Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.801

공공기관 개인정보보호 관리 수준 진단에서 평가 체계로의 전환: 정책적 접근 및 제언*

홍 윤 희†‡
충남대학교 (교수)

Transition from Diagnosis to Assessment System in Public Institution Personal Information Protection Management: Policy Approaches and Recommendations*

Youn-hee Hong†‡
Chungnam National University (Professor)

요 약

본 논문은 정보기술 시대에서 강조되는 개인 정보의 중요성과 공공기관의 개인 정보 관리의 필요성을 다룬다. 공공기관에서 처리하는 개인 정보의 양이 지속해서 증가함에 따라, 더욱 효과적인 관리체계의 필요성이 대두되었다. 이에 따라, 정부는 기존의 개인 정보 관리 수준 진단 방식을 넘어서, 더욱 강화된 평가 중심의 체계인 '개인정보 보호 수준 평가제'를 도입하였다. 본 연구는 이러한 체계 전환의 배경, 과정, 그리고 2024년에 시행된 개인정보보호법 개정안의 주요 내용을 분석한다. 또한, 문헌조사 및 사례분석을 통해 공공기관 개인정보보호 관리 수준 진단의 현황 및 한계를 평가하고, 체계 전환 후 예상되는 개선 효과와 정책적 제언을 제공한다. 본 연구는 개인정보보호 정책의 강화가 국민 신뢰 제고 및 디지털 시대의 안정적 발전에 이바지할 것으로 전망한다.

ABSTRACT

In the digital age, the importance of personal information has magnified, underscoring the need for enhanced personal information protection, especially within public institutions. Despite ongoing efforts since 2007, significant breaches in public sector information underline persistent vulnerabilities. This study advocates for a transition from a diagnostic to an assessment framework to fortify privacy management in public institutions, as mandated by recent legislative revisions. The amended Personal Information Protection Act introduces an assessment approach, aiming to comprehensively assess and mitigate risks by expanding the scope of evaluation and implementing robust regulatory measures. This study examines the limitations of the current diagnostic practices through literature review and case analysis and proposes a systematic approach to adopting the new assesment system. By enhancing the assessment framework, the study expects to improve the effectiveness of personal information management in public institutions, thereby restoring public trust and ensuring a stable progression into a more secure digital era. The transition to an assessment system is designed not only to address the gaps in the current framework but also to provide a methodical assessment that supports ongoing improvement and compliance with enhanced legal standards.

Keywords: public institutions, personal information management level, personal information protection, management level diagnosis, protection level assessment

Received(05. 03. 2024), Modified(06. 14. 2024), Accepted(06. 14. 2024)

* 본 연구는 2024년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력 기반 지역 혁신 사업의 결과입니다(2021RIS-04).

† 주저자, yhhong@cnu.ac.kr
‡ 교신저자, yhhong@cnu.ac.kr(Corresponding author)

I. 서 론

IT 시대의 가치 창출로 개인 정보와 데이터는 그 중요성이 더욱 증대되면서 개인정보보호의 필요성과 그 중요도가 사회적인 관심을 끌고 있다. 특히, 공공기관의 개인 정보는 기업과 기관에 큰 가치를 제공하고 있으며 공공기관의 개인 정보 관리 규모는 점차 확대되고 있다.

2021년 기준 230개 이상의 공공기관에서는 100만 명 이상의 개인 정보를 보유하고 있어 개인정보보호는 국민의 신뢰 확보에 선결적인 요소이다[1].

2007년부터 공공기관 개인 정보 관리 수준 진단을 이행하고 있음에도 불구하고 공공기관의 개인 정보 유출 건수는 2017년 3만 6천 건에서 2023년 34만 건으로 큰 폭으로 상승하여[2] 집단적 권리침해로 이루어질 수 있다. 더 큰 문제는 개인정보유출은 큰 폭으로 증가하고 있지만 제재는 낮고 전담 인력은 적어 정책을 안정적으로 시행하기에는 역부족인 상태이다.

정부는 이러한 문제점을 해소하기 위하여 개인정보보호 수준 평가 대상을 확대하고 평가 체계를 강화한 공공기관 개인정보보호 수준 평가제(이하 '보호수준 평가제') 시행을 계획하고 있다[3].

