미국 전자정부법(2002)의 프라이버시 조항 시행 지침 발표

미래한국연구실 주임연구원 최선희
(T. 570－4034, shchoi@kisdi.re.kr)

1. 개 요

2003년 9월 26일 OMB(Office of Management and Budget: 관리예산처)의 장인 Joshua B. Bolten은 전자정부법(2002)[1]의 프라이버시 조항을 시행하기 위한 OMB 지침을 행정부서의 장에게 시달하였다.

정부는 시민의 프라이버시를 보호할 의무가 있으며, 이 지침서는 시민이 정부와 상호작용할 때 프라이버시를 보호할 것을 담고 있다. 지침은 정보기술(IT)을 사용하여 새로운 정보를 수집할 때, 또는 수집된 개인식별정보를 취급할 새로운 IT시스템을 행정기관에서 개발하거나 구매할 때, 각 기관이 개인에 대한 정보를 내부적으로 어떻게 취급해야 하는지에 대한 고려사항을 안내하고 있다. 개인이 전자적으로 제공한 정보를 정부가 취급하는 방법에 대해 알려줌으로써 미국 시민들이 개인의 정보가 보호받고 있음을 확신시킨다.

전자정부법의 프라이버시 목표는 '안전한 사이버스페이스를 위한 위한 국가전략(National Strategy to Secure Cyberspace)'을 보완하는 것이다. 국가전략이 지적하는 바와 같이 프라이버시와 타 시민적 자유에 대한 보호를 강화하는 사이버스페이스 보안 프로그램은 연방정부 내에서 강력한 프라이버시 정책과 실천을 수반하여 정보를 보호함으로써 '프라이버시와 보안'이라는 두가지 목표를 달성할 수 있게 한다.

전자정부법(2002)의 제208조는 OMB가 법상 프라이버시 조항 이행과 관련한 지침을 공표하도록 규정하고 있고, 행정기관의 프라이버시 영향 평가(Privacy Impact Assessments)[2]에 대해 자세히 언급하고 있다. 따라서 법 조항과 지침 내용을 구체적으로 살펴보고자 한다.

2. 전자정부법 제208조(Section 208)의 주요 내용

법 제208조는 크게 7개 항목으로 구성되어 있다. Ⅰ. 총칙, Ⅱ. 프라이버시 영향 평가, Ⅲ. 기

1) 미국의 전자정부법(E-Government Act of 2002)은 2002년 12월 17일 대통령의 승인을 얻어 2003년 4월 17일부터 효력을 발생하였음

2) 새로운 정보시스템의 개발・시행이 개인정보권에 미칠 영향을 사전에 조사・예측・검토하는 제도

관 웹사이트에 대한 프라이버시 정책, Ⅳ. 기계판독형 형식(format)에 대한 프라이버시 정책, Ⅴ. 본 지침에 의해 편입된 프라이버시 정책, Ⅵ. 기관의 프라이버시 활동/담당자 임명, Ⅶ. 보고의무이며, 지침의 핵심에 해당하는 프라이버시 영향 평가에 대해 주로 안내하고자 한다.

가. 프라이버시 영향 평가(PIA)

본 항목이 제208조의 핵심이라고 볼 수 있으며, 정의, 적용시점, 평가내용 등에 대하여 자세히 규정하고 있다.

첫째, 각 용어에 대한 정의는 다음과 같다.

'개인(Individual)'은 미국시민권자와 영주권이 있는 외국인을 말한다.

'신원정보(Information in identifiable form)'는 IT 시스템 또는 온라인 집합체에 있는 정보로서 개인을 바로 식별할 수 있는 정보[3], 기관들이 다른 데이터 요소와의 결합을 통하여 특수하게 개인을 식별하도록 의도한 것[4]을 말한다.

'정보시스템(Information technology(IT))'은 데이터 또는 정보에 대하여 자동적인 획득, 저장, 조작, 관리, 이동, 통제, 전시, 스위칭, 교환, 전송, 수령하도록 설계된 장비, 소프트웨어, 상호연계된 시스템, 서브시스템 등을 의미한다.

'주정보시스템(Major information system)'은 OMB 회람 A-130과 A-11에서 정의한 '크고 민감한' 정보시스템을 포함한다. 기관업무에 매우 중요하고 개발・운영・유지비용이 높으며, 기관의 프로그램, 재정, 재산 등 행정에 있어 중요한 역할을 수행하기 때문에 특별한 관리주의 의무가 필요하다.

