해외 개인정보보호 동향 보고서

최신동향 보고서 2019년 3월 2주

KISA 한국인터넷진흥원

국외 개인정보보호 위험 평가 및 인증 사례

< 목 차 >

개요

▶ 개인정보 이용 관련 동의 절차에서 소비자가 개인정보침해 위험을 쉽게 인식할 수 있도록 설명을 단순화하고 등급 제도를 도입하는 방안과 관련, 이와 유사하거나 참고 가능한 국외 사례를 검토

- 이를 위해서는 개인정보보호 수준에 대한 평가를 보다 이해하기 쉽게 만드는 것과 보편적으로 수용 가능한 개인정보보호 평가 기준을 만드는 것이 중요
- 이와 관련, 이 보고서에서는 개인정보 위험 등급 산정과 관련한 유사 사례 및 기존의 개인정보 인증기관과 절차에 관해 검토

개인정보 위험 등급 평가 사례

(1) Common Sense Media의 교육용 앱 및 웹사이트 등급 평가

▶ 미국의 비영리기관 Common Sense Media[1]는 2015년부터 개인정보보호 평가(privacy

rating)를 진행하고 있으며, 2018년부터 개인정보보호 수준에 대해 더 쉽게 이해할 수 있도록 등급 평가 단계를 간소화

- Common Sense Media는 주로 교육 기자재나 교육용 웹사이트에 대한 개인정보보호 평가를 진행하고 있으며 평가 결과에 따라 다음과 같은 등급으로 구분

① "Use responsibly" 등급: 개인정보이용약관과 개인정보보호방침 내용이 최소한의 기준을 충족하고 투명성 역시 하한선을 통과했으나, 해당 서비스의 도입 여부를 심사하는 첫 단계에서 개인정보보호 평가(privacy evaluation)의 전체 내용을 검토하고 그 이후 학생 데이터를 공유 것을 권장

② "Use with caution" 등급: 교육과 관련 없는 데이터를 수집하거나 표적 광고 서비스를 위해 데이터를 이용하는 경우에 해당하며,"데이터 이용과 관련한 투명성이 부족"한 경우도 해당되므로 제3자 공유 등에 관한 상세 정책을 검토하는 것이 필요

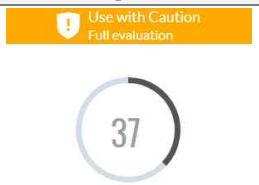
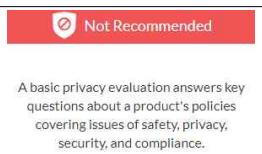
※ 단, 이러한 등급이 반드시 해당 공급 업체가 비윤리적이거나 불법적이라는 것을 의미하지는 않음

③ "Not recommended" 등급: 개인정보보호 처리방침이 전혀 공개되지 않거나 계정 생성 또는 로그인 활동을 과정에서 HTTPS 암호화를 지원하지 않거나 아예 요구하지 않는 경우에 해당되며, 이 경우 이용자의 개인정보보호를 위한 구체적인 조치를 취하지 않을 수도 있다는 점에 주의가 필요

▶ Common Sense Media는 평가 결과를 기관 웹사이트에 공개

- 평가 대상 앱이나 웹사이트에 대해 상세한 평가 내역과 함께 때로는 총점을 함께 계산하여 게시함으로써 사용자가 손쉽게 개인정보보호 등급을 판단할 수 있도록 지원

표 1_ Common Sense Media 웹사이트에 공개된 개인정보보호 등급 평가 결과 사례

평가대상 앱 또는 웹사이트	평가 내역	총점 또는 등급 선정 사유
		
		

출처: Common Sense Media (2019.3)

1 https://www.commonsensemedia.org/, https://privacy.commonsense.org/

개인정보보호 인증 사례

(1) 일본정보경제사회추진협회(JIPDEC): 프라이버시 마크 인증

▶ **(개요)** JIS Q 15001 개인정보보호관리시스템의 요구사항을 충족하며 개인정보에 대해 적절한 보호조치를 강구하는 체제를 정비하고 있는 사업자를 평가하여 프라이버시 인증 마크를 부여하고 사업활동에 관해 프라이버시 마크 사용을 인정하기 위한 제도