본 연구에서는 문헌분석 및 사례분석을 통해 그간

Table 1. Process of Implementing the Personal Information Protection Level System in Public Institutions[6][7]

Title	Personal Information Protection Level Diagnosis	Public Institution Management Level Diagnosis	Public Institution Personal Information Protection Level Assessment
Year	2007	2020	2024
Responsible Ministry	Ministry of the Interior and Safety	Personal Information Protection Commission	Personal Information Protection Commission
Legal Basis	Article 20 of the Act on the Protection of Personal Information in Public Institutions	Compliance with Article 11 of the Personal Information Protection Act (Request for Submission of Data, etc.)	Article 11-2 of the Personal Information Protection Act (Assessment of Personal Information Protection Level)
Target Institutions	In 2008, the phased level diagnosis program was expanded to central administrative agencies. ※ Central Administrative Agencies ('08) → Local Governments ('09) → Educational Institutions and Public Institutions ('10)	Approximately 800 public institutions Central Administrative Agencies, Metropolitan and Basic Local Governments, Public Institutions (Public Enterprises, Regional Corporations, and Foundations, etc.)	Approximately 1,600 public institutions Central Administrative Agencies and Affiliated Organizations, Metropolitan and Basic Local Governments, Provincial Offices of Education and District Offices of Education, Public Institutions (Public Enterprises, Regional Corporations, and Foundations, etc.)
Feedback of Results	Selection and Reward of Excellent Institutions, Actively Encouraging Competitive Benchmarking Among Institutions	Implementation of On-site Consulting and Planned Inspections for Under performing Institutions (※No Legal Basis)	excellent institutions and outstanding employees based on evaluation results Recommending improvements and requesting results of actions Implementing on-site consulting and inspections for under performing institutions
Sanction Measures	-	-	Imposition of Fines

의 공공기관 개인 정보 관리 수준 진단 현황을 토대로 진단 체계의 한계점을 살펴보고 개선된 보호 수준 평가제를 비교 분석하여 평가 체계 전환의 확정성을 고려하여 체계적인 평가가 이루어질 수 있도록 정책 제안을 하고자 한다.

II. 본 론

2.1 이론적 배경

2.1.1 관리 수준 제도 추진 과정

공공기관 개인정보보호 관리 수준 제도는 개인정보 보호법 제11조에 근거하여 공공기관의 개인 정보 보호 및 활용 업무를 객관적으로 진단하고 취약점 도출 및 개선을 유도하여 공공기관의 개인정보보호 역량을 향상하게 시키기 위함이다.

2007년부터 행정안전부가 주무 부처로 시행하였으며 2009년 '개인 정보 관리 수준 진단프로그램'을 개발하여 각 공공기관에 보급·확산하고자 하였다[4]. 2020년 '개인정보보호법'이 개정되면서 개인정보보호위원회로 업무가 이관되어 '제4차 개인정보보호 기본계획' 수립을 토대로 관리 수준 진단 체계를 개선하였다. 서면 중심의 진단 관리체계를 현장점검 중심으로 변경하여 관리 수준 진단의 내실화를 높이고 중앙부처가 보호 위와 협업하여 소속·산하기관의 관리 수준을 진단하는 등 개인 정보 처리관리·감독을 체계화하였다. 공공기관의 준수 정도에 따른 자체 개선 노력의 한계를 느끼고 개인정보보호위원회는 2023년 3월 개인정보보호법 일부개정안에, 이에 대한 사항을 담았다.

기존의 관리 수준 진단을 대폭 개선하고, "평가"의 체계로 강화한 '개인 정보 보호 수준 평가제'의 틀을 마련하였다. 기존의 개인정보보호법은 제11조를 근거로 하고 있었으나, 개정법에서는 제11조의2(개인정보보호 수준 평가)가 신설되었고 1년의 유예기간을 거쳐 지난 2024년 3월 15일에 시행이 되었다.

이에 따라 개인정보보호위원회는 전면 시행되는 제11조의2에 따른 개인 정보 보호 수준 평가제에 대한 계획을 마련하는 중이다. 관리 수준 진단에서 수준 평가제로의 변경에는 평가 대상의 확대도 함께 포함되어 있다. 기존의 교육부에서 일괄 관리하던 시·도 교육청과 교육지원청을 평가 대상 기간으로 추가하였다. 법상 변경된 주요 내용 중에는 평가 결과를 근거로 해당 기관의 장에게 개선을 권고할 수 있다는 점과 평가에 필요한 자료 요청에 대해서 정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출하였을 때는 1천만 원 이하의 과태료 처분을 할 수 있다는 점도 포함되어 있다[3].