'국가보안시스템(National Security System)'은 연방정부가 운영하는 정보시스템으로서 국가보안과 관련된 정보활동・암호활동, 군의 명령 및 통제・무기와 무기시스템의 필수장비, 군 또는 정보활동의 직접적 수행에 꼭 필요한 시스템을 포함한 기능, 운영, 사용 등을 말한다. 그러나 임금, 재정, 군수, 인사관리와 같은 일상적인 행정적 업무에 사용되는 시스템은 포함되지 않는다.

'프라이버시 영향 평가(Privacy Impact Assessment: PIA)'는 취급된 정보의 분석방법이다. 프라이버시와 관련된 적절한 법・제도적 정책요건을 따르도록 하고, 전자적 정보시스템에서 신원확인양식에 대한 정보를 수집・관리・전파할 때의 위험과 효과를 결정하며, 잠재적인 프라이버시 위험을 완화할 수 있는 정보취급 보호 및 대안 절차를 검사하고 평가한다.

'표준화된 기계판독형 포맷환경의 프라이버시 정책(Privacy policy in standardized machine-

3) 이름, 주소, 사회보장번호, 타 식별번호 또는 코드, 전화번호, 이메일 주소 등

4) 성별, 인종, 출생일, 지리적 표시 등의 조합을 통하여 알 수 있는 간접적인 식별 정보

readable format)'은 웹브라우저를 통해 자동판독이 가능한 표준컴퓨터언어로 쓰인 사이트 프라이버시 이행보고서를 말한다.

둘째, 프라이버시 영향 평가(PIA)의 적용시점은 다음과 같이 규정되었다.

전자정부법에서는 기관들이 일반인 관련 신원정보를 수집·관리·전파하는 IT시스템 또는 프로젝트를 개발·구매하기 전에 PIA를 행할 것을 요구하고, 문서감축법(PRA)을 따르도록 하며, 10명 이상[5]의 신원정보에 대한 새로운 전자적 수집행위를 시작하기 전에 실시하도록 권고한다.

일반적으로 PIA는 어떤 시스템 변화가 새로운 프라이버시 위험을 야기할 때마다 실행하고 갱신하도록 되어 있다. 다음의 〈표〉를 보면 적용시점을 자세히 알 수 있다.

〈표〉 PIA의 적용 시점

사 건	내 용
① 전환	문서기반의 기록이 전자적 시스템으로 변환될 때
② 익명 또는 실명	기존 정보목록에 적용된 기능들이 익명의 정보를 신원정보로 변화시킬 때
③ 중요한 시스템 관리상의 변화	신기술이 적용된 기존의 IT 시스템을 새롭게 사용함으로써 신원정보가 그 시스템에서 관리되는 방법이 명백히 변화될 때[6]
④ 중대한 통합	기관이 비즈니스 프로세스를 채택하거나 변경하여 신원정보를 담고 있는 정부 DB가 타 DB와 통합, 중앙화되거나 그렇지 않으면 중대하게 조작될 경우[7]
⑤ 새로운 공공접근	사용자 인증기술(예:비밀번호, 디지털인증서, 생체인식)이 일반인이 접속한 전자적 정보시스템에 새롭게 적용될 때
⑥ 상업적 소스	기관들이 상업적 또는 일반소스로부터 구매하거나 얻은 신원정보 DB를 기존의 정보시스템으로 시스템상 통합할 때
⑦ 관계부처간 새로운 사용	기관들이 신원정보를 새롭게 사용하거나 교환을 포함한 공유기능상으로 협력할 때(수평적 전자정부이니셔티브의 수행하는 경우로서 주관기관은 PIA를 준비해야 함)
⑧ 내부 흐름 또는 수집	비즈니스 프로세스의 변경이 정보의 새로운 사용이나 공개 또는 통합과 같이 신원정보의 시스템상 추가 아이템의 결과로 나타날 때
⑨ 데이터 특성에 따른 변경	수집목록에 부가된 새로운 신원정보가 개인적 프라이버시에 위험을 증대시킬 때[8]

5) 행정기관, 정부대행기관, 또는 연방정부 직원을 제외한 인원 수를 말함

6) 예를 들어, 어떤 기관이 복합의 데이터 저장소에 접근하기 위한 새로운 관련 DB 기술, 웹기반 프로세싱을 사용할 때로서, 이러한 추가적인 조치는 이전에 존재하지 않았던 데이터의 공개방법, 더 개방된 환경을 구현하게 됨

셋째, PIA에 반드시 포함되어야 할 내용에 대하여 규정하고 있다.

