

인공지능 시스템에서 개인정보 처리방침 수립을 위한 법적·기술적 요구사항 분석 연구*

전 주 현,^{1*} 이 경 현^{2†}
^{1,2}부경대학교 (대학원생, 교수)

A Legal and Technical Analysis for Establishing Privacy Policies on Artificial Intelligence Systems*

Ju-Hyun Jeon,^{1*} Kyung-Hyune Rhee^{2†}
^{1,2}Pukyong National University (Graduate student, Professor)

요 약

AI 기술의 급속한 발전과 더불어 AI 시스템에서 개인정보를 대량으로 수집, 처리, 활용하는 경우가 증가하고 있다. 이에 따라 AI 시스템의 개인정보 처리에 대한 투명성과 책임성, 정보주체 권리보장, 개인정보 침해 위험 최소화 등이 중요한 과제로 대두되고 있다. 그러나 기존 개인정보 처리방침에는 일반적인 개인정보 처리에 대한 내용만 공개되고 있으며, AI 시스템에 대한 개인정보 처리방침은 부재한 상황이다. 이러한 문제를 해결하기 위해 개인정보 보호법 개정에 따른 개인정보 처리방침 평가제 시행 대응과 함께 AI 시스템의 설계 및 개발, 운영 과정에서 개인정보 처리에 대한 AI 시스템 개인정보 처리방침 수립·공개를 새롭게 제안한다. 이를 통해 본 연구는 현행 개인정보 보호법상 자동화된 결정에 따른 정보주체의 설명요구권 및 거부권 행사 규정에도 보완적인 역할을 할 수 있을 것으로 기대된다.

ABSTRACT

With the rapid development of AI technology, AI systems are increasingly collecting, processing, and utilizing personal information in large quantities. As a result, transparency and accountability of personal information processing by AI systems, ensuring the rights of information subjects, and minimizing the risk of personal information infringement are becoming important issues. However, the existing privacy policy only discloses the personal information processing in general, and there is no privacy policy for AI systems. In order to solve these problems, In response to the implementation of the privacy policy evaluation system in accordance with the revision of the Personal Information Protection Act, we propose a new AI system privacy policy establishment and disclosure for personal in the design, development and operation of AI system. This study is expected to play a complementary role to the regulations on the right of data subjects to request an explanation and exercise the right of refusal for automated decisions under the current Personal Information Protection Act.

Keywords: Privacy Policy, Artificial Intelligence, Personal Information, Privacy Law, AI Privacy Policy

I. 서 론

최근 인공지능(Artificial Intelligence, AI) 기술의 급속한 발전으로 개인정보를 대량으로 수집, 처리, 활용하는 가운데 생성형 거대 언어 모델(Large Language Model, LLM)을 개발하거나 이를 기반으로 인공지능 서비스를 제공하는 6개 사업자에 대해 개인정보보호위원회는 개인정보 취약점 개선 권고를 의결하였다[1]. 이와 같은 조치는 AI 시스템의 개인정보 처리에 따른 투명성과 책임성 확보, 정보주체의 권리보장 등 개인정보 침해 위험 최소화가 인공지능 시대에 중요한 과제가 되고 있음을 보여준다. 최근 텍스트, 이미지, 음악, 비디오 등 인공지능 데이터 학습을 위한 개인정보 보호에 많은 관심과 요구가 증가하고 있어[2], AI 시스템 개인정보 처리방침의 수립·공개 의무가 필요한 시점이 되었다. 또한, 개인정보보호위원회 보도자료(24.4.29)에 따르면 올해 시행되는 '공공기관 개인정보 보호수준 평가' 지표 중에서 '신기술 환경에서 데이터의 안전한 활용 및 안전조치 적절성' 지표에 최대 가점 10점을 부여하고 정성지표 심층진단에서 '개인정보 처리방침 적절성 및 이행·개선 노력'에 5점을 부여하고 있어 AI 시스템 개인정보 처리방침 수립·공개 필요성은 더욱 크다고 볼 수 있다.

AI 서비스제공자는 AI 기술을 활용하여 정보주체에게 특정 서비스를 제공하는 기관·법인·단체로 인공지능 알고리즘, 학습 모델, 애플리케이션 등을 개발하고 운영하면서 이용자의 데이터를 수집, 처리, 가공, 분석하여 맞춤형 서비스를 제공한다. 예를 들면, 챗봇, 추천시스템, 음성비서, 이미지 인식, 자연어 처리, 거대언어모델 AI 시스템 등이 있다. AI 서비스제공자는 서비스 과정에서 이용자의 개인정보를 다루게 되므로 개인정보 보호법을 준수하고 이용자의 프라이버시를 보호할 책임이 있다[3]. 따라서 AI 서비스에서 개인정보 보호를 위한 데이터 익명화, 개인정보 정책 준수사항, 개인정보 처리 절차 및 보호 장치가 있어야 한다[4].

현행 개인정보 보호법 제30조는 개인정보 처리에 따른 개인정보 처리방침 수립·공개 의무를 일반법적인 기준에서 개인정보 처리에 관한 포괄적인 내용을 담고 있다. 개인정보 보호법 제25조에는 영상정보처리기기 설치·운영에 관한 내용을 규정하고 있고 개인영상정보도 개인정보이기 때문에 영상정보처리기기 운영·설치에 따른 처리방침을 수립·공개하도록 하였

다. 정보주체는 자신의 개인정보 및 개인영상정보가 동의 이후에 어떻게 처리가 되는지 개인정보처리자가 투명하게 공개함으로써 개인정보처리자의 책임성과 정보주체의 신뢰성을 확보하고 있다.

하지만, AI 시스템은 개발·설계 및 운영하는 과정에서 개인정보 처리를 정보주체가 확인 가능하도록 한 처리방침 수립·공개 의무의 법적 근거는 현재로서는 부재한 상황이다. 한편 데이터 3법(개인정보 보호법, 정보통신망법, 신용정보법) 개정(2020.8.5.) 이후 가명처리를 통해 데이터 학습이 필요한 경우에는 개인정보를 가명처리하여 통계작성, 과학적 연구(산업적 연구포함), 공익적 기록보존을 위해 개인정보를 정보주체 동의없이 사용할 수 있도록 법적 근거가 마련되었다. 따라서, AI 시스템에서도 개인정보 처리를 위해 수집하는 개인정보의 유형과 범위, 이용 목적 등을 명시하여 정보주체의 예측 가능성을 높일 필요가 있다. 또한, 개인정보 보호법 제37조의2 자동화된 결정이 시행됨에 따라 개인정보처리자가 자동화된 결정을 한 경우에 정보주체는 그 결정에 설명을 요구할 수 있으며 거부권을 행사할 수 있다. 여기서 자동화된 결정이란 AI 기술이 반영된 인간의 개입이 없는 결정을 말하며 AI 알고리즘에 의한 차별 및 편향성 배제와 공정성도 요구된다.

이에 본 논문에서는 AI 시스템 개인정보 처리에 대한 정보 투명성과 책임성에 대한 설명 수단으로 AI 시스템 개인정보 처리방침을 제안한다. 보다 세부적으로는 AI 시스템 개인정보 처리방침을 수립·공개하기 위한 법적 근거 제안, 구조화된 형식과 내용 도출, AI 시스템 설계·운영에 따른 개인정보 처리방침 필요성 분석을 수행한다.

본 논문의 구성으로 2장에서는 선행연구와 국내·외 입법 현황을 살펴보고 3장에서는 AI 시스템에서 개인정보 처리를 살펴본다. 4장에서는 AI 시스템 개인정보 처리방침 수립 공개 시 법적인 요구사항과 기술적 요구사항을 분석하고 5장에서는 AI 시스템 개인정보 처리방침(안)을 제안하며 6장에서는 결론과 향후 연구 방향에 대해 살펴본다.

II. 개인정보 처리방침 선행연구와 입법 현황

2.1 선행연구의 의의와 한계

개인정보 처리방침 선행연구를 살펴보면 [5]에서는 국내·외 포털 사이트에 대한 개인정보 처리방침

및 차이를 분석하였다. 분석한 결과 국내 포털 사이트는 법률 준수 범위가 넓고 수집 범위는 좁은 반면 해외 포털 사이트는 법률 준수항목 범위가 좁고 수집 범위가 넓다는 차이가 있었다. 이는 국내 법률 준수에 대한 엄격성을 나타내고 해외에는 상대적으로 완화된 차이임을 알 수 있었다. [6]에서는 인터넷 사용자가 웹사이트에서 회원가입 절차 등으로 개인정보 처리자가 요구하는 개인정보 수집·이용 및 요구에 대한 동의 과정에서 처리방침에 대해 사용자가 쉽게 인지할 수 있도록 제3자 인증기관이 처리방침을 요약하여 함께 제시할 때 사용자가 인식하는 정보이해 가능성, 지각되는 위험, 신뢰 가능성, 정보제공 의도 등의 측면에서 통계적으로 유의한 차이가 있는지 분석하였다. [7]에서는 생명보험회사 20개를 개인정보 알 권리 강화와 개인정보 처리방침 평가를 대비하여 정보주체의 권리를 보장할 수 있는지 현황을 분석하고 우수사례와 개선방안을 제안하였다. [8]에서는 모바일 앱 개인정보 처리방침을 분석하였으며 구글 앱스토어에 등록된 모바일 앱이 개인정보 처리방침에 정확히 공개된 내용과 일치하는지를 약 13,000개 안드로이드 앱 패키지 파일 텍스트 분석과 모바일 앱 분석을 진행한 후 개인정보 처리방침에 공개한 것보다 더 많은 개인정보에 접근할 수 있음을 증명하였다. [9]에서는 한국, 유럽연합(EU), 중국, 미국 4개 나라별 개인정보 처리방침(privacy policy)의 법률적 비교분석을 통한 시사점을 도출하였으며, [10]에서는 복잡한 개인정보 처리방침을 딥러닝 기술을 이용하여 분석하였으며, 정보주체로 하여금 가독성 높은 개인정보 처리방침을 구현하기 위한 모델을 제시한 것으로 국내 258개 개인정보 처리방침 데이터셋으로 구축하고 딥러닝 기술로 분석하는 방안을 제시하였다.

