정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

국제 개인정보보호 표준화 동향 분석
(2020년 4월 SC27 WG5 전자회의 결과를 중심으로)

염 흥 열*

요 약

우리나라에서 2020년 1월 데이터 3법이 개정되면서 개인정보의 보호와 활용의 기반이 마련되었다. 가명처리 개념이 도입되었고, 국제 표준에 근거한 가명 처리의 이행이 요구되는 시점이다. 개인정보보호 요구사항은 일반적으로 법제도, 위험평가, 조직간 계약에서 나온다. 국제표준은 이러한 개인정보보호와 활용과 보호에 대한 글로벌 표준을 제공하여 국경을 넘는 호환성있는 개인정보의 처리를 가능케 한다. 개인정보보호 국제표준화를 주도적으로 추진하는 표준화 그룹은 국제표준화위원회/전기위원회 합동위원회 1/서브위원회 27/작업반 5 (ISO/IEC JTC 1/SC 27/WG 5)이다. 2019년 10월 프랑스 파리 회의 이후에는 개인정보보호 분야 4건의 신규워크아이템 제안과 2건의 연구회기가 진행되었다. 2020년 4월 회의는 당초 러시아 상트페테르부르크에서 열릴 예정이었으나 코로나19의 확산으로 인해 전자회의로 개최되었다.

본고에서는 이 그룹에서 2019년 10월 이후 추진되고 있는 개인정보보호 관련 국제표준화 동향을 제시하고자 한다. 또한 지난 4월 SC27 WG5 전자 회의에서 논의된 개인정보보호 관련 주요 표준화 이슈와 대응 방안을 제시한다.

Ⅰ. 서 론

우리나라에서는 2020년 1월에 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법, 신용정보보호법이 전면 개정되어, 가명화 기법에 근거해 가명화된 데이터는 정보주체의 추가 동의 없이 제3자에게 제공이 가능하게 되었고, 사용자 동의에 기반해 개인정보를 적극적으로 활용하게 하는 마이데이터 서비스가 시작하게 되었다. 또한 여러 기관에서 오는 가명 데이터를 서로 결합하는 서비스를 제공하는 전문기관이 도입되었다. 4차 산업혁명에서 데이터의 활용의 중요성을 강조한 셈이다.

유럽연합 에서는 2018년 5월 25일부터 발효된 개인정보보호규정인 GDPR(general data protection regulation) [29]은 제43조에 개인정보 보호를 위한 인증 메커니즘을 제공하기 위한 법적 기반을 마련했다. 특히 GDPR에서는 고위험 군의 개인정보를 처리하는 개인정보 처리자에게 개인정보영향평가를 의무화하는 등 설계에 의한 개인정보 보호(privacy by design) 와 디폴트에 의한 개인정보 보호 (privacy by default) 개념을 강화했다. 또한 추가 정보를 사용하지 않고도 개인 데이터가 특정 데이터 주체에 더 이상 연결 될 수 없는 방식으로 데이터를 처리하는 가명화 (Pseudonymization) 개념이 도입되었다.

ISO/IEC JTC 1/SC 27/WG 5[18]에서는 개인정보보호와 관련된 국제표준을 개발하고 있는 표준화 그룹이다. 이 그룹에서는 프라이버시 프레임워크 (ISO/IEC 29100)[13], 프라이버시 영향평가 (ISO/IEC 29134)[15], 개인정보보호 준칙(ISO/IEC 29151)[16], 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (ISO/IEC 27018) [12], 개인정보관리체계와 관련된 요구사항 및 지침 (ISO/IEC 27701) [23], 사용자 친화 온라인 고지 및 동의 (ISO/IEC 29184)[26] 등의 국제표준을 개발 완료했다.

또한 이 작업반에서는 현재 스마트시티 프라이버시 가이드라인 (ISO/IEC 27570)[30], 프라이버시 선호도 기반 사용자 친화형 개인정보 처리 프레임워크 (ISO/IEC 27556)[32], 개인정보 삭제 절차 수립을 위한

"이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00660, 차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진)
* 순천향대학교 정보보호학과 (교수, hyyoum@sch.ac.kr),

프레임워크 (ISO/IEC 27555)[31], 조직 프라이버시 리스크 관리 (ISO/IEC 27557)[36], 프라이버시 개선 데이터 비식별화 프레임워크(ISO/IEC 27559)[37], ISO/IEC 27701과 ISO/IEC 27001 기반 개인정보보호 관리체계의 인증 및 심사 기관 요구사항 (ISO/IEC 27006-2)[38], 동의 레코드 정보 구조(ISO/IEC 27560)[39] 등의 국제표준을 개발하고 있다.

