

# 개인정보의 법적·기술적 특성을 고려한 라이프 사이클(Life Cycle) 모델

## The Life Cycle Model Considering Legal and Technical Characteristics of Personal Data

장재영(Jaeyoung Jang)\*, 박태환(Taehwan Park)\*\*, 김범수(Beomsoo Kim)\*\*\*

### 초 록

본 논문은 개인정보의 법적 및 기술적 특성을 고려한 라이프 사이클 모델들을 각각 검토했다. 그리고, 이를 토대로 국내 IT 기업에 적합한 ‘개인정보의 동의·관리 기반 모델’을 제안했다. 본 논문에서 제시한 모델은 기존의 모델이 간과하고 있던 ‘동의’와 ‘관리’ 요소를 모델에 적극 반영했다는 특징이 있다. 본 모델의 타당성은 2가지 방식으로 검증했다. 첫째, IT 기업의 개인정보 라이프 사이클 구성 요소를 파악 후 모델별로 적용하여 ‘동의·관리’ 모델의 우수성을 검증했다. 둘째, 개인정보의 라이프 사이클 전체 프로세스에 ‘동의’와 ‘관리’ 내용이 포함됨을 입증했다. 본 연구 결과를 활용하면 IT 기업이 개인정보 활용 현황을 분석하고 보호 체계를 마련하는데 기여할 수 있을 것으로 기대된다.

### ABSTRACT

This study reviews the life cycle models considering legal and technical characteristics of personal data respectively. Based on the reviews, this research proposes ‘consent and management based model of personal data’ which is applicable to the domestic IT companies. The model suggested in this paper has characteristics that ‘Consent’ and ‘Management’ factors are positively considered, which is overlooked in the other models. The validity of the model is examined by two methods, validation of the model of excellence by contrast of the other models, and ‘consent’ and ‘management’ factors cover all the life cycle processes. Using this model, IT companies will be contributed to the analysis of the personal data utilization and the development of IT system protection.

**키워드 :** 개인정보의 동의·관리 기반 모델, 라이프 사이클, 프레임워크

Consent and Management based Model of Personal Data, Life Cycle, Framework

---

\* 교신저자, 연세대학교 정보대학원 박사과정

\*\* 연세대학교 정보대학원 석사과정

\*\*\* 연세대학교 정보대학원 교수

2012년 05월 17일 접수, 2012년 07월 21일 심사완료 후 2012년 07월 31일 게재확정.

## 1. 서 론

개인정보란 이용자가 서비스를 위해 기업에 제공하는 주민등록번호, 성명, 주소 등의 식별 정보이다. IT 기업들은 이용자가 제공한 개인정보를 회원 인증, 서비스 제공, 민원 처리에 활용하고 있다[1]. 최근에는 데이터 마이닝(Data mining) 기법을 활용하여 이용자의 행태 정보를 생성, 처리하여 마케팅에 활용하는 사례도 증가하고 있다[10, 25].

IT 기업에서 개인정보의 활용은 기업 경영의 중요 요소 중 하나로 부각되고 있다. 하지만, 경쟁기업 및 외부 해커로부터 자사의 개인정보를 보호해야 하는 새로운 상황에 직면하고 있는 것도 주지의 사실이다[31].

이용자의 개인정보를 보호하는 것은 법, 정책 및 기술과 관련된 복잡하고 전문적인 영역이다[16]. IT 기업이 개인정보를 효과적으로 보호하기 위해서는 개인정보 및 개인정보 보호에 대한 체계적이고 종합적인 분석이 선행되어야 한다[3, 12]. 이러한 방법 중 하나가 IT 기업에 의해 개인정보가 수집되어 DB에 저장 및 이용 후 최종적으로 DB에서 파기되는 전체 프로세스를 분석하는 것이다. 개인정보의 전체 프로세스를 체계적으로 분석하는 것 중 하나가 개인정보의 라이프 사이클 모델이다[30, 35]. 현재 개인정보의 라이프 사이클 모델은 IT 기업의 개인정보 보호 대책 수립, 영향평가, 인증, 컨설팅, 내부 관리 계획의 수립 등에 활용되고 있다.

그 동안 개발되어 온 개인정보의 라이프 사이클 모델들은 IT 기업의 개인정보 보호현황을 고려하지 않고 법 또는 기술 등을 단편적으로 고려하여 이를 IT 기업에 바로 적용하기가

곤란하다는 한계가 있었다. 따라서, 본 연구에서는 개인정보의 법적·기술적 특징은 물론 최근 변화하고 있는 개인정보 보호의 기술적 환경을 고려한 라이프 사이클 모델인 ‘개인정보 동의·관리 기반 모델’(이하 ‘동의·관리 모델’이라 한다)에 관한 연구를 진행했다. 이 모델은 개인정보의 라이프 사이클 외에도 전체 라이프 사이클에 기반이 되는 개인정보의 법적 동의(Consent)와 정보보호 등의 기술을 포함한 개인정보 보호 관리(Management)를 동시에 고려하였다.

본 연구의 대상은 ‘정보통신망 이용 촉진 및 정보보호 등에 관한 법률(이하 ‘정보통신망법’이라 한다)에 적용 받는 국내 IT 기업으로 한정했다. 이는 개인정보가 가지는 법적·사회적 특성과 요구하는 보호 수준에 따라 개인정보의 라이프 사이클 모델이 상이하게 나타날 수 있기 때문이다. 따라서, 정보통신망법에 적용을 받지 않는 공공기관 및 준용 사업자 등의 경우에는 이 연구에서 제시한 동의·관리 모델의 적용이 곤란할 수 있다는 한계가 있다.

## 2. 선행 연구

IT 기업이 개인정보를 수집해서 파기하는 전체 영역에서 개인정보를 보호하기 위한 개인정보의 라이프 사이클 모델이나 프레임워크 모델 등에 대한 연구들은 아직 초기 단계이다. 이들 연구들 또한 현재까지 대부분 실무적인 차원에서 이루어져 왔으며 학문적인 분야에서의 연구는 두 영역에서 아주 제한적으로 나타나고 있다. 다만, 상대적으로 프레임워크 연구가 라이프 사이클 모델 연구보다 학계에서의

관심도가 상대적으로 높은 편이다.

<표 1>에 개인정보 프레임워크 관련 대표적인 선행 연구를 정리했다. 그 외에 국내에서는 [7, 13] 등의 연구가 국외에서는 [22, 23, 26] 등의 관련 연구가 있다.

<표 1> 프레임워크 선행 연구

| 프로젝트                       | 주요 내용                                                             |
|----------------------------|-------------------------------------------------------------------|
| PIMI [27]                  | 에릭슨사에서 개발한 모바일 환경에서의 프라이버시 보호 증대를 위한 데이터 보안과 정책 구현을 위한 P3P 기술     |
| PORTIA [17]                | 예일대와 스탠포드대 주관으로 만든 민감 정보 보호를 위한 데이터 마이닝, DB 정책 실행, ID 탈취 방지 체계    |
| ISTPA [21]                 | 시스템 설계에서 보안, 신뢰, 프라이버시 요구 수준을 포함하는 기준을 제시하기 위한 개방형, 정책 설정 모델      |
| Safe Harbor Framework [33] | 미국 기업들이 EU의 개인정보 보호 수준을 맞추기 위해 개발된 적절한 수준의 프라이버시 보호 원칙을 제시한 프레임워크 |
| APEC Framework [15]        | APEC 회원국 간 개인정보를 보호하면서 전자 상거래를 촉진하기 위한 9가지 원칙을 제시한 프레임워크          |

개인정보의 라이프 사이클 모델은 주로 국내에서 개발되었다. 이들 모델들은 국내 개인정보 관련 법률을 설명하거나 IT 기업이나 기관의 개인정보 보호 수준을 인증하기 위한 실무적 방법론으로 개발되었으며, 아직까지 학문적·이론적 체계를 가지고 있지는 못한 수준이다. 라이프 사이클 관련 선행 연구들 또한 모델 개발 또는 타당성 분석이 아닌 실무적으로 개발된 모델에 정보보호 기술을 적용하는 내용들이며, 연구된 성과들도 아주 제한적이다. 현재까지 알려진 개인정보 라이프 사이클 관련 선행 연구는 <표 2>에 정리했다.