2.1.2 선행연구

본 연구에서는 공공기관 개인정보보호 관리와 관련된 연구를 검토하였다. 먼저, 국외 유사한 제도에 대하여 최명길 외(2013)는 정보보안관리 프레임의 분석으로 공공기관 개인정보보호 적합성 여부 평가 사항을 언급하였다[5]. 박민정 외(2019)는 유럽의 ISMS-P와 GDPR의 개인정보보호 부문 연계성 분석을 추진하였으며[6] 홍성욱 외(2020)는 사례 연구를 토대로 대상 기관별 적절한 인증제도를 통한 효과적인 관리 방안을 제시하였다[7].

관리 수준 진단모델에 대하여 정형철(2010)은 2008년 개발된 18대 진단 지표의 가중치를 결정한 후, 가중치에 대한 중요도 해석을 비모수적 방법으로 해석하였으며[8] 정명수 외(2015)는 공공기관 개인정보보호 효율성을 DEA 모형으로 분석 제안하였다[9]. 신영진(2021)은 국외의 개인정보보호 및 정보보호 유사 평가 및 인증제도 분석을 토대로 제도적 확장성을 고려한 거버넌스를 강조하였으며[4] 지광준(2023)은 정보보호 수준 진단의 진단 절차와 진단 방법 등을 제안하였다[10].

선행연구는 관리 수준의 지표체계 및 진단 방법을 제시하고 제도적 확장성을 위한 개선 방안을 제시하였으나 그간의 관리 수준 현황분석 및 평가제 시행에 관한 연구는 이루어지지 않았다. 본 연구에서는 기존의 진단 지표 및 방법을 토대로 추진한 현황을 분석하고 평가제 전후의 평가 방법 체계를 분석하여 체계적인 제도안착을 위한 제언을 하고자 한다.

2.2 현재 공공기관 관리 수준 진단의 현황

2.2.1 주요 공공기관 관리 수준 진단 현황 상세 분석

공공기관 관리 수준 진단 제도는 개인정보 보호법 등 의무 사항 준수 여부를 확인하기 위하여 법령 준수사항 중심 13개 지표를 대상으로 시행한다. 2022년부터는 법령 준수사항 중심의 3개 분야(개인정보보호 관리체계, 보호 대책, 침해 대책)를 중점으로

자가 진단 지표로 설정하고 개인정보보호 정책 수립 이행 등 기관의 실질 관리 수준을 진단하는 정책분야, 기술 발달 등 환경변화 대응을 위한 특정 지표로 구성하여 진단위원회를 통한 자체 1차 진단 및 정책, 특정 분야 실적 제출을 통한 확인 진단, 이의신청 접수 및 현장 방문 등 2차 검증 절차를 거쳐 이행되었다.

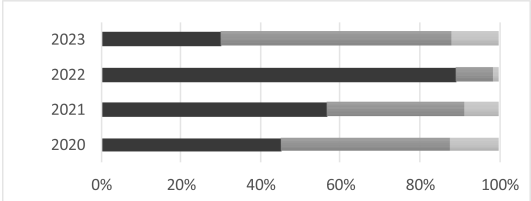
배점 기준은 종합점수를 산출하여 60점 미만의 미흡 기관의 경우에는 희망 기관의 수요를 받아 지역별, 기관 유형별 균형에 맞춰 선정된 기관에 현장 컨설팅을 시행한다.

본 연구에서는 관계 부처와 기관의 개인정보보호 관리 수준 진단계획 및 결과보고서, 개인정보보호 백서, 정보보호위원회 연차 보고서를 중심으로 문헌조사를 통해 진단 결과를 분석하였다.

최근 4년간의 관리 수준 진단 결과 '우수' (80점 이상), '보통' (60점~80점), '미흡'(60점 미만)으로 대상 기관의 비율을 나타내면 Fig. 1과 같다. '우수' 등급은 2023년 감소하였으며 '보통' 등급의 경우 2022년을 제외하고는 증가 추이를 보인다. '미흡' 등급을 받은 기관의 경우 2022년까지 일부 감소하다가 2023년 큰 폭의 증가세를 보였다.

