개인정보 처리정지 요청을 실시간 반영하는 모델 연구

[1]홍윤희, [2*]여상수

Research on a Model that reflects requests to suspend processing personal data in real time

[1]Younhee Hong, [2*]Sang-Soo Yeo

요 약

개인정보보호는 국내외를 막론하고 그 중요성이 더욱 강조되고 있으며, 국외에서는 관련정책과 동적 관리 기술을 다양하게 적용하고 있지만 우리나라에서는 법령 준수와 기술 적용 간의 일부 괴리가 존재하며, 정보주체의 개인정보 처리정지를 편리하게 제공하는 사용자 인터페이스가 거의 없는 상황이다. 본 연구에서는 먼저 개인정보 동의 동적 관리 기술의 필요성과 관련 산업의 실태 그리고 발전 가능성을 전망한다. 다음으로 국내 개인정보보호 법령을 엄격히 준수하면서도 정보주체의 개인정보 자기결정권을 최대한 보장하는 개인정보 동의 동적 관리 기본 모델을 제시하였다. 특히, 개인정보 처리정지와 관련된 국내 법령상 근거와 개인정보 동의 동적 관리 인터페이스 기본 모델을 설계하고, 그 효과성을 분석하여 제시한다. 본 연구의 결과를 통해서 제안된 개인정보 이용 동의에 대한 동적관리 모델은 앞으로 다양한 웹사이트 및 애플리케이션 등에 다각적으로 활용될 수 있을 것으로 예상한다.

Abstract

The importance of personal data protection is increasingly emphasized both at home and abroad, and while overseas countries are applying various policies and dynamic management technologies, there are some gaps between compliance with laws and regulations and the application of technologies in Korea, and there are few user interfaces that provide convenient ways for data subjects to stop processing personal data. This study first analyzes the need for dynamic personal information consent management technology, the current state of the industry, and the prospects for its development. Next, this study proposes a basic model for dynamic management of personal information consent that maximizes the data subject's right to personal data self-determination while strictly complying with personal data protection laws in Republic of Korea. In particular, this study analyzes the basis of domestic laws and regulations related to the suspension of personal data processing, designs a basic model of personal data consent dynamic management interface, and presents its effectiveness. Based on the results of this study, we expect that the proposed dynamic management model for personal data use consent can be used in various ways for various websites and applications in the future.

Keywords: *Right to Personal Data Self-determination, Personal Data Protection, Personal Data Processing, Data Subject's Rights, Suspension on Processing Personal Data*

[1] *충남대학교 반도체특성화사업단 교수 (yhhong@cnu.ac.kr)*
[2*] *교신저자 목원대학교 컴퓨터공학과 교수 (sangsooyeo@gmail.com)*

Received: Jan. 31, 2024, Revised: Feb. 22, 2024, Accepted: Feb. 26, 2024

I. 서론

데이터 경제 시대의 개인정보는 전자상거래 및 고객관리와 같은 사회적 요소로서 중요하며, 이는 부가가치를 창출할 수 있는 중요한 자산으로 간주된다. 특히, AI 기술은 의료, 교육, 유통 등 다양한 서비스 분야 고도화에 기여한다. 그러나 AI 기술의 발전으로 인한 개인정보 침해와 같은 문제로 우려가 커지고 있으며, 이러한 이슈로 대규모 개인정보 유출 사건 등이 발생하고 있다. 이러한 상황에서 개인정보 보호는 모든 국가가 직면한 공통된 문제로 여겨지며, 각 국가는 이에 대한 개인정보 보호 법령 및 정책을 강화하고 확대함으로써 산업 수요를 충족하려는 움직임을 보이고 있다.

개인정보 침해는 개인정보 자체로 인한 피해뿐만 아니라 추가적인 피해 위험도 높기 때문에 사전에 예방하는 것이 중요하다. 최근 개인정보 신고 건 수는 2019 년 대비 2021 년에 7,824 건으로 7 배 증가했으며, 이 중 민간 부문에서 발생한 사건이 7,646 건으로 대다수를 차지하고 있다[1]. 개인정보보호위원회는 2024 년부터 2026 년까지의 개인정보 보호 기본 계획을 수립하여 데이터 경제 시대를 선도할 다양한 정책을 제안하고 있으며, 이에는 개인정보 가치 창출, 신뢰할 수 있는 신기술의 활용, 안전한 데이터 활용 촉진, 공공부문에서의 보호 강화 등이 포함되어 있다[2]. 개인정보 침해를 줄이기 위해서는 적절한 제도와 정책을 수립하고 안정적인 데이터 환경을 구축하는 것과 더불어, 개인정보를 보유한 소비자가 직접적으로 제어하고 관리할 수 있는 시스템을 마련하는 것이 필요하다.