기업의 정보보호관리체계(information security management system, ISMS)를 운영하기 위해서는 체계 프로세스를 위한 요구사항 (ISO/IEC 27001)[6]과 보안 위험을 처리하기 위한 보안 통제 (ISO/IEC 27002)[7]가 필요하다. 개인정보 보호 요구사항은 개인정보보호 법 및 제도, 기업 간의 계약, 그리고 개인정보영향평가의 결과로부터 나온다. 이 요구사항은 보안 측면 요구사항 (ISO/IEC 27001)과 프라이버시 측면 요구사항 (ISO/IEC 27701)으로 구분되며, 통제도 보안 측면 통제(ISO/IEC 27002)와 프라이버시 측면 통제 (ISO/IEC 29151, ISO/IEC 27701)[16]로 구분된다. 보안 측면 통제는 ISO/IEC 27002 표준[7]의 보안 통제를 적용해야 하나, 프라이버시 측면 추가 통제와 관련 가이던스가 필요하다. 본 고는 [34], [35] 논문의 연차적 현행화 논문이라고 볼 수 있다.

본고의 2장에서는 ISO/IEC JTC 1/SC 27/WG 5에 개발된 주요 채택된 국제 표준을 살펴보고, 2019년 10월 및 2020년 4월 SC 27/WG 5 전자 회의에서 추진되고 있는 개인정보보호 관련 주요 국제 표준의 현황과 내용을 살펴본다. 3장에서는 결론을 맺는다.

Ⅱ. SC 27 개인정보보호 표준화 동향

2.1. 개인정보보호 관련 국제표준

개인정보보호와 관련된 국제표준은 신원 관리 및 프라이버시 작업반(WG5)[18]에서 채택되고 개발 중인 주요 국제 표준을 요약하면 [표 1]과 같다. 본 장에서는 채택 완료된 국제표준의 세부내용은 [35]를 참조하기 바란다. 여기서는 특히 2019년 10월 이후 새로 합의된 신규워크아이템과 이후 채택된 권고를 중점적으로 살펴본다.

2.2. 프라이버시 프레임워크(ISO/IEC 29100) [13]

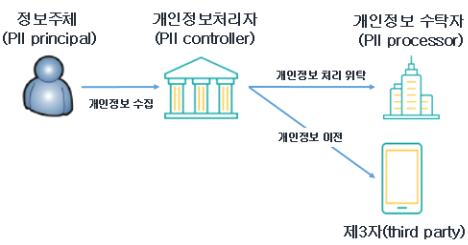
이 국제표준은 현재 IS (international standard) 상태에 있다. 이 국제 표준은 다음으로 구성되는 프라이버시 프레임워크 (privacy framework)를 제공한다.

- 널리 사용되는 프라이버시 용어를 규정한다.
- 참여자와 개인정보를 처리하는 과정에서 참여자의 역할을 정의한다.
- 프라이버시 보호 고려사항을 서술한다.
- 정보기술에 적용 가능한 알려진 프라이버시 원칙을 제공한다.

개인정보(personally identifiable information)는 어떤 정보와 연관된 (a) 개인정보 주체를 식별하는데 이용될 수 있거나 (b) 개인정보 주체와 직접 또는 간접으로 연결될 것 같은 정보로 정의된다.

개인정보 처리와 연관되는 주요 이해당사자는 [그림 1]과 같이 정보주체(PII principal), 개인정보처리자(PII controller), 개인정보 수탁자(PII processor), 제3자(third party)로 구성된다. 정보 주체(PII principal)는 개인정보 처리자(PII controller)와 개인정보 프로세서(PII processor)에게 개인정보를 제공한다. 개인정보처리자는 개인정보 처리 목적과 방법을 결정한다. 개인정보 처리자는 개인정보가 처리되는 동안 (예를 들어, 필요한 프라이버시 통제를 구현) 프라이버시 원칙의 준수를 보장해야 한다.

개인정보 수탁자(PII processor)는 개인정보 처리자를 대신해 개인정보 처리를 수행하고, 개인정보 처리자를 대신하거나 개인정보 처리자의 지시에 응해 활동하거나, 규정된 프라이버시 요구사항을 준수하고 대응하는 프라이버시 통제를 구현해야 한다.



