개인정보 영향평가 (Privacy Impact Assessment) 제도의 국내·외 현황 비교 및 시사점 분석

장 시 영*

최근 EU에서 EU 시민의 개인정보보호 및 개인정보의 자유로운 이동 보장 등을 위해 EU 일반 개인정보보호법(General Data Protection Regulation, GDPR)이 시행되었다. EU GDPR의 적용 대상이 EU 역외대상으로 확대되었으며, 위반사항에 대한 과징금 부과 등 강제성을 지님에 따라 국내 기업의 대응을 위한 핵심 사항으로써 개인정보보호 사전예방제도인 개인정보 영향평가(Privacy Impact Assessment, PIA)가 중요해지고 있다.

이에 본고에서는 이렇게 중요해지는 개인정보 영향평가의 기대효과가 무엇이며, 이를 통해 개인정보 영향평가를 수행하는 기업들이 실질적으로 얻게 되는 이익이 무엇이 있는지를 먼저 살펴보았다. 다음으로, 한국을 포함한 미국, EU, 캐나다, 호주, 뉴질랜드 등 개인정보 영향평가 제도를 시행하는 각 국가별 제도 현황 및 특징을 비교하여 각 나라별 개인정보 영향평가 대상, 방법 및 관련 법제, 후속조치 등에 있어 차이점을 확인하였다. 현재 한국에서 시행하는 개인정보 영향평가제도에 있어 민간분야로의 개인정보 영향평가 의무대상 확대, 개인정보 영향평가 수행 전 개인정보 처리 위험도 분석을 통한 예비PIA 실시, 개인정보 영향평가 수행 후 결과보고서 공개 등의 제도 개선을 통해 향후 개인정보 영향평가를 포함한 개인정보보호 제도 및 정책 발전에 있어 큰 진전을 이룰 수 있을 것으로 기대된다.

* 한국인터넷진흥원 개인정보협력팀 선임연구원, 061-820-1836, sychang@kisa.or.kr

목 차

1. 서론 / 2
2. 한국의 개인정보 영향평가 제도 현황 및 특징 / 4
3. 해외 주요국 개인정보 영향평가 제도 현황 및 특징 / 6
(1) 미국의 개인정보 영향평가 제도 / 6
(2) EU의 개인정보 영향평가 제도 / 7
(3) 캐나다의 개인정보 영향평가 제도 / 9
(4) 호주, 뉴질랜드 등 기타 국가의 개인정보 영향평가 제도 / 10
4. 한국의 개인정보 영향평가 제도 발전을 위한 시사점 / 11
5. 결론 / 12

1. 서 론

최근 EU 시민의 개인정보보호 및 EU 내에서의 개인정보의 자유로운 이동 보장 등을 위해 EU 'General Data Protection Regulation(일반 개인정보보호법 : 이하 "GDPR"이라 함)이 시행됨에 따라, EU 역내에 사업장(지사 포함)을 운영하며 개인정보 처리를 하는 사업자 뿐만이 아닌 EU 역외에서 EU 내 시민들에게 재화나 서비스를 제공하는 경우 혹은 EU 내 정보주체가 수행하는 활동을 모니터링하는 경우에도 폭넓게 적용범위가 확대되었으며, EU GDPR을 위반하는 경우 일반적 혹은 중요한 위반사항에 따라 차등적 과징금이 부과되는 등 강제성을 띠고 있다(한국인터넷진흥원, 2018). 이에 따라 EU 시민의 개인정보를 처리하려는 국내 기업의 경우 EU GDPR 대응을 위해 다방면으로 노력하고 있으며, 이러한 대응을 위한 핵심 사항으로써 개인정보 영향평가(Privacy Impact Assessment : 이하 "PIA")가 주목되고 있다(보안뉴스, 2018).