따라서 본 연구는 개인 정보 주체인 사용자가 개인정보 데이터를 스스로 선택적으로 제어하고 보호받을 수 있는 유연한 동적 모델을 제안하고자 한다. 이를 위해 개인정보 수집 및 이용의 법적 근거를 중심으로 관련 산업과 국외 사례를 분석하고 동적 관리 기본 모델을 구축하여 국내 적용 가능성을 모색하고자 한다. 이러한 개인정보 동의 동적 관리 모델은 개인정보 보호를 선택적으로 동의하 여 정보유출을 규제할 뿐 만 아니라 개인 정보를 보유한 주체 스스로가 정보 활용을 이해하고 분석하여 관리하는 데에도 도움을 줄 것으로 기대된다.

II. 관련연구

2.1 개인정보 수집 및 이용의 법적 근거

개인정보 보호법 제 2 조에 따르면 '개인정보'란 성명, 주민등록번호, 그리고 영상 등을 통해 특정 개인을 알아볼 수 있는 정보를 의미한다. 이는 해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 결합하여 특정 개인을 식별할 수 있는 정보를 포함한다. '개인정보 처리자'는 공공기관, 법인, 단체, 개인 등이며, 개인정보 보호법 제 15 조에 따라 개인정보 처리자는 정보주체의 동의를 받고 개인정보를 수집할 수 있다. 정보주체는 개인정보 보호법 제 17 조에 따라 개인정보 처리자에게 자신의 개인정보 처리를 중단하거나 동의를 철회할 수 있다. 개인정보 처리자는 처리정지 요청을 받으면 즉시 정보의 전부 또는 일부를 중지해야 하며, 정보주체가 동의를 철회한 경우 수집된 개인정보를 파기할 의무가 있다.

현재 국내 대다수의 웹사이트에서는 일반적으로 회원가입 시 개인정보 수집 및 이용에 대한 동의를 받는다. 이러한 동의는 정보 주체인 개인 역시 회원가입 시 이루어지며, 회원이 탈퇴할 때까지 일반적으로 별다른 설정 조치 없이 유지된다.

2.2 유럽 및 미국, 우리나라의 개인정보 관리 정책 및 기술 수준

2.2.1 유럽

기업과 공공기관의 웹사이트는 유럽연합(EU)의 일반데이터보호규정(GDPR, General Data Protection Regulation)과 전자통신 개인정보 보호 지침인 e-Privacy 지침(Directive 2002/58/EC)에 근거한다[3]. 이에 따라 해당 국가의 개인정보 보호 법령을 준수하여 개인정보 처리 방침을 수립하고, 그에 따른 고객 서비스를 제공하고 있다. 웹사이트 접속 시 사용자(정보 주체)가 어떤 쿠키를 허용할 지 여부를 선택할 수 있도록 엄격한 쿠키 규제를 통해 편리하고 직관적인

인터페이스를 제공하는 것이 법적 의무이다[4]. 이러한 의무는 유럽연합 내 사무실을 두고 있는 기업 및 기관 뿐만 아니라 유럽연합 시민에게 상품이나 서비스를 제공하는 모든 기업 및 기관에 적용되는 규정이다(GDPR 제 3 조). 유럽연합의 웹사이트들은 이미 충분한 검증을 거친 사용자 경험(UX)을 가지며, 초기 쿠키 설정 화면과 동적인 쿠키 설정 변경 링크(floating layer 를 통해 구현됨)를 제공하고 있는 것으로 알려져 있다.

2.2.2 미국

2020 년 미국 캘리포니아 주에서 「소비자보호법(CCPA)」이 발효되었고, 연방 정부 차원의 「개인정보 보호법」을 요구하는 입법 논의가 상원에서 진행 중이다[4]. 미국은 데이터 보호를 일반적으로 규제하는 연방 법률이 없으며, 교육, 통신, 보험 등의 분야에 대한 연방 법률만 존재한다. 각각의 법률에는 소비자 프라이버시를 보호하기 위한 규정이 포함되어 있지만, 연방 단위의 개인정보 보호법은 아직 없다.

미국에서는 기본적으로 아동 및 청소년을 제외한 성인에게는 개인정보 옵트-아웃(opt-out) 규정이 적용된다. 이는 정보주체의 개인정보가 기업 및 기관에 의해 제약 없이 사용될 수 있다는 의미이다. 그러나 정보주체는 자신의 정보가 더 이상 사용되지 않도록 Opt-out 을 요청할 권리가 있으며, CCPA(캘리포니아 소비자 프라이버시 법) 및 CPRA(캘리포니아 개인정보 보호법)도 이러한 메커니즘을 가지고 있다. 따라서 일정 규모 이상의 개인정보를 처리하는 기업 및 기관들은 정보주체가 쉽게 Opt-out 을 설정할 수 있도록 "Do Not Sell My Personal Information(내 개인정보 판매하지 않음)" 페이지를 웹사이트에 구현한다. 미국 캘리포니아 주에 본거지를 둔 기업 및 기관은 "Do Not Sell My Personal Information" 페이지를 제공할 의무가 있다.