• 2019년 3월 시점 동 협회가 발급하는 프라이버시 마크를 부여받은 기업은 총 16,220개사

▶ **(운영 체계)** 이 인증제도는 부여기관, 심사기관, 연수기관 등 복수 기관 고유의 역할을 통해 운영, 관리가 이뤄지고 있음

• 프라이버시 마크 부여 기관(부여 기관): 일본정보경제사회추진협회(JIPDEC)
  - 부여 기관은 심사 기관 지정, 사업자의 프라이버시 마크 부여 신청 심사 등 프라이버시 마크 제도를 적정하게 운용하는 역할을 담당
  - 학계, 전문가, 사업자 단체 대표, 소비자 대표, 법조인 등으로 구성된 프라이버시 마크 제도 위원회를 통해 1) 제도에 관한 기준/규정 등의 책정/개정, 2) 심사 기관/연수 기관 지정 및 지정 일시 정지/취소, 3) 프라이버시 마크 일시 정지/취소, 4) 제도의 운용 상황
• 프라이버시 마크 지정 심사 기관(심사 기관): 프라이버시 마크 제도 위원회의 심의를 거쳐 심사 기관으로 지정 받은 단체
  - 심사 기관은 사업자의 프라이버시 마크 부여 적격성 심사 신청 접수, 신청 내용의 심사·조사 등의 업무를 실시
• 프라이버시 마크 지정 연수 기관(연수 기관): 프라이버시 마크 제도 위원회의 심의를 거쳐 연수 기관으로 지정된 단체
  - 연수 기관은 보조 심사원을 양성하기 위한 연수와 함께 주임 심사원/심사원/보조 심사원이 자격을 유지하기 위한 후속 연수 실시

▶ **(제도 운영 규정)** 프라이버시인증제도 운영을 위한 규정 체계는 전체, 심사기관, 연수기관, 심사원 등록, 부여사업자, 기타 등으로 이뤄지며 주요 하위 체계별 운영 규칙 및 기준은 다음과 같음

표 2_ 프라이버시인증제도 운영 규정 체계

구분	체계 번호	명칭
전체	PMK100	프라이버시 마크 제도 기본 강령
	PMK110	프라이버시 마크 제도 위원회 운영 규칙
	PMK111	프라이버시 마크 제도 위원회 회의 운영 규칙
	PMK120	프라이버시 마크 이의 심사회 운영 규칙
심사기관	PMK200	프라이버시 마크 지정 심사 기관 지정에 관한 규약
	PMK210	프라이버시 마크 지정 심사 기관 지정 기준
	PMK220	프라이버시 마크 부여 적격성 심사를 실시 기준
	PMK230	프라이버시 마크 지정 심사 기관 지정 절차
	PMK240	프라이버시 마크 제도의 확인 심사 실시 기준
	PMK241	프라이버시 마크 지정 심사 기관이 확인 심사를 실시할 때 부여 기관의 승인에 관한 규약
연수기관	PMK300	프라이버시 마크 지정 교육 기관 지정에 관한 규약
	PMK310	프라이버시 마크 지정 교육 기관 지정 기준
	PMK320	프라이버시 마크 심사원 연수 기준
	PMK330	프라이버시 마크 지정 연수 기관 지정 절차

출처: JIPDEC (2019.3)

▶ **(프라이버시 마크 신청 절차)** 프라이버시 마크는 신청→문서심사→현지 심사의 과정을 거쳐 적격여부가 결정

- 신청: 신청서, 개인정보보호관리시스템(PMS)* 운용 기록 및 규정 제출 등

  * Personal information protection Management Systems. JIS Q 15001:2006에서 사업자가 개인 정보 보호를 실천하기 위해서 지는 관리 시스템을 일컫는 표현

- 문서 심사: 형식 심사(서류 검토) + PMS 문서 심사(JIS Q 15001에 근거) + 프라이버시 마크 부여 적정성 심사(표 2 참조) 등
- 현지 심사: 문서 심사의 실제 적용 여부 판단을 위한 현지 실사: 최고경영진 인터뷰, PMS 운용 상황 확인, 현장 실제 적용 상황 확인, 총평
- 적격 여부 결정: 문서 심사 및 현지 심사 결과를 토대로 각 심사 기관의 심사회에서, 프라이버시 마크 부여 적격 여부를 결정

표 3_프라이버시 마크 부여 적정성 심사 기준[2]