개인정보 영향평가(PIA)는 개인정보처리 신규 시스템 구축 또는 기존 운영 중인 시스템 변경 시 개인정보 처리로 인한 잠재적인 개인정보 침해 발생 가능성 및 영향을 사전에 조사·예측·검토하여 개선방안을 도출하는 체계적인 절차(개인정보 보호법 제33조)를 말한다. 국제 표준화 기구(International Organization for Standardization : 이

하 ISO)에서 발간한 개인정보 영향평가 국제표준지침(ISO29134)에서는 '개인정보를 처리하는 프로세스, 정보시스템, 프로그램, 소프트웨어 모듈, 장치 등에 의한 프라이버시 측면의 잠재적 영향(potential impacts on privacy)을 평가(assessing)하기 위한 조치'로 '개인정보보호적용설계(Privacy by Design)[1]' 보장을 위한 프로세스라고 설명하고 있다. 특히 ISO 국제표준지침에서는 '조직의 광범위한 위험 관리 프레임워크 내에서 개인정보 처리와 관련된 잠재적 위험을 식별, 분석, 평가, 협의, 의사소통 및 조치계획을 포괄하는 프로세스'로써 가능한 초기 단계부터 시작되어야 하며, 프로젝트가 전개된 이후에도 계속되는 프로세스로써 지속성을 강조하고 있다.

그러면 이러한 개인정보 영향평가를 수행함으로써 기업들이 가지는 기대효과는 무엇일까? 왜 EU GDPR을 포함한 세계 여러 나라 개인정보보호 법제에서는 개인정보 영향평가를 규정하고 있는가? 첫 째로, 개인정보 영향평가를 수행함으로써 대상기관(공공 및 민간기관)은 개인정보 침해 발생 가능성을 사전에 확인하고 조치함으로서 개인정보 침해 피해를 사전에 예방할 수 있다. 특히 이를 통해 사후 개인정보 처리시스템 등을 운영할 때 발생하는 문제점들을 해결하는 데 발생하는 비용을 절약할 있다는 점에서 경제적 이익이 있다. 둘 째로, 개인정보 영향평가를 수행함에 있어 대상기관 개인정보보호 담당자는 개인정보 법제도에 대한 이해도 제고와 함께 개인정보보호 관련 규제준수를 충실히 수행할 수 있다. 특히 최근 행정안전부에서 공개한 개인정보 보호법을 위반하여 과태료 1,000만원 이상의 행정처분을 받은 기업들의 법 위반내용을 살펴보면 대부분이 개인정보 영향평가를 수행 시 점검하는 관리적·기술적·법적 개인정보보호조치라는 점(행정안전부, 2018)에서 이를 뒷받침하고 있다. 마지막으로, 개인정보 영향평가를 수행함으로써 개인정보를 수집하는 정보주체에게 개인정보보호를 위해 필요한 조치를 하고 있다는 노력 입증을 통한 대상기관의 대외 이미지 제고도 할 수 있다는 점에서 부과적 이익이 있다고 하겠다.

---

1) 개인정보보호적용설계(Privacy by Design) : 온라인 서비스를 포함하는 IT 기술의 발전에 따라 서비스 기획 단계에서부터 폐기 단계까지의 전체 생애주기(life cycle)에 걸쳐 이용자의 프라이버시와 데이터를 보호하는 기술 및 정책을 적절하게 적용하는 것.

이렇게 대상기관의 개인정보보호를 위해 중요한 개인정보 영향평가는 한국을 포함한 미국, EU, 캐나다, 호주, 뉴질랜드 등 여러 나라들이 시행하고 있으며, 각 나라별로 개인정보 영향평가 대상, 방법 및 관련 법제 등에 있어 차이점이 존재한다. 이에, Ⅱ장에서는 한국의 개인정보 영향평가 제도를 소개하고, Ⅲ장에서는 해외 각 국가별 개인정보 영향평가 제도의 특징 및 한국과의 차이점을 비교하고 이를 통해, Ⅳ장에서는 한국의 개인정보 영향평가 제도의 발전을 위해 필요한 점들을 살피고, Ⅴ장에서 향후 한국의 개인정보 영향평가 제도 발전을 위한 제언을 끝으로 글을 마무리하고자 한다.