〔그림 1〕 개인정보처리 관련 주요 이해당사자

〔표 1〕 SC 27/WG 5에서 개발 주요 국제 표준 요약

	표준 제목 및 번호	주요 내용	문서 상태
ISO/IEC JTC 1/SC 27/WG 5	▪ ISO/IEC 29100:2011, 프라이버시 프레임워크 [13]	▪ 프라이버시 관련 용어, 개인정보 처리에 있어서 주요 주체의 역할, 보호 요구사항, 프라이버시 보호 원칙 등을 포함한 프라이버시 프레임워크를 제시한다.	IS (2011.12)
	▪ ISO/IEC 27018:2014, 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙[12]	▪ 공공 클라우드 환경에서 개인정보를 보호하기 위한 통제, 통제 목표, 통제 구현 가이드라인을 제시한다. 이 문서는 ISO/IEC 27002에 근거한다.	IS (2014.8제정/2019.1 개정)
	▪ ISO/IEC 29134:2017, 개인정보영향평가 가이드라인 [15]	▪ 개인정보영향평가(privacy impact assessment)를 위한 과정과 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (2017.06)
	▪ ISO/IEC 29151:2017, 개인정보보호 지침[16]	▪ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	IS (2017.04)
	▪ ISO/IEC 29190:2014, 개인정보보호 능력 평가 모델 [14]	▪ 개인정보보호 프로세스(process)를 관리하기 위한 조직의 능력(capability)을 평가하는 방법에 대한 상위 수준의 지침을 제공한다.	IS (2014.04)
	▪ ISO/IEC 20889:2018, 데이터 비식별 기법 및 유형[24]	▪ 다양한 데이터 비식별화 기술, 주요 용어 정의, 그리고 비식별화 기법의 유형을 제시한다.	IS (2017.11)
	▪ ISO/IEC 29003:2018, 온라인 신원증명 (identity proofing) [27]	▪ 온라인에서 사용자에 대한 신원을 증명하는 가이드라인을 제공하고, 신원 확인을 위한 등급, 그리고 이 등급을 만족하기 위한 요구사항을 제시한다.	TS (2018.03)
	▪ ISO/IEC 27701:2019 (구 ISO/IEC 27552), 프라이버시 관리를 위한 ISO/IEC 27001과 ISO/IEC 27002의 확장 – 요구사항 및 가이드라인 [23]	▪ 개인정보 보호 관리를 위한 ISO/IEC 27001 개선을 위한 요구사항과 ISO/IEC 27002 통제를 보완한 개인정보처리자와 개인정보 수탁자를 위한 추가적인 프라이버시 통제를 제시한다.	IS (2019.08)
	▪ ISO/IEC 29184:2020, 사용자 친화 고지 및 통보 [26]	▪ 사용자 친화적 고지 및 통보 방법을 제시한다.	IS(2020.06)
	▪ ISO/IEC 3rd DTS 27570, 스마트 시티 프라이버시 가이드라인 [30]	▪ 스마트시티 서비스를 위한 프라이버시 관련 표준이 글로벌 또는 조직 차원에서 이용자의 이익을 위해 사용되는지에 대한 가이드라인을 제시한다.	3rd DTS
	▪ ISO/IEC 2nd CD 27555, 조직에서 개인정보 삭제 개념의 수립 [31]	▪ 개인정보 삭제 절차를 개발하기 위한 프레임워크를 제시한다.	2nd CD
	▪ ISO/IEC 1st CD 27556, 프라이버시 선호도 기반의 사용자 친화적 개인정보처리 프레임워크 [32]	▪ 프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 시스템의 프레임워크를 제시한다.	1st CD
	▪ ISO/IEC 27557, 조직 프라이버시 위험 관리[36]	▪ 조직의 개인정보 위험 관리 지침을 제공한다.	1st WD (2019.10 NWIP)
	▪ ISO/IEC 1st WD 27559, 프라이버시 개선 데이터 비식별화 프레임워크[37]	▪ 비식별화된 데이터의 수명 주기와 관련된 위험과 재 식별 위험을 찾고 완화하기 위한 프레임워크를 제공한다.	1st WD (2019.10 NWIP)
	▪ ISO/IEC DTS 27006-2, ISO/IEC 27701과 ISO/IEC 27001에 기반한 개인정보보호 관리체계의 인증 및 심사기관 요구사항[38]	▪ ISO/IEC 27001과 ISO/IEC 27701에 기반해 조직의 개인정보 관리체계 (PIMS)를 심사 및 인증을 제공하는 기관에 대한 요구사항을 지정하고 지침을 제공한다. 주로 PIMS 인증을 제공하는 인증 기관의 인증을 지원하기 위한 것이다.	DTS
	▪ ISO/IEC 21st WD 27560, 동의 레코드 정보 구조[39]	▪ 데이터 주체의 데이터 처리 동의를 기록하기 위해 상호 운용 가능하고 개방적이며 확장 가능한 정보 구조를 정의한다.	1st WD (2019.10 NWIP)
	▪ 핀테크 서비스 프라이버시 SP [40]	▪ 이 SP는 핀테크에서 프라이버시 가이드라인을 국제표으로 개발하기 위한 사전 연구회기 활동이다.	SP (2020.09 NWIP 추진 예정)
	▪ 인공지능 프라이버시 영향 SP [41]	▪ 이 SP는 인공지능 프라이버시 영향을 평가하기 위한 국제표준으로 개발하기 위한 사전 연구회기 활동이다	SP
	▪ WG5 SD2, 프라이버시 참조 리스트 [33]	▪ 이 문서는 한국, 영국, 독일 등 주요국의 프라이버시 관련 법과 규정, (2) 데이터 보유 기간, (3) 주요 국제표준, (4) 지침, 그리고 (5) 법/표준/가이드라인간의 관계를 제시하고 있다.	SD