먼저 PIA는 다음과 같은 컨텐츠를 분석·기술해야 된다. ⅰ) 어떤 정보가 수집되는가?(성질과 소스), ⅱ) 정보는 왜 수집되어야 하는가?(적격성 결정), ⅲ) 정보의 예정된 활용인가?(기존 데이터의 확인), ⅳ) 정보가 누구와 공유될 것인가?(상세한 프로그램상의 목적으로 타 기관과 공유하는 것), ⅴ) 어떤 때에 개인이 정보제공을 줄여야 하는가?(정보의 자발적 제공이 필요한 곳) 또는 정보의 특수한 사용을 동의해야 하는가?(필요로 하거나 공인된 사용과는 다른 것) 또는 개인은 동의를 어떻게 표현할 수 있고, 정보는 어떻게 보호될 것인가?(행정적, 기술적 통제방법들), ⅵ) 기록을 담당하는 시스템이 프라이버시법(1974) 하에서 만들어진 것인가? 그리고 PIA는 그 수행의 결과로서 IT 시스템이나 정보수집목록과 관계된 기관의 선택을 규명해야 한다.

또한 기관들은 새롭거나 많이 변경·보완된 IT시스템 및 정보수집목록을 개발하고자 할 때 PIA를 시작해야 한다. PIA의 정도와 내용은 수집된 정보의 성격과 IT 시스템의 크기와 복잡성에 적합해야 한다. IT 개발단계에서 이와 관련된 문서화 작업시 프라이버시를 공표해야 하고, 시스템이 개인의 프라이버시에 영향을 미칠 수 있음을 공지해야 한다. 주정보시스템에 있어서도 PIA는 정보의 수집과 흐름의 영향, 수집방안 및 설계에 따르는 취급과정, 파악된 위험을 해소하기 위한 적절한 조치 등에 대한 광범위한 분석이 반영되어야 한다. 루틴한 DB 시스템의 경우 기관들은 PIA에 대해 표준화된 접근방법을 사용하여야 한다.[9] PIA의 정도와 내용 외에도 정보의 라이프사이클에 대한 분석/공동연구가 진행되어야 한다. 즉 기관들은 수집, 사용, 유지, 처리, 공개, 삭제와 같은 정보의 라이프사이클을 고려하여 각 단계별로 정보의 처리실태가 개인의 프라이버시에 어떻게 영향을 주는지 평가해야 한다.

마지막으로 검토와 발표에 대해 규정하고 있다. 기관들은 PIA 문서와 요약문을 검사관[10]으로부터 승인받아야 한다. 2005년 재원을 요구하고, 이전 OMB의 지침을 따르는 각각의 IT 시스템은 늦어도 2003년 10월 3일까지 OMB의 장에게 PIA를 제출해야 한다.[11]

넷째, 문서감축법(Paperwork Reduction Act: PRA)과의 관계가 제시되어 있다. 공동으로 정보수집신청(Information Collection Request: ICR)을 하고 PIA를 제출하여야 한다.

7) 예를 들어 DB가 정보에 있어 하나의 중앙소스를 창출하기 위해 통합될 때로서, 하나의 링크가 데이터를 여러방법으로 수집하게 되어 이전에는 논쟁한 적이 없는 프라이버시 문제를 낳음
8) 건강 또는 금융정보가 부가된 경우
9) 예를 들어 체크리스트나 템플릿 사용
10) 기관의 CIO나 타 기관의 피지명자 대표로서 바로 시스템을 구매하는 공무원 또는 PIA를 수행하는 공무원을 말함
11) 이러한 PIA 문서와 요약문은 공개적으로 이용할 수 있어야 한다.

PRA 하에서 단순한 정보수집의 재신청일 경우 새로운 PIA는 시행할 필요가 없고, 원본과 특성상 명백한 차이가 있는 정보를 수집하기 위한 ICR을 고칠 경우에 새로운 PIA가 필요하다.

다섯째, 프라이버시법(1974)과의 관련성은 다음과 같다. 시스템상 기록의 범주, 기록의 활용, 취급정책과 실행 등에서 PIA와 기록제도(System of Records)가 중복된다면 기관들은 프라이버시법 하부조항에서 요구한 기록제도 주의사항을 개발할 때 PIA 시행을 선택할 수 있다. 또한 PIA는 연방관보에 공개적으로 이용될 수 있다.

나. 보고의무 규정과 기타 프라이버시 정책

기관들은 본 지침에 따라 매년 전자정부법 실태보고서의 일부로서 OMB에 해마다 결과보고서를 제출해야 한다. IT 시스템을 이용하고 정보수집활동을 하는 모든 기관들은 2003년 12월 15일까지 OMB에 예산안의 제출여부와 관계없이 1차보고서를 제출해야 한다.