Ⅱ. 한국의 개인정보 영향평가 제도 현황 및 특징

한국의 개인정보 영향평가 제도는 2011년 9월 30일, 일반법인 「개인정보 보호법」이 발효됨에 따라 공식적으로 시행되었다. 개인정보 영향평가에 관해 「개인정보 보호법」 제33조에서는 영향평가 대상을 특정 조건에 해당[2]하는 공공기관은 의무적으로 수행하여야 하며, 민간은 영향평가를 적극적으로 수행토록 권고하고 있다. 이는 당시에 민원처리 등 공공의 목적으로 정보주체의 개인정보를 대량으로 수집·처리하고 있던 공공기관의 개인정보보호 강화를 위해 의무대상을 공공기관으로 한정하여 법에서 시행하고 있던 것으로, 「개인정보 보호법」 제정 이전에 기 운영 중인 개인정보처리시스템의 경우, 법 시행 후 5년 이내인 2016년 9월 30일까지 영향평가를 수행토록 경과규정을 두어 현재는 개인정보처리시스템 구축 전 혹은 기존 시스템에서 변동사항이 생긴 경우에만 영향평가를 수행토록 대상을 규정하고 있다.

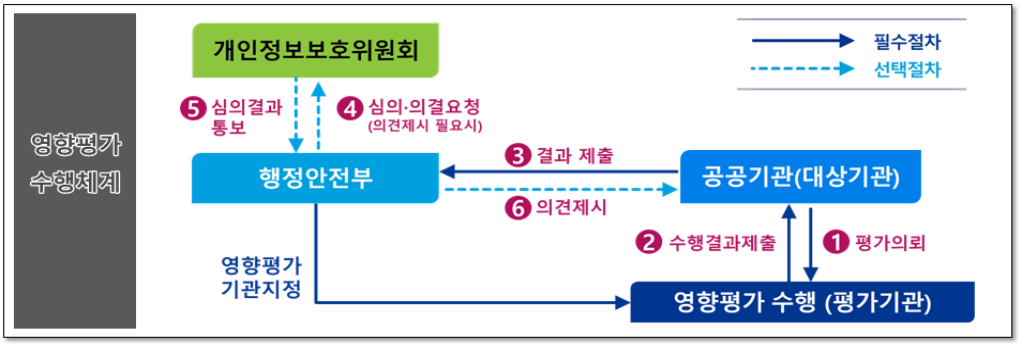
한국의 개인정보 영향평가 제도 수행에 있어 특이점으로는 개인정보 영향평가를 행정안전부장관이 지정하는 기관(이하 “평가기관”)[3] 중에서 의뢰하여 수행토록 평가기관을

2) 「개인정보 보호법 시행령」제35조(개인정보 영향평가의 대상)에서는 ① 의료정보 등 민감정보 또는 주민등록번호 등 고유식별정보 5만명 이상, ② 내·외부 시스템 연계정보 50만명 이상, ③ 일반 개인정보 100만명 이상의 전자적으로 처리할 수 있는 개인정보 파일을 구축·운용할 경우 또는 기존 운영 중인 시스템 내 개인정보파일의 운영체계를 변경하려는 경우 영향평가를 의무수행토록 규정하고 있음

지정하고 있다. 이는 대상기관 및 대상시스템의 기술적 관리적 개인정보 보호조치, 개인정보 수집부터 파기에 이르는 처리단계별 개인정보 보호조치를 전문적이고 독립적으로 수행할 수 있는 외부 평가기관을 통해 공정하고 체계적으로 수행토록 한 조치로써, 「개인정보 보호법」 소관부처인 행정안전부와 개인정보 영향평가 전문기관인 한국인터넷진흥원을 통해 영향평가 지표 및 수행절차에 관한 안내서인 영향평가 수행안내서 발간 및 배포, 영향평가 결과보고서 품질검토, 전문인력의 수행품질제고를 위한 관련 교육 등을 통해 매년 평가기관의 수행품질 향상을 위한 여러 활동들이 수행되고 있다. 이와 함께, 평가기관의 지정 유효기간(3년)을 고시로 정하여 평가기관 갱신을 원하는 기관은 갱신 심사 평가를 받고 일정 점수 이상을 획득한 경우에만 갱신이 가능토록 규정하여 평가기관의 지속적인 영향평가 수행능력 확보를 위해 노력하고 있다.