Fig. 2는 유형별 연도별 개인정보보호 관리 수준 평가점수를 나타낸 것이다. 중앙부처는 일관적으로 평균 점수 이상의 높은 수준으로 보이지만, 기초지자체는 모든 연도에서 평균 점수 이하의 성과를 보여 개선이 필요함을 시사한다.

공공기관 관리 수준 진단 지표상 최근 3년간 분야별 정량 지표 결과는 대체로 우수한 수준이다. 개인정보 보호 대책이 91.4점으로 가장 높았으며 개인정보보호 관리체계 85.2점, 개인 정보 침해 대책이 83.4점으로 나타났다.



	2020	2021	2022	2023
Excellent	45%	57%	89%	30%
Average	42%	34%	10%	58%
Poor	12%	9%	1%	12%

Fig. 1. Annual Evaluation Score Distribution Ratio by Institution

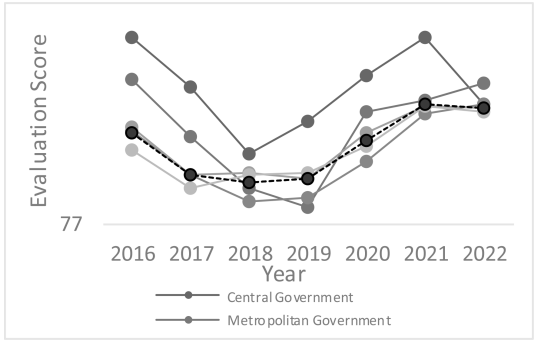


Fig. 2. Annual Privacy Management Evaluation Scores by Institution Type

개인 정보 침해 대책 세부 지표별로는 해킹 사고의 원인이 되는 접근 권한 관리 등 개인정보처리 시스템 관리가 2020년, 2021년 연속으로 가장 미흡했으며 2022년, 2023년의 경우에도 유출, 침해 대응이 가장 낮게 나타났다.

Table 2는 연도별 '미흡' 등급을 받은 기관의 수를 나타낸 것이다. 최근 4년간 '미흡' 등급을 받은 광역·기초지자체, 공공기관의 경우 기간 중 '미흡' 등급을 2회 이상 받은 기관은 43곳이며, 여기에는 '미흡' 등급을 3회 받은 기관도 10곳이 포함되어 있다.

Table 2. 'Poor' grade institutions by year

	Year				Institutions having more than two 'Poor's	
	2020	2021	2022	2023	Two times	Three times
Central Government	2			2		
Metropolitan Government	1	2		1	1	
Basic Local Government	30	20	1	32	13	3
Public Institution	39	30	10	59	19	7
Total	72	52	11	94	33	10

2.2.2 진단 체계의 한계 및 문제점

공공기관 관리 수준 진단은 2008년부터 적용되어 매년 800여 개의 기관이 개인정보보호법과 정책을 준수하고 관리 수준을 향상하는 제도로 안착시켰다.

이에 공공기관의 관리 수준을 진단하여 개선하는 견인적 역할을 하고 있으나 확정성을 고려해 볼 때

Table 3. Assessment indicators and scoring for Diagnosis(2023) the level of personal information management of public institutions, and Assessment(2024) the level of personal information protection of public institutions

Domain & Score	Field & Score	Indicator (2023)	Indicator ID (2023)	Number of Indicators	
				2023	2024
Quantitative / Self-assessment (60pts)	Personal Information Management System (15pts)	Foundation for personal information protection	1~2	9	5
		Fulfil the role of personal information officer	3~5		
		Manage personal information files and conduct privacy impact assessment	6~8, 40		
	Protection of Data Subject's Rights (15pts)	Personal information processing policy and access, correction, deletion, suspension of processing, etc.	9, 45~46	11	10
		Procedures for collection, use, provision, and off-purpose use and provision	10~14		
		Management of entrustment of personal information processing works	15~17		
	Prevention of Personal Information Breach (30pts)	Management of access rights and inspection of access records	18~20, 29~33	33	28
		Measures to prevent and respond to personal information breach incidents	21~28, 34, 39, 41~44, 53		
		Encryption of personally identifiable information (and biometric information)	35 ~ 38		
		Operation of visual data processing devices and processing of pseudonym information	47 ~ 52		
Qualitative / In-depth Evaluation (40pts)	Investments and efforts to protect personal information				
	Adequacy of processing privacy policies and efforts to implement and improve them				
	Measures to ensure the safety of personal information				
	Management on entrustment of personal information processing works				
	Protection and management of personal information, and incident response such as personal information breach				
	Adequacy of internal management plan				
	Management and registration of personal information files				
	·(Extra points) Implementation of the plan to strengthen personal information safeguards of the intensive management system (up to 5 points)				
	* Derive excellent and deficient cases by indicators				
Points deducted (reduction)	·Maximum -10 points per incident such as leakage ·Maximum -3 points per administrative penalty ·Maximum -2 points per false or fraudulent incident (Self-diagnosis will be subject to additional points for the corresponding indicators) (Reduction) Efforts to minimise damage to the information subject after an accident such as a leak (follow-up report) Up to 50% of the total points				