이러한 선행연구에서는 기존 개인정보 처리방침

에 대한 법률적 문헌상 연구나 개인정보 처리방침 자체 내용 및 가독성, 이해도, 수용요인 등이 주로 연구 대상이었다. 하지만 신기술의 출현에 따른 개인정보 처리에 대한 개인정보 처리방침 연구는 현재 부재한 상황이다. AI 시스템 개인정보 처리방침은 AI 시스템이 처리하는 개인정보의 범위와 처리 목적, 처리 항목, 보유 기간 등 처리하는 과정에서 보호조치나 정보주체의 권리 등을 나타낸 문서이다. AI 시스템 개발과정에서 AI 시스템 개발자와 운영자는 개인정보 원칙을 내재화하고 개인정보처리자는 AI 시스템의 개인정보 처리에 대한 법적 준수사항을 지켜야 한다[11]. AI 기술 발전에 따라 개인정보 보호법상 보호 원칙을 기본으로 자율적 보호 활동을 위한 '개인정보 중심 설계(Privacy by Design, PbD)' 원칙과 윤리적 이슈 대응을 위한 '인공지능 윤리기준'을 반영하여 2021년 5월에 개인정보보호위원회는 인공지능 개인정보 보호 6대 원칙을 도출하였다[12]. Table 1.은 개인정보보호위원회가 제정한 '인공지능 개인정보 보호 자율점검표(개발자·운영자용)'에 따른 적법성(legality), 안전성(safety), 투명성(transparency), 참여성(participation), 책임성(accountability), 공정성(fairness) 등 6가지 인공지능 개인정보 보호 원칙을 제시하고 있으며 AI 시스템 설계 및 개발 운영에 참고하도록 안내하고 있다.

개인정보 처리방침에 대한 선행연구의 의의는 개인정보 보호법 제30조제1항 및 동법 시행령 제31조제1항에서 요구하는 법률 문헌상 연구와 개인정보 처리방침 내용상 가독성, 이해도, 수용요인 등 연구로 정보주체의 개인정보 자기결정권 보장에 기여하였다. 이러한 연구성과에도 불구하고 개인정보 처리방침의 통일된 구조 미비, 모호한 법률 해석, 생성형 AI 기술 등 급속한 기술발전에서 따른 새로운 기술 출현 시에 개인정보 처리 형태를 기존 개인정보 처리방

Table 1. principles of personal information

Principles	Detail
Legality	The basis for processing personal information in development and operation must be lawful and clear
Safety	Personal information is managed safely
Transparency	Disclose the processing of personal information in an understandable way
Participation	Collect data subjects' opinions and ensure their rights in the processing of their personal data
Accountability	Clarify responsibilities for processing personal information
Fairness	Avoid invasion of privacy and social discrimination

침에 신속히 반영하지 못한다는 한계가 있다.

또한, 정부에서 개인정보 처리방침의 개인정보처리자 책임성과 정보주체를 위한 투명성을 위해 평가제를 첫 도입 시행(24.3.15 시행)하였으며 최근 생성형 AI 시스템 등에 따른 개인정보처리자의 개인정보 처리 및 개인정보 처리방침 수립·공개의 학술적 연구가 추가적으로 필요해졌다.

2.2 국외 인공지능 입법 현황

인공지능 관련 국내·외 입법 현황을 유럽연합(EU), 미국, 중국, 일본 등 나라별로 정리하면 다음과 같다.

2.2.1 유럽연합(EU)

유럽연합(EU)은 개인정보 보호 일반규정(General Data Protection Regulation, GDPR)을 시행하고 있으며 GDPR 제4조 제4항 프로파일(profile)이 개인정보와 관련이 있다. 프로파일링을 '자연인의 특정한 개인적 특성을 평가하기 위해 자동화된 방식으로 행해지는 모든 형태의 개인정보 처리'를 의미한다고 규정하고 있다. 프로파일링을 통해 정보주체를 분류하고 이를 통한 광고를 추천하는 것은 가장 대표적인 AI와 개인정보 관련 내용이다. 또한, 2021년 4월, 'AI 규율을 위한 법률안(AI Act)'을 발의하여 인공지능 시스템의 위험 등급에 따른 규제 체계를 마련하고 있다[13]. AI Act는 AI 시스템의 위험 수준에 따라 허용되지 않는 위험, 고위험, 제한된 위험, 최소 위험 네가지의 범주로 구분하고 고위험 인공지능시스템에 대해 규제를 하고 있다. GDPR에서는 책임성의 원칙(accountability)으로 개인정보 처리방침을 채택 및 시행하도록 하고 있다[14]. 사전에 정보주체에게 동의에 필요한 충분한 정보를 제공해야 한다는 점을 강조하는 방법으로 개인정보 처리방침을 이용하는데 컨트롤러의 신원, 개인정보를 이전 할 경우 적정성 결정 및 보호 조치가 이루어지지 않는 제3국으로 개인정보 전송에 따라 발생할 수 있는 위험에 대한 정보를 공개하도록 안내하고 있다[15]. GDPR에서 제13조와 제14조 역시 정보주체의 개인정보를 누가 어떤 목적으로 처리 하는지 등의 정보를 해당 정보주체에게 모두 '제공'하여야 할 의무를 부여하고 있으며 이에 대한 방법의 하나로 개인정보 처리방침을 명시하고 있다[16]. 컨트롤러는 개인정

보를 수집하는 시점뿐만 아니라 전체 기간에 걸쳐 적용되며 기존 개인정보 처리방침의 내용이나 조건을 변경할 때 컨트롤러는 정보주체가 실제로 인지할 수 있는 방식으로 변경이 통지되도록 하여야 한다. 또한, 정보주체에게 개인정보 정책·고지 변경 또는 업데이트를 주기적으로 확인하여야 한다는 취지의 언급을 정책·고지에 포함 시키는 것만으로는 불충분하고 불공정하다고 안내하고 있다[17]. GDPR은 컨트롤러의 책임성과 투명성을 강조하기 위한 수단으로 개인정보 처리방침을 적극적으로 활용하도록 안내하고 있다.

2.2.2 미국

미국은 개인정보 보호와 관련하여 연방 차원에서는 관련 법은 현재 부재하나 주별로 개인정보 보호법을 제정하고 최근 연방(federal government)도 개인정보 관련 법을 발의하였다. 캘리포니아 소비자 보호법(California Consumer Privacy Act, CCPA)은 인공지능 시스템에 의한 자동화된 의사결정에 대한 소비자 권리 규정을 구체적으로 다루고 있지 않지만 CCPA를 개정하고 확장한 법안으로 캘리포니아 프라이버시 권리 법(California Privacy Rights Act, CPRA)에는 자동화된 의사결정과 프로파일링에 관한 규정을 도입하였다. 주요 내용은 첫째, 사업자는 소비자의 요청이 있으면 프로파일링을 포함한 자동화된 의사결정에 사용된 논리에 대한 의미 있는 정보를 제공해야 한다(1798.185(a)(16)). 둘째, 소비자는 프로파일링을 포함한 자동화된 의사결정의 결과 때문에 법적 효력이나 중대한 영향을 받는 경우가 결정에 따르지 않을 권리가 있다(1798.185(a)(16)). 셋째, 사업자는 소비자의 민감한 개인정보 프로파일링을 포함한 자동화된 의사결정에 사용하기 전에 소비자로부터 명시적인 동의를 받아야 한다(1798.121(d)). 이러한 규정은 소비자 프로파일링 및 자동화된 의사결정에 대한 권리를 강화하고 사업자의 투명성과 책임성 의무를 확대하였다는데 의의가 있다.

CCPA에서는 개인정보 처리방침의 최소 검토 주기를 12개월마다 1회 이상 현행화하도록 하고 있으며, 미국을 대상으로 서비스를 하면 소비자 개인정보의 판매금지 청구권을 반영하여 사업자는 개인정보 처리방침 안에 개인정보를 판매하지 않도록 요청할 수 있는 페이지를 포함하여 해당 페이지를 링크하고 직전 12개월 안에 사업자가 소비자에 대해 수집 및

공개한 개인정보 범주 목록을 포함하여야 한다. 소비자가 해당 권리를 행사할 수 있는 구체적인 권리 행사의 방법을 필수로 두가지 이상 개인정보 처리방침에 공개해야 하며, 수신자 무료 전화는 필수적으로 제공하여야 한다. 해당 권리 행사를 요청하는 자가 정당한 권리자인지 아닌지를 확인하는 절차에 대한 설명도 포함되어 기재하게 되어 있다[18].

2.2.3 중국

2021년 8월, 중국에서도 개인정보 보호법을 제정하여 AI 시스템에서 개인정보 보호 의무를 하도록 명시하고 있다. 개인정보처리자가 개인정보를 이용하여 자동화된 결정을 하는 경우, 자동화 처리의 투명

성과 결과의 공정성, 공정성을 보증해야 하며, 거래 가격 등 거래조건에 있어서 개인에 대해 불합리한 차별대우를 해서는 안 된다고 법 제24조 제1항에 명시하고 있다[19]. 중국은 생성형 인공지능에 대해서도 규제 입법을 추진하고 있으며[20], 2023년 5월 10일 중국 국무원은 '생성형 인공지능서비스 관리 방법 법률(안)'에 대한 의견 수렴을 마쳤다. 입법 절차에 따라 해당 법률(안)에 대한 제정 여부는 중국 전국인민대표대회 상무위원회가 검토한 후 결정한다. 현재 시점으로 아직 정식 제정되지 않았으며 주요 내용은 생성형 인공지능 서비스제공자는 중국인터넷 정보 사무국(Cyberspace Administration of China, CAC)에 등록하고 콘텐츠 필터링과 불법·유해한 콘텐츠 생성 방식을 구현하도록 한다. 개인정보 보호와