개인정보 영향평가를 수행한 공공기관의 경우, 그 결과를 행정안전부장관에게 제출토록 법으로 의무화하고 있으며, 영향평가 수행 시 개선사항으로 지적된 부분에 대한 이행계획 등을 영향평가서를 평가기관으로부터 제출받은 날로부터 1년 이내에 행정안전부장관에게 제출토록 하여, 영향평가 수행 후속조치에 관해서도 확인할 수 있는 법적 근거를 마련하여 추진하고 있다.

[그림 1] 한국 개인정보 영향평가 수행체계



3) 2018년 7월 31일 현재, 총 17개 영향평가기관이 지정되어 있으며, 보안전문업체, 감리업체, SI 업체 등 다양한 회사들로 구성되어 있다(영향평가기관 지정현황은 개인정보보호종합포털(www.privacy.go.kr) 영향평가 자료실 참조).

Ⅲ. 해외 주요국 개인정보 영향평가 제도 현황 및 특징

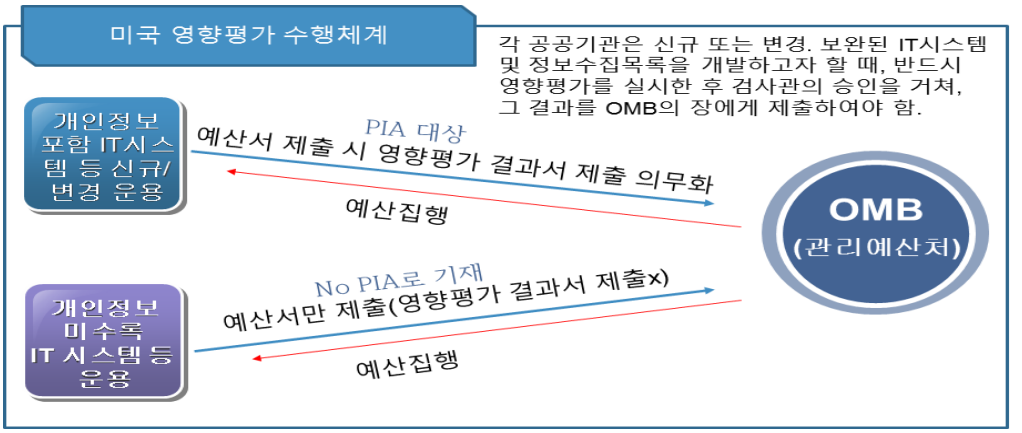
1. 미국의 개인정보 영향평가 제도

미국은 2002년 제정된 전자정부법 제208조에서 전자정부 구현 과정에서 프라이버시가 충분히 보호될 수 있도록 정부기관(공공)의 개인정보 영향평가를 의무화하고 있다. 개인정보 영향평가 대상의 경우, 관리예산처(Office of Management and Budget : 이하 "OMB")[4] 지침에서는 평가되는 정보체계의 규모, 정보의 민감성, 정보의 무단 공개로 초래되는 위험에 비례하여 영향평가를 수행토록 규정하고 있다. 특히, 신규 시스템 구축 시에는 국민의 개인정보를 수집 · 관리 · 배포하는 IT 시스템 혹은 프로젝트의 개발, 10인 이상의 개인정보를 온라인으로 수집하는 경우에 영향평가를 의무적으로 수행하며, 절차 및 시스템 변경 시에는 종이문서 기반 기록을 전자시스템으로 변형하거나 새로운 기술 적용과 같은 IT시스템의 신규 운용이 기존 개인정보에 중대한 변화를 야기하는 경우로 규정하여, 한국의 영향평가 대상과 거의 유사하게 지침에서 규정하고 있다.

특히 미국의 경우, 위 법조항을 이행하기 위해 공공기관으로 하여금 신규 또는 변경, 보완된 IT시스템 등을 개발하고자 할 때, 영향평가 대상기관의 경우는 영향평가 결과보고서를, 그리고 영향평가 미대상기관의 경우에는 영향평가 미대상으로 규정한 근거자료인 예비PIA 보고서를 OMB의 장에게 제출하여 예산집행을 받도록 법으로 강제화하고 있다. 또한, 영향평가를 수행한 경우 그 결과를 연방관보 등을 통해 일반인에게 공개토록 하여 개인정보 처리에 대한 공정성, 투명성, 신뢰성 제고를 위해 노력하고 있다.