<표 2> 라이프 사이클 선행 연구

| 저자                       | 내용                                                                                                   |
|--------------------------|------------------------------------------------------------------------------------------------------|
| 한국정보보호진흥원 [8]            | 개인정보 라이프 사이클을 수집, 저장 및 관리, 이용, 제공, 파기 순으로 정의하고 각 단계별로 필요한 보호 기술을 정의                                  |
| Kang, Lee, and Song [24] | 개인정보 라이프 사이클을 수집, 저장, 관리, 이용, 제공, 파기 순으로 정의하고 각 단계별 적용 가능한 Privacy Enhanced Technologies(PET) 기술을 제시 |

국외에서는 영향평가 등에서 개인정보 흐름을 주요 분석 도구로 활용하고 있다. 그러나 국내에서처럼 별도의 라이프 사이클 모델을 개발하지는 않았다[34]. 예를 들면 미국, 캐나다, 호주, 영국 등은 개인정보의 영향평가 시 개인정보의 흐름 분석을 평가 요소 중 하나로 다루고 있으며, 개인정보 흐름도나 다이어그램을 작성하도록 하고 있다[18~20, 28, 29, 31].

### 3. 연구 수행 방법

본 연구는 선행 연구를 기반으로 총 3단계로 수행했다.

첫째, 국내에서 개발되어 활용되고 있는 개인정보 라이프 사이클 모델들을 법적 기반 모델과 흐름 기반 모델로 분류하여 정리하고 각 모델별 장·단점을 분석했다. 그리고 이들 모델이 가지고 있는 공통적인 한계를 도출했다.

둘째, 각 모델들의 장·단점을 토대로 IT 기업들에 적용되는 정보통신망법과 동 법령상의 보호 조치 항목들을 고려한 새로운 모델인 ‘개인정보의 동의·관리 기반 모델’을 제안했다.

셋째, 제안한 모델의 적합도를 평가하기 위해 국내 주요 IT 기업들이 공통적으로 포함하

고 있는 개인정보의 라이프 사이클 구성 요소를 도출했다. 도출된 개인정보 라이프 사이클 구성 요소에 기존에 개발된 4가지 모델과 새로 제안한 모델을 적용하여 동의·관리 모델의 우수성을 검증했다. 또한 새로 제안한 ‘동의’와 ‘관리’가 전체 라이프 사이클 프로세스에 포함되는 항목임을 입증했다.

#### 4. 개인정보의 라이프 사이클 모델

국내에서 실무적 차원에서 개발되어 IT 기업에 적용되고 있는 개인정보의 라이프 사이클 모델은 사용 목적에 따라 두 가지로 나눌 수 있다. 첫째는 법률적 측면에서 만들어진 ‘CUPD 모델’ 및 ‘PIMS 모델’이다. 둘째는 개인정보의 흐름 측면에서 만들어진 ‘CSUD 모델’ 및 ‘영향평가 모델’이다. 참고로 지금까지 국내에서 활용하고 있는 개인정보의 라이프 사이클은 모델명이 없어서 필자가 논문의 편의를 위해 임의로 이름을 부여했다.

##### 4.1 CUPD 모델

<그림 1>의 수집(Collection)·이용(Use)·제공(Provision)·파기(Deletion) 모델(이하 ‘CUPD 모델’이라 한다)은 정보통신망법의 개인정보 보호 규정의 각 절 제목을 토대로 만들어졌다. 2001년 7월에 개정된 정보통신망법의 개인정보 보호 규정 제 4장은 ‘제 1절 개인정보의 수집’, ‘제 2절 개인정보의 이용 및 제공’, ‘제 3절 이용자의 권리’ 순으로 되어있다. CUPD 모델은 제 1절 제목을 그대로 가져오고 제 2절의 제목을 분리하여 ‘이용’과 ‘제공’ 단계를 만들었다. 마지막으로 라이프 사이클이라는 단어의 의미

를 살리기 위해 제 1절 하단에 있던 파기 부분을 별도로 분리했다.

CUPD 모델은 (舊)한국정보보호진흥원(현, 한국인터넷진흥원)에서 정보통신망법을 쉽게 설명하기 위해 개발되었다. 그러나, 이 모델은 체계적인 연구 없이 개발되어 정형화된 형식이 없고 사용하는 사람들마다 각 단계별 구성이 다르다는 단점이 있다.



〈그림 1〉 CUPD 모델

CUPD 모델의 수집 단계는 수집 시 동의, 개인정보 수집 제한 등의 내용이 포함되어 있다. 이용 단계는 목적 외 이용 금지, 개인 정보관리 책임자의 지정, 개인정보의 보호조치로 구성되어 있다. 제공 단계는 동의 없는 제 3자 제공 금지 및 개인정보 처리 위탁 규정, 영업의 양수 등의 통지 등을 다루고 있다. 마지막으로 파기 단계는 수집 또는 제공 받은 목적을 달성한 때에는 즉시 파기하는 내용으로 이루어져 있다. <표 3>은 CUPD 모델의 세부 구성을 정리한 것이다.

〈표 3〉 CUPD 모델의 세부 구성

| 구 분 | 내 용                                             |
|-----|-------------------------------------------------|
| 수 집 | 개인정보의 수집<br>개인정보의 수집의 제한 등                      |
| 이 용 | 목적 외 이용 금지<br>개인정보관리 책임자 지정<br>개인정보의 보호조치       |
| 제 공 | 동의 없는 제 3자 제공 금지<br>개인정보의 위탁 규정<br>영업의 양수 등의 통지 |
| 파 기 | 개인정보의 파기                                        |

CUPD 모델은 정보통신망법의 개인정보 보호 규정을 기반으로 하고 있다. 이 모델은 개인정보 보호 규정이 처음 만들어질 당시의 모델이므로 모델에 포함되는 세부적인 항목의 수가 적고 라이프 사이클에서 이용과 제공을 구분하고 있다는 것이 특징이다. 반면, CUPD 모델은 일반적인 개인정보 처리 프로세스를 반영하지 못하고 있다. IT 기업의 개인정보 흐름은 일반적으로 수집·저장·이용·파기 순이다. 특히, 개인정보의 흐름 단계 중 저장 단계를 라이프 사이클 모델에 포함시키지 않고, 이용 단계의 하위 개념에 포함시키고 있는 것은 문제이다. 이렇게 되면 CUPD 모델을 적용할 경우 SK Communications, 농협, Nexon, 현대캐피탈 등의 외부자에 의한 해킹 사고가 개인정보 이용 과정에서 발생한 것으로 잘못 해석될 수 있다. 또한, 개인정보 보호에서 가장 중요한 동의 부분이 모델에서 다루어 지지 않고 있다. 동의는 개인정보 보호의 가장 중요한 원칙 중 하나이다. CUPD 모델에서는 파기 단계를 개인정보의 이용 목적 달성 후 파기하는 경우로 한정된 것도 문제이다. 1999년 7월 정보통신망법의 개인정보 조항이 처음 만들어졌을 때 이미 이용자가 동의를 철회할 경우 수집한 개인정보를 지체 없이 파기하도록 하고 있다.

