情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

개인정보 유·노출 등의 통지 관련 국내외 법제 현황

변순정*, 이강신**, 박광진***

요 약

최근 개인정보 유·노출 사건이 급격히 증가하면서, 개인정보를 수집·이용하는 기업들의 개인정보 유·노출에 대한 대응 행태에 큰 관심이 모아지고 있다. 정보통신 기술이 급속히 발달함에 따라, 유·노출된 개인정보가 야기할 수 있는 피해의 정도가 점점 커지고 있지만, 정작 해당 기업들은 회사 이미지나 경제적인 이유 등으로 대응에 소극적이기 때문이다. 실제로 최근 많은 사업자들의 개인정보가 해킹으로 100만건 이상 유출된 바 있지만, 이들 사업자 중 유출 사실을 고객에게 통지한 기업은 전무하였다.

금년 8월, 방송통신위원회는 이러한 세계적 트랜드에 발 맞추어 개정 정보통신망법(안)에 개인정보 노출사고 발생 시 정보통신서비스 제공자가 노출된 정보, 노출시점 및 대처방법 등을 이용자에게 통지하고 방송통신위원회에 신고하도록 의무화하는 내용을 추가하였다.

이미 미국은 거의 모든 주(州)가 이러한 유·노출이 발생하였을 경우, 이를 고지하도록 하는 법안을 마련하였으며, 영국, 캐나다, 호주 등도 관련 지침을 마련하여 운영 중에 있다. 본 고에서는 개인정보 유·노출과 관련한 국내외 관련 법제 현황에 대해 살펴본다.

Ⅰ. 서 론

최근 개인정보 유노출 사건이 급격히 증가하고 있다. 실제로 금년 7월, 우리나라 최대 포털 사이트 중 한 곳에서 내부 직원의 실수로 고객 53만명의 이메일 수신 리스트가 노출되어 큰 사회적 이슈가 된 바 있다. 또한 연초에는 해킹으로 인해 한 경매 사이트에서 천만명이 넘는 고객의 개인정보가 대량으로 유출되기도 했고, 9월에는 한 정유 업체의 내부 직원이 고의적으로 천만이 넘는 고객의 개인정보를 유출하여 사회적으로 문제가 되기도 했다. 이렇듯 개인정보 유노출의 원인은 관리자의 관리 소홀이나 해킹, 내부 직원의 고의적 유출, 마케팅을 위한 개인정보의 오남용 등 다양하다.

이렇게 개인정보 유노출 사고가 계속적으로 증가하는 이유는, 정보통신망의 발달로 인해 온라인상에서 수집·활용되는 개인정보가 실질적 경제적 가치를 가지기 때문이다. 사업자들에게 개인정보는 고객에 대한 더 많은 정보를 제공해줌으로써, 보다 효율적인 제품 및 서비스 개발을 가능하게 하는 자산이다. 또한 스팸메일과 같은 간접광고를 통해 매출을 증대시킬 수 있다. 아이디 도용을 통해 다양한 경제적 이득을 취하려하는 자에게 개인정보는 필수 불가결의 기본 조건이다. 신용카드 위조, 전화 개통, 게임 사이트 아이템 매매 등이 모두 타인의 명의로 가능하다. 보이스 피싱을 하고자 하는 악덕 사기단에게도 개인정보는 훌륭한 자산이다.

이는 역으로 말하면, 개인정보의 가치가 증가하면 할수록, 개인정보 유노출로 인한 피해가 크다는 뜻이므로, 개인정보를 수집·활용하는 기업 및 개인은 이러한 일이 발생하는 것을 미연에 방지하도록 적절한 기술적 관리적 조치를 이행하여야 한다.