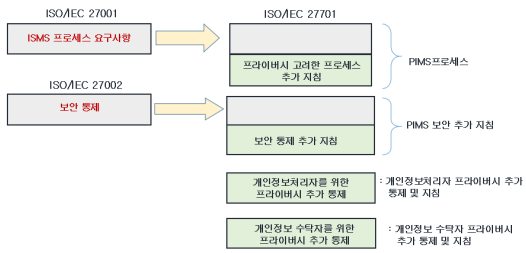
제3자(third party)는 개인정보 처리자를 대신해 개인정보를 처리하는 것이 아니라 별개의 개인정보처리자로서 다른 개인정보처리자로부터 개인정보를 이전(transfer)받아서 개인정보를 처리한다.

이 표준에서는 다음과 같은 11개의 프라이버시 원칙을 정의하고 있다.

- 동의와 선택
- 목적 합법성과 명세성
- 수집 제한
- 데이터 최소화
- 이용, 보유, 그리고 공개 제한
- 정확성과 품질
- 공개성, 투명성 그리고 고지
- 개별 참여와 접근
- 책임성
- 정보 보안
- 프라이버시 준수

2.3. 개인정보관리 요구사항 및 가이드라인(ISO/IEC 27701, 구 27552) [23]

유럽 GDPR의 제43조에 규정된 인증 메커니즘을 구축하기 위해서는 국제표준이 필요하다. 이 국제표준은 2019년 4월 텔아비브 WG5 회의에서 DIS 투표과정에서 반대 투표를 표시하는 국가가 없었고, NB가 제출한 모든 콤맨트가 해결되었음을 고려해 FDIS (final draft international standard)상태 없이 바로 IS(international standard) 로 진전하기로 결정하여 2019년 8월에 국제표준으로 공표되었다. 이 국제표준은 개발과정의 표준번호는 ISO/IEC 27552였으나, 이 국제표준이 개인정보 부문의 관리체계임을 고려해 ISO/IEC 27701로 변경하기로 했다.이 국제표준은 조직 내에서 개인정보관리를 위한 개인정보관리체계 (PIMS)을 수립, 구현, 유지 및 지속적으로 개선하기 위한 지침을 제공한다. 이 문서에서는 개인정보관리체계 관련 요구사항을 지정하고 개인정보처리자와 개인정보 수탁자에 대한 추가 지침을 제공하고 있다. 이 국제표준은 개인정보관리체계를 위한 ISO/IEC 27001에서 정의된 추가적인 요구사항과 ISO/IEC 27002에서 정의된 보안 통제에 더해 추가적인 보안 통제와 프라이버시 통제를 제공하고 있다.



〔그림 2〕 ISO/IEC 27701 구조

이 국제표준은 [그림 2]와 같은 구조를 가지며, 관리체계를 위한 프로세스 요구사항은 ISO/IEC 27001에 기반을 두고 있고, 보안 통제는 ISO/IEC 27002네 기반을 두고 있다. 프라이버시를 고려하기 위해 이 국제표준에서는 추가적인 프로세스 요구사항 지침과 보안 통제를 위한 추가적인 지침이 개발되었다. 또한 개인정보처리자를 위한 프라이버시 측면의 통제와 개인정보 수탁자를 위한 추가적인 프라이버시 통제를 개발했다. 이 국제표준에서 “개인정보관리체계(PIMS, privacy information management system)”는 “개인정보 처리에 의해 영향을 받을 수 있는 프라이버시 보호를 다루는 정보보호관리체계” 라고 정의되었다.

이 국제표준은 개인정보관리체계 구축을 위한 국제표준으로 활용될 것이다. 필자는 이 국제표준의 코에디터로 국제표준 개발을 주도했다.

2.4. 온라인 고지 및 동의(ISO/IEC 29184:2020) [26]

이 국제표준은 정보주체로부터 개인정보를 수집하고 처리하기 위한 동의를 요청하는 온라인 프라이버시 고지와 문서의 내용과 구조를 규정한다. 지난 2019년 10월 파리 회의에서 FDIS (final draft international standard)로 진행하기로 합의했다. 이 국제표준은 FDIS 투표가 성공적으로 완료되어 2020년 4월에 국제표준으로 공표되었다.