Table 2. Comparison of Privacy Policies under GDPR, USA, and South Korea

Category	EU (GDPR)	USA	South Korea
Key Legislation	General Data Protection Regulation (GDPR)	California Consumer Privacy Act (CCPA), Federal Trade Commission Act (FTC Act), etc.	Personal Information Protection Act
Scope	All companies in the EU and those processing EU citizens' data	Mainly California residents or specific industries (CCPA, GLBA, HIPAA, etc.)	All personal information processors in the country
Main Articles	Article 13, 14 (Information provision obligation)	CCPA Section 1798.130(a)(5), FTC Act Section 5	Article 30 (Establishment and Disclosure of Privacy Policy)
Privacy Policy Required	Not explicitly required, but information provision obligation specified	Required by some laws (e.g., CCPA)	Explicitly required
Key Contents	<ol style="list-style-type: none"> 1. Controller information 2. Processing purpose and legal basis 3. Recipients 4. International transfers 5. Retention period 6. Data subject rights 7. Right to withdraw consent 8. Right to lodge a complaint 	<ol style="list-style-type: none"> 1. Information collected 2. Purpose of use 3. Third-party sharing 4. Data subject rights 5. Security measures (Varies by law) 	<ol style="list-style-type: none"> 1. Processing purpose 2. Processing items 3. Retention period 4. Third-party provision 5. Outsourcing details 6. Data subject rights 7. Security measures
Disclosure Method	Transparent and easily accessible format	Posted on website (CCPA)	Internet homepage, etc.
Update Obligation	Provided at collection time or within reasonable period	Updated every 12 months (CCPA)	Disclosed upon changes
Penalties for Violation	Up to €20 million or 4% of global turnover	Varies by state law (e.g., CCPA - up to \$7,500 per violation)	within the scope not exceeding 3/100 of the total sales
Consent Requirements	Explicit consent needed	Opt-out right provided (CCPA)	Explicit consent needed
Data Subject Rights	Right of access, rectification, erasure, restriction of processing, portability, etc.	Right of access, deletion, opt-out of sale (CCPA)	Right of access, rectification, deletion, restriction of processing, etc.

데이터 보안에 관한 내용과 위반 시 최대 10만 위안(약 1800만 원) 처벌 규정이 있다.

중국 개인정보 보호법 제7조에 따르면 개인정보를 처리하면서 공개적이고 투명한 원칙을 준수해야 한다. ‘공개성과 투명성’ 원칙은 개인정보처리자가 개인정보의 처리 규칙, 처리의 목적, 방법, 범위 등을 명확히 알기 쉬운 방식을 통해 개인정보 주체에게 공개적으로 알림으로써 정보주체의 알 권리와 선택권을 보장하고 정보주체의 동의가 관련 사항에 대한 충분한 이해를 기반으로 이루어진 자발적인 의사 표시임을 보장하도록 한다고 규정하고 있다. 예를 들면, 기업이 앱을 운영할 경우 정보주체에게 명확한 방식(예컨대 알림창 등)으로 개인정보 보호 정책 또는 개인정보 처리방침을 발송하여 개인정보 처리 상황을 알려야 하는 방식이다.

2.2.4 일본

일본의 개정된 개인정보 보호법에서 AI 시스템에 의한 자동화된 의사결정에 관한 정보주체의 권리를 신설하였다. AI 서비스제공자의 설명 의무, 이용자의 이의 제기권 등을 규정하고 있다[21]. 일본 개인정보 보호법 제27조1항에 따르면 개인정보 취급사업자는 보유한 개인 데이터와 관련해 개인이 알 수 있는 상태로 해 두어야 하므로 사업자는 개인정보 취급 사업자의 성명 또는 명칭, 개인 데이터의 이용 목적, 이용 목적의 통지를 요구 및 공개의 청구 절차 및 권리 행사 시 부과될 수 있는 수수료 금액, 개인 데이터의 처리에 대한 민원 신청 방법 등 정보를 개인정보 처리방침에 공개해야 한다.

Table.2는 개인정보 처리방침을 유럽 GDPR과 미국의 CCPA, 한국의 개인정보 보호법을 근거로 개인정보 처리방침 공개에 포함되는 내용 중심으로 비교 정리하였다.

2.3 국내 AI 관련 법·제도적 현황

현재 AI 관련 규제 법률은 부재한 상황이나 개인정보보호위원회 ‘인공지능 개인정보 보호 자율점검표’(21.5.31)나 과학기술정보통신부·정보통신정책연구원에서 배포한 ‘2023 인공지능 윤리실천을 위한 자율점검표(안)’에 개인정보 보호에 대한 실천점검 문항을 반영하고 있다. 또한, 입법을 위한 활동도 활발하게 이루어지고 있다[22].

2.3.1 AI 관련 법안 주요 발의 사항

국회 의안정보시스템에서 AI 관련 법률(안) 발의 현황 중 최근 발의한 주요 사항을 살펴보면 다음과 같다.

• AI 산업육성 및 신뢰 확보에 관한 법안(안철수 의원 발의, 2024.5)

이 법안의 주요 내용은 안전하고 신뢰할 수 있는 인공지능 개발 및 이용을 위한 기반을 마련하고, 인공지능 관련 정책을 수립하여 국민의 권익과 존엄성을 보호하며 삶의 질을 높이는 것이다. 이를 위해 인공지능의 유형을 고위험과 저위험으로 구분하고, 인공지능 사업자의 책무와 이용자의 권리를 규정하며, 인공지능 기술 개발 및 산업 진흥을 위한 종합적인 정책을 추진하고자 발의한 법안이다.

• 인공지능 발전과 신뢰 기반 조성 등에 관한 법률안(정점식 의원 발의, 2024.6)

이 법안은 인공지능의 안전성과 신뢰성을 확보하기 위한 규율 체계를 마련하고, 인공지능산업의 발전을 지원하며, 국민의 권익과 삶의 질을 향상시키는 것을 목표로 한다. 이를 위해 인공지능의 정의, 고위험영역 인공지능, 생성형 인공지능 등 다양한 개념을 규정하고, 과학기술정보통신부장관이 3년마다 인공지능 기본계획을 수립하도록 하며, 국가인공지능위원회를 설치하여 인공지능 사회의 구현과 산업 신뢰 확보를 위한 사항을 심의·의결하는 등의 내용을 포함하고 발의한 법안이다.

• 인공지능 산업 육성 및 신뢰 확보에 관한 법률안(조인철 의원 발의, 2024.6)

이 법안은 인공지능 산업의 육성과 신뢰 확보를 목적으로 주요 내용으로는 인공지능 기본계획 수립, 국가인공지능위원회 설치, 인공지능 기술 개발 및 산업 활성화 지원 등을 포함하고 있다. 또한 인공지능 윤리원칙 제정, 고위험 영역 인공지능에 대한 규제, 인공지능의 신뢰성 확보를 위한 조치 등 인공지능 사회의 신뢰 기반 조성에 관한 사항을 규정하고 있다. 인공지능 산업 진흥을 위한 재원 확충, 실태조사 및 통계 작성, 권한의 위임 및 업무 위탁 등을 발의한 법안이다.

• 인공지능기술 기본법안(민형배 의원 발의, 2024.06)

이 법안은 인공지능의 건전한 발전과 신뢰 기반 조성을 위한 기본법 제정을 목적으로 하고 주요 내용으로 국가인공지능위원회 및 지역인공지능위원회 설치, 국가 인공지능 기본계획 수립, 인공지능정책센터 설치 등 인공지능 정책 추진체계를 구축한다. 또한 인공지능 기술 개발 및 산업 육성을 위해 기업 지원, 창업 활성화, 국제협력 증진, 인공지능집적단지 지정 등의 정책을 제시하고 있다. 데이터, 표준화, 전문인력 양성 등 인공지능 산업 기반 조성을 위한 시책도 포함되어 있으며 인공지능 윤리원칙 제정, 고위험영역 인공지능에 대한 규제, 생성형 인공지능 고지 의무 등 인공지능의 윤리와 신뢰성 확보를 위한 조치들을 규정하고 발의한 법안이다.

위 내용은 AI 기술 자체에 대한 입법(안) 발의 내용이고, 직접적인 AI 시스템 개인정보 처리 관련된 내용은 현행법상 일반법적 지위에 있는 개정된 '개인정보 보호법'[법률 192345호, 23.9.15]과 '신용정보의 이용 및 보호에 관한 법률'(이하 신용정보법)에서 확인할 수 있으며 발의한 대부분 법률안을 보면 고위험 AI 시스템 경우 고지의무를 포함하고 있다.

2.3.2 자동화된 결정 관련 법률

개인정보 보호법 제37조의2에 자동화된 결정에 대한 정보주체 권리 등을 규정하고 있다. 이는 완전히 자동화된 시스템(AI 기술을 적용한 시스템을 포함)으로 개인정보를 처리하여 이루어지는 결정을 '자동화된 결정'으로 정의하고 있다. 행정관청의 자동적 처분은 제외하고 있으며, 정보주체의 권리나 의무에 중대한 영향을 미칠 때에는 개인정보처리자가 결정한 자동화된 결정을 정보주체는 거부할 수 있는 권리를 가진다. 다만, 자동화된 결정에 정보주체 동의, 법률에 근거, 계약 이행이나 체결 과정에서 정보주체의 요구가 필요한 경우에는 제외하고 있다. 또한, 정보주체는 자동화된 결정에 대한 설명을 개인정보처리자에게 요구 가능하고, 개인정보처리자는 자동화된 결정의 기준과 절차, 개인정보 처리 방식 등을 공개해야 한다. 이는 AI 시스템의 개인정보 처리 과정에 투명성을 요구하는 것으로 해석된다.

이에 앞서 2020년 8월 5일에 개정된 신용정보법은 개인정보 보호법과 특별법 관계에 있으며, 법 제2

조에서 '자동화 평가'에 대한 정의를 새로 도입 하였다. 자동화 평가란 신용정보회사 종사자가 평가 업무에 직접 관여하지 않고, 컴퓨터 등 정보처리장치만을 사용하여 개인신용정보 및 기타 정보를 처리함으로써 개인인 신용정보주체를 평가하는 행위를 말한다. 이는 인공지능, 기계학습 등의 기술을 활용하여 대량의 개인신용정보를 자동으로 분석하고 평가하는 과정을 의미하며, 신용평가 업무에 있어 자동화 및 효율성에 중요한 개념으로 본다. 신용정보주체는 자동화 평가의 주요 기준과 이용된 기초정보의 개요 등에 대한 설명을 요구할 수 있고, 자동화 평가 결과의 산출에 유리하다고 판단되는 정보를 제출할 수 있다. 자동화된 평가에 이용된 기초정보가 정확하지 않거나 최신의 정보가 아니라고 판단된 경우에는 해당 기초정보의 정정이나 삭제를 요구할 수 있고 기초정보의 변경에 따라 자동화 평가 결과의 재산출을 요구 가능하다. 이러한 사항은 개인정보 보호법과 신용정보 보호법에 자동화된 결정에 따른 정보주체의 권리보장 내용이 입법화되어 있다.