하지만 이러한 노력에도 불구하고 개인정보가 유노출되는 사고가 발생하였다면, 노출되고 나서의 피해를 최소화하기 위한 사후 대응이 철저히 이루어져야 할 것이다. 그러나 사업자는 회사 이미지에 미칠 부정적 영향 혹은 비용적인 문제 등을 이유로 이러한 사고가 발생하여도 이를 숨기려는 경향이 강하여, 이용자들은 자신의

* 한국정보보호진흥원 개인정보보호기획팀 (sjbyun@kisa.or.kr)
* 한국정보보호진흥원 개인정보보호기획팀 (kslee@kisa.or.kr)
* 한국정보보호진흥원 개인정보보호기획팀 (kjpark@kisa.or.kr)

개인정보가 노출되었는지의 여부를 즉각적으로 알기가 어렵다. 자연히 이로 인해 발생할 수 있는 피해에 대해서도 미리 대비하거나 예방할 수 있는 조치를 취하기 어렵다.

또한 정보통신망법 및 관련 지침 등에서도 개인정보 침해의 가능성을 사전적으로 방지하기 위한 노력은 꾸준히 반영되어왔지만, 사후적 대응 체계에 대해서는 소홀한 점이 없지 않았던 것이 사실이었다.

이에 방송통신위는 금년 8월, 개정 정보통신망법(안)에 개인정보 노출 사고 발생 시 정보통신서비스제공자가 노출된 정보, 노출시점 및 대처방법 등을 이용자에게 통지하고 방통송신위원회에 신고하도록 의무화하는 내용을 추가하였다.

이미 미국에서는 각 주에서 개인정보 유출 시 정보주체에게 고지토록 하는 법제도를 운영 중이며, 캐나다, 호주, 영국, 일본 등의 국가에서도 지침 등의 형태로 의무화하거나 권고하고 있다. 본 고에서는 한국 및 해외 주요 국가의 개인정보 유·노출 침해에 대한 사후 조치 관련 현황을 소개한다.

Ⅱ. 정보통신망이용촉진및정보보호에관한 법률

정보통신망법에서는 개인정보의 침해를 최소화하기 위해 수집부터 이용, 파기에 이르기까지 다양한 보호규정을 마련해왔다.

동 법에 따라 정보통신서비스 제공자는 정보통신서비스 제공을 위하여 필요한 최소한의 정보만를 수집하여야 한다. 정보주체가 자신의 정보가 어떻게 취급되는지에 대한 정보를 언제든 쉽게 확인 가능하도록 개인정보취급방침을 마련하여 공개하여햐 아며, 수집 당시에는 1)개인정보의 수집·이용 목적, 2)수집하는 개인정보의 항목, 3)개인정보의 보유·이용 기간 등을 정보 주체에게 알리고 동의를 받아야 한다.

또한 개인정보를 이용자로부터 동의받은 목적 이외로 사용하여서는 안되며, 해당 개인정보를 제3자에게 제공하기 위해서는 1)개인정보를 제공받는 자, 2)개인정보를 제공받는 자의 개인정보 이용 목적, 3)제공하는 개인정보의 항목, 4)개인정보를 제공받는 자의 개인정보 보유 및 이용기간을 알리고 동의를 받도록 하여 정보주체의 알권리 및 자기 통제권을 강화하였다. 한편으로는 개인정보 관리 책임자를 지정하여 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하도록 하였으며, 개인정보를 취급할 때 개인정보의 분실·도난·노출·변조 또는 훼손을 방지하기 위하여 기술적·관리적 조치를 하여야 하며, 정보주체가 언제든지 자신의 개인정보를 열람, 정정, 삭제할 수 있도록 하였다. 또한 동의를 받은 개인정보의 수집 및 이용목적이 달성된 경우에는 해당 개인정보를 지체없이 파기하도록 하였다.

그러나 이러한 다양한 보호조치에도 불구하고 개인정보가 의도하거나 혹은 의도하지 않게 유·노출되는 사건들이 계속해서 발생해왔으며, 정보통신서비스가 점점 더 발달함에 따라 이러한 유·노출의 범위와 깊이는 더욱 더 심각해지고 있다.