2.2.3 우리나라

우리나라의 개인정보보호법은 2021 년 12 월 EU GDPR 제 45 조에 근거한 적정성 결정(Adequcy Decision)을 통해서 EU GDPR 과 동등한 수준의 개인정보보호법 체계를 갖춘 국가로 인정받았으며, 이를 통해서 우리나라 개인정보 보호법 체계가 세계적 수준에 이르러 있음을 확인할 수 있다. 다만, 국민들은 자신의 개인정보가 어떻게 처리되는지 또는 개인정보를 어떻게 효과적으로 관리할 수 있는지에 대한 인식은 여전히 개선의 여지가 많은 것으로 인식된다. 일반적으로 대다수 국민의 경우, 웹사이트 회원 가입 과정에서 처음으로 개인정보 필수 동의 및 선택 동의를 마치고 나면, 이후에는 자신의 개인정보 처리과정에 대해 큰 관심을 가지지 않는 문화가 형성되어 있다.

더구나, 유럽연합처럼 쿠키 설정에 대한 명시적은 강행 규정이 없다는 점은 웹사이트 사용자들이 자신의 개인정보와 프라이버시의 중요성을 충분히 이해하지 못한 채로 웹서비스를 이용하게 되는 상황을 지속적으로 만들어가고 있다고 판단된다. 이와 별개로, 삼성전자, LG 전자와 같은 글로벌 기업은 이미 쿠키 설정이나 "Do Not Sell My Personal Information" 페이지를 구현하고 있지만, 이러한 기능을 한국 국민을 대상으로 하는 웹페이지에서는 제공하지 않고 있는 것은 사실이다.

III. 개인정보보호 산업분야 발전 가능성

3.1 개인정보보호 관련 국내외 산업 동향

2021 년 정보보호 실태 조사 보고서에 따르면, 민간기업을 대상으로 한 설문조사 결과, 전체 기업 중 89.9%가 개인정보보호의 중요성을 인식하고 있으며, 이 중 11.6%의 기업만이 정보보호를 위한 조직을 구성하고 있는 것으로 나타났다. 또한, 조사 대상 기업 중 27%가 정보보호와 관련된 예산을 수립하고 있으며, 정보보호 시스템 유지보수 비용 및 정보보호 제품 구입 비용이 전체 예산의 85%를 차지하는 것으로 나타났다. 국내 민간기업의 개인정보 보호 예산은 표 1 과 같다. 84%의 기업이 1 백만원 미만으로 가장 많았으며, 그 다음으로 1 천만원 미만이 9%, 1 억 미만이 6%, 1 억 이상은 1%의 비율을 보였다. 더 큰 규모의 사업체일수록 정보보호 예산을 수립하는 비율이 높은 경향을 보였다[5].

전 세계 사이버 보안 시장규모는 2026 년까지 연평균 9.6%의 성장률을 보여 2,098 억 4,200 만 달러(한화로 약 247 조 원)에 이를 것으로 전망된다. IT 서비스는 2022 년부터 연평균 11.9% 증가하여 2026 년에는 전체 시장의 51.7%를 차지할 것으로 예상되며. 소프트웨어는 2022 년 이후 연평균 6.6%의 성장률로 전체 사이버보안 시장의 29.4%를 차지할 것으로 예상된다. 하드웨어는 2022 년 연평균 8.8%의 성장률을 보이며 동년 대비 세계 시장의 19.0%를 차지할 것으로 예상된다[6].

개인정보 보호와 관련된 글로벌 시장규모는 표 2 와 같다. 개인정보보호 데이터 시장은 2019 년 대비 2027 년까지 16.23% 성장할 것으로 예측되며, 개인정보보호 소프트웨어 시장은 2022 년 대비 2029 년까지 40.77% 이상 성장할 것으로 전망되고 있다[7].

Table1. Percentage of Personal Data Protection Budget in Domestic Private Companies (%)
표 1. 국내 기업의 개인정보 보호 예산의 비율 (%)

	Less than 1 million won	From 1 million won to 10 million won	From 10 million won to 100 million won	More than 100 million won
2018	79%	10%	11%	1%
2019	84%	11%	4%	1%
2020	76%	14%	8%	1%
2021	97%	3%	0%	0%

Table 2. Forecast of the Global Market Size for Personal Data Protection
표 2. 개인정보 보호를 위한 글로벌 시장 규모 예측

Market Research Institution	Market Segmen-tation	Publi-cation (Year)	Training Data (Year)	Start of Prediction (Year)	Market Size (million USD)	Prediction End (Year)	Market Size (million USD)	Annual Growth Rate (CAGR)
Verified Market Research	Data Privacy Market	2019	2016-2018	2019	77	2027	258	16.23%
Fortune Business Insights	Data Privacy Software Market	2022	2018-2020	2022	2,360	2029	25,850	40.77%
Fact.MR	Data Privacy Software Market	2022	2017-2021	2022	1,195	2032	18,500	31.52%