2.3.3 개인정보 처리방침 평가제

개정된 개인정보 보호법(23.9.15)시행으로 개인정보 처리방침 평가 관련 조항이 새롭게 포함되었다. 개정된 개인정보 보호법 제30조의2에 따르면 보호위원회는 개인정보 처리방침을 평가할 수 있으며 평가 결과 개선이 필요하다고 판단되는 경우 개인정보처리자에게 개선을 권고할 수 있다. 이러한 개선 권고는 개인정보 보호법 제61조 제2항에 근거하며 평가기준으로는 첫째, 개인정보 보호법에서 요구하는 사항을 개인정보 처리방침에 적절히 포함하고 있는지 여부 둘째, 개인정보 처리방침이 정보주체가 이해하기 쉽게 작성되었는지 여부 셋째, 개인정보 처리방침을 정보주체가 쉽게 확인 가능한 방법으로 공개하고 있는지 여부가 있다. 개인정보 처리방침 평가의 도입은 처리방침의 중요성을 강조하는 것으로 볼 수 있으며 정보주체의 권리를 보장하기 위한 조치이기도 하다. 개인정보 처리방침 평가의 세부사항은 '개인정보 처리방침 평가에 관한 고시'에 위임하고 있고 이에 따라 AI 시스템을 활용하여 개인정보를 처리하는 경우 해당 내용을 기존의 개인정보 처리방침에 포함하거나 별도의 AI 시스템 개인정보 처리방침을 수립해야 한다. 어떤 방식을 택하든 AI 시스템을 통한 개인정보 처리에 관한 사항은 개인정보 처리방침 평가제 시행

에 따른 개인정보처리자 준수 대상 범위에 포함되는 점은 분명하다.

2.3.4 사전 적정성 검토제

사전 적정성 검토제란 “AI 등 신기술 서비스 분야에서 개인정보 보호법을 준수하는 방안을 민간 사업자와 정부가 함께 마련하고 이를 사업자가 적정히 적용하였다면 추후 환경·사정 변화가 없는 한 행정처분 대상에서 제외하는 제도”를 말한다. 정부는 신기술에서 디지털 데이터 중 개인과 관련된 비중이 높아 개인정보에 대해 법 규범이 어떻게 적용되는지에 따라 국가의 산업경쟁력 및 소비자 보호 수준이 좌우된다고 보기 때문에 신기술의 발전에 따른 법의 사각지대를 해소하기 위한 제도적 정책이다.

2.4 국내 개인정보 처리방침 유사 제도 사례

2.4.1 개인위치정보 처리방침의 공개

위치정보의 보호 및 이용 등에 관한 법률(이하 ‘위치정보법’) 제21조의2에는 개인위치정보 처리방침의 공개에 따라 개인위치정보사업자 등은 개인정보 보호법 제30조에 따라 개인정보 처리방침을 수립하여 공개하는 경우 해당 개인정보 처리방침에 다음 각호의 사항을 포함하여야 한다고 규정하고 있다. 1. 개인위치정보의 처리 목적 및 보유 기간 2. 개인위치정보 수집·이용·제공사실 확인자료의 보유근거 및 보유 기간 3. 개인위치정보의 파기 절차 및 방법 4. 개인위치정보의 제3자 제공에 관한 사항 5. 그 밖에 개인위치정보의 처리에 관하여 대통령령으로 정하는 사항이다. 개인위치정보사업자들은 개인정보 처리방침을 수립하여 공개하는 경우 포함하는 사항으로 신설된 조항이며(2021.10.19) 일반적인 개인정보 처리방침에 개인위치정보주체의 개인위치정보를 이용하면서 위치정보 보호 및 이용의 투명성과 개인위치정보사업자들의 책임성을 부여한 법률적 근거 조항이다.

2.4.2 고정형·이동형 영상정보 처리기기 운영·관리

개인정보 보호법 중 고정형·이동형 영상정보 처리기기 운영·관리 방침은 개인정보 보호법 제25조 제7항에 따라 고정형(CCTV) 영상정보처리기기 운영자

는 대통령령으로 정하는 바에 따라 고정형 영상정보 처리기기 운영·관리 방침을 마련하여야 한다. 다만, 법 제30조에 따라 개인정보 처리방침을 수립할 때 고정형·이동형 영상정보처리기기 운영·관리에 관한 사항을 포함하는 경우에는 고정형·이동형 영상정보처리기기 운영·관리방침을 마련하지 않아도 된다. 제8항에는 ‘고정형 영상정보처리기기 운영자는 고정형(CCTV) 영상정보처리기기의 설치·운영에 관한 사항을 위탁 처리하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다’라고 규정하고 있어 개인위치정보 처리방침과 유사하게 제도화하고 있다. 개인위치정보 처리방침과 고정형 영상정보 처리기기 방침 수립·공개 방법을 기존 개인정보 처리방침 안에 포함하는 경우도 있고, 독립적으로 분리하여 수립·공개하기도 한다. 최근 개정된 법에 따라 이동형 영상정보 처리기기도 법 제25조의2 제4항에는 고정형 영상정보처리기기 제25조 제6항부터 8항까지 준용한다고 규정하고 있다.

2.4.3 전화 녹취시스템 운영·관리 방침

최근 민원행정 제도 개선 차원에서 전화 녹취시스템을 도입하고 있다. 전화 녹취에 따른 개인의 음성과 녹취 내용 중에 개인정보가 포함될 수 있으므로 개인정보 수집·이용의 법적 근거가 필요하다. 이에 대한 근거로 개인정보 보호법 제15조제1항제6호 규정에 따르면 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 개인정보처리자의 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 않는 경우에 한한다고 규정하고 있다. 이에 민원행정 개선 차원에서 전화 녹취시스템을 도입하여 민원행정을 개선하고 개인정보와 관련성이 있으므로 전화 녹취시스템 관리방침을 홈페이지에 공개하고 있다.

위 사례에서 볼 때 일반적인 개인정보 처리방침에 반영되는 법적 요구사항이 많아짐에 따라 개인정보 처리방침 수립·공개 내용도 많아지고 있어 개인정보 처리와 유형이 다른 개인영상정보나 위치정보, 전화 녹취시스템 등을 구분할 필요가 있다. 이는 AI 시스템에서 처리하는 개인정보도 정보주체의 개인정보가 어떻게 수집·이용되고 어떤 목적으로 사용되고 3자 제공이 되는지 정보주체는 개인정보자기결정권 보장을 위해 알 권리가 필요하다. 본 논문에서 제안하고자 하는 방식은 AI 시스템 개인정보 처리방침을 독

립적으로 수립·공개함으로써 정보주체는 AI 시스템 개인정보 처리의 투명성 확보가 가능하다. 이러한 AI 시스템 개인정보 처리방침은 AI 산업과 개인정보 보호 측면에서 개인정보처리자의 책임성과 정보주체 신뢰성 확보로 이어져 개인정보 처리에 불안감을 해소하고 AI 산업 생태계 활성화에 적극 활용이 될 수 있을 것이다.

2.5 AI 시스템에서 개인정보 처리방침 도입 효과

AI 시스템이 개인정보를 처리하는 추세가 증가하는 가운데 AI 시스템 개인정보 처리방침 도입한다면 다음과 같은 효과를 기대 가능하다.

2.5.1 투명성과 이해도 향상

새로운 기술 출현에 따른 개인정보 처리에 있어 기존 개인정보 처리방침에 추가하는 구조는 복잡하고 점점 긴 문장으로 이어지기 때문에 제안하는 AI 시스템 개인정보 처리방침 구조화 모델을 독립적으로 구성함에 따라 복잡한 AI 시스템 개인정보 처리 과정을 명확하게 제시 가능하다.

2.5.2 법규 준수의 용이성

AI 관련 규제 법률이 시행될 경우 관련 법규의 개인정보 처리에 대한 요구사항을 구조화된 개인정보 처리방침을 통해 체계적으로 반영이 가능하며 AI 또는 개인정보 관련 법이 개정이 되더라도 해당 부분만 수정 가능하다.

2.5.3 AI 특성 반영

개인정보 보호법 제37조의2 자동화된 결정, 동법 시행령 제44조의4 자동화된 결정의 기준과 절차 등 각 호에 해당하는 사항을 적극적으로 반영이 가능하다.

다. 자동화된 결정이 이루어진다는 사실을 알리고 그 목적 및 대상이 되는 정보주체의 범위를 정한다. 자동화 결정에 사용되는 주요 개인정보의 유형과 자동화된 결정의 관계, 자동화된 결정 과정에서의 고려사항 및 주요 개인정보가 처리되는 절차, 자동화된 결정 과정에서 민감정보 또는 14세 미만 아동의 개인정보를 처리하는 경우 그 목적 및 처리하는 개인정보의 구체적인 항목, 자동화된 결정에 대하여 정보주체가 거부·설명 등 요구를 할 수 있다는 사실과 그 방법 및 절차 등 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등을 통해 공개하도록 하는 법령 준수 이행이 가능하다.

2.5.4 AI 시스템 개인정보처리자의 책임성 강화

AI 시스템에서 개인정보 처리방침을 구조화하여 공개함으로써 개인정보처리자의 개인정보 보호에 대한 책임성을 명확히 보여준다. 또한, AI 시스템 문제 발생 시 책임소재를 명확히 할 수 있어 개인정보 처리자 신뢰도 향상에 기여할 수 있다.