진단 체계의 한계점을 다음과 같이 찾아볼 수 있다. 먼저, 공공기관의 진단 결과는 매년 개선되는 추세가 확인되지 않는다. 앞서 살펴본 바와 같이 진단 지표의 정량평가 결과 22년을 제외하고는 우수기관은 감소하고 보통, 미흡 기관은 증가하는 추세로 보인다. 둘째, 지표 중 점수가 낮은 지표는 매년 개선되지 않고 있다. 미비점을 보완하여 개선하는 것이 제도의 목적인 만큼 전년도에 미비한 지표가 중점적으로 개

선되어야 하지만 3대 분야 정량 지표 중 개인 정보 침해 대책은 매년 가장 낮은 진단 결과를 나타내고 있다. 셋째, 하위등급으로 판정된 대상 기관은 지속해서 하위등급을 유지하고 있다. 하위등급의 경우 현장 컨설팅을 이행하도록 하고 있으나, 의무 사항이 아닌 지역별 배분을 고려하여 진행되는 것으로 사후 관리(컨설팅) 강제성이 부족하여 다음 연도에도 개선되지 못한다는 문제점이 있다.

관리 수준 진단 제도는 법적 의무 사항 이행 여부만을 판단하는 자체진단과 정성지표를 진단하는 심층진단으로 이원화되어 있다. 기관에서는 자체진단을 실시하고 심층 진단 보고서를 제출하여 진단위원회에서 검증하는 방식으로 이행되지만, 온라인 서면 평가 형식으로 서류 제출이 미비하거나 담당자가 미 인지하여 서류를 제출하지 않으면 아예 수준 진단에 대응하는 데 어려움이 있다.

현재 공공기관의 개인 정보 담당자는 0.3명, 조직의 3% 내외로 겸직의 형태로 근무[11]하고 있어 제도의 이해도가 떨어지면 실제 일선에서 개인정보보호법 준수를 위하여 개정되는 법령을 쫓아가는 데는 한계를 지니고 있다.

2.3 평가 체계로의 전환

2.3.1 전환의 필요성 및 기대효과

공공기관 개인 정보 보호 수준 평가제 전환은 개인 정보 보호 관리 취약점 도출 개선 유도를 통한 실질적인 보호 역량 향상을 위함이다.

평가제를 통해 현재의 관리 수준을 더욱 체계적으로 진단하고 정보 관리 체계의 질을 높여 관련법률 및 규정을 준수했는지 여부를 점검하여 법적 문제를 미리 방지할 수 있을 것이다. 매년 서류 제출을 토대로 형식적인 온라인 진단 결과에 따라 이행되었던 “진단”에서 “평가제”의 전환은 개인 정보 관리체계의 효율성을 증진하는 데 이바지할 것이다.

최종적으로 평가를 통해 발생한 문제를 보완하여 더욱 효과적으로 위험관리를 실행할 수 있으며 장기적으로 공공기관 개인 정보 관리의 안정성과 효율성을 증진할 것으로 기대된다.

2.3.2 공공기관 개인 정보 보호 수준 평가제 주요 내용

공공기관 개인 정보 보호 수준 평가제는 대상 기관을 확대하고 평가 체계를 강화하는 것을 주요 골자로 하고 있다. 대상 기관은 기존의 800개의 중앙행정기관, 지자체, 공공기관, 지방공기업을 포함한 중앙행정기관의 소속기관, 시도교육청과 교육지원청을 포함한 1,400여 곳이다.