#### 4.2 개인정보 보호관리체계(PIMS) 모델

CUPD 모델은 개발 당시에는 유용했을지 모르지만 2007년 1월 26일에 정보통신망법이 전면 개정되면서 활용도가 떨어졌다. 최근에는 개정된 법령을 반영한 개인정보 보호관리체계(Personal Information Management Systems

(PIMS), 이하 'PIMS'라 한다) 모델을 더 많이 사용하고 있다. PIMS란 IT 기업이 개인정보를 자율적으로 관리할 수 있도록 만든 인증 체계이다. PIMS에서는 사업자가 개인정보 보호 수준을 인증하는 방법으로 <그림 2>의 개인정보의 라이프 사이클 모델을 활용하고 있다. PIMS 모델은 CUPD 모델과 같이 정보통신망법의 개인정보 보호 규정을 설명하기 위해 만들어졌다. CUPD 모델은 라이프 사이클이라는 단어의 의미를 살리기 위해 당시의 정보통신망법 제 4장 제 1절 하단의 파기 부분을 라이프 사이클에 포함시켰다. 반면, PIMS 모델은 정보통신망법의 개인정보 보호 규정의 각 절 제목을 수정 없이 라이프 사이클에 반영했다. 정보통신망법이 2007년에 개정되었을 때 절의 제목은 '제 1절 개인정보의 수집·이용 및 제공 등', '제 2절 개인정보의 관리 및 파기 등'이다.



〈그림 2〉 PIMS 모델

PIMS 모델은 개인정보를 수집(Collection)·이용(Use)/제공(Provision)·관리(Management)/파기(Deletion)하는 3단계로 되어있다. 개인정보 수집 단계는 최소의 개인정보 수집, 중요(민감)정보 수집 제한, 간접 수집 시 조치, 정보주체의 동의, 법정대리인의 동의획득 및 고지, 동의기록 보관, 취급방침 마련 등으로 되어 있다. 개인정보 이용/제공 단계는 목적 내 개인정보 이용, 이용자의 불만 처리, 열람 정정 요구권 보장 및 처리, 동의 철회, 이용자

고지 및 동의, 위탁자 책임, 제 3자 제공 시 동의, 제 3자 보안 관리, 개인정보 이전 시 보호 조치, 해외 이전 시 보호조치 등을 포함하고 있다. 마지막으로 관리/파기 단계는 개인정보 파기 시 내부 규정을 마련하고 이에 따라 개인정보의 수집 목적이 달성된 경우 개인정보를 안전한 방법으로 지체 없이 파기하는 내용을 담고 있다[5]. <표 4>는 PIMS 모델의 세부 항목을 정리한 것이다.

PIMS 모델은 사업자가 정보통신망법의 의무

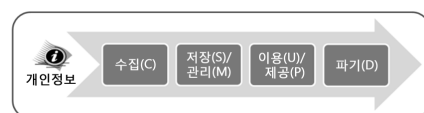
<표 4> PIMS 모델의 세부 구성

| 구 분     | 내 용                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 수 집     | 최소한의 정보 수집<br>중요 정보 수집 제한<br>간접 수집 시 조치<br>정보주체의 동의<br>법정대리인 동의획득 및 고지<br>동의기록 보관<br>개인정보취급방침                                                                                                                                                       |
| 이용/제공   | 목적 내 개인정보 이용<br>이용자의 불만 처리<br>열람정정 요구권 보장 및 처리<br>동의철회<br>이용자 요청의 처리<br>이용자 고지 및 동의<br>위탁자 책임<br>외부위탁관리 감독<br>외부위탁계약 관련사항<br>제 3자 제공 시 동의<br>제공받은 개인정보의 관리<br>제 3자 보안관리<br>제 3자 제공 시 계약 관련사항<br>개인정보 이전 시 보호조치<br>개인정보 이전 받을 시 보호조치<br>해외 이전 시 보호조치 |
| 관 리/파 기 | 개인정보의 저장 및 관리<br>파기규정<br>파기시점<br>파기방법<br>목적 달성 후 보유                                                                                                                                                                                                 |

사항을 준수하고 있는 지를 인증하기 위해 개발되었다. PIMS 모델은 최근에 개발되어 현행 정보통신망법의 내용을 가장 잘 반영하고 있는 모델이기도 하다. 이 모델은 기존의 4단계 모델을 1단계 줄인 3단계로 되어 있다. 따라서, 개인정보의 라이프 사이클 모델 중 가장 단순한 모델이다. 수집하는 개인정보에 간접 수집 시 조치 사항을 두어 쿠키, 위치정보 등 동적인 정보를 포함하여 수집 단계의 정보를 구체화 했다는 장점을 가지고 있다. 반면, PIMS 모델은 CUPD 모델과 동일한 단점을 가지고 있다. 최근에 개발된 모델임에도 개인정보에서 정보보호 기술이 차지하는 중요성을 간과하고 있기도 하다. 행태정보의 생성, SNS 이용의 보편화, 스마트폰 대중화에 따른 위치정보 정확도 증가와 같은 최근의 개인정보 현상 또한 반영하고 있지 못한 모델이다[9].

#### 4.3 CSUD 모델

<그림 3>의 수집(Collection)·저장(Storage)/관리(Management)·이용(Use)/제공(Provision)·파기(Deletion)모델(이하 ‘CSUD 모델’이라 한다)은 개인정보 보호 기술의 중요성이 부각되던 시기에 개발되었다[4]. CSUD 모델은 현재 ‘개인정보 생명주기별 보안 관리모델’로 한국정보통신기술협회 단체 표준으로 제정되어 있는 모델이기도 하다[11].



<그림 3> CSUD 모델

CSUD 모델은 개인정보의 라이프 사이클을 4단계로 분류하고 있다. 수집 단계는 인터넷 서비스 이용자의 서비스 이용신청과 동시에 자신의 개인정보를 IT 기업에게 제공하는 단계이다. 수집되는 개인정보는 성명, 연락처 등의 정적 정보 외에 위치정보, 인터넷 접속 기록 등의 동적 정보를 포함하고 있다. 저장/관리 단계는 수집된 개인정보를 DB 등에 저장하고 개인정보보호정책에 따라 허가 받은 자만이 해당 개인정보에 접속할 수 있는 권한 관리 등을 다루고 있다. 이용/제공 단계는 개인정보 소유자의 개인정보를 여러 가지 필요에 의해 이용하는 것으로 위탁업체나 제휴업체 등 제 3자에게 제공하는 내용을 포함하고 있다. 마지막으로 파기 단계는 해당 개인정보의 보유기간이 종료하여 파기하는 것을 말한다. 정적인 개인정보는 서비스 탈퇴 이후 동적인 개인정보는 전체 서비스 탈퇴 시점이 아닌 요청한 서비스가 종료되는 시점에 파기하는 것을 말한다. <표 5>는 CSUD 모델의 세부 내용을 정리한 것이다.