3.2 개인정보보호 정책 및 인식 변화에 따른 산업 전망

각 나라의 개인 정보 보호 법령 및 정책은 꾸준히 확대되고 있으며, 이는 개인정보 산업의 수요를 끌어올리고 있다. 글로벌 IT 기업들은 주로 자사나 리테일을 위한 Compliance 솔루션 개발에 주력한다. 대규모의 개인정보 해킹 사건으로 우려가 높아지면서, 개인정보 보호에 대한 수요는 급격히 증가하고, 또한 국민들의 인식 변화와 생활양식의 변화로 인해, 개인정보 보호와 활용의 중요성에 대한 인식이 더욱 강조되고 있다. 감염병 방역, 바이러스 전파 경로 추적, 예방접종 관리 등과 관련하여 개인정보 수집이 보급되고 있으며, 재택근무가 확대되면서 개인정보 보호 산업의 성장을 촉진하고 있다.

한편, 다양한 산업군에서 제공되는 제품 및 서비스와 관련된 개인정보보호 기술의 필요성이 증가하고 있다. 자율주행 자동차, 자율주행 드론, 에어 모빌리티(Air Mobility, UAM/RAM) 시장의 확대에 따라 광학 카메라를 비롯한 다양한 센싱 장치를 통한 의도치 않은 개인정보 수집에 대응하는 기술 개발이 요구되고 있으며 위치정보 관련 수집에 대한 개인의 세밀한 통제기술(해상도, 시간, 지역, 상황 등)의 개발 또한 확대되고 있다. 뿐만 아니라, 실시간 트랙킹 관리 및 통제기술, 데이터 연계-결합시장, 은행, 금융서비스, 보험 시장 등에서도 개인정보 제공 및 관리에 대한 기술이 필요로 하고 있다.

IV. 개인정보 처리정지 요구를 실시간으로 반영하는 모델 설계

4.1 처리정지 요구 실시간 반영 모델의 필요성

「개인정보 보호법」(PIPA, Personal Information Protection Act [법률 제 19234 호, 2023. 3. 14., 일부개정]) 제 37 조는 정보주체가 본인 개인정보에 대한 처리정지를 개인정보처리자에 요구할 수 있는 권리가 있음과 개인정보처리자가 이러한 정보주체의 요구를 받았을 때 '지체 없이' 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 함을 규정하고 있다[8]. 「개인정보 보호법」 및 같은 법 시행령에 대한 조항 중 본 논문과 관련된 조항은 표 3 으로 요약하여 설명하였다.

Table 3. Data Subject's right to suspend processing his or her personal data in the Personal Information Protection Act (PIPA) and its Enforcement Decree in Republic of Korea [8][9]
표 3. 개인정보보호법 및 같은 법 시행령의 정보주체의 본인 개인정보에 대한 처리정지 권한 [8][9]

PIPA : *Article 37* (Suspension of Processing of Personal Information)	
①	A data subject may request the relevant personal information controller to suspend the processing of his or her personal information or may withdraw his or her consent to personal information processing. In such cases, if the personal information controller is a public institution, the data subject may request the institution to suspend the processing of his or her personal information contained in the personal information files to be registered pursuant to Article 32 or may withdraw his or her consent to personal information processing. <Amended on Mar. 14, 2023>
②	Upon receipt of the request for suspension of processing under paragraph (1), the personal information controller shall, without delay, suspend processing of some or all of the personal information as requested by the data subject: Provided, That, where any of the following is applicable, the personal information controller may deny the request of such data subject: <Amended on Mar. 14, 2023> 1. Where special provisions exist in other statutes or it is unavoidable to observe obligations under statutes or regulations; 2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person; 3. Where the public institution cannot perform its work as prescribed by any Act without processing the personal information in question; 4. Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement.
③	A personal information controller shall, when a data subject withdraws his or her consent pursuant to paragraph (1), take necessary measures without delay, such as destroying collected personal information to prevent recovery and reproduction thereof: Provided, That in cases falling under any subparagraph of paragraph (2), a personal information controller need not take measures following the withdrawal of consent. <Newly Inserted on Mar. 14, 2023>
④	When rejecting a request for suspension of processing pursuant to the proviso of paragraph (2) or failing to take measures following the withdrawal of consent pursuant to the proviso of paragraph (3), the personal information controller shall notify the data subject of the reason without delay. <Amended on Mar. 14, 2023>
⑤	The personal information controller shall, without delay, take necessary measures including destruction of the relevant personal information when suspending the processing of personal information as requested by data subjects. <Amended on Mar. 14, 2023>
⑥	Matters necessary for the methods and procedures to request the suspension of processing, to withdraw consent, to reject such request, and to give notification, etc. ***pursuant to paragraphs (1) through (5) shall be prescribed by Presidential Decree***. <Amended on Mar. 14, 2023>
Enforcement Decree of PIPA : *Article 44* (Suspension of Processing Personal Information)	
①	A data subject who intends to request a personal information controller to suspend the processing of his or her own personal information pursuant to Article 37 (1) of the Act shall submit a request in the manner and following the procedure determined by the personal information controller. In such cases, Article 41 (2) shall apply mutatis mutandis where the personal information controller determines the manner and procedure for requesting the suspension of processing personal information; and "access" shall be construed as "suspension of processing". <Amended on Oct. 17, 2017>
②	A personal information controller shall inform the relevant data subject of the fact that it has duly suspended the processing of personal information pursuant to the main clause of Article 37 (2) of the Act ***within 10 days*** from the receipt of a request to suspend the processing of personal information made under paragraph (1); otherwise, if the suspension of processing personal information is denied because it falls under the proviso of Article 37 (2) of the Act, the personal information controller shall serve the relevant data subject with the Personal Information Processing Suspension Outcome Notice, stating the fact and grounds for the denial and how to appeal, in the form prescribed by Notification of the Protection Commission. <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>

