립하기 위해 개선 방안을 제시하였다. 먼저 위탁시 기업의 안전성을 확보하기 위해서는 개인정보 영향평가 전문가들의 의견을 수렴하여 개인정보 책임자를 대상으로 한 평가 제도의 객관성과 실용성을 확보할 필요가 있다. 이를 기반으로 지속적인 사회의 변화 속에 개인정보 보호법이 개정되면서 데이터 3법 관련한 가명 정보 도입을 통한 정보들에 대한 결합과 익명 처리에 대한 적정성 평가에 관한 연구가 추가로 이루어질 필요가 있고 개인정보 영향평가는 더욱 확장될 것이다.

현재 본 논문에서는 기업이 서비스를 제공하기 위해 개인정보 처리 업무를 위탁하는 구조에서 법적 준거성을 확보하고 이를 체계적으로 관리할 방안을 제시하면서 개인정보를 안전하게 처리할 수 있는 보호 체계 수립의 필요성을 강조하였다. 또한 본 연구 결과를 기반으로 향후 공공 마이데이터 유통 체계 구축 등 개인정보 영향평가를 수행하는데서 개인정보 관리체계와 유출·침해 예방의 방안으로 활용될 수 있을 것으로 기대된다.

REFERENCES

[1] T. H. Kang, "A study on consigned party management system enhancement for personal information protection", Vol.23, No. 4, pp. 781-797, August 2013. DOI: 10.13089/JKIISC.2013.23.4.781

[2] Personal Information Portal [Internet] : https://www.privacy.go.kr/front/contents/cntntsView.do?contsNo=109

[3] 2020 Dispute Resolution Casebook [Internet], https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS232&mCode=D070010020&nttId=7320.

[4] 2022 Survey on the Personal Information Protection & Usage, Korea Internet & Security Agency, 2023.03

[5] J. H. Lee, "A Comparative study on Revised Personal Information Protection Act and GDPR s Transparency Principle and Procedure for Consent - comparing two cases : Google s violation of GDPR and Homeplus s violation of Personal Information Protection Act" The Journal of Law & technology Society,Vol. 36, No. 4, pp. 53-82. December 2020. DOI : 10.22397/wlri.

[6] National Legal Information Center [Internet] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95/%EC%A0%9C26%EC%A1%B0

[7] S. G. Kim and S. K. Kim, "An Exploration on Personal Information Regulation Factors and Data Combination Factors Affecting Big Data Utilization" Journal of The Korea Institute of Information Security&Cryptology, Vol. 30, No.2, pp. 287-, April, 2020. DOI: 10.13089/JKIISC.2020.30.2.287

[8] Y. J. Shin, "A Study on Developing the Model of Reasonable Cost Calculation for Privacy Impact Assessment of Personal Information Processing System in Public Sector" Korea Information Society Agency, Vol. 22, No. 1, pp.47-72, March 2015. DOI:10.22693/NIAIP.2015.22.1.047.

[9] Z. Jin, "A Study on the Legal Protection in Relation to Personal Information Collection in China and Its Overseas Transfer",Journal of Yonsei Law Journal, Vol.20, No.2, pp. 171-199, June 2020. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09369418

[10] Personal Information Protection Act [Internet], https://www.privacy.go.kr/front/contents/cntntsView.do?contsNo=36

[11] TTAS [Internet], https://committee.tta.or.kr/data/standard_view.jsp?rn1=Y&standard_no=TTAS.KO-12.0053&pk_num=TTAS.KO-12.0053&nowSu=1&rn=1

[12] G. Y. Noh, "Punitive damages as a means of guaranteeing the rights of personal information subjects under the Personal Information Protection Act" The Journal of Legal Research Institute KMU, Vol. 40, No. 4, pp. 197-241, December 2020.

[13] Y. J. Shin, "A Study on the Development of Evaluation Criteria for Personal Data Protection Suitability for IoT Service Providers" The Korean Information Processing Society, Vol. 13, No. 6, pp. 83-207, June 2020. UCI: I410-ECN-0102-2021-300-001102124.

[14] A. Kanaan, A. Hawamleh, A. Abulfaraj, A. H. M. Kaseasbeh, & A. Alorfi, “The effect of quality, security and privacy factors on trust and intention to use e-government services”, International Journal of Data and Network Science, Vol. 7, No.1, pp.185-198, July 2023. DOI: 10.5267/j.ijdns.2022.11.004

[15] Y. R. Bak and Y. T. Shin, "Research on Framework and Inspection Method to Strengthen Personal Information Protection of Trustees" The Journal of Information Protection Society, Vol. 12, No. 11, pp. 329-336, November 2023.

[16] National Legal Information Center [Internet] : https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95/%EC%A0%9C33%EC%A1%B0

[17] Personal Information Protection Commission [Internet], https://www.pipc.go.kr, Personal information processing entrustment guide.

[18] Supreme Court of Korea precedent [Internet] : https://casenote.kr/%EB%8C%80%EB%B2%95%EC%9B%90/2018%EB%8B%A4223214

[19] Supreme Court precedent, 2016도13263 judgment [Internet] https://casenote.kr/%EB%8C%80%EB%B2%95% EC%9B%90/2016%EB%8F%8413263

Authors

Young-Bok Cho received the M.S., and Ph.D. degrees in Computer Science from Chungbuk National University, Korea, in 2003 and 2012, respectively. also Dr. Cho received more Ph.D degrees in Medical and Law from Chungbuk National University and Chungnam National University , Korea, in 2019 and 2024, respectively. She has Professor of Information Security at Daejeon University, Daejeon, Korea , in 2018 to 2024, She is currently a Professor in the Computer Education at Andong National University, Andong, Korea, in 2024. Her research interests include AI medical image processing, information security and medical information protection, mobile security.