<표 5> CSUD 모델의 세부 구성

| 구 분   | 내용                                      |
|-------|-----------------------------------------|
| 수집    | 서비스 이용신청과 함께 제공되는 정보(정적 및 동적 정보를 포함)    |
| 저장/관리 | 개인정보를 DB에 저장<br>허가 받은 자만이 개인정보에 접속      |
| 이용/제공 | 서비스 이용<br>제 3자 제공과 위탁                   |
| 파기    | 보유기간 종료 후 파기<br>(정적 정보는 해당 서비스 종료 후 파기) |

CSUD 모델은 CUPD 모델과 달리 개인정보의 흐름을 기반으로 만들어졌다. 또한, 정보

통신 단체표준으로 되어 있어 개인정보의 라이프 사이클 모델 중 공신력이 가장 높다. 이 모델은 정보보안 관리 모델을 위해 개발된 모델이므로 사업자의 보안 수준을 평가하고 정보보호 관점에서 필요한 조치를 취하기 쉽다는 장점이 있다. PIMS 모델과 같이 쿠키, 위치정보 등 동적인 정보를 포함하여 수집 대상을 확장하기도 했다. 또한 CUPD 모델에서 간과하고 있는 저장과 관리 단계를 강조했다라는 점이 특징이다. 이 모델을 적용할 경우 IT 기업 입장에서는 DB 보안 솔루션, 개인정보에 대한 접근 권한 등 정보보호 기술의 적용이 쉽고, 해킹, 취급 부주의 등 보안 사고에 대한 분석 및 대응이 용이하다. 반면, CSUD 모델은 프로세스만을 고려하여 개인정보의 법적 특성을 설명하기 어렵다는 단점이 있다. 특히, 모델의 세부 사항은 너무 일반적인 사항으로 구성되어 개인정보 보호 규정 적용을 위해서는 별도의 법률 검토가 필요하다. 저장과 관리를 같은 단계에서 설명하고 있어 개인정보의 수집, 이용/제공, 파기 단계에서의 보안 등 기술적인 관리 부분을 간과하고 있는 점 또한 문제이며 CUPD 모델과 같이 개인정보의 동의와 철회 부분을 설명하지 못하고 있다는 단점도 가지고 있다.

#### 4.4 개인정보 영향평가 모델

개인정보 영향평가(Privacy Impact Assessment(PIA))란 개인정보를 활용하는 새로운 개인정보 처리 시스템의 도입 및 기존 시스템의 중대한 변경 시 시스템의 구축·운영이 고객 및 국민의 프라이버시에 미칠 영향에 대하여 미리 조사·분석·평가하는 체계적인 절차이다[9].

개인정보 영향평가는 개인정보 파일을 신규 구축하거나, 기존에 구축된 개인정보 파일의 취급 절차를 변경하거나, 개인정보 파일을 타 기관과 연계·제공하는 경우 등에 사용된다. ‘개인정보 영향평가 모델’은 CSUD 모델과 같이 개인정보의 흐름을 기반으로 한다. <그림 4>와 같이 이 모델은 수집(Collection)·보유(Retention)·이용(Use)/제공(Provision)·파기(Deletion) 단계로 되어있다. 또한, 2011년 9월 통합 ‘개인정보 보호법’ 제정으로 인해 모든 공공기관은 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향평가를 하도록 되어 있어 최근에 활용도가 가장 높은 모델이다[5].



〈그림 4〉 개인정보 영향평가 모델

개인정보 영향평가 모델에서는 개인정보의 라이프 사이클을 수집·보유·이용/제공·파기의 4단계로 구분하고 있다[14]. 개인정보 수집 단계는 정보 주체의 개인정보를 취득하는 단계로서 통상적인 웹사이트 회원 가입, 서면 신청서 작성, 민원 접수 등을 포함하고 있다. 보유 단계는 수집한 개인정보를 보유하는 단계로서 보유한 개인정보를 안전하게 관리하며 정보 주체의 개인정보 열람·정정 권리의 보장 등의 내용으로 되어 있다. 이용/제공 단계는 취득·저장한 개인정보를 수집한 공공기관 외의 제 3의 기관에게 정보를 제공하는 행위 등을 포함한다. 마지막으로 파기 단계는 수집 및 이용 목적이 달성된 개인정보를 파기하는 단계이다.

<표 6>은 ‘영향평가 모델’의 세부 내용이다.

〈표 6〉 영향평가 모델의 세부 구성

| 구 분   | 내용                            |
|-------|-------------------------------|
| 수집    | 웹 사이트 회원 가입<br>서면 신청서 작성      |
| 보유    | 개인정보의 안전한 관리<br>개인정보 열람·정정 권리 |
| 이용/제공 | 취득·저장 개인정보의 제 3자 제공           |
| 파기    | 수집 및 이용 목적 달성 정보의 파기          |

개인정보 영향평가 모델은 CSUD 모델과 같이 개인정보의 흐름을 기준으로 만들어졌다. 이 모델은 IT 기업 측면에서 자사의 시스템 전반을 분석하고 보안 등 대책을 수립하는데 활용도가 높다. 특히, 보유라는 개념에 저장과 관리를 모두 포함시켜 CSUD 모델에 비해 모델을 단순화 시켰다. 개인정보의 라이프 사이클 모델 중에 개인정보의 흐름을 가장 잘 표현하고 있는 모델이기도 하다. 반면, 영향평가 모델은 PIMS 모델과 같이 IT 기업에 의한 개인정보 생성을 다루고 있지 않다. 개인정보의 동의와 이용자 권리 부분인 철회 절차도 누락되어 있다. 보안 측면에서 만들어진 모델임에도 보안을 보유 단계에만 국한시켜 수집·이용/제공·파기 단계에서의 보안의 역할을 간과하고 있다는 단점도 있다.

CUPD 모델과 PIMS 모델은 법률에 기반하여 만들어져 법률 적용이 쉬우나 프로세스 이해도가 떨어지는 단점이 있다. CSUD 모델과 개인정보 영향평가 모델은 개인정보 흐름 기반으로 만들어져 프로세스 이해도는 높으나 정보통신망법 상의 개인정보 보호 규정들과 연결시켜서 설명하기가 어렵다. 또한, 본 장에서 설명한 4개의 라이프 사이클 모델 모두



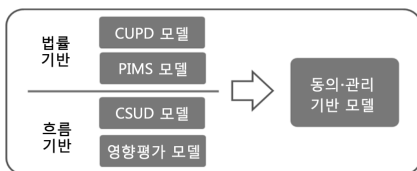
〈표 7〉 라이프 사이클 모델 비교

| 모델   | 장점                            | 단점                           | 고려 분야 | 공통적 한계                                             |
|------|-------------------------------|------------------------------|-------|----------------------------------------------------|
| CUPD | 법률 적용이 쉬움<br>모델이 단순함          | 저장 단계 설명이 곤란<br>프로세스 이해도가 낮음 | 법률측면  | ‘동의’와 ‘철회’를<br>모델 구성에 포함<br>하지 않고 세부 설<br>명에 일부 포함 |
| PIMS | 법률 적용이 쉬움<br>최신 법률 개정 사항을 반영  | 프로세스 이해도가 낮음                 |       |                                                    |
| CSUD | 프로세스 이해도가 높음<br>보안 기술 적용도가 높음 | 법률 적용이 곤란                    | 흐름측면  | 모든 단계와 관련<br>된 보안 문제를 제<br>한적인 단계에서만<br>설명         |
| 영향평가 | 프로세스 이해도가 높음<br>보안 기술 적용도가 높음 | 법률 적용이 곤란                    |       |                                                    |

동의와 철회를 모델에서 설명하고 있지 않고, 보안 및 관리 이슈를 제한된 영역에서만 설명하고 있다는 단점이 있다. <표 7>은 지금까지 설명한 개인정보의 라이프 사이클 모델의 장·단점을 정리한 것이다.