Enforcement Decree of PIPA : *Article 41* (Procedures for Access to Personal Information)

①	A data subject who intends to request access to his or her own personal information processed by a personal information controller pursuant to Article 35 (1) of the Act shall submit a request, stating the information that he or she intends to access among the following information, in the manner and following the procedure determined by the personal information controller; <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017> 1. Particulars and substance of personal information; 2. The purpose of collecting and using personal information; 3. The period for retaining and using personal information; 4. Status of personal information provided to a third party; 5. The fact that the data subject has given consent to the processing of his or her personal information and the content thereof.
②	To determine the manner and procedure for requesting access under paragraph (1), a personal information controller shall comply with the following to ensure that such manner and procedure are not more difficult than the manner and procedure that the personal information controller uses to collect the relevant personal information: <Newly Inserted on Oct. 17, 2017> 1. To provide the requested personal information in a data subject-friendly manner, such as in writing, by telephone or electronic mail, or via the Internet; 2. To allow data subjects to request access to their own personal information at least through the same window or in the same manner that the personal information controller uses to collect such personal information, unless good cause exists, such as difficulty in continuously operating such window; 3. To post on a website the manner and procedure for requesting access if the personal information controller operates the website.
③	A data subject who intends to request access to his or her own personal information via the Protection Commission pursuant to Article 35 (2) of the Act shall submit to the Protection Commission a Personal Information Access Request specifying the information to access among the information referred to in paragraph (1), as prescribed by Notification of the Protection Commission. In such cases, the Protection Commission shall forward the Personal Information Access Request to the relevant public institution without delay. <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>
④	"Period prescribed by Presidential Decree" in the former part of Article 35 (3) of the Act means 10 days. <Amended on Oct. 17, 2017>
⑤	Where a personal information controller allows a data subject to access the relevant personal information within 10 days from the receipt of the Personal Information Access Request under paragraph (1) or (3), or limits access to the relevant person information under Article 42 (1), the personal information controller shall serve the data subject with the Access Notice, stating the accessible personal information, date and time, venue, etc. for access (in the case of partial access pursuant to Article 42 (1), the ground therefor and how to appeal shall be included), in the form prescribed by Notification of the Protection Commission: Provided, That where he or she allows immediate access, the Access Notice may be omitted. <Amended on Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Oct. 17, 2017; Aug. 4, 2020>

처리정지를 요청하는 방법에 대해서는 같은 법 시행령(Enforcement Decree of PIPA) 제 41 조를 준용하여, '서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공'하도록 규정하고 있다[9].

한편, 처리정지 요청을 이행하여야 하는 최대 기간은 법 제 37 조에 규정한 '지체 없이'를 같은 법 시행령 제 44 조에서는 개인정보처리자는 개인정보 처리정지 요구를 받은 날부터 '10 일 이내'로 매우 넓게 규정하고 있다. 이 법정 처리 기한 '지체 없이'를 같은 법 시행령에서 규정한 최대 기간 '10 일 이내'로 처리하는 것은 고도로 스마트화된 현시대를 살아가는 정보주체의 개인정보 자기결정권을 더욱 자유롭고 높은 수준으로 누리는데에는 그 한계가 있다고 볼 수 있다[9].

「개인정보 보호법」 및 같은 법 시행령을 전자적인 형태(즉, 컴퓨터로 구현된) '개인정보 파일' 뿐만 아니라 수기로 관리되더라도 체계성을 가진 형태를 가진 비전자적인 형태의 '개인정보 파일'과 이를 처리하는 개인정보처리자를 수범자로 보고 있기 때문에, '지체 없이'의 기준 시한을 '10 일'로 보는 것이 일면 보편 타당할 수 있다. 하지만, 전자적인 형태의 '개인정보 파일'을 처리하는 개인정보처리자는 정보주체의 처리정지 요청을 최대한 빨리 적용하는 것이

1) 정보주체의 편리성 및 개인정보 자기결정권의 수준을 높일 수 있고,
2) 개인정보처리자의 업무 처리효율 및 법준수의 수준도 높일 수 있다.