고지(notice)의 내용은 처리 목적 설명, 개인정보 처리자의 신원, 수집되는 정보 유형, 수집 방법, 수집 시점과 장소, 이용 방법, 저장되는 곳의 법적 관할, 제3자 제공, 보유기간, 정보주체 참여 방법, 질의 및 불만처리 연락처, 처리 근거, 처리 관련 위험 등을 포함한다. 동의를 위해서는 동의가 필요한지 여부, 숙지되고 자유로운 동의, 정보주체가 사용하는 계정에 관한 정보, 다른 동의와 독립적인 동의, 필수 및 선택 동의의 구분, 새 동의

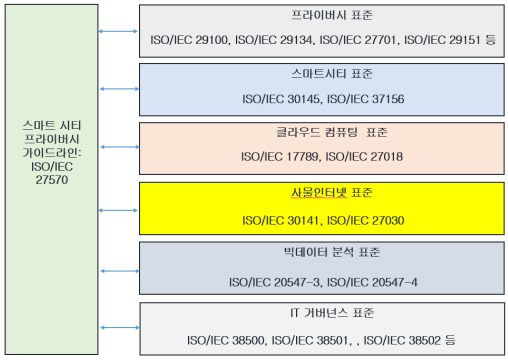
획득 빈도, 시점 등을 규정하고 있다.

2.5. 스마트시티 프라이버시 가이드라인 (ISO/IEC 27570) [30]

이 국제표준은 스마트 시티 환경에서 프라이버시 가이드라인을 제시하고 있다. 논문 작성 시점에 이 문서의 상태는 3rd DTS (draft technical standard) 상태에 있다. 이 국제표준은 2018년 4월 WG5 회의에서 신규워크아이템 투표가 통과된 바 있다. 이 문서는 시민들을 개인정보 보호를 위해 기존 및 향후 개발될 개인정보보호 관련 표준을 글로벌 수준과 조직 수준에서 어떻게 사용할 수 있는지에 대한 지침을 제공한다.

[그림 3]은 스마트시티 프라이버시 가이드라인과 관련된 국제표준은 그 영역에 따라 ISO/IEC 29100 등과 같은 프라이버시 표준, 스마트 시티 거버넌스를 포함하는 스마트 시티 표준, 클라우드 컴퓨팅 표준, 사물인터넷 표준, 빅데이터 분석 표준, IT 거버넌스 표준과 연관된다.

필자는 이 국제표준의 코에디터로 참여하고 있다.



〔그림 3〕 스마티 시티 프라이버시 가이드라인과 연관되는 표준 군

2.6. 개인정보 삭제 가이드라인(ISO/IEC 2nd CD 27555) [31]

삭제(deletion)는 개인정보를 돌이킬 수 없는 방식으로 변경되는 프로세스[31]로 정의되며, 삭제 기간은 특정 데이터 모음이 삭제되어야 하는 기간으로 정의된다.

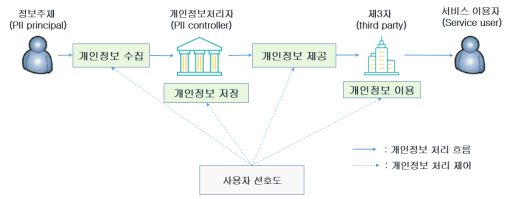
이 국제표준은 2019년 4월 WG5 회의에서 신규워크아이템 투표가 통과되었다. 이 국제표준은 2020년 4월 전자회의에서 2번째 CD (committee draft) 상태로 진행하기로 합의했다.

이 국제표준은 개인정보를 파기하는 절차를 수립하기 위한 프레임워크를 제시하고 있다. 이 표준에서는 용어 정의, 필요한 문서화, 역할과 책임성 그리고 과정을 정의한다.

2.7. 프라이버시 선호도 개인정보처리 프레임워크 (ISO/IEC 1st CD 27556) [32]

프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 프레임워크를 제시한다. 이 국제표준은 현재 첫 번째 CD 상태에 있다. 한편 이 국제표준은 2019년 5월 텔아비브 WG5 회의에서 신규워크아이템 투표가 통과되었다. 이 국제표준은 [그림 4]와 같이 사용자의 프라이버시 선호도에 기반해 수집되는 데이터 유형과 시점, 제공되는 개인정보처리자 목록과 제공되는 개인정보 유형, 이용 가능한 개인정보의 유형을 제어 가능하게 한다. 선호도 기능은 개인정보처리자에 의해 제공되며, 정보주체가 자신의 선호도를 설계하도록 인터페이스를 제공해야 한다.