기관들의 웹사이트와 관련한 프라이버시 정책으로 OMB의 Memorandum 99-18에 따라 정보수집과 공유에 대한 동의, 프라이버시법 또는 기타 프라이버시 관련법들(아동프라이버시 보호법 등) 하에서의 권리 등이 규정되었다.

한편 본 지침을 통하여 연방기록에 대한 개인정보보호와 프라이버시정책의 1차 책임을 지우는 절차와 관련된 Memorandum 99-05, 시민의 구체적인 개인정보를 수집하는 정부웹사이트 또는 어떤 웹페이지라도 주요 진입접점에 프라이버시 정책을 고지하도록 하는 Memorandum 99-18, 아동 온라인 프라이버시 보호법(Childeren's Online Privacy Protection Act: COPPA)에 대한 Memorandum 00-13을 수정하고 있다.

3. 맺음말

지금까지 미국의 전자정부법상의 프라이버시 조항에 대한 내용을 정리하였다. 주된 내용으로는 행정기관이 전자적 정보시스템과 그 집합체에 대한 프라이버시 영향 평가의 수행을 규정하고, 그 평가물에 대하여 공개함을 원칙으로 하며, 기관의 웹사이트에 프라이버시 정책을 공지하고, 표준화된 기계판독형 포맷으로 프라이버시 정책을 전환할 뿐만 아니라, 매년 OMB에 보고하도록 요구하고 있다는 점이다.

본 지침은 시민과의 상호작용을 목적으로 정보기술을 사용하거나 웹사이트를 운영하는 모든 행정부서와 기관, 계약업체들에게 적용되며, 성숙한 전자정부로 가기 위한 관련 부처간 이니셔티브에도 적용된다. 또한 Memorandum 99-18의 인터넷 프라이버시 정책, Memorandum 00-13의 추적기술, Memorandum 99-05의 프라이버시 책임에 대하여 새롭게 내용을 보완하였다.

미국 외에 이를 실시하는 국가로, 캐나다는 2002년 5월 세계 최초로 공공기관의 사업에 프라이버시 영향평가를 의무화하여 평가 결과에 따라 예산기관이 보완·수정 등의 권고를 내리고 예산 배정에도 반영하도록 하고 있다. 뉴질랜드, 영국, 호주 등도 2002년을 기점으로 이 제도를 도입했으나 미국·캐나다와 달리 의무가 아닌 권고사항에 머물러 있다.

국내에서도 개인정보의 수집·이용과 관련된 국책사업 추진 시 사전에 해당 사업이 초래할 개인정보권 침해 여부를 조사하는 '프라이버시영향평가제(개인정보 영향평가제)'를 도입해야 한다는 논의가 최근 들어 활발히 일어나고 있다.

지난 정부에 이어 참여정부에서도 전자정부사업이 31개 사업을 선정·추진 중에 있다. 대부분의 사업이 부처간 공통사업인 경우가 많고, 대민서비스의 원활한 제공을 위하여 기관간 정보공유와 활용이 더욱 중시됨에 따라 프라이버시를 침해할 가능성이 높아 보인다. 정보공동활용을 통한 행정의 효율성 달성과 개인정보보호 문제는 동시에 성취하기 어렵게 여겨지는 만큼 프라이버시 영향평가제라는 매개적 장치를 활용함으로써 양자를 모두 달성할 수 있는데 도움이 될 것이라고 본다. 이를 위하여 관계법령과 주관부처의 지침 등의 개정 및 보완이 절실히 요구되는 바이다.

참고자료:

[1] 전자신문, "PIA(프라이버시영향평가제) 법제화 신중 검토", 2003. 8. 25
[2] 한겨레신문, '개인정보 영향평가제' 논의 활발, 2003. 6. 17
[3] MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, http://www.whitehouse.gov/omb/memoranda/m03-22.html
[4] MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES, http://www.whitehouse.gov/omb/memoranda/m99-05.html
[5] MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, http://www.whitehouse.gov/omb/memoranda/m99-18.html
[6] MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, http://www.whitehouse.gov/omb/memoranda/m00-13.html
[7] CIRCULAR NO. A-130, http://www.whitehouse.gov/omb/circulars/a130/a130.html
[8] EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET WASHINGTON, D.C. 20503, http://www.whitehouse.gov/omb/inforeg/cookies_letter90500.html