평가 방법은 평가지표를 활용하여 법적 준수 여부를 포함한 정량 지표 중심의 자체 평가와 업무추진의 적절성 및 충실성을 포함한 정성지표 중심의 전문가 심층 평가로 이루어진다. 평가제 전환 시에도 평가 방법은 기존의 방식을 준용하되 평가에 대한 전문성, 신뢰성을 높이기 위해 평가위원을 2배로 확대하는 것으로 하였다.

평가지표는 정량 지표와 정성지표로 이루어지며 정량 지표는 개인정보보호 법령상 의무 사항 및 이행 여부를 진단하는 진단 지표 53개의 내용을 함축한 43개의 지표로 조정되었으며 Table 3과 같다[12][3].

심층 평가지표는 실효성 있는 개인 정보 관리가 될 수 있도록 조정되었다. 개인정보보호 관리조직의 인력, 예산 등의 지표를 포함하여 개인정보보호 책임자 지정 지표 등을 토대로 역할과 권한을 강화한 것으로 보인다. 진단 지표의 경우 가점 지표로 집중관리 시스템 개인 정보 강화 안전조치 계획 이행 실태를 포함했지만, 평가제의 경우 인공지능, 디지털화에 따른 신기술 환경에서의 데이터의 안전한 활용 및 안전조치의 적절성 등에 대한 가점 부여를 포함하고 있다.

평가 결과는 기관별 5단계의 평가 등급을 부여한다. 중앙행정기관 자체 평가 및 공공기관 경영평가에 포함되도록 하고 우수자에게는 표창 등을 수여하고 미흡 기관에는 개선 권고 및 실태점검을 시행한다.

2.3.3 보호 수준 평가제의 실효성 및 특장점

개인 정보 보호 수준 평가의 실효성은 다음과 같이 정리할 수 있다. 첫째, 평가 대상을 약 1,400개 기관으로 확대하여 개인 정보 보호 정책의 적용 범위를 넓혔다는 점. 둘째, 기존 관리 수준 진단과 비교해 더 명시적인 법적 근거로 시행되는 만큼, 법적 의무 사항 준수 여부와 보호 업무의 적절성을 평가하는 점. 셋째, 개인 정보 보호 인력·조직 및 예산 지표를 강화하고 정보 주체 권리보장 지표를 신설하여 대상 기관들의 내부 역량 강화를 유도한다는 점. 넷째, 인공지능(AI) 등의 신기술 환경에서도 안전한 데이터

활용을 평가하는 지표를 도입하여 최신 기술 환경에서도 보호를 보장한다는 점이다.

이러한 요소들은 개인 정보 보호 수준 평가의 실효성을 높여 국민의 신뢰를 제고하는 데 이바지할 것으로 판단된다. 또한, 개인정보보호위원회는 개인 정보 보호 수준 평가의 첫 시행을 대비하여, 평가단을 확대하고 맞춤형 자문 및 설명회를 통해 기관들이 평가를 잘 준비할 수 있도록 지원한다고 밝혔으며, 법에 따라 우수기관 표창 및 미흡 기관 개선 권고(실태점검 포함)를 올해부터 바로 시행할 것으로 밝힌 바 있어, 개인 정보 보호 수준 평가제의 실행력 강화에 기여하고 본 제도의 실효성을 높일 것으로 판단된다.

개인 정보 보호 수준 평가제가 가지는 장점은 대상 기관의 개인 정보 보호 수준 향상을 위한 기관장의 노력, 주요 개인 정보 정책 등에 대한 심층 평가가 강화됨으로써, 해당 기관의 전반적인 개인 정보 보호 수준이 제고된다는 점이다[3]. 특히, 개인정보보호위원회는 개인 정보 보호 인력·조직·예산의 확보와 운영을 잘하는지, 정보 주체의 실질적 권리를 보장하는 체계가 잘 갖추어져 있는지, 개인 정보 보호 책임자의 활동이 적절한지에 대한 것을 개인 정보 보호 수준 평가제에 담았음을 공지한 바 있다[3]. 또 하나의 장점은 인공지능(AI) 등 디지털 심화에 따른 신기술 환경에서의 데이터의 안전한 활용 및 안전조치의 적절성을 평가하는 지표를 신설하여 최대 10점까지 가점을 부여할 계획임을 밝혔다는 점이다[3].