2.6 AI 시스템에서 개인정보 처리방침 타당성 분석

‘2023년도 개인정보 연차보고서’에 따르면 Table.3과 같이 공공기관의 94.5%가 개인정보 처리방침에 법에서 요구하는 내용을 반영하여 작성하고 있으나, 민간기업의 경우 개인정보 처리현황(처리방침)이 없는 경우가 92.2%에 달하였다. 종사자 수 300명 이상 민간기업은 ‘모든 기재사항 작성’(29.4%), ‘일부만 작성’(26.8%), ‘없음’(43.9%)으로 응답하였다 [24]. 또한, 조사대상 전체 민간기업의 경우 7.8%만이 개인정보 처리방침을 수립·공개하는 것으로 조사되었다. 그 중에서도 법에서 요구하는 내용을 모두 반영하여 작성하는 경우는 조사대상의 1.3% 밖에 응답하지 않았다. 최근 거대생성형언어모델(LLM) 기술을 활용한 이미지, 영상, 프로그래밍 코드 등 다

Table 3. Status of reflection of the Privacy Policy

(Unit: %)

Type	Processing of Personal Information			No Processing
	Total	Complete all fields	Partially complete	
Public organizations	99.0	94.5	4.5	1.0
Private companies	7.8	1.3	6.5	92.2
others (300+ employees)	56.2	29.4	26.8	43.9

양한 AI 시스템 플랫폼 서비스가 이루어지고 있다. 그 중에서 이미지 생성 플랫폼 'Canva'와 구글의 코랩 플랫폼 'Colab'의 사례를 통해 타당성을 살펴본다.

2.6.1 AI 이미지 생성 Canva 사례

AI 시스템을 이용한 이미지 생성 플랫폼 'canva'의 경우 개인정보 처리방침과 독립적으로 인공지능 시스템을 이용한 이미지 생성 서비스 약관을 분리하여 GDPR을 준수하고 있다.

Fig.1.은 canva 서비스 개인정보 처리방침과 AI 이용약관을 기존 개인정보 처리방침에 포함하여 고지하지 않고 분리하여 AI 서비스 약관에 대해 그 내용을 이용자에게 고지하고 있다.

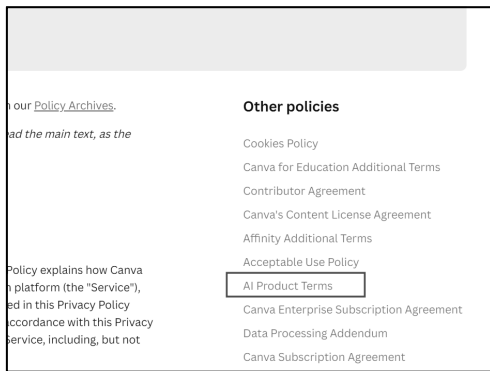


Fig. 1. Canva AI Product Terms

2.6.2 구글 코랩 (Colab) 사례

구글 코랩(colab)서비스는 웹브라우저로 텍스트와 프로그램 코드를 자유롭게 작성 가능하고 클라우드 환경에서 특별한 설정 없이도 사용이 가능하며 GPU(Graphic Processing Unit)와 TPU(Tensor Processing Unit)를 비롯한 리소스를 무료로 사용할 수 있는 플랫폼이다. 구글 계정이 있는 사용자라면 쉽게 이용약관 및 개인정보 처리방침에 동의하고 사용이 가능하다. Fig.2.에서 서비스 약관을 살펴보면 "colab의 생성형 AI는 실험용 기술이며 google의 관점을 반영하지 않는 부정확하거나 불쾌감을 주는 정보를 표시하는 경우도 있으므로 주의해서 코드를 사용하세요. colab 생성형 AI 기능으로 생성된 응

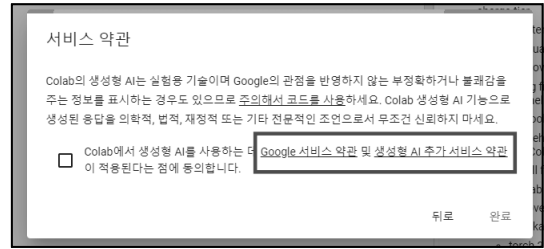


Fig. 2. Google terms of service

답을 의학적, 법적, 재정적 또는 기타 전문적인 조언으로서 무조건 신뢰하지 마세요.” 라고 유의사항을 이용자에게 안내하고 있다.

또한, 구글 서비스 이용약관과 생성형 AI 서비스 이용약관을 독립적으로 구분하여 동의를 받고 생성형 AI 추가 서비스 약관이 링크로 연결되어 있어 언제든지 확인이 가능하다.

Fig.3.에서는 생성형 AI 사용정책의 금지된 사항을 기존 구글 서비스 이용약관 또는 개인정보 처리방침(Privacy Policy)와 독립적으로 구분하여 금지사항을 안내하여 이용자가 생성형 AI 서비스 이용에 있어 금지사항을 알 수 있도록 투명하게 공개하고 있다. 즉, 일반적인 생성형 AI 서비스에 대한 약관과 생성형 AI 금지 사용을 구분하여 안내하고 있다. 글로벌 서비스를 하고 있는 위의 두 사례를 고려할 때 국내 AI 시스템에서 개인정보 처리의 경우 기존 개인정보 처리방침과 분리된 AI 개인정보 처리방침에 대한 수립·공개 의무의 타당성이 있다고 판단된다.

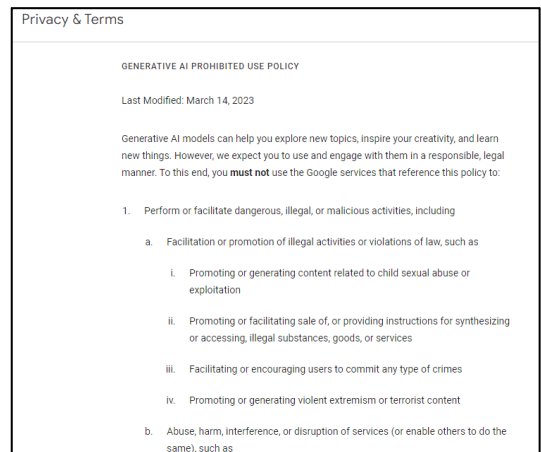


Fig. 3. Generative AI prohibited use policy

III. AI 시스템과 개인정보 처리

3.1 AI 시스템에서의 개인정보 처리 과정

AI 시스템에서 개발과정에 따라 개인정보 처리 과정을 통해 살펴보면 데이터 수집, 데이터 전처리, 모델 학습, 모델 평가 및 검증, 모델 배포 및 운영, 모니터링 및 피드백의 6단계로 나누어 볼 수 있다. 일반적인 AI 시스템 개발과정에서 개인정보 처리에 대한 사항은 Fig 4.에 기술하고 있다.

3.1.1 데이터 수집 단계

개인정보가 포함된 데이터를 수집하는 과정으로 데이터 수집 출처와 방법을 명확히 하고 개인정보 보호법에서 요구하는 수집·이용의 법적 고지사항인 수집 목적, 수집 항목, 보유 기간, 거부에 따른 불이익을 안내하고 개인정보 수집·이용에 따른 동의를 받는다. 수집된 개인정보는 안전하게 보관·관리하여야 한다.

3.1.2 데이터 전처리 단계

수집된 데이터를 AI 모델 학습에 적합한 형태로 가공하는 과정이다. 개인정보가 포함되지 않도록 하

는 조치에는 데이터 3법 개정에 따른 개인정보를 가명처리 또는 익명화하여 개인을 식별할 수 없도록 조치하여야 한다. 모든 개인정보를 가명 처리하여 사용할 수 있는 것이 아닌 통계작성과 과학적 연구(산업적 연구포함), 공익적 기록보존을 목적으로 하는 가명정보 처리에만 가능하다. 가명처리 시에는 식별성을 제거하기 위해 특이치 정보를 제거하거나 보정한다.

3.1.3 모델 학습 단계

전 처리된 데이터를 사용하여 AI 모델을 학습시키는 과정이다. 개인정보를 포함한 데이터는 개인정보가 유출되지 않도록 주의해야 하는 단계이며, 개인정보가 포함되지 않은 데이터는 재식별 되지 않도록 하여야 한다. AI 시스템 개발에서 모델 학습 단계에서 모델의 편향성을 최소화하여 AI 시스템의 공정성 확보를 위한 조치를 해야 하는 과정이다.

3.1.4 모델 평가 및 검증 단계

학습된 모델의 성능을 평가하고 검증하는 과정이다. 개인정보 보호 관점에서 AI 시스템 모델의 출력 결과를 분석하고 개인정보 유출 위험성을 평가해야

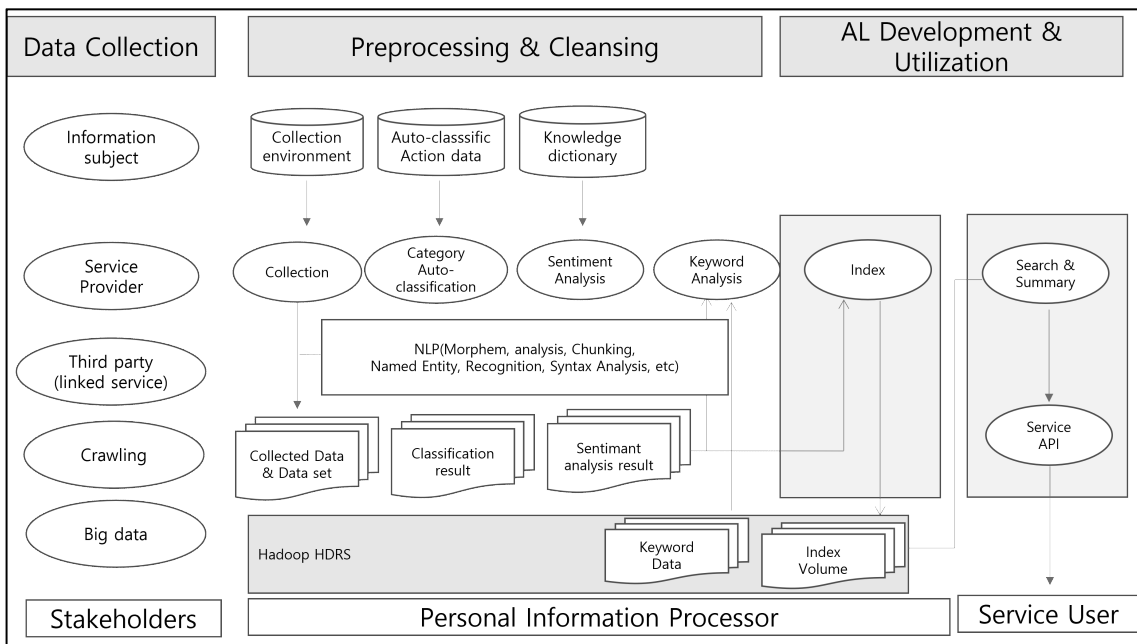


Fig. 4. Personal information processing process in AI service [23]

한다. 평가 결과에 따라 개인정보 유출 위험도가 높으면 개인정보 보호를 위해 필요한 조치를 한다.