〔표 1〕 2008년 개인정보 유·노출 관련 통계

월	기업명	사건 내용	
9월	GS 칼텍스	유출정보	이름, 주민번호, 이메일
		범위	정부 부처의 고위 관계자들이 포함된 전국 시도의 한국 국적자
		유형	자회사 직원의 고의적 의도
		피해규모	개인정보 1천125만 건
		기타	집단소송 준비 중
7월	다음	유출정보	메일노출 - 받은메일함, 수신 확인 목록, 첨부파일
		유형	메일 서비스 기능 개선을 위한 업그레이드 과정에서의 실수
		피해 규모	ID 55만개, 메일목록 노출 ID 43만개, 메일 내용 노출 370건, 메일 삭제 피해 고객 신고 415건, 첨부파일 다운로드 피해 1건
2월	옥션	유출정보	주민번호, 성명, 주소, 이메일, 전화번호, 휴대전화번호, 카드번호, 비밀번호, 환불정보(일부), 재무정보(제한적)
		유형	중국 IP의 지속적 접근(해킹)
		피해규모	개인정보 1760만 건
		기타	회원들의 손해배상청구 소송

그럼에도 불구하고 기업들은 회사 이미지의 실추, 금전적 피해 등을 이유로 개인정보 유출사고가 발생해도 이를 적극적으로 해결하려하기 보다는 숨기려하는 경향이 강한 것이 사실이다. 실제로 최근 많은 사업자들의 개인정보가 해킹으로 100만건 이상 유출된 바 있지만, 이들 사업자 중 유출 사실을 고객에게 통지한 기업은

전무하였다.

정보주체가 향후 발생 가능한 다양한 잠재적 피해를 예방할 수 있기 위해서는 개인정보 유출 사실을 즉각적으로 인지할 수 있어야 하지만 현실은 그렇지 못한 것이다. 개인은 갑자기 증가한 스팸문자나 메일을 보면서 의아해하거나 누군가가 자신의 명의를 도용하여 전화나 신용카드를 사용했다는 사실을 뒤늦게 알고 대응하려 하겠지만, 이미 피해는 발생하고 난 뒤다.

하지만 현재까지는 이러한 개인정보 유출 사실을 기업들이 알려야할 어떠한 법적 의무도 존재하지 않았다.

〔표 2〕 국내 유사 입법례

	주요 내용
정보통신기반보호법	제13조 (침해사고의 통지) ① 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. ② 정부는 제1항의 규정에 의하여 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위안에서 복구비 등 재정적 지원을 할 수 있다.
정보통신망법	제48조의3 (침해사고의 신고 등) ① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생한 때에는 즉시 그 사실을 방송통신위원회 또는 보호진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항의 규정에 따른 통지가 있는 때에는 전단의 규정에 의한 신고로 본다. 1. 정보통신서비스제공자 2. 집적정보통신시설사업자 ② 방송통신위원회 또는 보호진흥원은 제1항의 규정에 의하여 침해사고의 신고를 받거나 침해사고를 인지한 경우에는 제48조의2제1항 각호의 규정에 의한 필요한 조치를 취하여야 한다.

[표 2]에서 볼 수 있듯이, 해킹 등으로 인해 통신시설 등의 마비 등이 인지되었을 경우 관련 기관에 통지하도록 하는 유사 규정은 있지만, 정보주체에게 직접 통지하도록 의무화하는 규정은 부재하였다.

이에 방송통신위원회는 지난 8월, 개인정보 유출사고 발생 시 신속한 대응 및 피해확산 방지를 위해 사업자로 하여금 이용자 및 관계기관에 동 유출 사실에 대하여 지체없이 통지 및 신고하도록 의무화 규정을 신설하였다. 동 규정에 따르면 정보통신서비스제공자등은 해킹, 부주의, 내부자 고의 등에 의해 개인정보가 분실, 도난, 노출되었을 경우, 이를 지체없이 이용자에게 통지하고 방송통신위원회에 신고하여야 한다. 통지 및 신고 시에는 유출된 개인정보의 항목, 발생시점과 경위, 피해최소화를 위한 조치, 사업자의 대응조치, 피해접수 연락처 등을 알려야 한다.

