정 보 보 호 학 회 지
제 29 권 제4호, 2019. 8

국제 개인정보보호 표준화 동향 분석
(2019년 4월 이스라엘 텔아비브 SC27 WG5 회의 결과를 중심으로)

염 흥 열*

요 약

데이터 중심 사회가 되면서 데이터의 활용에 대한 요구가 증가하고 있으며, 데이터에 포함된 개인정보를 보호하기 위한 국제표준화가 매우 중요하게 되었다. 개인정보보호 국제표준화를 주도적으로 추진하는 표준화 그룹은 국제표준화위원회/전기위원회 합동위원회 1 서브위원회 작업반 5 (ISO/IEC JTC 1/SC 27/WG 5)이다.

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

Ⅰ. 서 론

유럽 차원의 디지털 경제를 구축하기 위해 유럽 연합(EU) 28개국 회원국에 적용되는 개인정보보호규정인 GDPR(general data protection regulation)이 2016년 4월에 제정되었고 2018년 5월 25일에 발효되었다[29]. GDPR에서는 개인정보 보호 인증 메커니즘을 도입하였고, 고위험 군의 개인정보를 처리하는 개인정보 처리자에게 개인정보영향평가를 의무화하는 등 개인정보 내재화(privacy by design) 개념을 강화했다. 또한 추가 정보를 사용하지 않고도 개인 데이터가 특정 데이터 주체에 더 이상 귀속될 수 없는 방식으로 개인 데이터를 처리하는 가명화 (pseudonymization) 개념을 도입했다.

ISO/IEC JTC 1/SC 27/WG 5[18]에서는 개인정보보호와 관련된 국제표준을 개발하고 있는 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] 등의 국제표준을 개발했다. 또한 이 작업반에서는 개인정보관리체계와 관련된 요구사항 및 가이드라인 (ISO/IEC 27552) [23], 사용자 친화 온라인 고지 및 동의 (ISO/IEC 29184)[26], 스마트시티 프라이버시 가이드라인 (ISO/IEC 27570)[30], 프라이버시 선호도 기반 사용자 친화형 개인정보 처리 프레임워크 (ISO/IEC 27556)[32], 그리고 개인정보 삭제 절차 수립을 위한 프레임워크 (ISO/IEC 27555)[31] 등의 국제표준을 개발하고 있다.

기업의 기술적, 관리적, 조직적 보호조치를 제공하는 정보보호관리체계(information security management system, ISMS)를 운영하기 위해서는 체계 프로세스를 위한 요구사항(ISO/IEC 27001)[6]과 보안 위험을 치료하기 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 27552)으로 구분되며, 통제도 보안 측면 통제(ISO/IEC 27002)와 프라이버시 측면 통제(ISO/IEC 29151, ISO/IEC 27552)[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] 논문의 현행화와 개선이라고 볼 수 있다. 본 고의 2장에서는 ISO/IEC JTC 1/SC 27/WG 5에 개발된 주요 표준을 살펴보고, 2019년 4월 SC 27/WG

"이 논문은 2019년도 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 (hyyoum@sch.ac.kr),

5 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 개발되고 있는 주요 국제 표준을 요약하면 [표 1]과 같다.

2.2. 프라이버시 프레임워크(ISO/IEC 29100) [13]

이 국제표준은 현재 IS (international standard) 상태에 있다. 이 국제 표준은 다음으로 구성되는 프라이버시 프레임워크를 제공한다.

- 널리 사용되는 프라이버시 용어를 규정한다.
- 참여자와 개인정보를 처리하는 과정에서 참여자의 역할을 정의한다.
- 프라이버시 보호 고려사항을 서술한다.
- 정보기술에 적용 가능한 알려진 프라이버시 원칙의 참조를 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 주체(PII principal)는 개인정보 처리자(PII controller)와 개인정보 프로세서(PII processor)에게 개인정보를 제공하고, 준거법에 의해 다른 방법으로 제공되지 않을 때 개인정보 처리 방법에 대한 자신의 개인정보 선호를 결정하고 동의를 제공한다. 개인정보 처리자는 개인정보 처리 목적과 방법을 결정한다. 개인정보 처리자는 개인정보가 처리되는 동안 (예를 들어, 필요한 프라이버시 통제를 구현) 프라이버시 원칙의 준수를 보장해야 한다.

개인정보 프로세서(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.