심사항목	문항 수	심사항목	문항 수
일반	1	익명가공정보 취득 관련	2
내부 개인정보보호방침	3	정확성 확보	2
외부 개인정보보호방침	3	안전관리 조치	1
개인정보 특정	4	직원 감독	1
법령이나 국가가 정하는 지침 외의 규범	2	위탁자 감독	6
위기 평가 및 위기 대책	6	개인정보에 관한 권리	2
개인정보보호를 위한 자원, 역할, 책임 및 권한	6	개시 등 청구 등에 따른 절차	3
개인정보 내부 규정	2	보유 개인데이터에 관한 사항을 공지	1
개인정보보고 계획수립	2	보유 개인 데이터의 이용 목적 통지	3
긴급사태 대응	4	보유 개인 데이터의 개시	3
운영 절차	1	보유 개인 데이터의 정정, 추가 또는 삭제	3
개인정보 이용 목적 특정	2	보유 개인 데이터의 이용 또는 제공 거부권	4
개인정보의 적정한 취득 여부	1	인식	5
배려가 필요한 개인정보	3	문서화한 정보의 범위	1
개인정보를 취득한 경우의 조치	2	문서화한 정보의 관리	3
개인정보를 취득한 경우의 조치 중 본인에 의해 직접 서면으로 취득된 경우의 조치	3	문서화한 정보 중 기록의 관리	3
개인정보 이용에 관한 조치	3	익명정보 및 상담 대응	5
본인에게 연락 또는 접촉하는 경우의 조치	3	운용 확인	4
개인데이터의 제공에 관한 조치	3	내부 감사	6
외국의 제3자에 대한 제공 제한	2	관리자 검토	4
제3자 제공에 관한 기록 작성 등	2	시정조치	4
제3자 제공을 허락한 때의 확인 등	2		

출처: JIPDEC (2018.7)

2 https://privacymark.jp/system/guideline/pdf/pm_shinsakijun.pdf

(2) 일본품질보증기구(JQA): JIS Q 15001

▶ **(개요)** 일본품질보증기구(JQA)가 조직 차원에서 개인정보를 적절하게 관리하기 위한 관리시스템의 요구사항을 정한 규격

- JIS Q 15001 단독심사와 함께 ISO/IEC 27001(정보보안 관리시스템)과의 조합 심사서비스도 병행 제공

▶ **(인증 범위)** JIS Q 15001은 적용 범위를 조직의 특성과 규모에 따라 탄력적으로 정의하여 인증을 발급

- 동 인증은 기업이나 조직의 사업 전략에 따라 개인정보를 많이 취급하는 부서나 사업부 등에 한정하여 적용 범위를 설정할 수 있음
- 또한 조직의 자원이나 진척 상황에 따른 단계적인 인증이 가능

표 4_JIS Q 15001인증과 프라이버시 마크 인증 비교

구분	JIS Q 15001 인증	프라이버시 마크 인증
대상·단위	법인 단위/조직 단위	법인 단위
적용/인정 기준	JIS Q 15001	JIS Q 15001
유효 기간 (갱신 기간)	3년 갱신 (1년마다 정기 심사)	2년 갱신
심사 기관	JQA	지정 심사 기관
증서	JQA발행의 JIS Q 15001등록증	JIPDEC 발행 프라이버시 마크등록증
타 규격과의 조합	ISO/IEC 27001와 조합 심사가 가능	프라이버시 마크 단독 심사
비고	• JIS Q 15001 규격은 일본개인정보보호법, 정부 기본 방침, 분야별 가이드라인을 조직 경영에 보편적으로 반영하기 위한 비교적 상위 수준의 요구 사항을 기술 • 개별 사업자들이 JIS Q 15001 규격을 제대로 적용하기 위해서는 각자의 비즈니스 특성이나 조직 체계 등을 고려한 고유의 개인정보관리 시스템 구축과 이를 실천하기 위한 규정집 마련이 필요	• JIS Q 15001 규격이 기업 단위에서 적절히 반영되고 있는지, 다양한 업무 환경에서 시행되고 있는지에 대해 심사하여 이를 인증하기 위한 제도 • PDCA(Plan-Do-Check-Act) 사이클에 따라 지속적, 동태적으로 개선될 수 있는 구조가 확립되어 있는 지 역시 중요한 평가 요인

출처: JQA 홈페이지 (2019.3)