2.3.4 안정적인 평가 체계 운영을 위한 정책적 제언

앞 절에서 살펴본 개인정보보호위원회가 바라보는 개인 정보 보호 수준 평가의 실효성 및 특장점에 대한 견해는 충분히 공감이 가능한 부분이다. 다만, 대상 기관의 확대, 법적인 개선 권고 가능성, 과태료 부과의 가능성 등이 포함된 점은 개인 정보보호 수준 평가의 대상이 되는 공공기관, 교육(지원)청의 개인 정보 보호 책임자 및 실무자의 입장에서는 매우 우려가 되는 사항이라는 점을 간과해서는 안 된다.

공공기관 개인 정보 보호 수준에 대한 평가제가 도입된 만큼 체계적인 운영을 위해 다음과 같은 사항을 고려해 볼 필요가 있다. 진단은 운영의 효율화를 위하여 일련의 목표를 체계적으로 집계·관리·환류하기 위한 과정이다. 평가는 진단 과정을 포함하여 운영관리의 전반에 대하여 명확히 측정하고 그 결과에 따른 사후 조치도 명확히 이루어져야 한다.

평가 측정은 기존의 진단 지표를 중심으로 더욱 실효성 있게 조정·개선된 것으로 판단되나 평가 방법에 있어서는 온라인 서면 평가 방식을 그대로 준용하고 있다. 온라인으로만 이행되는 서면 평가를 일부 대면 평가로 확대하거나 현장 심사를 확대·강화할 필요가 있다. 평가제를 도입하였지만, 기존의 진단제도 방식을 그대로 유지한다면 평가제의 효과성은 그리 높지 않을 것이다. 1,400개의 모든 기관에 대해 모두 대면 평가를 진행한다는 물적, 인적자원이 많이 소요되니 2년, 3년 이상 미흡한 기관 혹은 해당연도 미흡 기관에 대해서는 컨설팅뿐 아니라 다음 연도 대면 평가를 고려해 볼 수 있다.

또한 평가지표는 모든 기관에 공통으로 적용되는 공통 지표이다. 공공기관도 업무의 영역 상 51개의 모든 지표를 공통으로 적용하기에는 무리가 있다. 이에, 수준별 평가지표의 가이드라인을 조정하여 기관 유형별 지표를 구분하거나 기관 유형별 세부 지표의 선별하고 가점 등을 적용할 수 있는 방안을 모색해 보아야 할 것이다. 아울러 평가제 시행과 동시에 각 기관 유형별 공공기관 개인 정보 보호 수준 평가에 대한 교육이 반드시 선행되어야 할 것이다. 평가제를 명확히 이해하고 평가지표에 맞게 증빙자료를 준비해야 평가에 제대로 참여할 수 있다. 평가 결과 미흡한 공공기관 혹은 신규 평가 대상 기관의 담당자는 의무적으로 별도 교육을 이행하도록 하여야 할 것이다. 더하여, 평가를 위한 평가위원회의 구성 및 평가위원회 위원들이 적절하게 평가할 수 있도록 구성된 평가위원의 평가 방법에 대한 교육도 동시에 이루어져야 할 것이다.

한편으로는 개인정보보호위원회가 시행한 본 제도 개선 운용을 통해서 공공기관의 개인 정보 보호 수준을 더욱 엄격하게 평가함으로써, 정부나 공공기관에 대한 국민의 신뢰가 높아질 것으로 기대한다. 하지만, 변경된 제도 시행과 관련해서는 사회환경적 관점에서는 추가적인 검토가 필요해 보인다. 2022년에 개인정보보호위원회가 수행한 “디지털 시대에 맞는 정보 주체 중심의 개인 정보 보호·활용 체계 연구[13]” 등과 같은 사회환경적 정책 연구에 이어, 최근 1~2년 사이에 급격하게 변화되고 있는 디지털 환경, 특히 생성형 인공지능 활용이 가져온 사회적 변화에 맞는 개인 정보 보호 수준 평가에 대한 정책 연구가 정부 차원에서 이루어져야 할 필요할 것으로 판단된다.