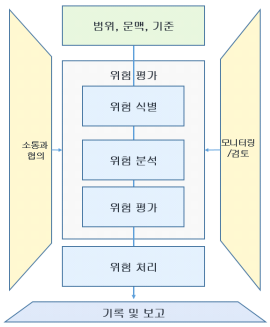
이 국제표준은 개인정보 주체, 개인정보처리자, 개인정보 프로세서, 프라이버시 선호 관리자 등으로 구성된 주요 참여 주체를 정의하고, 데이터 수집, 비식별화, 개인정보 제공 등으로 구성된 주요 구성요소를 제시한다. 또한 프라이버시 참조 관리의 역할을 정의하고 있다. 필자는 이 표준의 코에디터로 국제표준을 개발하고 있다.



〔그림 4〕 사용자 선호도 기반의 개인정보 처리 개념

2.8. 조직 프라이버시 위험 관리(ISO/IEC 27557) [36]

이 국제표준은 2019년 10월 회의에서 신규워크아이템 제안으로 추진해서 2020년 4월 전자회의에서 첫 번째 WD로 진행하기로 했다.



〔그림 5〕 위험 관리 프로세스

ISO/IEC 31000 에서는 [그림 5]와 같이 위험 관리를 위한 프로세스로 소통과 협의, 범위/문맥/기준, 위험 식별/분석 등으로 구성되는 위험 평가, 모니터링/검토, 그리고 기록과 보고 프로세스로 구성된다.

일반적인 위험 관리는 조직의 활동에 통합되어야 하며, 구조적이고 통합적인 접근 방법이어야 하며, 맞춤형으로 조직에 적응 되어야 하며, 주요 이해당사자의 적절하고 시기적절한 관여를 통해 지식, 견해, 인식이 고려되도록 해야 하며, 능동적이고, 인간적 및 문화적 요인이 고려되어야 하며, 지속적인 개선되어야 한다.

이 국제표준에서는 ISO/IEC 31000에서 제공되는 프로세스와 요구사항에 프라이버시를 고려한 추가적인 지침을 제공한다. 대표적으로 포괄적 원칙에 프라이버시를 고려한 지침은 다음과 같다.

- (기존 원칙) “이해 관계자의 적절하고시기 적절한 참여는 지식, 견해 및 인식을 고려할 수 있게 한다. 이를 통해 인지도 향상 및 위험 관리에 대한 정보를 얻을 수 있다.”
- (추가 지침) 조직의 프라이버시 위험을 고려할 때 이해 관계자의 지식, 견해 및 인식을 고려하는 것 외에도 정보주체에 대한 프라이버시 영향을 포함시켜야 한다.

2.9. 프라이버시 개선 데이터 비식별화 프레임워크 (ISO/IEC 27559) [37]

이 국제표준은 2019년 10월 회의에서 신규워크아이템 제안으로 추진해서 2020년 4월 전자회의에서 첫번째 WD로 진행하기로 했다. 이 국제표준은 2019년 10월 회의에서 신규워크아이템 제안으로 추진해서 2020년 4월 전자회의에서 첫번째 WD로 진행하기로 했다. 이 국제표준은 비식별화 기법의 모든 유형을 제시하고 비식별화 관련 용어를 정의하는 ISO/IEC 20889 와 긴밀히 연계된다. 사실 ISO/IEC 20889에서는 규범적 요구사항과 지침은 포함되어 있지 않다. 이 표준에서는 조직이 비식별화를 구현할 때 조직이 의지할 지침을 제공한다.

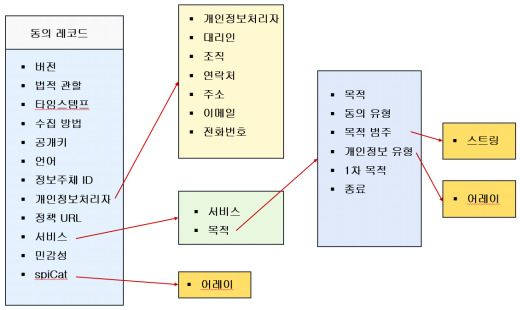
2.10. ISO/IEC 27701과 ISO/IEC 27001 기반 개인정보보호 관리체계 인증 및 심사기관 요구사항 (ISO/IEC 27006-2, 또는 27558) [38]

이 국제표준은 2019년 10월 회의에서 신규워크아이템 제안으로 추진해서 2020년 4월 전자회의에서 산업체의 긴급한 필요를 고려해 DTS로 진행하기로 했다. 이 국제표준은 기존 정보보호관리체계의 인증 및 심사기관의 요구사항을 정의하고 있는 ISO/IEC 27006에서 정의되는 지침에 프라이버시를 고려한 추가 지침을 개발하고자 한다.