4) 관리예산처(OMB)는 공공기관의 개인정보 영향평가 수행을 위한 정책 및 지침을 개발하고, 영향평가 수행을 감독함.

[그림 2] 미국 개인정보 영향평가 수행체계



2. EU의 개인정보 영향평가 제도

앞서 설명한 것처럼, EU는 2018년 5월 25일 시행된 EU GDPR 제35조[5]에서 개인정보 영향평가(Data Protection Impact Assessment : 이하 "DPIA")에 관한 법률적 근거를 규정하고 있다. EU GDPR 내 영향평가 대상은 한국과 미국이 공공기관을 의무로 규정한 것에 반해, 해당 개인정보 처리가 정보주체의 권리·자유에 높은 위험(high risk)을 초래할 것이 예상되는 경우 개인정보 처리 전 컨트롤러(공공 및 민간 포함)[6]로 의무화하고 있다. 또한, 평가대상이 되는 개인정보 처리유형을 규정하고, 영향평가 결과 개인정보의 처리가 높은 위험을 초래할 가능성이 있는 경우 감독기구와 사전에 협의토록 규정(EU GDPR 제36조)하고 있다.

EU GDPR 제35조제3항에서는 높은 위험을 초래할 것이 예상되어 개인정보 영향평가가 의무적으로 시행할 것이 요구되는 경우로, ① 프로파일링을 포함한 자동화 처리에 근거한 자연인에 대한 체계적이고 광범위한 평가(해당 평가에 기반한 결정이 해당

5) EU GDPR 제35조 : 개인정보 영향평가 대상, 방법, 후속조치 등에 대한 전반적인 사항을 규정.
6) 컨트롤러(Controller) : 개인정보 처리의 목적과 수단을 결정하는 주체로써 자연인을 비롯한 법인, 정부부처 및 관련기관, 기타 단체 등을 포함하고 있다(EU GDPR 제4조제7항)

정보주체에게 법적 효력을 미치거나 이와 유사하게 중대한 영향을 미치는 경우), ② 민감정보 또는 유죄판결 및 형사범죄에 관한 대규모 처리정보, ③ 공개적으로 접근 가능한 장소에 대한 대규모의 체계적 모니터링정보 등을 규정하고 있다.