따라서, 본 연구에서는 다양한 방식의 '개인정보 파일 처리 환경' 하에서 전자적인 형태의 '개인정보 파일'을 운용하는 개인정보처리자가 정보주체의 '처리정지' 및 '처리정지 취소'(이를, 본 논문에서는 '처리재개'라 한다)에 대한 요구를 '실시간' (또는 '동적'이라 한다) 처리할 수 있는 모델을 제안한다.

4.2 개인정보 파일 처리 환경에 따른 처리정지 요구 반영 모델의 설계

4.2.1 서버에 운영되는 개인정보 파일이 있는 경우

대부분의 클라이언트 앱(애플리케이션, application)에서는 클라이언트 기기(client device) 내에 임시로 저장되는 개인정보 파일이 존재하고, 네트워크를 통해서 이 내용이 서버에 있는 개인정보 파일에 반영되는 구조로 구현된다. 클라이언트 앱은 클라이언트-서버 모델에서 클라이언트 앱일 수도 있으며, 웹서버로부터 웹페이지를 받아 렌더링해서 보여주는 웹브라우저일 수도 있다.

클라이언트 기기의 앱을 사용하는 정보주체(자연인, natural person)가 앱을 시작하는 단계에서는 또는 앱을 사용하는 중에 본인의 개인정보에 대한 처리정지 요청을 클라이언트 기기의 앱에 입력할 수 있다. 또한 처리정지가 된 상태에서 처리를 재개하는 요청을 클라이언트 기기의 앱에 입력할 수도 있다. 이러한 환경에서 개인정보 처리정지/재개가 가능한 모델을 아래와 같이 제안한다.

정보주체의 입력을 받은 클라이언트 기기의 앱은 정상적인 앱 기능에 우선하여 개인정보 처리정지/재개 요청을 처리하도록 설계하고, 이를 위하여 네트워크를 통하여 서버 기기(server device)의 서버 SW(백엔드 SW)가 제공하는 API(Application Programming Interface)를 호출하게 된다. API 는 정보주체의 신원 증명 토큰 및 애플리케이션에 입력된 애플리케이션 고유 키 값(Application Key 또는 Application Token ID), 처리정지 대상이 되는 개인정보 파일 등을 전달인자로 넘겨받게 된다. API 를 통해서 특정 개인정보에 대한 처리정지 또는 처리재개를 요청을 접수한 서버 SW 는 개인정보 파일 내에서 특정 개인정보에 대한 처리정리/재개를 반영한다. 반영된 이후에는 요청이 완료된 상황을 네트워크를 통하여 클라이언트 앱에 응답함으로서, 실시간 개인정보 처리정지/재개하는 인터페이스와 모델이 완성된다.

다만, 여기에서 일부 클라이언트앱의 경우는 네트워크를 통한 개인정보 전송을 실시간으로 수행하지 않고, 배치작업으로 처리하는 경우도 있다. 이러한 경우에는 클라이언트 기기 내 또는 클라이언트 앱 내의 로컬 개인정보 파일이 운영되고 여기에 실시간 개인정보 수집이 이루어진다. 이 경우에 대해서도 본 모델이 정확하게 동작하기 위해서는 로컬 개인정보 파일에 대한 개인정보 처리정지 또는 처리재개를 위한 루틴이 별도로 필요하며, 이러한 루틴은 서버에서 제공하는 API 와 유사한 수준의 함수 설계로 구현이 가능하다.

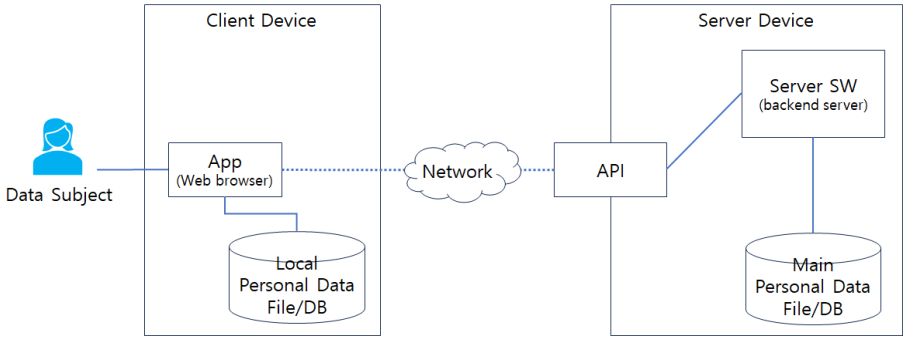

Figure 1. Request Processing Model to suspend the processing personal data in the client-server environment
그림 1. 클라이언트 서버 환경에서의 개인정보 처리정지를 요청 처리하는 모델

앞서 클라이언트 기기의 앱이 네트워크 효율을 위해서 로컬에 개인정보 파일을 별도로 운영할 수도 있다는 것을 설명하였지만, 사실 그러한 경우외에도 네트워크가 단절되어 있는 상황 또는 클라이언트 기기의 전원 사용량을 낮추기 위하여 네트워크 기능을 사용하지 않는 상황도 역시 로컬 개인정보 파일을 운용이 필요한 경우라고 볼 수 있으며 이러한 경우에 개인정보 처리정지/재개는 로컬에서 이루어져야 한다.