이 국제표준은 ISO/IEC 27001과 ISO/IEC 27701에 기반한 개인정보 보호 관리체계 (PIMS)의 심사 및 인증을 제공하는 기관에 대한 요구사항을 정하고 지침을 제공한다. 주로 PIMS 인증을 제공하는 인증기관의 인증을 지원하기 위함이다. PIMS 인증을 제공하는 기관은 이 표준에서 포함된 요구사항을 역량 및 신뢰성 측면에서 입증해야 하며, 이 표준에 포함된 지침은 PIMS 인증을 제공하는 모든 기관에 대한 요구사항에 대한 추가 해석을 제공한다.

2.11. 동의 레코드 정보 구조(ISO/IEC 27560) [39]

이 국제표준은 2019년 10월 회의에서 신규워크아이템 제안으로 추진해서 2020년 4월 전자회의에서 첫번째 WD로 진행하기로 했다. 이 국제표준에서 정하고 있는 동의 레코드의 필드는 [그림 6]와 같이 버전, 법적 관할, 타임스템프, 수집방법, 공개키, 언어, 정보주체 ID, 개인정보처리자, 정책 URL, 서비스, 민감성 등으로 구성된다. 개인정보처리자 필드는 대리인, 조직, 연락처, 주소, 이메일, 전화번호 등으로 다시 구성된다.



〔그림 6〕 동의 레코드의 전반적 정보구조

2.12. 핀테크 서비스 프라이버시 가이드라인 연구회기 (SP) [40]

연구회기(study period)는 본격적으로 국제표준의 신규워크아이템제안을 수행하기 전에 사전 준비과정이다. 우리나라는 2019년 10월 핀테크 서비스를 위한 프라이버시 가이드라인을 국제표준으로 개발하기 위해 연구회기를 제안해 채택했다. 지난 4월 전자회의에서는 핀테크 서비스에 대한 일반 프라이버시 가이드라인을 2020년 9월 회의에 추진하기로 합의했다. 이 잠재적 워크 아이템은 인도, 필리핀, 프랑스, 독일 등이 개발과정에 적극 참여할 것으로 예측된다. 특히, 돈세탁방지와 사기 탐지를 위한 개인정보 수집과, 이와 관련된 위협을 식별하고 그 위협을 처리하기 위한 프라이버시 통제를 제시할 예정이다. 필자는 이 연구회기의 라포처 역할을 수행하고 있다.

2.13. 인공지능의 프라이버시 영향 연구회기 [41]

이 연구회기는 인공지능에 미치는 프라이버시 영향에 대한 국제표준을 개발하기 위함이다. 이 연구회기는 지금까지 프라이버시 지침에 집중했으나, 지난 4월 회의에서 보안 이슈를 추가로 연구하기로 합의했다. 다음 9월 전자회의에서는 보안과 프라이버시에 대한 인공지능의 영향에 대한 기술보고서 형태의 보고서로 개발할지 아니면 다른 형태의 문서를 개발할지 결정될 예정이다. 필자는 이 연구회의의 코라포처 역할을 수행하고 있다.

2.14. 프라이버시 참조 리스트 (WG5 SD2) [33]

이 문서는 국제 표준이 아닌 WG5에서 유지하고 있는 문서이며, 매 회의마다 업데이트된다. 이 문서는 한국, 미국, 영국 등의 26개국의 개인정보보호 법과 규정을 제시하고 있고, 한국, 프랑스, 영국 등 주요국의 개인정보 보유 기간을 보여 주며, 프라이버시 보호 관련 국제표준을 제시하며, 금융분야를 포함한 11개 분야의 프라이버시 가이드라인을 제시하고 있다. 또한 2019년 4월 회의에서 EU GDPR의 관련 조항과 ISO/IEC 27701의 주요 통제에 대한 매핑을 포함했고, 주요 국제 표준에서 사용되는 비식별화 관련 용어에 대한 비교 표를 제시하고 있다. 더불어 글로벌 주요 프라이버시 단체에 대한 정보도 제공하고 있다. 우리나라는 2020년 4월 전자회의에 우리나라 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법의 수정안의 내용을 제출해 반영했다.

Ⅲ. 결 론

본고에서는 SC 27/WG 5에서 개발되었거나 개발 중에 있는 개인정보보호 관련 주요 국제표준의 내용을 제시한다. 데이터 중심사회에서 데이터에 포함되어 있는 개인정보를 보호 필요성이 증가하고 있고 동시에 활용 요구가 급증하고 있다. 본고에서는 지난 2019년 10월 이후에 이뤄진 개인정보보호 분야의 활동 결과를 중심으로 기술했다. 개인정보 제도나 관행은 국제표준의 근거해 시행되어야 글로벌 차원의 상호연동성을 보장받는다.

본고의 결과는 국내 개인정보 참여 주체의 개인정보보호 수준 제고를 위해 활용 가능하다.