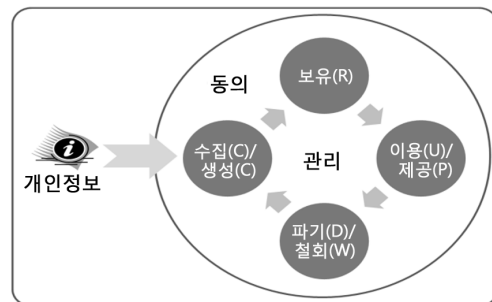
## 5. 개인정보의 동의·관리 기반 모델

제 4장에서 살펴본 개인정보의 라이프 사이클 모델 중 개인정보의 법적·기술적 특성을 모두 반영하고 있는 모델은 없다. 따라서, 새로운 모델은 법률과 개인정보의 흐름은 물론 보안을 포함한 관리까지를 고려한 ‘개인정보의 동의·관리 기반 모델’로 발전하는 것이 바람직하다. <그림 5>는 개인정보의 라이프 사이클 모델의 발전 방향이다.



〈그림 5〉 라이프 사이클 모델의 발전 방향

동의·관리 기반 모델은 개인정보 흐름 기반 모델의 일반적 프로세스인 수집·보유·이용·파기 단계를 기반으로 한다. 여기에 최근의 정보보호 기술 발전 방향을 고려하여 일부 항목을 수정·보완한 모델을 제시했다. 이전 모델에서 중요하게 고려하고 있지 않은 동의와 관리를 라이프 사이클 전체와 연관 지어 설명했다. 파기 부분에서 간과하고 있는 이용자의 동의 철회 부분은 파기 부분에서 같이 기술했다. <그림 6>은 개인정보 동의·관리 기반 모델 개념도이다.



〈그림 6〉 개인정보의 동의·관리 기반 모델

동의·관리 기반 모델은 세부적으로 다음과 같이 기술할 수 있다.

**수집/생성 단계** : 기존 모델에서는 수집을 이용자가 제공하는 개인정보 만으로 국한시켰다. 그러나 IT 기업은 이용자 PC의 쿠키정보를 수집하거나 검색결과, 접속지 IP, 스마트폰 위치 등의 행태정보를 수집하고 있다. 따라서, 수집 단계에서는 이용자에 의한 수집 외에 사업자가 타겟 마케팅과 회원 관리를 위한 개인정보 생성까지도 포함시키는 것이 바람직하다.

**보유 단계** : 이용자 또는 타인으로부터 제공된 개인정보는 IT 기업의 DB에 저장된다. 이 외에 IT 기업은 이용자를 프로파일링하여 새로운 개인정보를 생성하기도 한다. 일부 모델에서는 보유 단계를 저장 또는 보유로 정의하고 있다. 두 단어의 사전적인 차이는 거의 없으나 이 논문에서는 IT 기업이 능동적으로 개인정보를 생산하는 내용이 포함되어 있으므로 저장보다는 ‘보유’를 사용하기로 한다.

**이용/제공 단계** : 이용 단계에서는 IT 기업이 자사의 서비스 등을 위해 개인정보를 이용하는 단계이다. 차이가 있다면 이전의 모델에서는 서비스만을 위한 것으로 이용 단계를 제한했으나 최근에는 개인정보의 생성을 위해서도 개인정보를 이용하고 있다는 점이다. IT 기업의 개인정보 활용이 증가함에 따라 제공 단계도 복잡해지고 있다. 그러나 이전 모델에서 설명하고 있는 개인정보의 이용과 위탁, 제 3자 제공의 범주 안에 포함되는 수준이다.

**파기/철회 단계** : 사업자가 수집·저장·이용/제공한 개인정보는 목적이 달성되면 파기해야 한다. 이 외에도 이용자의 철회 요구에 의해 개인정보 수집·이용/제공 목적이 달성

되지 않았음에도 불구하고 해당 개인정보를 파기해야 하는 경우도 있다. 이 경우도 개인정보를 복구할 수 없도록 완전히 파기해야 한다. 파기와 철회는 사용하는 목적이 다르므로 파기와 철회 둘 다 본 단계에 포함시키는 것이 바람직하다.

전체 라이프 사이클 모델에서 빠져 있거나 일부만 표현하고 있는 동의와 관리를 새로 제안한 본 모델에 반영했다. 동의와 관리는 라이프 사이클 전반과 관련이 있다.

‘동의’는 개인정보 수집 과정 중 일부로 생각하는 경우가 많다. 그러나 수집 단계 외에 이용 단계에서는 제 3자 제공 및 위탁 단계에서 동의하고, 삭제 단계의 경우도 이용 목적이 달성된 개인정보의 파기도 동의와 관련이 있다. 정보통신망법 제22조에서도 개인정보 수집 시 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간을 명시하고 동의를 받도록 하고 있다. 수집·이용 목적은 개인정보의 라이프 사이클의 이용·제공 단계에 해당한다. 개인정보의 보유·이용 기간은 저장·파기 단계에 해당한다.

‘관리’는 개인정보의 저장 단계 중 일부로 간주하는 경우가 많다. 그러나 개인정보 수집 시는 개인정보의 해킹 방지를 위해 Secure Socket Layer(SSL) 또는 TLS(Transport Layer Security(TLS) 등의 기술이 적용된다. 이용 단계에서의 SSL/TLS 적용 및 취급 사업자에 대한 관리, 개인정보 제공 시 기술적 조치 항목도 관리에 해당한다. 삭제의 경우도 DB에서의 개인정보 삭제는 물론 저장 매체인 하드디스크 파괴, 문서 파쇄 등이 관리와 관

련이 있다. 따라서, 동의와 관리는 라이프 사이클 전반을 포함할 수 있도록 모델을 구현하는 것이 바람직하다.

관리의 대부분이 정보보호와 관련이 되어 있으므로 보안 또는 정보보호라는 용어를 사용할 수도 있다. 그러나, 취급 사업자 관리 및 현행법상 기술적 조치 외에 관리적 조치도 의무화하고 있으므로 포괄적인 의미인 관리를 사용하는 것이 타당하다.

모델의 구성에 있어서는 라이프 사이클의 의미를 살리고, 동의는 외부, 관리는 내부와 관련이 있다는 것을 강조하는 측면에서는 모델을 원형으로 구현하는 것이 바람직해 보인다. 다만, 이는 편의상의 구분으로 동의나 관리는 IT 기업 환경의 내·외부 모두와 관계가 있는 요소이다.

## 6. 동의·관리 기반 모델의 타당성 검증

‘개인정보의 동의·관리 기반 모델’의 타당성 검증은 2가지 단계로 진행했다. 우선, IT 기업의 개인정보 라이프 사이클 구성 요소를 기존의 4가지 모델과 동의·관리 기반 모델의 각 단계에 적용했을 때 얼마나 많은 부분이 포함되는지를 확인하여 동의·관리 기반 모델의 우수성을 검증했다. 둘째, 개인정보의 라이프 사이클 전체 프로세스에 ‘동의’와 ‘관리’ 항목이 포함됨을 증명했다.

### 6.1 구성 요소 검증

기존에 개발된 4개의 개인정보의 라이프 사이클 모델과 새로 제안한 ‘개인정보의 동

의·관리 모델 기반 모델’이 IT 기업의 개인정보 라이프 사이클 분석에 적용 시 우수성 및 타당성을 파악하기 위해 국내 IT 기업의 개인정보취급방침을 토대로 IT 기업의 일반적인 개인정보 라이프 사이클 구성 요소를 조사했다.