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. 클라우드 개인정보보호 준칙 (ISO/IEC 27018) [12]

이 국제표준은 현재 IS상태에 있다. 이 국제 표준은 퍼블릭 클라우드 컴퓨팅 환경에 대한 개인정보 보호 원칙에 따라 개인정보를 보호하기 위한 보호 조치를 구현하기 위해 필요한 통제 목적, 통제 그리고 지침을 수립한다. 특히 본 국제 표준은 퍼블릭 클라우드 서비스 제공자의 정보 보안 위험 환경의 맥락에서 적용될 수 있는 개인정보 보호에 대한 규제 요구 사항을 고려하여 보안 통제에 기반한 지침을 규정한다. 이 표준에서는 추가적인 개인정보 통제의 대표적인 사례는 다음과 같다.

- 개인정보 주체의 권한을 행사 할 수 있는 수단 제공
- 목적 명세와 수집 제한 원칙 보장 - 고객의 요구한 목적으로만 개인정보 처리
- 별도 동의 없이 상업 및 홍보용 개인정보 이용 제한
- 개인정보 포함 임시 파일 삭제
- 클라우드 서비스 제공자의 위탁 기관 정보 사전 공개
- 주요 주체간의 보안 역할과 책임을 명확히 할당
- 데이터 유출, 비인가된 접근 등의 사건 발생 시 통보
- 개인정보 저장 시 지정학적 위치 규정 및 문서화
- 전송망 개인정보 암호화 조치

〔표 1〕 개인정보보호 (privacy) 관련 국제표준〔2019.7 현재〕

작업반	표준 제목 및 번호	주요 내용	문서 상태
WG 5	■ ISO/IEC 29100, 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, 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 (2014.8/2019.1)
	■ ISO/IEC 29134, 개인정보영향평가 가이드라인 [15]	■ 개인정보영향평가(privacy impact assessment)를 위한 과정과 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (2017.06)
	■ ISO/IEC 29151, 개인정보보호 지침[16]	■ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	IS (2017.04)
	■ ISO/IEC 29190, 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, 데이터 비식별 기법 및 유형[24]	■ 다양한 데이터 비식별화 기술, 주요 용어, 그리고 비식별화 기법의 유형을 제시한다.	IS (2017.11)
	■ ISO/IEC 29003, 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 27552, 프라이버시 관리를 위한 ISO/IEC 27001의 확장 - 요구사항 및 가이드라인 [23]	■ 개인정보관리를 위한 ISO/IEC 27001 개선을 위한 요구사항과 통제를 제시한다.	IS 진행중 (표준 번호가 27071로 변경될 가능성 있음)
	■ ISO/IEC 29184, 사용자 친화 고지 및 통보 [26]	■ 사용자 친화적 고지 및 통보 방법을 제시한다.	DIS
	■ ISO/IEC 27570, 스마트 시티 프라이버시 가이드라인 [30]	■ 프라이버시 관련 표준이 글로벌 또는 조직 차원에서 이용자의 이익을 위해 사용되는지에 대한 가이드라인을 제시한다.	PDTS
	■ ISO/IEC 27555, 조직에서 개인정보 삭제 개념의 수립 [31]	■ 개인정보 삭제 절차를 개발하기 위한 프레임워크를 제시한다.	2nd WD
	■ ISO/IEC 27556, 프라이버시 선호도 기반의 상요자 친화적 개인정보처리 프레임워크 [32]	■ 프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 시스템의 프레임워크를 제시한다.	2nd WD
	■ WG5 SD2, 프라이버시 참조 리스트 [33]	■ 이 문서는 한국, 영국, 독일 등 주요국의 프라이버시 관련 법과 규정, (2) 데이터 보유 기간, (3) 주요 국제표준, 지침, 그리고 법/표준/가이드라인간의 관계를 제시하고 있다.	SD

2.4. 개인정보보호 능력 평가 모델 (ISO/IEC 29190) [14]

이 국제표준은 현재 IS상태에 있다. 이 표준은

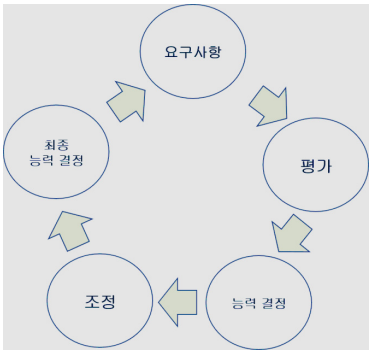
- 개인정보보호 능력을 결정하기 위해 프로세스를 평가하는 단계를 규정하고,
- 개인정보보호 능력을 평가하기 위한 여러 등급(level)을 정의하며,
- 개인정보보호 능력이 평가되는 주요 프로세스 영역에 대한 평가 지침을 제공하고,
- 프로세스 평가를 구현하기 위한 지침을 제공하며,

· 개인정보보호 능력 평가를 조직 운영으로 통합하는 방법에 대한 지침을 제공한다.