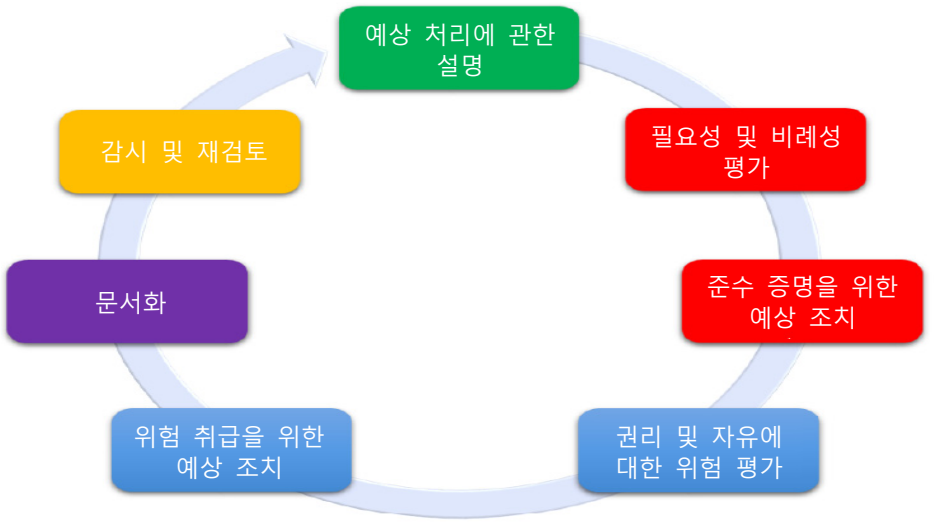
[그림 3]개인정보 처리 시 높은 위험의 판단 기준

[출처] 한국인터넷진흥원(2018), 우리 기업을 위한 유럽 개인정보보호법(GDPR) 가이드북 136~137면 참조

EU GDPR에서 규정하는 개인정보 영향평가 시 포함되어야할 최소한의 내용으로는 ① 예상되는 개인정보 처리(processing)의 목적에 대한 체계적 기술, ② 목적 관련 개인정보 처리작업의 필요성과 비례성에 대한 평가, ③ 정보주체의 권리와 자유에 대한 위험평가, ④ 개인정보 보호와 GDPR 준수를 입증하기 위한 보안(security) 및 보호조치(safeguards), 메커니즘(mechanisms) 등 위험을 처리할 것으로 예상되는 조치를 규정하고 있으며, 미국에서와 같이 영향평가 결과보고서 공개가 법적으로 의무화되어 있지는 않지만 개인정보보호책임자(Data Protection Officer, DPO)는 영향평가 결과보고서의 전체 또는 일부라도 공개할 것을 검토할 필요가 있으며, 결과보고서를 공

개하는 경우에는 평가결과 전체가 아닌 기관의 영업비밀 및 상업적으로 민감한 정보를 제외한 주요 결과 요약만이라도 공개토록 권고하고 있다.

[그림 4] 개인정보 영향평가 수행절차



[출처] EU 제29조 작업반(Working Party 29), 개인정보 영향평가 가이드라인(2017.4)

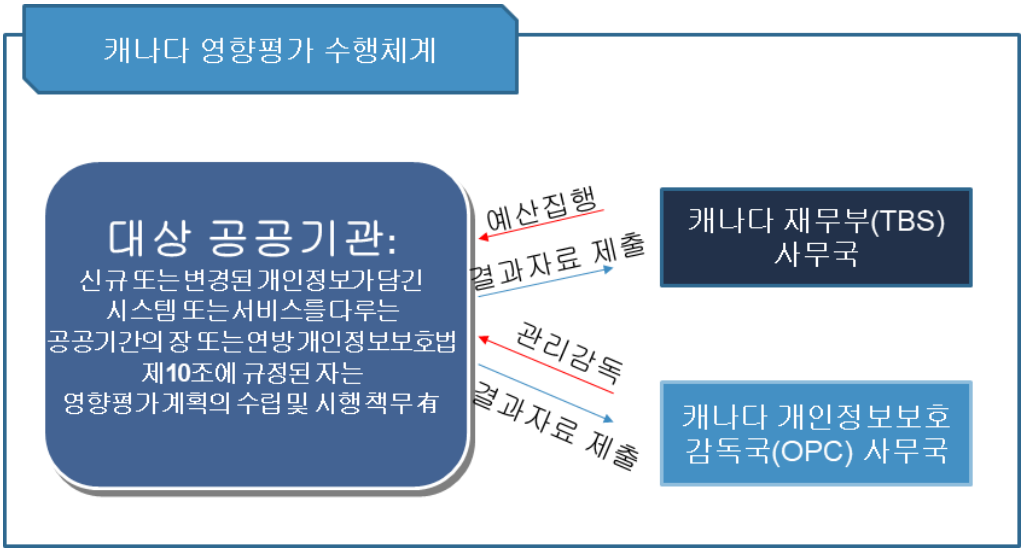
3. 캐나다의 개인정보 영향평가 제도

캐나다는 연방 개인정보보호법(Privacy Act) 제10조에 따라 대상 공공기관[7]은 개인정보 영향평가를 수행토록 법적으로 의무화하고 있으며, 민간기관은 개인정보보호 및 전자문서법(PIPEDA)을 통해 특정분야(금융, 의료)만 영향평가를 법적으로 의무화하고 있다. 특히 미국에서와 같이 영향평가 대상 공공기관이 영향평가 수행 시 영향평가 결과를 캐나다 재무부(TBS)에 제출해야 해당 사업에 대한 예산집행을 받으며, 영향평가 결과자료 제출 및 수행에 대한 전반적인 사항은 캐나다 개인정보보호 감독기구(Office of the Privacy Commissioner of Canada, OPC)의 감독을 받는다.