3.1.5 모델 배포 및 운영 단계

AI 시스템에 적용 가능한 검증된 모델을 실제 서비스에 적용하고 운영하는 과정이다. 실제 AI 시스템 개발 완료 후 적용하는 단계이므로 서비스 과정에서 수집되는 개인정보는 개인정보 처리방침 및 AI 개인정보 처리방침을 수립·공개하고 준수하여야 한다.

3.1.6 모니터링 및 피드백 단계

AI 시스템에 적용된 모델의 성능과 개인정보 처리 현황을 지속적으로 모니터링하면서 개인정보 처리에 대한 사용자 피드백을 수렴하고 대응을 해야 한다. 이 경우 법 개정이나 가이드라인 등이 배포될 경우 변경사항을 반영하여 시스템을 업데이트해야 한다.

국내에서는 AI 관련 개인정보 처리 규제의 법적 근거가 없는 가운데 개인정보 보호법 제37조의2가 개인정보 처리의 자동화된 결정에 정보주체는 설명요구권과 거부권이 가능해졌다. 따라서 AI 시스템 개발과정에서 AI 시스템 개인정보 처리방침은 개인정보를 어떻게 처리할 것인지에 대한 개인정보 정책과 정보주체의 동의 후 개인정보 처리의 투명성 측면에서도 중요한 의미를 지닌다. 또한, 개인정보 보호위원회에서 배포한 '자동처리 되는 개인정보 보호 가이드라인'(2020.12.)에 따르면 기획, 설계, 점검 3개 분야로 구분하였으며 개인정보 보호 10대 수칙별 조치 사례를 통해 자동 처리되는 개인정보에 대한 안내는 Fig. 5와 같다.

기획단계에서는 ① 서비스에 꼭 필요한 개인정보 확인 ② 개인정보 수집 시 법적 준수사항 확인하고 설계에서는 ③ 반드시 필요한 개인정보만 최소한으로 처리 ④ 개인정보 처리단계별 적절한 안전조치 적용

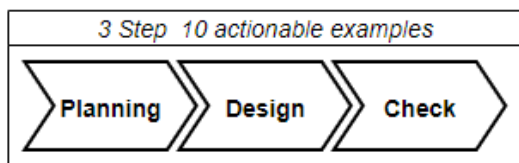


Fig. 5. 3 Step 10 Actionable Example

- ⑤ 개인정보의 처리 절차 및 방법을 투명하게 공개
- ⑥ 정보주체가 권리 행사를 쉽게 할 수 있도록 보장
- ⑦ 개인정보의 제3자 제공 및 위탁 시, 정보주체에게 명확히 안내
- ⑧ 정보주체가 서비스 해지 시 개인정보 파기 및 추가 수집 방지
- ⑨ 사업 종료 시 정보주체의 권리 보장 방안을 마련하며 점검 단계에서는
- ⑩ 서비스 출시 전 개인정보 침해 위험요소를 점검하도록 안내한다.

IV. AI 개인정보 처리방침 수립·공개 고려사항

AI 시스템 설계 및 개발·운영 과정에서 개인정보 처리에 대한 사항을 개인정보 처리 단계에 따라 살펴보고 AI 시스템과 정보주체 관점에서 고찰하고자 한다.

4.1 AI 시스템 개인정보 처리 법적 고려사항

4.1.1 개인정보 수집·이용

AI 시스템 개인정보 처리방침을 수립할 때 개인정보의 수집·이용의 법적 고려사항은 매우 중요하다. 개인정보처리자는 개인정보를 수집한 목적 범위 내에서만 수집·이용해야 하고, AI 시스템 개발 및 운영 과정에서 개인정보를 수집·이용할 때에는 정보주체에게 수집 목적, 수집 항목, 보유 및 이용 기간 등을 명확히 알리고 동의를 받아야 한다. 다만, 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 등 일정한 예외 사유가 인정된다(법 제15조 제1항 각 호). 특히, 개정된 개인정보 보호법(법률 제19234호)은 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하는 데 필요한 경우에도 개인정보를 수집하여 그 수집 목적 범위에서 이용할 수 있도록 개정되었다. 정보주체의 동의 없이 개인정보를 수집·이용하는 경우 개인정보 처리방침에 공개하게 되어 있어 기존 개인정보 처리방침에 AI 시스템 개인정보 처리를 반영한 추가적인 공개 의무사항은 개인정보 처리자에게 부담으로 작용할 가능성이 있다. 법에서는 홈페이지에 공개 또는 개인정보 처리방침에 공개하도록 규정하고 있지만, 표준화 또는 공개 방법과 절차에 대한 부분이 명시적으로 규정화된 규칙이 아직 없어 정보주체 입장에서 AI 시스템 개인정보 수집·이용 처리에 있어 투명성 확보에 한계가 있다.

4.1.2 개인정보의 목적의 이용 및 제3자 제공

개인정보처리자는 개인정보를 수집한 목적 범위 내에서만 이용하고 예외적으로 목적 외 이용이 가능하다. 제3자에게 제공할 때도 목적 범위 내와 목적 범위 외로 구분하고 개인정보처리자 입장에서 목적 외 이용은 개인정보처리자 내부에서 이용하고 목적 외 제공은 제3자에게 제공하는 방식이다. 통제 책임에서 목적 외 이용은 개인정보처리자 직접 통제 및 관리를 하고 목적 외 제공은 제3자에게 통제 책임이 이전된다. 따라서, 안전조치 의무사항도 목적 외 이용은 개인정보처리자 안전조치 의무 범위 내에 있으며 목적 외 제공 시에는 제3자에게 안전조치 의무가 발생한다. AI 시스템 설계 및 개발 운영할 때 처음 수집·이용 목적과 다르게 개인정보를 AI 시스템에 이용할 때에는 별도의 동의를 받아야 하고 법에서 요구하는 사항을 준수해야 한다.

4.1.3 개인정보 위탁

AI 시스템 설계 및 개발·운영하는 과정에서 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우를 말한다. 개인정보가 3자에게 제공된다는 점에서는 3자 제공과 위탁은 공통점이 있지만, 처리 업무의 목적과 관리·감독, 책임의 이전 등에서 차이점이 있다. 위탁은 위탁자 처리 목적 범위 내에 있고 동의를 불필요하며 개인정보 유출 시 위탁자에게 책임이 있다. 반면에 제3자 제공은 3자에게 이익을 제공하고 별도의 동의를 받아야 하며 유출 사고 시 3자에게 책임이 이전된다.

수집 목적에 따라 수집 목적 내 이용인지 목적 외 이용인지와 처리 업무를 개인정보처리자가 주체인지 아니면 3자가 처리하는지에 따라 3자 제공으로 구분되고 있다. 특히, AI 시스템 개발에 참여하는 외부 참여자가 많아짐에 따라 위탁과 제3자 제공에 대한 책임과 역할을 구체화하고 책임소재를 명확하게 할 필요가 있다.

4.1.4 개인정보 파기

개인정보 수집부터 파기까지 절차를 포함한 파기 계획을 수립하고 파기 관련 법적 근거와 내부 절차를 수립 시행해야 한다. 일반적으로 내부관리계획에 따른 파기를 수행하고 있으며 파기 시 파기 관리대장에

기록 관리하여야 한다. 법적 근거에 의해 보존할 때는 개인정보와 분리 보관하여야 하고 AI 시스템에 개인정보 학습용 데이터 또는 가명정보를 이용하는 경우에는 개인정보가 유출되지 않도록 하고 가명정보는 재식별 위험을 최소화하고 재식별의 경우 즉시 가명정보처리를 중단해야 한다.

4.1.5 개인정보 국외 이전

클라우드 기술과 환경이 발전하고 초기 기업의 경우 대부분 클라우드 환경으로 AI 시스템 설계 및 운영을 고려하는 경우가 다수이므로 국외 기업에서 제공하는 클라우드 서비스에 따른 개인정보 국외 이전에 대한 별도의 동의를 얻고 정보주체에게 알려야 한다. 최근 개인정보 보호법이 개정되면서 법 제28조의9에 따라 개인정보처리자에게 국외 이전을 중지할 것을 명할 수 있다.

4.2 AI 시스템 개인정보 처리 기술적 고려사항

AI 개인정보 처리방침 기술적 고려사항은 AI 시스템 설계 및 개발 단계와 AI 시스템 운영 및 모니터링 단계로 구분하여 살펴볼 필요가 있다.

4.2.1 AI 시스템 설계 및 개발 단계

AI 시스템 설계 및 개발 단계에서 사전예방 제도 중에 하나로 '프라이버시 중심 설계(PbD)' 원칙을 적용할 수 있다. AI 시스템 설계 및 기획 단계부터 프라이버시 보호 및 강화 조치를 마련하게 된다. 또한, AI 시스템에 적용되는 데이터를 최소화하고 가명처리 또는 익명화 기술을 활용하여 익명처리 한다. AI 모델을 합리적으로 선택하고 알고리즘의 공정성 및 차별성을 설계 단계에서부터 고려해야 한다.

4.2.2 AI 시스템 운영 및 모니터링 단계

AI 시스템 운영 및 모니터링에서 실제 서비스를 운영하는 경우에 각종 로깅 및 모니터링을 통해 개인정보 처리에 문제가 없는지 확인을 하고 AI 시스템 성능 평가 및 검증을 통해 컴플라이언스 리스크를 최소화한다. 이는 보안성을 높이고 개인정보 침해 대응을 강화하는 계기가 된다.