프로세스 능력 평가는 [그림 1]과 같이 연속적 개선 주기를 갖는다.

능력 평가 모델은 효과적 프로세스의 특징을 설명하는 구조화된 요소들의 집합이다. 이 모델은 조직이 다음과 같은 6개 등급으로 프로세스를 평가하도록 한다.

· 등급 0 (불완전한 프로세스): 프로세스가 구현되어 있지 않거나 프로세스 목표를 달성하지 못한다. 이 등급에서는 프로세스 목적의 체계적 달성에 대한 증거가 거의 없거나 존재하지 않는다.
· 등급 1(수행된 프로세스): 구현된 프로세스는 프로세스의 목적을 달성한다.
· 등급 2(관리된 프로세스): 수행된 프로세스는 관리된 방식(계획되고, 감시되고 조정됨)으로 구현되며, 작업 산출물은 적절히 수립, 통제, 그리고 유지된다.
· 등급 3(수립된 프로세스): 관리된 프로세스가 프로세스 산출물을 달성할 수 있는 정의된 프로세스를 이용해 구현된다.
· 등급 4(예측된 프로세스): 수립된 프로세스가 프로세스 산출물을 달성하기 위해 정의된 범위 내에서 작동한다.
· 등급 5(혁신되는 프로세스): 예측 가능한 프로세스는 조직의 목표에 일치해 변화에 지속적으로 개선된다.



〔그림 1〕 개인정보보호 능력 평가 생명 주기

2.5. 개인정보영향평가 (ISO/IEC 29134)[15]

개인정보영향평가(privacy impact assessment)는 조직의 광범위한 위험 관리 프레임워크 내에서 개인정보 처리와 관련하여 잠재적 프라이버시 영향을 식별, 분석, 평가, 컨설팅, 의사소통 및 계획하는 전반적인 프로세스로 정의되고 있다. 개인정보영향평가는 개인정보를 처리하는 정보시스템의 설계 시나 중대한 변경 시에 수행되는 프로세스이다. 이 국제 표준은 2017년 6월에 IS로 채택되었다. 이 국제표준은 프라이버시 영향평가에서 요구되는 프로세스와 프라이버시 영향평가 보고서의 구조에 대한 가이드라인을 제시하고 있다.

유럽 GDPR에서는 일정 규모 이상의 민감 정보를 처리하는 개인정보 처리자는 프라이버시 영향평가를 의무적으로 수행하도록 요구하고 있다. 우리나라 개인정보보호법[3]에서는 공공분야의 일정 규모 이상의 개인정보파일을 보유하는 기관은 의무적으로 개인정보영향 평가를 수행하도록 요구하고 있다. 필자는 이 국제표준의 코에디터로 국제표준 개발을 주도했다.

2.6. 개인정보보호 준칙 (X.1058|ISO/IEC 29151)[16]

이 국제표준은 2017년 8월 IS로 채택되었다. 이 국제표준은 ISO/IEC JTC 1/SC 27과 ITU-T SG17 이 공동으로 개발한 국제표준이다.

ISO/IEC 29151은 개인정보 처리자(PII controller)에 적용 가능한 보호조치를 위한 통제 목표, 통제 항목, 구현 가이던스, 그리고 기타 정보를 제공한다[16]. 이 표준은 ISO/IEC 27002에서 제공하는 정보보호 통제에 더하여 개인정보보호를 위해 추가적으로 요구되는 가이던스와 프라이버시 보호 원칙을 만족하는 추가적인 프라이버시 통제를 제공하고 있다. ISO/IEC 27002에서 제공하는 통제를 변경 없이 적용하되 추가적인 가이던스가 필요한 경우는 해당 절에 추가하는 방법으로 기술되었다. 또한 개인정보보호 특화 통제는 부록 A에 기술되어 있으며, 개인정보보호 원칙별로 추가 통제 목표, 통제 항목, 가이던스, 그리고 기타 정보가 제공된다. 이 국제표준은 개인정보보호 관리체계를 운영하기 위해 요구되는 프라이버시 통제를 개발함에 그 목적이 있다. 이 국제 표준은 자산관리, 접근통제, 암호, 운영보안, 통신보안, 그리고 공급자 보안 등의 정보보안 측면의 개인정보보호 특화 가이던스를 기술했다. 또한, 개인정보보호 정책, 동의 및 선택, 목적 합법성, 데이터 최소화, 이용/보유/공유 최소화, 정확성 및 품질, 투명성, 정보주체 참

여, 책임성, 정보보안, 프라이버시 법 준수 측면에서 개인정보보호 특화 통제를 기술하고 있다.