개인정보 유누출 사실을 이용자에게 통보하는 외에 방통위에 신고하도록 한 것은 유출 개인정보의 인터넷 유포, 거래 등의 불법 행위를 예방할 수 있는 긴급조치를 취하도록 함으로써 제2차 3차의 피해를 최소화하기 위함이다.

〔표 3〕 정보통신망법 개정법안 관련 조항

현행	개정안
신설	제91조(개인정보 누출 등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 '누출 등'이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회에 신고하여야 한다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령이 정하는 바에 따라 통지에 갈음하는 조치를 취할 수 있다. 1. 누출 등이 된 개인정보 항목 2. 누출 등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 ② 제1항에 따른 통지 및 신고의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다. ③ 정보통신서비스 제공자등은 개인정보의 누출 등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.

동 개정법안은 10월 입법 예고되었으며, 의견수렴 결과를 반영한 최종 개정안은 법제처 심사, 국무회의 등을 거쳐 올해 11월에 정기국회에 제출될 것으로 예상된다.

Ⅲ. 개인정보(프라이버시) 침해 사실 고지 의무 관련 해외 입법례

미국을 비롯한 해외 주요 국가들도 최근 ID 도용으로 인한 사회적 피해가 증대함에 따라 개인정보 유출과 같은 개인정보보안 침해에 많은 관심을 가지게 되었다. 사회보장번호와 같은 개인정보가 도용되어 신용카드를 신청하기도 하고 부도수표를 작성하기도 하고, 차를 사거나 여러 가지 금융 범죄를 범하는데 이용되고 있는

것이다.

본 절에서는 개인정보보안 침해 고지 의무를 입법화한 미국과 각종 지침 등을 통해 적극 권장하고 있는 캐나다, 영국, 호주와 같은 국가의 관련 법제에 대해 살펴보고자 한다.

3.1 미국

미국의 경우 캘리포니아주를 포함한 거의 모든 주(州)가 개인정보 침해 혹은 유출 사실을 고지하도록 의무화하고 있다.

캘리포니아주의 경우 보안위반정보법(Security breach information Act, 2003년 7월)를 통해 사회보장번호, 운전면허번호, 캘리포니아 식별카드번호, 금융 정보 등의 정보를 컴퓨터 파일 형태로 보유하는 공공 민간 기관은 허가받지 않은 자에 의해 암호화되지 않은 정보가 침해되었거나, 침해되었다고 믿을만한 상당한 이유가 있는 경우에 동 사실을 정보주체에게 고지하도록 하고 있다.

고지방법은 서면, 전자고지가 대표적이지만 유출이 발생한 업체가 업체 자체의 절차를 보유하고 있는 경우, 그리고 이러한 절차가 시간적 관점에서 동 법을 준수하고 있는 경우, 내부 절차에 따라 정보주체에게 동 사실을 고지할 경우 법을 준수한 것으로 간주한다.

또한, 해당 업체가 고지에 소요되는 비용이 250,000 달러가 초과하거나, 고지하여야 할 주체가 5십만명이 넘거나 적절한 연락처 정보를 보유하고 있지 못하다는 사실을 증명할 수 있을 경우, 이메일, 웹사이트 고지(conspicuous posting), 주 전체를 커버하는 미디어에의 고지로 대체 가능하다.

동 법을 준수하지 않아 발생한 피해에 대해서는 민사소송에 의해 소를 제기할 수 있으며, 동 법을 위반하거나 위반했거나 위반하려고 한 업체는 규제받을 것(enjoined)이다. 동 규정에 의해 가능한 권리와 피해구제는 cumulative이며 다른 법에서의 그것과도 마찬가지이다. 만약 법집행 기관이 이러한 고지가 범죄 조사를 방해할 것이라 결정한 경우는 연기가 가능하다.

[표 5]에서는 미국 내 주요 주의 고지 의무 관련 법안을 간략하게 정리하였다.