V. AI 시스템 개인정보 처리방침(안)

5.1 AI 시스템에서 개인정보 처리 방침

5.1.1 개인정보 보호법 제30조 개정 제안

개인정보 보호법 제30조 개인정보 처리방침의 수립 및 공개에 추가 항목을 신설하여 AI 개인정보 처리시스템에서 서비스를 제공하는 경우 AI 개인정보 처리방침을 수립·공개하도록 법률 개정을 통해 법적인 근거 마련을 제안한다. 법 개정(안)으로 제30조(개인정보 처리방침의 수립 및 공개)에 제5항을 '⑤ 개인정보처리자는 인공지능(AI) 시스템 사용할 경우 개인정보처리 방침을 홈페이지에 수립·공개하여야 한다. 단, 개인정보를 포함하지 않을 때에는 예외로 한다. 이에 따른 입증책임은 개인정보처리자가 입증한다.'고 규정을 신설한다. 또한, 개인정보 처리방침 작성지침(24.4 개정) 가이드를 통해 생성형 AI 시스템에서 개인정보 처리 시 구조화 방법, 형태, 공개방법 등 예시를 보여주고 개인정보처리자가 생성형 AI 시스템 운영에 따른 개인정보 처리방침 작성에 혼란이 없도록 안내하는 것이 필요하다.

5.2 기존 개인정보 처리방침 AI 특수성 반영한 구조화

제안된 AI 시스템 개인정보 처리방침 수립·공개 의무의 신설이 이루어지면 AI 개인정보 처리방침에 맞는 표준화된 구조가 필요하다. 이는 기존 개인정보 보호법에 따른 개인정보처리방침 수립·공개에 특수한 형태로 AI 특수성을 반영한 개인정보 처리방침으로 수립하는 방법과 또 다른 형태로 AI 시스템 설계 및 개발·운영 과정에서 개인정보를 처리하는 경우 적용 가능한 AI 시스템 개인정보 처리방침이다. 위의 2가지 방안을 각각 구조화한 형태로 다음과 같이 제안한다.

• 수집 목적

AI 서비스 제공 및 이용자 식별, 회원 관리, 이용자 맞춤형 콘텐츠 및 광고 제공, 서비스 이용 통계 분석 등에 대한 AI 시스템 개인정보 처리에 대한 수집 목적을 설명한다.

• 수집 항목

AI 서비스 이용기록, 검색내역, 채팅 내용, 음성

명령 내역, 서비스 과정에서 생성되는 정보 등 AI 시스템에서 사용하는 개인정보 수집 항목을 설명한다.

- 이름, 주소, 전화번호 등 최소 정보, 쿠키, 접속 IP, 방문일시, 기기 정보 등 자동수집 정보

• 보유 및 이용 기간

개인정보 수집 목적 달성, 정보주체 동의 철회 시 지체없이 파기를 원칙으로 한다. AI 서비스 이용 회원 탈퇴 또는 개인정보 유효기간 만료 시까지 보관한다. 단, 법령에 특별한 규정이 있을 경우 규정에 따라 보관한다.

• 제3자 제공 및 위탁

AI 서비스에 이용하는 개인정보는 정보주체의 명시적인 동의 후 제3자에게 제공하고 제공 받은자는 목적 달성 시 즉시 파기한다. 또한, 일반적인 개인정보 3자 제공에 따르며 개인정보 처리방침에 공개한다. 위탁인 경우 위탁 업무 내용 및 수탁자를 공개한다.

• 파기

개인정보 이용 기간 및 보유 기간 만료 또는 수집 목적을 달성하면 지체없이 파기를 원칙으로 한다. 파기에 대한 절차, 파기 방법, 파기 사실의 기록 보관, 안전조치에 대한 사항을 설명한다.

• 정보주체 권리보장

정보주체의 열람, 정정, 삭제, 처리정지에 대한 권리보장이 되어 있음을 알리고 이에 대한 절차와 방법을 자세히 설명한다.

• 자동화된 개인정보 처리

자동화된 처리의 설명, 자동화된 결정의 거부권 안내 등 개인정보 보호법 제37조의2 자동화된 결정에 대한 상세한 내용을 설명한다.

• 안전성 확보조치

AI 서비스 개인정보 처리에 대한 접근 권한, 접속 기록, 암호화, 보안 프로그램 등 기술적 조치에 대한 안전성 확보에 대한 사항을 설명한다.

• 연락처

AI 서비스 개인정보 처리에 대한 개인정보 책임자 및 담당 부서와 연락처를 알린다.

- **이력 관리**

개인정보 처리방침 변경 및 이력을 관리하고 변경 전과 변경 후에 대한 전후 비교표를 사용하여 정보주체가 알기 쉽게 알린다.

5.3 AI 설계 및 개발·운영에서 개인정보 처리방침 구조(안)

- **데이터 수집 출처**

AI 시스템 자료수집에 대한 출처 및 이용 조건을 명시한다. 자체 수집 시 적법한 절차에 따라 정보주체의 동의 및 공개 데이터 수집 출처를 알린다. 예를 들어 공개 데이터셋을 사용한다면 공개 데이터셋 사용과 출처를 알린다.

- **데이터 수집 항목**

AI 시스템에 사용되는 이미지, 생체정보, 음성 데이터, 이용행태 정보 등 민감정보, 고유식별 정보는 별도의 동의를 받는다.

- **데이터 전처리**

학습 데이터에서 식별자 삭제 및 가명처리를 하고 익명화는 익명처리를 하는 등 데이터 전처리 방법을 설명한다.

- **모델 평가 및 검증**

AI 시스템 개인정보 처리에 식별 가능한 개인정보 포함 여부를 검증하고 AI 판단의 설명 가능성을 높이고 민감정보는 가명처리 또는 익명화한다. 또한, 알고리즘 공정성에 대한 평가와 검증의 방법을 설명한다.

- **모델 배포 및 운영**

AI 동작 원리 및 처리 과정을 간략하게 설명하고 AI 결정에 대한 정보주체의 설명요구권 및 거부권 처리절차를 마련하여 알린다.

- **개인정보 영향평가**

AI 시스템이 개인정보에 미치는 영향을 사전에 분석하기 위한 방법으로 개인정보 영향평가를 하고 평가 결과에 따른 관리적·기술적 조치를 알린다. AI 시스템 개인정보 영향평가 이행 결과를 공개한다.

- **모니터링 및 피드백**

AI 시스템 개인정보 처리에 대한 피드백과 개인정보 처리방침의 변경에 따른 이력 관리를 한다.

5.4 AI 시스템 개인정보 처리방침 구조화 사례 -AI 음성 인식 음식 주문 플랫폼

기존 개인정보 처리방침에 구조화하여 제안한 전자와 AI 설계 및 개발 운영 과정에서 개인정보 처리방침 구조화(안)를 제안한 후자를 동시에 반영한 통합된 개인정보 처리방침 구조화 형식을 가상의 AI 음성인식 비서 서비스 플랫폼 가칭 '보이스 오더'를 통한 개인정보 처리방침 템플릿을 다음과 같이 제안한다.

① 개요 및 처리 목적

AI 기반 음성비서 서비스 '보이스오더'를 제공하여 음성 명령 인식을 통한 주문이 가능. 음식명, 배달시간, 음식 주문 수량, 옵션, 음식배달 주소, 음식 주문을 정보검색 등 정보주체에게 음식 주문 접수에 최적화된 서비스 제공을 위해 개인정보 처리를 수행.

② 처리하는 개인정보 항목 및 출처

(음성데이터) 이용자의 음성 명령 및 대화 내용 (기기 내 마이크를 통해 수집) / (정보주체 프로필 정보) 이름, 주소 등 (이용자가 앱에 직접 입력) / (서비스 이용기록) 검색 내역, 알림 설정, 연동 기기 정보 등 (서비스 이용 과정에서 자동 생성).

③ 개인정보의 보유 및 이용 기간

수집된 음성정보는 서비스 제공 및 개선 목적으로 이용자의 서비스 이용 기간 보유 및 이용. 개인정보 삭제를 요청할 경우, 해당 정보는 즉시 파기. (단, 관계 법령에 따라 일정 기간 보관해야 하는 정보는 해당 기간 안전하게 보관되며 법적 의무 보유 기간 경과 후 지체없이 파기).

④ 개인정보의 제3자 제공

원칙적으로 이용자의 개인정보를 제3자에게 제공하지 않음. 단, 정보주체의 동의가 있거나 법령에 특별한 규정이 있는 경우, 음성 명령어 서비스 제공을 위해 필요한 최소한의 개인정보를 제3자에게 제공할 수 있음. 제3자 제공 시 제공 받는자, 개인정보의 항목, 제공 받는자의 이용 목적 및 보유 기간 등을 정

보주체에게 알리고 동의를 받음.

⑤ 개인정보의 처리 위탁

음식 주문 음성 명령어 서비스의 원활한 서비스 제공을 위해 필요한 경우, 개인정보 처리 업무의 일부를 외부 위탁 업체에 위탁할 수 있음. 개인정보 처리 위탁 시 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 개인정보 처리방침에 공개함. 수탁자는 위탁 계약에 따라 개인정보 보호 관련 법규의 준수, 개인정보에 관한 비밀유지, 제3자 제공 금지, 사고 시 책임부담 등을 명확히 규정하고 이를 준수하도록 관리·감독.

⑥ 개인정보의 파기

음식 주문 음성 명령어 서비스의 개인정보 보유 기간의 경과, 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 해당 정보를 지체없이 파기함. 파기 방법은 복구 또는 재생되지 않도록 안전하게 처리하며 정보주체가 요청할 경우 파기 사실을 통지함. 단, 관계 법령에 따라 보존할 필요가 있는 경우에는 해당 기간 개인정보를 안전하게 보관한 후 파기.

⑦ 개인정보 안전성 확보조치 및 관리체계

이용자 음성 명령어 필요 시 개인정보 암호화 저장, 엄격한 접근 통제와 로깅 및 모니터링 실시, 접속 권한의 차등 부여, 접속기록과 개인정보파일 다운로드 모니터링을 실시하며 안전한 관리를 위해 ISMS, ISMS-P, ISO27001 인증 획득하여 관리체계 고도화.

⑧ 인공지능 시스템의 작동 원리 및 결정 로직에 대한 설명

음성 명령어를 자연어 처리(Natural Language Processing) 기술로 분석하고 기계학습을 통해 사용자 음식 주문 의도를 파악하여 관련 데이터베이스와 외부 API(Application Programming Interface)를 활용하여 적절한 응답 제공 / 이용 패턴과 선호도 분석을 통해 개인화된 서비스 제안 (협업 필터링, 강화 학습 등 알고리즘 사용).