국내 IT 기업의 일반적인 개인정보 라이프 사이클 구성 요소 도출을 위한 표본은 웹 사이트 분석 평가 사이트인 랭키닷컴([www.rankey.com](http://www.rankey.com))의 국내 인터넷 접속자 순위를 기준으로 했다. 국내 인터넷 사이트 접속 순위는 2012년 6월 26일 기준으로 최상위 50개 사이트를 조사 대상으로 선정했다. 다만, 정보통신망법에 따른 개인정보취급방침의 규칙을 따르지 않고 있는 국외 웹사이트인 페이스북, 구글, 유튜브, 트위터는 조사 대상에서 제외하여 총 46개 IT 기업을 조사했다. 조사 대상 기업은 <표 8>과 같다.

조사 결과 <표 9>와 같이 개인정보 라이프 사이클 구성 요소가 도출됐다. 도출된 요소는 총 14개이다. 세부적으로 이용자의 개인정보가 제공되는 방식에 따라 2개 요소(회원가입, 서비스 이용), IT 기업이 개인정보를 저장 및 관리하는 2개 요소, 활용하는 목적에 따라 8개 요소, IT 기업에서 개인정보가 삭제되는 사유에 따라 2개 요소가 도출되었다.

개인정보의 라이프 사이클 요소는 이용자 측면에서 회원가입 시 제공하는 개인 식별 정보와 서비스 이용 중 제공하는 IP, MAC 주소, 쿠키, 위치정보 등이 있다. 또한 IT 기업에서는 타깃마케팅을 위한 개인행태 정보 생성이나 회원의 이용 기록을 통해 부정 이용 또는 비인가 사용 방지를 위한 정보 등을

〈표 8〉 개인정보취급방침에 따른 라이프 사이클 요소 조사 대상 IT 기업

| 순위 | 사이트명   | 대상 | 순위 | 사이트명    | 대상 | 순위 | 사이트명     | 대상 |
|----|--------|----|----|---------|----|----|----------|----|
| 1  | 네이버    | ○  | 18 | 머니투데이   | ○  | 35 | 신한은행     | ○  |
| 2  | 다음     | ○  | 19 | zum     | ○  | 36 | SBS      | ○  |
| 3  | 네이트    | ○  | 20 | 파란      | ○  | 37 | GS SHOP  | ○  |
| 4  | 싸이월드   | ○  | 21 | 인터파크    | ○  | 38 | 서울경제신문   | ○  |
| 5  | G마켓    | ○  | 22 | 아시아경제   | ○  | 39 | Youtube  | ×  |
| 6  | 옥션     | ○  | 23 | 쿠팡      | ○  | 40 | 파이낸셜뉴스   | ○  |
| 7  | 페이스북   | ×  | 24 | 야후!코리아  | ○  | 41 | 일간스포츠    | ○  |
| 8  | 11번가   | ○  | 25 | 서울신문    | ○  | 42 | 스포츠동아    | ○  |
| 9  | Google | ×  | 26 | 경향닷컴    | ○  | 43 | 잡코리아     | ○  |
| 10 | 조선닷컴   | ○  | 27 | 우리은행    | ○  | 44 | 트위터      | ×  |
| 11 | 매일경제   | ○  | 28 | NH농협    | ○  | 45 | 와우넷      | ○  |
| 12 | 한국경제   | ○  | 29 | 헤럴드경제   | ○  | 46 | CJmall   | ○  |
| 13 | 조인스MSN | ○  | 30 | MBN     | ○  | 47 | Olleh    | ○  |
| 14 | KB국민은행 | ○  | 31 | 스포츠조선   | ○  | 48 | 그루폰코리아   | ○  |
| 15 | 티스토리   | ○  | 32 | 롯데닷컴    | ○  | 49 | 위메이크프라이스 | ○  |
| 16 | 한국닷컴   | ○  | 33 | 세계닷컴    | ○  | 50 | 신세계      | ○  |
| 17 | 동아닷컴   | ○  | 34 | 스포츠서울닷컴 | ○  |    |          |    |

생성하는 것으로 나타났다. 조사대상 기업들은 개인정보를 DB에 저장하여 기술적 보호 조치 수행 등 개인정보를 관리하고 있었다. 이용 측면에서는 회원 인증, 마케팅, 불만처리 등을 공통적인 요소로 하고 있었다. 다만, IT 기업들의 사업 특성에 따라 요금정산, 대금결제, 물품 배송 등의 요소가 다르게 나타나는 기업들이 있었다. IT 기업들은 모두 개인정보의 이용목적이 달성되거나 회원 등이 탈퇴하는 경우 일정 기간을 두고 개인정보를 삭제하는 것으로 나타났다. 또한 IT 기업들은 개인정보를 제 3자에게 제공할 때는 법에 따른 위탁과 제공을 구분하고 있는 것으로 나타났다.

국내 IT 기업의 개인정보 라이프 사이클 구성 요소를 도출한 결과를 토대로 기존의 4

〈표 9〉 IT 기업의 개인정보 라이프 사이클 구성 요소

| 구 분   | 이용자    | IT 기업           | 제 3자 |
|-------|--------|-----------------|------|
| 수집    | 회원가입   | -               | -    |
|       | 서비스 이용 | -               | -    |
| 생성    | -      | 타겟마케팅           | -    |
|       | -      | 회원 관리           | -    |
| 보유    | -      | DB 저장           | -    |
|       | -      | 관리              | -    |
| 이용/제공 | -      | 회원인증            | -    |
|       | -      | 서비스 이용/<br>요금정산 | -    |
|       | -      | 마케팅(광고)         | -    |
|       | -      | 불만처리            | -    |
|       | -      | -               | 위탁   |
|       | -      | -               | 제공   |
| 파기/철회 | 탈퇴     | -               | -    |
|       | -      | 이용목적달성          | -    |

〈표 10〉 IT 기업의 개인정보 라이프 사이클 구성 요소에 대한 모델별 포함 항목 비교

| 구성 요소       | CUPD | PIMS  | CSUD  | 영향평가  | 동의 · 관리 |
|-------------|------|-------|-------|-------|---------|
| 회원가입        | 수집   | 수집    | 수집    | 수집    | 수집/생성   |
| 서비스 이용      |      |       |       |       |         |
| 타겟마케팅       |      |       |       |       |         |
| 회원 관리       |      |       |       |       |         |
| DB 저장       |      | 관리/파기 | 저장/관리 | 보유    | 관리      |
| 관리          | 이용   |       |       |       |         |
| 회원인증        |      | 이용/제공 | 이용/제공 | 이용/제공 | 이용/제공   |
| 서비스 이용/요금정산 |      |       |       |       |         |
| 마케팅(광고)     |      |       |       |       |         |
| 불만처리        |      |       |       |       |         |
| 위탁          | 제공   |       |       |       |         |
| 제공          |      |       |       |       |         |
| 탈퇴          |      | 관리/파기 |       |       | 탈퇴/파기   |
| 이용목적 달성     | 파기   |       | 파기    | 파기    |         |
| 계           | 9    | 12    | 11    | 10    | 14      |

개 모델과 동의·관리 기반 모델의 적합도를 분석했다.