그림 1 은 클라이언트 앱과 서버 앱이 네트워크를 거쳐 API 를 통하여 개인정보 처리정지 요청이 전송되는 과정과 그 요청이 수행된 결과를 전송하는 데이터 라인을 도식화한 것이다.

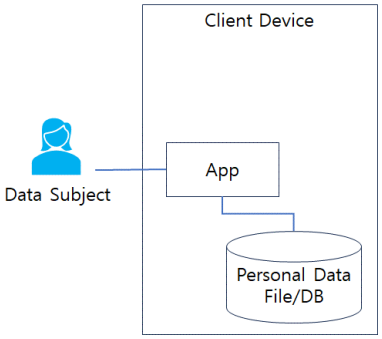

Figure 2. Request Processing Model to suspend the processing personal data in the stand-alone environment
그림 2. 단독 실행 환경에서의 개인정보 처리정지를 요청 처리하는 모델

4.2.2 클라이언트에만 개인정보 파일이 있는 경우

클라이언트 기기 내에서만 개인정보를 수집하고 처리하는 앱의 경우에는 앞선 모델이 유효하지 않다. 따라서 이러한 경우 대한 개인정보 처리정지/재개 모델을 제안한다.

정보주체가 앱사용 중에 본인의 개인정보에 대한 처리정지 요청을 클라이언트 기기의 앱에 입력하였을 때, 앱이 관리하고 있는 개인정보 파일에 해당 정보주체의 개인정보에 해당하는 부분을 처리하는 루틴이 필요하며 이러한 루틴은 앞 절에서 논의된 서버 API 와 유사한 수준의 함수 설계로 구현이 가능하다.

그림 2 는 클라이언트 내에만 개인정보 파일이 있는 경우의 개인정보 처리정지/재개 모델을 도식화한 것이다.

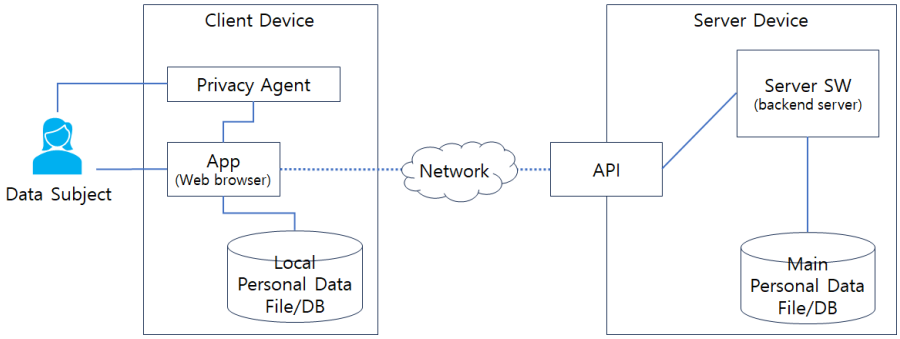

Figure 3. Request Processing Model to suspend the processing personal data in the client-server environment using a privacy agent
그림 3. 클라이언트 서버 환경에서 프라이버시 에이전트를 이용하여 개인정보 처리정지를 요청 처리하는 모델

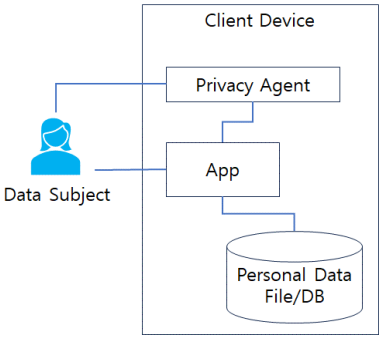

Figure 4 Request Processing Model to suspend the processing personal data in the stand-alone environment using a privacy agent
그림 4. 단독 실행 환경에서 프라이버시 에이전트를 이용하여 개인정보 처리정지를 요청 처리하는 모델

4.2.3 정보주체를 대리하는 에이전트가 존재하는 경우

클라이언트-서버 환경 또는 클라이언트에서만 개인정보 파일을 운용하는 환경에 프라이버시 에이전트(Privacy Agent)를 설계하여 넣는 모델을 제안한다. 프라이버시 에이전트의 역할은 클라이언트 기기 내에 있는 다수의 앱 및 웹브라우저에 대해서 일관성 있는 개인정보 처리정지/재개를 수행하도록 도와주는 특별한 기능의 앱으로서, 기기 관리자 권한을 가지는 앱으로 개발되어야 한다.