필자는 이 국제표준의 메인 에디터로 표준 개발을 주도했다.

2.7. 개인정보관리 요구사항 및 가이드라인(ISO/IEC 27552)[23]

유럽 GDPR의 제43조에 규정된 인증 메커니즘을 구축하기 위해서는 국제표준이 필요하다.

이 국제표준은 2019년 4월 텔아비브 WG5 회의에서 DIS 투표과정에서 반대 투표가 없었고, NB가 제출한 모든 콤맨트가 해결되었음을 고려해 FDIS (final draft inernational standard) 없이 바로 IS로 진전하기로 결정했다.

이 국제표준은 조직 내에서 개인정보보관리를 위한 개인정보관리체계 (PIMS)을 수립, 구현, 유지 및 지속적으로 개선하기 위한 지침을 제공한다. 이 문서에서는 개인정보관리체계 관련 요구 사항을 지정하고 개인정보처리자와 개인정보 수탁자에 대한 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.

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

2.8. 데이터 비식별화 기법(ISO/IEC 20889)[24]

이 국제 표준은 2018년 11월 IS (international standard)로 발표되었다. 이 국제 표준은 ISO/IEC 29100에서 제시된 개인정보보호 원칙에 입각해 데이터 비식별화 (data de-identification) 기술을 제시한다. 이 표준은 비식별화 관련 용어 정의, 특성에 따른 분류 비식별화 기술 분류, 재식별 (re-identification)의 위험을 줄이기 위한 비식별화 기법의 적용 가능성을 기술한다.

국내에서는 현재 개인정보보호법, 정보통신망 이용촉진 및 정보보호에 관한 법[4], 신용정보보호법을 개정안을 국회에서 논의하고 있고, 개정 개인정보보호법에는 가명화 기법이라는 비식별화 개념을 도입했다. 비식별화 기법은 빅데이터 환경에서 데이터에 포함된 개인정보의 보호 요구사항을 만족하면서 데이터 활용이 가능케 하는 기법이다. 이 국제표준은 비식별화를 위한 다양한 데이터 처리 시스템에서 활용될 수 있다.

국내에서는 행정안전부와 방송통신위원회가 2016년 6월 30일 비식별화 조치 가이드라인을 발표했다[25]. 비식별화된 데이터는 개인정보로 보지 않으나, 언제든지 재식별화될 가능성이 있어서 비식별화된 데이터에 대한 기술적 관리적 보호조치를 취하도록 요구하고 있다. 또한 비식별화 전문기관에 의해 비식별화 데이터를 결합하는 서비스를 제공하고 있다. 빅데이터 환경에서 개인정보의 보호와 활용을 위한 절충점을 제시하고 있다고 볼 수 있다. 따라서 비식별화 기법은 개인정보 침해 소지 없이 빅데이터와 개인정보를 처리하기 위한 핵심 기술이다. 따라서 국내 산업적 파급효과가 매우 큰 표준이다.

2.9. 온라인 고지 및 동의(ISO/IEC 29184)[26]

이 국제표준은 정보주체로부터 개인정보를 수집하고 처리하기 위한 동의를 요청하는 온라인 프라이버시 고지와 문서의 내용과 구조를 규정한다. 지난 2019년 4월 텔아비브 회의에서 DIS (draft international standard)로 진행하기로 합의했다. 고지의 목적은 정보 주체가 쉽게 동의 할 수 있는 시점, PII 주체가 쉽게 인식할 수 있는 장소 및 정보 주체를 제공하는 참조를 사용하여 정보 주체에 적합한 언어로 통지를 제공하는 것입니다. 사전 통지 및 그 답변을 포함하여 보충 자료에 액세스 할 수 있습니다. 고지 목적은 정보 주체가 쉽게 인식 할 수 있는 곳에서, 정보주체가 동의를 행사할 수 있을 때, 정보주체에게 적절한 언어로, 정보 주체에게 사전 고지와 그 답변을 포함한 보충 자료에 접근할 수 있는 참조를 갖도록 고지를 제공하기 위함이다. 동의 목적은 동의가 개인정보를 수집하기 위한 근거가 되는 경우, 개인정보처리자가 정보주체로부터 동의를 공정하고, 명백하며, 투명하고, 모호하지 않으며 취소 가능한 방식으로 얻도록 하기 위함이다.