7) 대상 공공기관 : 신규 또는 변경된 개인정보가 담긴 시스템 또는 서비스를 다루는 공공기관 등

특히 공공기관 개인정보보호 담당자는 OPC가 제공하는 지침에 따라 개인정보 파일 운용 시 개인정보 영향평가 수행 전 프로세스인 예비PIA를 수행토록 권고받으며, 예비 PIA를 수행 시에는 ① 수집, 이용, 공개되는 개인정보의 양 및 유형, ② 해당 프로그램 또는 서비스에 대한 법률 및 정책권한, ③ 해당 프로그램 또는 서비스에서의 개인정보 침해가능성, ④ 개인정보 감독기구와의 협의절차 구상, ⑤ 최종 평가범위 및 일정 등을 점검 후 개인정보 영향평가 실시여부를 최종 결정하도록 규정하고 있다.

[그림 5] 캐나다 개인정보 영향평가 수행체계



4. 호주, 뉴질랜드 등 기타 국가의 개인정보 영향평가 제도

호주, 뉴질랜드 등 개인정보 영향평가를 수행하는 다른 국가들의 경우, 각 국가의 개인정보보호 감독기구(감독관)가 개인정보 영향평가 수행지침(가이드)을 발간하여 자율적으로 영향평가를 수행토록 권고하고 있다. 특히 뉴질랜드에서는 실제 영향평가를 수행하기 전 영향평가 실시여부를 판단할 수 있는 예비PIA를 자체적으로 수행할 수 있는 예비PIA 수행안내서를 통해 최소한 영향평가 수행여부를 사전에 판단할 수 있도록 하고 있다.

Ⅳ. 한국의 개인정보 영향평가 제도 발전을 위한 시사점

위에서 한국의 개인정보 영향평가 제도와 해외 다른 국가들의 영향평가 제도를 살펴본 결과, 개인정보를 취급하는 정보시스템 혹은 프로젝트 구축(개인정보처리) 전 개인정보 침해 요인을 파악하고 개선방안을 수립·적용하여 개인정보 침해사고를 사전에 예방하려는 영향평가의 목적은 모두 같으며, 실제 영향평가 수행방식에 있어서도 개인정보 영향평가 국제표준지침(ISO29134)에서 일반적인 운영구조로 규정한 ① 영향평가 준비단계(법률, 지침, 규칙, 기존 정책 등을 바탕으로 개인정보 영향평가 필요성 판단), ② 영향평가 수행단계(개인정보보호 프레임워크를 바탕으로 시스템의 데이터 흐름 분석 및 개인정보 위험평가를 통한 개선사항 도출), ③ 영향평가 후속조치(영향평가 보고서 준비 및 개선사항 반영)를 모두 공통적으로 따르고 있는 것을 확인하였다.

다만, 영향평가 의무대상에 있어, 한국, 미국, 캐나다의 경우 공공을 의무로 규정하고 있던 것에 반해, EU GDPR에서는 공공 및 민간을 모두 포함한 개인정보처리자를 의무대상으로 규정하였으며, 호주, 뉴질랜드 등 다른 국가들은 공공 및 민간 모두 영향평가 수행을 권고하고 있다는 점에서 차이점을 발견하였다. 또한, 영향평가 수행여부를 판단하는 기준에 있어서도 한국의 경우는 일정 규모의 개인정보를 처리하는 개인정보 파일을 대상으로 영향평가 수행을 의무토록 법으로 규정하여 양적인 기준을 바탕으로 영향평가 수행여부를 판단토록 하고 있는 것에 반해, EU, 호주, 뉴질랜드 등 다른 국가들에서는 해당 개인정보를 처리 시 높은 위험을 초래할 것이 예상되는 경우에 대해 사전에 개인정보 처리에 따른 위험도 분석을 통한 예비PIA를 바탕으로 자체적으로 영향평가 수행여부를 판단토록 규정하고 있다.

마지막으로, 한국의 경우, 영향평가 수행 후 영향평가 결과보고서를 행정안전부장관에게 제출토록 법으로 규정하고 있는 반면, 미국, EU, 캐나다 등 다른 국가들은 영향평가 결과보고서 제출과 함께 일반인들에게 영향평가 결과를 전부 혹은 부분적으로나마 공개토록 하고 있다는 점에서 차이점이 있다. 이는 개인정보처리에 있어 투명성 제고와 정보주체로부터의 신뢰성 제고를 위해 한국을 제외한 다른 국가들에게는 중요한

영향평가 후속절차로써 실제 국민들의 세금으로 운영되며, 공공의 업무를 위해 막대한 양의 개인정보를 처리하는 공공기관의 경우, 정보주체의 개인정보를 안전하게 관리하고 있다는 것을 보여주는 하나의 좋은 사례일 것이다.