III. 결 론

공공기관 개인 정보 보호 수준 평가 체계 강화에 따라 개인 정보 보호 정책을 효과적으로 제고하고 국민 신뢰를 확보하고 디지털 시대의 안정적인 발전을 지원할 것으로 판단된다. 개인 정보 보호 수준 평가 대상 범위의 확대는 사각지대를 없애는 방향으로 진행될 것이다.

다만, 좋은 방향으로 변화일지라도 첫해의 평가는 개인정보보호위원회 및 한국인터넷진흥원의 다양한 홍보 및 교육 등과 같은 다각적인 지원책도 명시적으로 제공되어야 할 것이며, 대면 평가 확대, 기관별 맞춤형 지표 적용 등도 함께 고려되어야 할 것이다.

향후, 개인 정보 보호 수준 평가 결과를 바탕으로 실제적인 효과성을 확인하기 위한 연구가 필요하다고 판단된다. 올해에 진행되는 평가 결과가 발표되는 내년 상반기에는 본 논문에서 다룬 개인 정보 보호 수준의 특장점 및 실효성을 중심으로 이해관계자 자문, 수검 대상 기관 실무자 설문 등을 포함하는 연구를 진행할 예정이다.

References

[1] Inter-ministerial Collaboration, "Public Sector Personal Information Leakage Prevention Plan," 2022(33), July. 2022.

[2] e-Nara Gipyo, "Number of personal information infringement reports and consultations during 2020.9~2024.4.", https://www.index.go.kr/unity/potal/main/EachDtlPageDetail.do?idx_cd=1366, April. 2024.

[3] Personal Information Protection Commission, "First implementation of the Public Institution Personal Information Protection Level Assessment", https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10116, April. 2024.

[4] Shin Young-Jin, "The Improvement Plan for Diagnosis and Operation Procedure of Personal Information Management Level Diagnosis System", Korea Criminal Intelligence Review, 7(2), pp. 71-99, Dec. 2021.

[5] Choi Myeong-gil and Jeong Jae-hun, "Trends in Overseas Information Security Management", Review of KIISC, 23(5), pp. 12-19, Jan. 2013.

[6] Minjung Park, Jieun Yu and Sangmi Chai, "Analysis of the Connection between ISMS-P and GDPR in the Personal Information Protection Sector". Journal of the Korea Society of IT Services, 18(2), pp. 55-73, June. 2019.

[7] Sung Wook Hong and Jae-Pyo Park, "Effective Management of Personal Information & Information Security Management System(ISMS-P) Authentication systems", Journal of the Korea Academia-Industrial cooperation Society, 21(1), 634-640, Jan. 2020.

[8] Hyeong Chul Jeong, "Study on AHP and Non-Parametric Verification on the Importance of the Diagnosis Indicators of Personal Information Security Level", Journal of The Korean Data Analysis Society (JKDAS), 12(3), pp. 1499-1510, June 2010.

[9] Myeong-soo Jeong and Kyung-ho Lee, "A Study on Personal Information Protection Management Assessment Method by DEA", Journal of the Korea Institute of Information Security & Cryptology, 25(3), pp. 691-701, Jan. 2015.

[10] Kwang - Joon Ji, "Research on information security management level diagnosis and continuous management of goverment institutions", Master's Thesis, Graduate School of Paichai University, Aug. 2023.

[11] Gwang-il Ju, Seon-Hui Choi, and Hark-Soo Park, "Compliance and

Implications for Public Officials in Charge of Personal Information Protection by Policy Trends", JOURNAL OF THE KOREA CONTENTS ASSOCIATION, 17(4), pp. 461-467, Jan. 2017

〔12〕 Personal Information Protection Commission, 4th Basic Plan for Personal Information Protection, Feb. 2020.

〔13〕 Personal Information Protection Commission, Research on Information Subject-Centered Personal Information Protection and Utilization System in the Digital Age. Oct. 2022.

〈저자소개〉

홍 윤 희 (Youn-hee Hong) 종신회원
2012년 8월 상명대학교 대학원 경제학과 박사
2023년 3월~현재: 목원대학교 대학원 IT공학과 박사과정
2023년 9월~현재: 충남대학교 반도체특성화대학사업단 산학협력중점교수
〈관심분야〉 정보보안, 개인정보보호 정책 및 교육, 정보교육, 영재교육, 환경정책