참 고 문 헌

[1] BS 10012:2009, Data protection – Specification for a personal information management system, BSI, 2009

[2] KCS.KO-12.0001, 개인정보보호관리체계(PIMS), 2011

[3] 법제처, 개인정보보호법

[4] 법제처, 정보통신망이용촉진 및 정보보호 등에 관한 법

[5] ISO/IEC 27000:2014, Information security management systems – Overview and vocabulary

[6] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements
[7] ISO/IEC 27002:2013, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system
[8] ISO/IEC 27005:2011, Information security risk management
[9] ISO/IEC 27009: 2016, Information technology — Security techniques — Sector specific application of ISO/IEC 27001 – Requirements
[10] ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
[11] ISO/IEC 27017:2016, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[12] ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PIII processors
[13] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework
[14] ISO/IEC 29190:2015, Information technology – Security techniques – Information technology -- Security techniques -- Privacy capability assessment model
[15] ISO/IEC 29134:2017, Privacy Impact Assessment - Methodology
[16] ISO/IEC 29151:2017, Code of practice for the protection of personally identifiable information, 2017.8
[17] WG 5/SD 5, Explanation on the use of ISO/IEC 27001 (ISMS) for privacy management, 2015.8
[18] ISO/IEC JTC 1/SC 27, Information security, cybersecurity, privacy protection, http://www.iso.org/iso/iso_technical_committee?commid=45306
[19] WG 5/SD 1, WG 5 Roadmap, 2019.4
[20] 염흥열, “개인정보보호 관리체계 국제 표준화 필요성,” 정보보호학회지, 제23권 제4호, pp.65-72, 2013.8
[21] 염흥열, “개인정보보호 기술 및 국제표준 동향,” OSIA Standards & Technology Review Journal, June 2014, Vol.27, No.2
[22] 염흥열, 개인정보보호 국제표준화 분석, 한국정보보호학회 학회지, 제25권 제4호, pp.5-9, 2015.8
[23] ISO/IEC IS 27552, Enhancement to ISO/IEC 27001 for privacy management – Requirements, 2019.8.
[24] ISO/IEC 20889:2018, Information technology – Security techniques – Privacy enhancing data de-identification terminology and classification of techniques
[25] 행정안전부, 방송통신위원회 등, “비식별화조치 가이드라인,” 2016.6.30.
[26] ISO/IEC 29184, Guidelines for online privacy notices and consent, 2019.07
[27] ISO/IEC TS 29003:2018, Identity proofing
[28] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2016년 4월 탬퍼 SC27 회의 결과를 중심으로), 정보보호학회지, v.26, no.4, 6-10, 2016.8
[29] EU, GDPR (general data protection regulation), 27 April 2016
[30] ISO/IEC DTS 27570, Privacy guidelines for smart cities
[31] ISO/IEC CD, 27555, Establishing a PII deletion concept in organizations
[32] ISO/IEC CD, 27556, User-centric framework for PII handling based on privacy preferences
[33] WG 5/SD 2, SC 27/WG 5 Standing Document 2 (WG 5 SD2) -- Privacy references list , 2020.8
[34] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2017년 4월 해밀턴 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제27권 제5호, pp.6-11, 2017.10
[35] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2019년 4월 이스라엘 텔아비브 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제29권 제4호, 2019.08
[36] ISO/IEC WD 27557, Organizational privacy risk management
[37] ISO/IEC WD 27559, Privacy enhancing data de-identification framework
[38] ISO/IEC DTS 27006-2 (27558), Requirements for

bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC 27001

[39] ISO/IEC WD 27560, Privacy technologies – Consent record information structure

[40] ISO/IEC JTC 1/SC 27/WG 5 N 2304, Call for contributions for the WG 5 Study Period on Privacy for fintech services, 2020-06-02

[41] ISO/IEC JTC 1/SC 27/WG 5 N 2377, Call for contributions for the WG 5 Study Period on Impact of Artificial Intelligence on Privacy, 2020-06-02

[42] ISO 31000:2018, Risk management

〈저 자 소 개〉

염 흥 열 (Heung Youl Youm)

종신회원

한양대학교 전자공학과 학사 졸업

한양대학교 대학원 전자공학과 석사 졸업

한양대학교 대학원 전자공학과 박사 졸업

1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원

1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수

2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)

2009년~2016년 : ITU-T SG17 부의장

2009년~2016년 : ITU-T SG17 WP3 의장

2017년~현재 : ITU-T SG17 의장

2012년 6월~2015년 5월 : 정보보호포럼 의장

2016년 5월 ~현재 : 개인정보보호포럼 의장

<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 네트워크 보안, 암호 프로토콜, 블록체인 보안, 5G 보안