분석 결과 동의·관리 기반 모델만이 국내 IT 기업의 개인정보 라이프 사이클 구성 요소를 모두 포함하고 있으며, PIMS 모델이 IT 기업의 개인정보를 생성하는 부분을 누락하여 12개 요소를 포함하고 있었다. CSUD 모델 또한 IT 기업의 개인정보 생성 부분을 누락하고 있었다. 이 외에도 개인정보의 탈퇴 부분을 다루고 있지 않아 총 3가지 요소를 누락하여 11개 요소를 포함하고 있었다. 다음으로는 영향평가 모델이 CSUD 모델의 3가지와 개인정보가 서비스 이용 중에 수집되는 것을 포함하지 않아 4개를 누락한 10개 요소를 포함하고 있었다. 마지막으로 CUPD 모델이 영향평가 모델이 포함하고 있지 않은 모델에 이어 개인정보의 저장 부분을 포함하고

있지 않아 총 5개를 누락한 9개 요소만을 포함하고 있었다. <표 10>에서 음영으로 처리되어 있는 부분이 IT 기업의 개인정보 라이프 사이클 요소 중 해당 모델이 포함하고 있지 않은 부분이다.

이번 검증을 통해 ‘동의·관리 기반 모델이 IT 기업의 개인정보 라이프 사이클 구성 요소를 가장 정확히 포함하고 있음은 물론 유일하게 모든 항목을 포함하고 있음이 증명됐다.

## 6.2 동의·관리 항목의 전체 프로세스 관련성 검증

동의와 관리 항목이 개인정보의 라이프 사이클 전체 프로세스와 관련되어 있다는 것을 밝히기 위한 방식으로는 IT 기업이 준수해야

하는 정보통신망법 및 동법의 보호조치 내용을 담고 있는 개인정보의 기술적·관리적 보호 조치 기준을 활용했다[2].

‘개인정보의 동의·관리 기반 모델’의 각 프로세스를 기준으로 정보통신망법과 개인정보의 기술적·관리적 보호 조치 항목들을 분류했다. 이를 통해 전체 프로세스에 법적 ‘동의’와 기술적 ‘관리’ 관련 항목이 모두 존재한다는 사실을 <표 11>과 같이 밝혔다.

‘동의’의 경우 수집·이용·제공 등의 동의 철회권 및 법정 대리인의 동의는 라이프 사이클 전체를 포함하고 있고, 수집 시 사전동의는 수집/생성 단계, 보유 및 이용 기간, 보유 항목은 보유 단계, 제 3자 제공 동의 및

취급위탁 시 동의는 이용/제공 단계, 이용목적 달성 후 파기는 파기/철회 단계의 ‘동의’ 사항에 해당한다.

‘관리’의 경우 관리 책임자 지정, 취급방침 공개, 고충처리, 누설 금지, 취급자 최소화, 내부관리계획의 수립, 백신소프트웨어 설치 등은 전체 프로세스와 관련이 있으며, SSL과 비밀번호 생성 규칙 설정은 수집/생성 단계, DB 암호화 등은 보유단계, 취급사업자 관리·감독은 이용/제공 단계, DB 삭제, HDD 파괴 등은 파기/철회 단계의 ‘관리’ 분야에 포함됨을 알 수 있다.

이를 통해 ‘동의’와 ‘관리’가 전체 프로세스와 연관성이 있음을 증명했다.

<표 11> 동의·관리 기반 모델의 프로세스에 따른 정보통신망법 및 보호조치 항목 분류

| 구 분         |    | 수집/생성                                                                  | 보유                                                  | 이용/제공                                                                                                                                                               | 파기/철회                                                                       |
|-------------|----|------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 정 보 통 신 망 법 | 조항 | 주민번호 등<br>민감정보 수집 금지<br>최소정보 수집<br>주민번호 대체<br>수단 마련<br>접속정보파일 자동<br>생성 | 개인정보 누출 통지제<br>목적 달성된<br>개인정보 별도 보관                 | 목적 외 이용 금지<br>필수정보 외 수집 시<br>서비스 제공 거부 금지<br>주민번호 이용 금지<br>취급위탁사실 고지<br>양수양도에 따른<br>개인정보 이전<br>국외 개인정보 이전<br>수탁자의 손해배상<br>책임 의제<br><br>이용내역 통지<br>열람 및 제공 오류의<br>수정 | 파기 절차 및 방법<br>이용기간 통보제<br>이용 및 보유기간 후<br>즉시 삭제<br><br>이용 철회 요구 시<br>개인정보 삭제 |
|             | 동의 | 수집 · 이용 · 제공 등의 동의 철회권, 법정 대리인의 동의                                     |                                                     |                                                                                                                                                                     |                                                                             |
|             |    | 수집 시 사전 동의                                                             | 보유 및 이용 기간,<br>보유 항목                                | 제3자 제공 동의<br>취급위탁 시 동의                                                                                                                                              | 이용목적 달성 후 파기                                                                |
| 보 호 조 치 기 준 | 조항 | SSL<br>비밀번호 생성<br>규칙 설정                                                | DB 암호화<br>차단 시스템의 설치<br>주민번호 저장금지<br>접속기록 위 · 변조 방지 | SSL<br>취급사업자<br>관리 · 감독                                                                                                                                             | DB 삭제<br>HDD 파괴<br>문서 파쇄                                                    |
|             | 공통 | 관리 책임자 지정, 취급방침 공개, 고충처리, 누설 금지, 취급자 최소화,<br>내부 관리계획의 수립, 백신소프트웨어 설치   |                                                     |                                                                                                                                                                     |                                                                             |

## 7. 결 론

이 연구에서 검토한 CUPD 모델과 PIMS 모델은 규제 기관 입장에서 법률을 설명하거나 적용하기 위해 개발되었다. CSUD 모델과 개인정보 영향평가 모델은 IT 기업이 정보보호 관점에서 개인정보를 보호하기 위해 개발되었다. 개인정보 라이프 사이클이 이렇게 특정 목적에 따라 개발됨에 따라 각각의 모델들은 개인정보 보호를 전체적인 시각에서 설명하는데 일정한 한계를 가지고 있다. 특히, ‘동의’와 ‘관리’ 단계가 개인정보 전체 라이프 사이클과 연관이 있는 중요한 개념임에도 불구하고 일부 라이프 사이클 단계에서만 설명되고 있다. 이 연구를 통하여 위에서 언급한 문제점들을 반영한 새로운 개인정보의 라이프 사이클 모델인 ‘개인정보의 동의·관리 기반 모델’을 제시했다.

동의·관리 기반 모델은 개인정보가 수집·저장·이용·파기 되는 전체 개인정보 프로세스를 기반으로 최근의 개인정보 보호 환경 변화를 고려한 모델이다. 이 모델은 라이프 사이클을 수집/생성·보유·이용/제공·파기/철회 단계로 구분하고 사이클을 선형이 아닌 원형 모델로 정의했다. 또한, 개인정보 전체 프로세스와 관련이 있는 동의와 관리 부분을 강조했다. 동의는 외부 환경과 관련이 있으므로 라이프 사이클 모형의 외부에 위치하게 했다. 관리는 모형의 안쪽에 놓음으로써 IT 기업의 내부 환경 및 정보보호 등의 기술과 관련이 있는 항목임을 표현했다.

동의·관리 기반 모델의 각 단계가 앞에서 설명한 다른 4가지 모델에 비해 IT 기업의 개인정보 라이프 사이클 구성 요소 중 얼마

나 많은 부분을 포함하고 있는 지를 검증했다. 그리고 ‘동의’와 ‘관리’가 개인정보의 라이프 사이클 전체 프로세스에 관련되어 있음을 밝혔다. 이를 통해 동의·관리 모델이 국내 IT 기업에 적용했을 때 타당성이 가장 높은 모델임을 입증했다.