⑨ 자동화된 결정에 따른 정보주체의 권리

음성 명령어 음식 주문 미서 '보이스 오더'를 통해 자동화된 결정으로 법적 효력 발생 또는 중대한 영향을 미치는 경우, 결정에 대한 설명요구 및 이의제기

가능하며 결정에 거부권 행사. 요구 방법은 하단 문의 창구 통해 가능.

⑩ 인공지능 시스템의 편향성

차별 및 편향성 등 윤리적 이슈에 대한 대응방안으로 음성 명령어 학습 데이터와 알고리즘의 불공정한 편향성 모니터링을 시행하며, 윤리위원회 설치, 주기적 알고리즘 감사 수행, 편향·차별 의심 시 외부 전문가 자문을 받아 수정 조치.

⑪ 개인정보 보호 책임자 및 문의 창구

개인정보 보호 책임자: 000 이사, privacy@company.com, 개인정보 문의 창구: 고객센터 (123-4567) 또는 고객센터 이메일(support@company.com)

⑫ 개인정보 처리방침 개정 이력

현 음식 주문 음성 명령어 서비스 '보이스오더' 개인정보 처리방침은 20XX 년 X월 X일에 개정되었으며 정부 정책 변경, 보안 기술 발전 등에 따라 내용의 추가, 삭제 및 수정이 있을 수 있음. 개인정보 처리방침이 변경되는 경우 변경사항을 홈페이지 공지하며 중요한 변경사항에 대해서는 정보주체에게 별도 알림을 제공함. 이전의 개인정보 처리방침은 웹사이트 내 별도 페이지 보관하여 개정 전과 개정 후 비교를 통해 정보주체가 확인할 수 있도록 함.

이상과 같이 AI 시스템에서 개인정보 처리를 할 경우 AI 개인정보 처리방침 수립·공개하는 방법과 가상의 음식 주문 음성 명령어 서비스 '보이스 오더'를 사례로 템플릿을 제안하였으며 AI 개인정보 처리방침 구조화를 반영한 예시를 도출하였다.

VI. 결 론

AI 기술의 발전과 함께 AI 시스템에서 처리되는 개인정보 보호의 중요성과 필요성에 따라 AI 시스템에 특화된 개인정보 처리방침 수립·공개 방안을 제시하였다. 이를 위해 첫째, 개인정보 보호법 법 개정이 필요하다. 개인정보 보호법 제30조 제⑤항에 AI 시스템 개인정보 처리방침 신설을 제안하였다. 이는 AI 시스템 개인정보 처리의 책임성과 투명성을 확보하는 견제 장치가 될 수 있다. 개인정보 처리방침 평가제와 자동화된 결정의 법적 신설에 따른 대응책 마

련에도 활용할 수 있다. 둘째, 기존의 일반적인 개인정보 처리방침을 기반으로 AI 특수성을 반영한 AI 개인정보 처리방침의 구성요소를 도출하였고 일반 개인정보 처리방침에 AI 시스템이 수집하는 개인정보 항목, 수집 목적, 보유 및 이용 기간, 제3자 제공, 처리 위탁, 정보주체의 권리 행사 방법, 파기 절차, 안전성 확보조치, 개인정보 책임자 및 담당 부서 연락처 등을 포함하였다. 셋째, AI 시스템 설계·개발 과정에서 AI 알고리즘에 의한 자동화된 개인정보 처리, AI 서비스 제공을 위한 수집 및 이용, AI 서비스 관련 제3자 제공, AI 서비스의 개인정보 자동수집, 이용자 권리 및 피해구제 항목을 새롭게 도출하였다. 또한, 가상의 AI 비서 음식 주문 음성 명령어 서비스 '보이스 오더'를 가상으로 AI 시스템에서 개인정보 처리방침 구조화 방법과 예시 템플릿을 도출하고 제안하였다.

이러한 AI 시스템 개인정보 처리방침은 AI 서비스제공자가 정보주체의 프라이버시를 보호하고 개인정보 자기 결정권을 존중하기 위한 기반이 될 것이며, AI 시스템의 개인정보 처리에 대한 정보주체 신뢰성을 확보하고 지속 가능한 AI 생태계 조성에 기여할 것으로 기대된다. 향후 연구 방향으로서는 개인정보 처리방침을 민간기업보다 많이 공개하고 있는 공공기관을 중심으로 독립된 AI 시스템 개인정보 처리방침 공개로 인한 이용자 개인정보 자기결정권 행사에 수용요인을 분석하고 AI 시스템 개인정보 처리방침 실효성 제고 방안을 모색할 것이다. AI 서비스제공자의 개인정보 처리 실태를 점검 후 알고리즘 투명성과 설명 가능한 인공지능(eXplainable Artificial Intelligence, XAI)을 위한 추가적인 연구도 수행할 예정이다.

References

- [1] Privacy Commissioner's Office, "Privacy Commissioner Announces Results of Preliminary Inspection of Major Artificial Intelligence Services," Press Release, March 28, 2024.
- [2] Xudong Pan, Mi Zhang, Shouling Ji and Min Yang, "Privacy Risks of General-Purpose Language Models," 2020 IEEE Symposium on Security and Privacy, pp. 1314-1331, May, 2020.
- [3] Yong-Jin Shin, "Compliance with Personal Information Protection in the AI Service Process for AI Service Providers: Development and Importance Analysis," Journal of Korean Association for Regional Information Society, 25(2), pp. 1-29. June. 2022.
- [4] Jin-ho Ryu, "A study on Protecting Privacy in Artificial Intelligence environment," Korea Society of Information Communication Security Ethics. pp. 14 1-157. Nov, 2020.
- [5] Chang-Uk Jeon, "A Study on the Comparison of the Domestic and Foreign Privacy Policies by Internet Sites," Master's Thesis, Sangmyung University, Feb 2017.
- [6] Il-Yong Kim, "A Privacy Certification Systems Improving the Information comprehension, Trustworthiness, Risk perception and Intention to Provide Personal Information," Master's Thesis, Yonsei University, Dec 2020.
- [7] Ha Ram Kim, "A Study on the improvement of privacy policy : Focusing on Life-Insurance Company," Master's Thesis, Dongguk University, Dec 2023.
- [8] Yoon-Kyo Jeong, "Reliability Analysis of Privacy Policies Using Android Static Analysis," KIPS Transactions on Computer and Communication Systems, vol. 12, no. 1, pp. 17-24, 2023.
- [9] Tae-Chul Jung and Hun-yeong Kwon, "A Comparative Analysis of the Legal Systems of Four Major Countries on Privacy Policy Disclosure," vol. 22, no. 6, pp. 1-15, 2023.
- [10] Yong-Hyun Jo, Young-Kyun Cha, "Privacy Policy Analysis Techniques Using Deep Learning," Journal of The Korea Institute of Information Security & Cryptology, vol. 30, no.2, pp. 305-312, Apr. 2020.
- [11] Yong-Jin Shin, "Compliance with Pers

- onal Information Protection in the AI Service Process for AI Service Providers: Development and Importance Analysis,” *Journal of Korean Association for Regional Information Society*, 25(2), pp. 1-29, June, 2022.
- [12] Korea Internet & Security Agency, AI Personal Information Protection Self-Checklist, May, 2021.
- [13] Veale, M., & Borgesius, F. Z. “Demystifying the Draft EU Artificial Intelligence Act,” *Computer Law Review International*, 22(4), pp. 97-112, 2021.
- [14] Korea Internet & Security Agency, G DPR guidebook revision, pp. 71, 202
- [15] Korea Internet & Security Agency, G DPR guidebook revision, pp. 107, 2022.
- [16] Korea Internet & Security Agency, G DPR guidebook revision, pp. 126, 2022.
- [17] Korea Internet & Security Agency, G DPR guidebook revision, pp. 129-130, 2022.
- [18] Chang-Sun Choi, “A Study on the Comparison and Improvement of Management Standards for Responding to Global Personal Information Protection Regulations of Korean Companies : EU GDPR and CCPA in California, USA,” Master’s Thesis, KonKuk University, pp. 62-63, May, 2022.
- [19] Feng, Y., & Huang, T. “China’s Personal Information Protection Law: An overview and comparison with the EU GDPR.” *Computer Law & Security Review*, 45, 105694, 2022.
- [20] Word Law Information Center, “china generative AI,” https://world.moleg.go.kr/web/dta/lgsITrendReadPage.do?&CTS_SEQ=50676&AST_SEQ=55&ETC=6, May 20, 2024.
- [21] Matsuo, T. “The impact of Japan’s amended data protection law on artificial intelligence.” *International Data Privacy Law*, 12(1), pp. 51-68, 2022.
- [22] Bill information, “Artificial Intelligence,” <https://likms.assembly.go.kr/bill/main.do>, Aug 9, 2024.
- [23] Yong-Jin Shin, “The Improvement Plan for Personal Information Protection for Artificial Intelligence(AI) Service in South Korea,” *Journal of Convergence for Information Technology*, vol. 11, no. 3, pp. 20-33, 2021.
- [24] Personal Information Protection Commission, 2023 Annual Report on Personal Information Protection. pp. 40, 2023.

 < 저자 소개 >



전 주 현 (Ju-Hyun Jeon) 학생회원
 1989년 2월: 강릉원주대학교 무역학과 졸업
 2008년 8월: 부경대학교 일반대학원 정보보호학과 석사
 2018년 3월~현재: 부경대학교 일반대학원 정보보호학과 박사과정
 <관심분야> 시스템 보안, 네트워크 보안, 개인정보, 정보보호 및 개인정보 보호 관리체계



이 경 현 (Kyung-Hyune Rhee) 종신회원
 1982년 2월: 경북대학교 수학교육과 졸업
 1985년 2월: 한국과학기술원 응용수학과 석사
 1992년 2월: 한국과학기술원 수학과 박사
 1985년~1993년 한국전자통신연구원 선임연구원
 1993년~현재: 부경대학교 컴퓨터·인공지능공학부
 <관심분야> 정보보호, 모바일 통신보안, 블록체인, 인공지능