프라이버스 에이전트는 iOS 의 쉬리 또는 삼성 갤럭시의 빅스비 루틴과 같은 역할을 통해서,

1) 미리 설정된 조건이 달성이 될 경우 개인정보 처리정지/재개를 시행하거나
2) 인공지능 학습을 통해 정보주체의 개인정보 관리 습관이 반영된 인공지능 모델에 따라 개인정보 처리정지/재개를 시행할 수 있다.

그림 3 및 그림 4 는 각각 클라이언트-서버 환경 및 클라이언트 단독 환경에 프라이버시 에이전트가 설치된 경우에 대한 개인정보 처리정지/재개 모델을 도식화한 것이다.

4.2 관련 법령 준수 분석

본 논문에서 제안된 개인정보 파일 처리 환경에 따른 처리정지 요구 반영 모델(Figure 1~4)들은 현행 국내에서 시행 중인 「개인정보 보호법」 제 37 조 및 같은 법 시행령 제 41 조, 제 44 조에서 제시된 규정인 처리정지 요청의 반영 기한 ‘10 일’을 준수할 뿐만 아니라 실시간으로 처리정지와 처리재개를 해당 앱 또는 서버에 있는 개인정보 파일까지 적용되는 모델들이다.

V. 결론

본 연구는 개인정보 보호 산업의 현황과 미래를 조망하며, 현 시대를 살고 있는 정보주체가 이제까지 경험하지 못한 실시간 및 동적인 개인정보 처리정지 권리보장 효과를 누릴 수 있는 새로운 모델을 제시하였다. 이를 각종 기기에 적용한다면, 우리 나라 개인정보 보호의 법 준수의 수준과 국민 개개인의 개인정보 자기결정권 보장의 수준을 높일 수 있는 중요한 계기와 실효성 있는 기술이 될 것으로 기대된다.

본 연구에서 제시된 모델을 적용하는 앱 또는 웹이 제공하는 이러한 편리성과 높은 수준의 법령 준수 효과는 해당 앱 또는 웹에 대한 신뢰성과 만족도를 높일 수 있을 것으로 예상되며, 해당 앱 또는 웹을 이용하는 고객의 증가와 중장기적 매출 증대를 이끌 수 있는 주요한 전환점이 될 것으로 예상한다.

VI. 감사의 글

본 논문은 2023 년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다 (2021RIS-04).

VII. 참고문헌

[1] Statistics Korea - e-National Indicators: Statistics on the number of personal information infringement reports and consultations (data from the KISA Personal Information Infringement Reporting Center), https://www.index.go.kr/unity/potal/main/EachDtlPageDetail.do?idx_cd=1366

[2] Personal Information Protection Commission, Basic Plan for Personal Information Protection (2024-2026), Press Release, July 3, 2023.

[3] Sae-Hong Cho, "A Study on the Privacy Protection Trends and Policies of Korea - the U.S. - EU," The Journal of Korea Navigation Institute, Vol. 26, No. 4, 244-248, 2022.

[4] Kyu-Yup Lee and Jun-Hyun Um, "Legislative Trends of the U.S. Personal Information Protection

Act: Comparison and Implications with the Korean Revised Act," The World Economy Today, Vol. 2020, No. 1, pp.1-14, 2022.
[5] Ministry of Science and ICT, 2021 Information Protection Survey Report, Jan. 2022.
[6] Korea Internet & Security Agency, Global Information Security Market Trend Report 2021, Dec. 2021.
[7] Sang-Soo Yeo, "Status and Prospects of the Personal Information Protection Industry Ecosystem," Presentation at the 2022 Personal Information Technology Forum Inaugural General Assembly, Sep. 28, 2020.
[8] Korean Law Information Center, "Personal Information Protection Act," [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
[9] Korean Law Information Center, "Enforcement Decree of 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

저자소개

홍윤희 (*Younhee Hong*)

2012 년 8 월 상명대학교 대학원 경제학과 박사
2023 년 3 월~현재 목원대학교 대학원 IT 공학과 박사과정
2023 년 9 월~현재 충남대학교 반도체특성화사업단 교수

관심분야 : 정보보안, 개인정보보호 정책 및 교육, 영재교육, 경제, 환경정책

여상수 (*Sang-Soo Yeo*)

1999 년 2 월 중앙대학교 대학원 컴퓨터공학과 석사
2005 년 8 월 중앙대학교 대학원 컴퓨터공학과 박사
2009 년 3 월~현재 목원대학교 공과대학 컴퓨터공학과 교수

관심분야 : 개인정보보호 기술, 개인정보보호 정책, 정보보안, 정보통신, 디지털 콘텐츠, 생물정보호학, 대학교육혁신