개인정보 보호 특성과 최근의 개인정보 보호 환경을 고려한 동의·관리 모델이 제시됨에 따라 IT 기업은 자사의 개인정보 관리 대책, 사내 개인정보 감사, 개인정보 영향 평가 등에 본 모델의 활용이 가능하다. 다만, 동의·관리 모델은 기존의 모델에 비해 복잡하다는 단점이 있다. 이는 기존 모델들이 간과하고 있던 내용들을 동의·관리 모델에 적극 반영했기 때문이다. 또한, 개인정보의 특성상 개인정보를 정의하고 있는 특정 법률을 기반으로 모델을 구성해 IT 기업을 제외한 다른 분야에서 적용에 제한을 받을 수 있다는 점과 한국의 상황에만 적합한 모델이라는 한계가 있다. 따라서, 향후에는 동의·관리 모델을 일반적인 개인정보 보호 환경을 고려하여 수정하는 후속 연구가 필요해 보인다.

---

## 참 고 문 헌

---

- [1] 백운철, 이창범, 장교식, 개인정보보호법, 한국학술정보(주), 2008.
- [2] 방송통신위원회, 개인정보의 기술적·관리적 보호조치 기준(제2011-01호), 2011.
- [3] 장인주, 유영선, “개인정보보호 강화를 위한 동적 보안 수준 결정”, 한국전자거래학회지, 제17권, 제1호, 2012.

- [4] 정보통신부, u-프라이버시 환경 구축을 위한 개인정보보호기술 개발 추진 방향 (중장기 기술개발 계획(안)), 2005.
- [5] 한국인터넷진흥원, 「개인정보법」 조문별 설명자료, 2010.
- [6] 한국인터넷진흥원, 개인정보보호관리 체계 인증준비 안내서(사업자용), 2010.
- [7] 한국인터넷진흥원, 개인정보보호 프레임 워크 개발, 2009.
- [8] 한국정보보호진흥원, 개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구, 2006.
- [9] 한국정보보호진흥원, 개인정보 영향 평가 기준 정비 방안에 관한 연구, 2005.
- [10] 한국정보사회진흥원, “신 가치창출 엔진, 빅 데이터의 새로운 가능성과 대응 전략”, IT and Future Strategy, 제18호, 2011, pp. 1-29.
- [11] 한국정보통신기술협회, 정보통신 단체 표준 개인정보 생명주기별 보안 관리모델, TTAS.KO-12.0063, 2007.
- [12] 한창희, 채승환, 유병준 등, “기업의 개인정보 유출로 인한 경제적 피해규모 산출 방법”, 한국전자거래학회지, 제16권, 제4호, 2011.
- [13] 홍승필, 이철수, “유비쿼터스 컴퓨팅 환경 내 개인정보보호 프레임워크 적용 방안”, 한국정보보호학회논문지, 제16권, 제3호, pp. 157-164, 2006.
- [14] 행정안전부·한국인터넷진흥원, 공공 기관 개인정보 영향평가 수행안내서, 2011.
- [15] APEC, APEC Privacy Framework, 2005.
- [16] Aquilina, K., “Public security versus privacy in technology law : A balancing act?,” Computer Law and Security Review : International Journal of Technology and Practice, Vol. 26, No. 2, pp. 130-141, 2010.
- [17] Boneh, D., Feigenbaum, J., Silberschatz, A., and Wright, R. N., “PORTIA : Privacy, Obligations, and Rights in Technologies of Information Assessment,” Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, Vol. 27, pp. 10-18, 2004.
- [18] Clarke, R., “Privacy impact assessment : Its origins and development,” Computer Law and Security Review, Vol. 25, pp. 123-135, 2009.
- [19] Homeland Security, Privacy Impact Assessments : The Privacy Office Official Guidance, 2010.
- [20] Information Commissioner’s office, The ICO Privacy Impact Assessment Handbook, 2007.
- [21] International Security, Trust, and Privacy Alliance(ISTPA), <http://www.is-tapa.org/ISTPA>.
- [22] Jafari-Lafti, M., Huang, C., and Farkas, C., “P2F : A User-Centric Privacy Protection Framework,” 2009 International Conference on Availability, Reliability and Security, pp. 386-391, 2009.
- [23] Jendricke, U. and Gerd tom Markotten, D., “Usability Meets Security-the Identity Manager as Your Personal Security Assistant for the Internet,” Proceedings 16th Annual Computer Security Applica-



- tions Conference, pp. 344-353, 2000.
- [24] Kang, Y., Lee, H., Chun, K., and Song, J., "Classification of Privacy Enhancing Technologies on Life-cycle of Information," International Conference on Emerging Security Information, Systems and Technologies, IEEE, pp. 66-70, 2007.
- [25] Laudon, K. C. and Laudon J. P., *Management Information Systems : Managing the Digital firm*, Pearson, 2011.
- [26] Meziane, H. and Benbernou, S., "A dynamic privacy model for web services," *Computer Standards and Interfaces*, Vol. 32, pp. 288-304, 2010.
- [27] Nilsson, M., Lindskog, H., and Fischer-Hubner, S., "Privacy Enhancements in the Mobile Internet," *IFIP WG9.6*, 2001.
- [28] Office of the New Zealand Privacy Commissioner, *Privacy Impact Assessment Handbook*, 2002.
- [29] Office of the Privacy Commissioner(Australian Government), *Privacy Impact Assessment Guide* 2006.
- [30] Peng, H., Gu, J., and Ye, X., "Towards Compliance and Accountability : A Framework for Privacy Online," *Journal of Computers*, Vol. 4, No. 6, pp. 494-501, 2009.
- [31] Perkel, J., "How safe are your data? Many scientists want to keep their data and resources free; cyber security specialists want them under lock and key," *Nature*, Vol. 464(7293), pp. 1260-1261, 2010.
- [32] The Treasury Board Secretariat of Canada, *Privacy Impact Assessment Guidelines : A Framework to Manage Privacy Risks*, 2007.
- [33] U.S. Department of Commerce(DOC), *Safe harbor*, 2000.
- [34] Weider D., Doddapaneni, S., and Murthy, S., "A Privacy Assessment Approach for Serviced Oriented Architecture Applications," 2006 second IEEE International Symposium on Service-Oriented System Engineering, pp. 67-75, 2006.
- [35] Williams, M., "Privacy Management," *The Law and Business Strategies*, 2009 International Conference on Computational Science and Engineering, pp. 60-67, 2009.

## 저 자 소 개



장재영  
2002년  
2003년  
2012년~현재  
2003년~현재

(E-mail : jyjang31@gmail.com)  
동국대학교 신문방송학과 (학사)  
영국 University of Westminster 방송통신정책학과 (석사)  
연세대학교 정보대학원 (박사과정)  
한국인터넷진흥원 (책임연구원)



박태환  
2005년  
2012년~현재

(E-mail : pth3030@yonsei.ac.kr)  
연세대학교 정보통신공학과 (학사)  
연세대학교 정보대학원 (석사과정)



김범수  
1999년  
1999년~2002년  
2002년~현재  
2011년~현재  
2012년~현재

(E-mail : beomsookim@gmail.com)  
미국 University of Texas at Austin Ph.D  
미국 University of Illinois at Chicago 조교수  
연세대학교 정보대학원 교수  
지식서비스보안과정 주임교수, ISACA Korea 부회장  
연세대학교 정보대학원 부원장