2.10. 신원 확인 (ISO/IEC 29003)[27]

신원 확인(identity proofing)은 신원관리체계

(identity management system) 에 입력될 신원 속성을 검증하고, 신원 속성이 등록될 정보주체에 속한다는 것을 확인하는 프로세스이다. 이 국제 표준은 사람의 신원확인 (identity proofing)에 대한 지침을 제공하고 신원확인 수준 및 이 수준을 달성하기 위한 요구 사항을 규정하고 있다. 이 국제 표준은 2018년 3월에 TS (technical specification) 로 채택되었다. 이 국제 표준에서는 [표 2]와 같이 3개의 신원확인 보증 등급 (Level of identity proofing)을 정의하고 있다. ISO/IEC 29003 (identity Proofing) 는 국내에서 시행하고 있는 비대면 인증을 위한 신원확인 과정에 활용될 수 있다.

〔표 2〕 신원확인 보증 수준

보증 수준	설명	목적
LoIP 1	낮은 신뢰 등급	▪ 신원이 유일함 ▪ 신원이 존재한다고 가정함 ▪ 정보주체가 신원과 결속되었다고 가정함
LoIP 2	중간 신뢰 등급	▪ 신원이 유일함 ▪ 신원이 존재한다고 적절히 입증함 ▪ 정보주체가 신원에 적절히 결합되어 있음
LoIP 3	높은 신뢰 등급	▪ 신원이 유일함 ▪ 신원이 존재한다고 강하게 입증함 ▪ 정보주체가 신원에 강하게 결합되어 있음

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

이 국제표준은 스마트 시티 환경에서 프라이버시 가이드라인을 제시하고 있다. 논문 작성 시점에 이 문서의 상태는 PDTS (proposed 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. 필자는 이 국제표준의 코에디터로 참여하고 있다.

2.12. 개인정보 삭제 가이드라인(ISO/IEC 27555)[31]

삭제(deletion)는 개인정보를 돌이킬 수 없는 방식으로 변경되는 프로세스로 정의되며, 삭제 기간은 특정 데이터 모음이 삭제되어야 하는 기간으로 정의된다.

이 국제표준은 2019년 4월 WG5 회의에서 신규워크아이템 투표가 통과되었다. 이 국제표준은 2번째 WD (working draft) 상태에 있다.

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

2.13. 프라이버시 선호도 개인정보처리 프레임워크(ISO/IEC 27556)[32]

프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 프레임워크를 제시한다. 이 국제표준은 현재 2번째 WD 상태에 있다. 이 국제표준은 2019년 5월 텔아비브 WG5 회의에서 신규워크아이템 투표가 통과되었다.

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.

2.14. 프라이버시 참조 리스트 (WG5 SD2)[33]

이 문서는 국제 표준이 아닌 WG5에서 유지하고 있는 문서이다. 이 문서는 한국, 미국, 영국 등의 26개국의 개인정보보호 법과 규정을 제시하고 있고, 한국, 프랑스 등의 8개국의 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 27552의 주요 통제에 대한 매핑을 포함했고, 주요 국제 표준에서 사용되는 비식별화 관련 용어에 대한 비교 표를 제시하고 있다. 더불어 글로벌 주

요 프라이버시 단체에 대한 정보도 제공하고 있다.

Ⅲ. 결 론

본고에서는 SC 27/WG 5에서 개발되거나 개발 중에 있는 개인정보보호 관련 주요 국제표준의 내용을 제시한다. 데이터 중심사회에서 데이터에 포함되어 있는 개인정보를 보호 필요성이 증가하고 있다.

본고의 결과는 국내 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 1st PDTS 27570, Privacy guidelines for smart cities

[31] ISO/IEC 2nd WD, 27555, Establishing a PII deletion concept in organizations

[32] ISO/IEC 2nd WD, 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 , 2019.8

[34] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2017년 4월 해밀턴 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제27권 제5호, pp.6-11, 2017.10

〈저자소개〉

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

2017년~현재 : ITU-T SG17 의장

2009년~2016년 : ITU-T SG17 부의장, WP3 의장

2011년 1월~12월 : 한국정보보호학회 회장(역)

2012년 1월~현재 : 한국정보보호학회 명예회장

2016년 5월~현재 : 개인정보보호표준포럼 의장

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