▶ **(인증평가 주안점)** JIS Q 15001은 ▲개인정보의 라이프 사이클에 따른 위기 평가 실시 상황, ▲개인정보의 취득·이용·제공에 관한 상세한 규칙 설정 및 적용 상황, ▲'개인 정보에 대한 본인의 권리'에 대한 상세 규칙 설정 상황 등을 중심으로 평가를 실시

- JIS Q 15001 인증에서는 조직 내에 감사 책임자를 지정하고 정기적 또는 필요 시 개인정보보호 관리시스템(PMS)의 운영 체계가 동 인증 기준에 적합하게 운영되고 있는지 감사를 의무화
- 동 인증에서는 개인정보를 취득할 경우, 이용 목적을 명확히 하고 적법하고도 공정한 방법으로 취득하며, 본인의 동의하에 취득할 것을 요구
- 동의를 받을 때는 본인에게 사업자의 개인정보 보호 책임자를 명시하고 이용 목적을 알려야 하며, 개인정보의 공개·정정·삭제의 권리를 알릴 필요가 있음
- 개인정보를 보유하는 사업자는 이를 안전하게 관리하고 분실, 파괴, 누설 등으로 인해 개인정보를 훼손하고 본인에게 불이익을 주지 않도록 조치를 강구해야 함

▶ **(취득 기간)** 준비 개시부터 등록증 발급까지 통상 1년 정도 소요되며, ISO/IEC 27001 인증을 보유한 조직은 약 6개월 소요

(3) TrustArc의 TRUSTe

▶ **(개요)** 미국의 CBPR 인증평가 제도로서 미 연방/주법, GDPR 및 각국 규제와 베스트 프랙티스 관행에 따라 기업 및 조직의 프라이버시 관리 프로세스 업데이트를 지원하기 위해 마련

- EFF(Electronic Frontier Foundation)와 CommerceNet 컨소시엄에 의해 설립된 TRUSTe는 인터넷에서 사용자들의 신뢰를 확보할 수 있도록 TRUSTe "trustmark" 프로그램을 운영
- 제3자 심사기관의 평가 및 인증을 통해 개인 정보를 다루는 웹사이트에 대한 신용도 및 신뢰도를 향상시키는 것이 목적
- TRUSTe는 CBPR 및 TRUSTe 자체 개발 인증을 포함한 각종 인증제도의 평가를 수행하고 있으며, APEC DPS 또는 TRUSTe 자체 채널을 통해 EU 집행위원회 등 국외 관계 기구와도 소통 및 협업
- 현재 Enterprise Privacy, Privacy Shield, APEC CBPR, APEC PRP, Children's Privacy, EDAA Privacy, Data Collection 등의 인증서를 발급

▶ **(인증방식 및 책임)** 신청한 기업들을 대상으로 현장 실사 없이 제출된 문서 검토를 통해

평가하며 약 4주간의 기간에 걸쳐 인증을 진행

- TRUSTe 자체 인증 수행 경험을 바탕으로 구성된 내부의 세부 인증 가이드가 마련되어 있으며, 이를 소프트웨어 기반의 시스템으로 구축하여 활용
- 인증을 신청하는 기업은 개인정보보호에 대한 서약을 수행하겠다는 의사를 증명하기 위해 자사의 개인정보보호 관행을 공개하고 TRUSTe가 자사의 개인정보 보호관행 준수 여부를 조사하는 것에 대해 동의
- TRUSTe 개인정보보호 정책에 대한 인증을 의미하는 TRUSTe의 인장은 해당 인장을 표시하고 있는 기업 또는 조직의 개인정보보호 프로그램, 개인정보처리방침, 개인정보보호 관행 등이 유럽연합과 미국의 개인정보보호 요구사항에 부합한다는 것을 입증
- TRUSTe는 연간 단위의 재인증 및 개인정보 보호 정책에 관한 의견 제도에 따른 불만 사항 접수를 통해 인증 내용에 대한 준수 상황을 지속적으로 모니터링
- 한편, TRUSTe의 인증을 받은 기업은 각 기업의 개인정보보호 관련 정책 및 개인정보처리방침 혹은 기업에 대한 검증 상태에 영향을 줄만한 변화가 발생하는 경우 TRUSTe에 신속히 알려야 할 책임이 있음

KISA 한국인터넷진흥원

발 행 일 2019년 3월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀
주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118