Ⅴ. 결론

앞서 살펴본 것처럼, 한국을 포함한 미국, EU, 캐나다 등 많은 국가들이 'Privacy by Design(개인정보보호적용설계)' 원칙을 가장 잘 반영하여 선제적으로 개인정보보호를 할 수 있는 좋은 제도로써 개인정보 영향평가 제도를 수행하고 있다. 한국의 경우도 2011년「개인정보 보호법」시행 당시부터 개인정보 영향평가를 시행하여 현재는 많은 공공기관들이 개인정보처리시스템을 구축하고 운용하는 데 있어 개인정보보호 관련 법제도에 대한 이해도 제고와 함께, 관련 규제 준수를 충실히 이행하고 있으며 개인정보보호에 있어 많은 기대효과를 보고 있는 것으로 생각된다. 다만, EU GDPR에서 영향평가 수행 의무대상을 공공만이 아닌 민간을 포함한 개인정보처리자로 규정하였다는 점에서 향후 EU 시민의 개인정보를 처리할 예정이거나 EU에 진출할 국내 민간기업들의 규제준수 비용 절감 등을 위해 적용 의무대상을 민간으로까지 확대할 필요성에 대해 검토할 필요가 있다. 특히, 이를 통해 의무대상을 민간으로까지 확대하여 국내법에서 규정한 개인정보 영향평가를 수행 시 EU GDPR 등 다른 나라 법에서 규정한 영향평가 요건을 충족하도록 규정하면 민간기업들에 있어서도 많은 실익이 있을 것으로 생각된다.

또한, 현재 EU, 호주, 뉴질랜드 등 많은 국가들에게서 개인정보 처리에 따른 위험도 분석을 통한 예비PIA를 수행하여 영향평가 수행여부를 자체적으로 판단하고 있으며, 이는 국내법에서 규정하고 있는 양적인 수행기준을 바탕으로 영향평가 의무대상을 판단하는 현 제도에서 발생할 수 있는 약점(실제 처리하는 개인정보 수 이외의 판단요소들을 고려하지 못하는)을 보완할 수 있을 것으로 기대된다. 마지막으로, 한국을 제외한

다른 국가들이 개인정보 영향평가를 수행 후 영향평가 결과보고서를 일반에게 공개하고 있다는 점에 주목할 필요가 있다. 다른 국가들은 결과보고서 공개를 통해 개인정보 처리에 대한 투명성 제고 및 정보주체로부터의 신뢰도 제고 등을 가능케하며, 실제 영향평가를 수행하여 기업의 인식제고에도 도움을 받고 있는 것으로 생각된다. 이에, 한국의 경우도 영향평가 수행 후 공개할 수 있는 범위 내에서 결과를 공개토록 법을 개정한다면, 영향평가를 수행하는 대상기관 및 개인정보를 제공하는 정보주체 모두에게 상호이익이 발생할 것으로 생각된다.

앞에서 열거한 여러 다른 나라들의 개인정보 영향평가 제도의 좋은 점은 받아들이고, 또 한국의 개인정보 영향평가 제도의 좋은 수행 사례들은 다른 나라들에게 공유한다면 향후 한국 개인정보보호 제도 및 정책 발전에 있어 큰 진전이 있을 것으로 생각된다.

참고문헌

보안뉴스, 2018. “[PIS FAIR 2018] GDPR 대응, 개인정보 영향평가에 주목해야” 김경애, 2018. 6. 1.

한국인터넷진흥원, 2018. “우리 기업을 위한 EU 일반 개인정보보호법 가이드북” 2018.5.

행정안전부, 2018, “개인정보 보호법 위반 행정처분 결과 공표” 2018. 6. 26.

ISO/IEC 29134, 2017, “Guidelines for Privacy Impact Assessment” 2017. 6.

Article 29 Data Protection Working Party, 2017, “Guidelines on Data Protection Impact Assessment(DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679” 2017. 10. 4.

EU GDPR 2016, “Regulation(EU) 2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation)” 2016. 4. 6.