3.2 호주

호주의 프라이버시법(Privacy act 1998) 내의 정보프라이버시원칙(The Information Privacy Principles :

〔표 5〕 미국 주요 주의 고지 관련 법안

주	법안 내용
캘리포니아	Civil Code Sec. 1798.80-1798.82, 2003년 7월 1일부터 발효 만약 정부 기관 또는 사업체가 보유하고 있는 암호화가 되지 않고 전산화된 개인정보의 보안, 비밀성 혹은 통합성 등에 침해가 발생했을 경우 이를 소비자에게 통지해야 함 만약 개인 또는 사업체가 일관된 소비자 고지 절차를 갖추고 관련 정책에 따라 고지를 했거나, 또는 개인 또는 사업체가 주법 또는 연방법에서 제시하는 더 강한 보호 및 노출에 관한 법안을 준수할 경우, 본 법안을 준수한 것으로 간주
콜롬비아	DC Code Sec 28-3851 et seq. 2007년 1월 1일부터 발효 암호화되지 않고 전산화된 혹은 여타 전자적 개인정보의 보안, 비밀성, 혹은 통합성에 침해가 발생하였을 경우 이를 소비자에게 통보하여야 함 동 법은 그라함-리치 빌리 법안의 적용 대상인 법률 주체 및 사람에게 적용되지 않음 동 법은 또한 동 법안의 고지의무 규정과 관련하여 즉시성의 조건에 부합하는 내부 고지 절차를 보유하고 있는 개인인이나 업체에는 적용되지 않음
플로리다	HB 481, 2005년 7월 1일부터 발효 Fla.Stat.Ann. 817.5681 et seq에서 인용 플로리다 주(State)에서 사업을 수행하는 사람으로 그가 보유한 암호화되지 않고 전산화된 개인정보의 보안, 비밀성 및 보안이 침해되었을 경우, 동 사실을 소비자에게 통지해야 함 아래의 경우, 동 법을 적용하지 않음 - 법 집행 기관의 적절한 자문 및 적절한 조사 후, 해당인의 행위가 개인에게 해를 끼칠 가능성이 낮았거나 낮을 것이라고 판단될 경우. 이에 대한 판단은 반드시 문서화되어야 하며, 본 문건은 5년 동안 보관되어야 함 만약 해당인의 고지 과정이 본 법안에서 요구하는 적시 요구를 일관되게 준수하고 있는 경우, 또는 고지 과정이 개인의 1차적인 또는 기능적인 역할을 하는 연방 규제기관에 의해 만들어 졌을 때에는 동 법을 준수하는 것으로 간주함.
미시건	SB 209, 2006년 12월에 법안 통과됨, 2007년 7월 2일부로 발효 본 주(State)에서 사업을 하는 자로서, 비암호화되고 전산화된 개인정보의 통합, 비밀보장, 보안 규정을 위반했을 경우 동 사실을 고지하여야 함 개인, 기관의 보안규정 위반이 심각한 손실 및 손상을 입히거나, ID 도용의 결과를 야기할 것으로 판단될 경우에는 통지함 HIPPA 법률 주체 또는 금융기관에는 적용하지 않음

뉴욕	A4254,A3492 2005년 12월 8일부로 발효 NY Bus.Law Sec.899-aa에서 인용함 공공, 민간 법률주체가 보유하고 있는 개인정보, 암호화되지 않고 전산화된 개인정보 혹은 암호화 키가 설치된 암호화된 개인정보의 보안 규정 위반시 이를 통보함
워싱턴	SB 6043 2005년 6월 24일 발효 RCW 42.17 et seq 인용 개인, 사업체, 정부기관이 보유하고 있는 비암호화, 전산화된 개인정보에 대해 통합, 비밀보장, 보안 사항 위반시 이를 통지함 시스템의 실질적인 보안 침해로 인해 해당 소비자가 범죄 활동에 노출될 가능성이 있다고 판단되어지지 않는 경우, 고지를 요구하지 않음 만약 법률주체가 개인정보 취급에 대한 개인보안 정책의 일환으로 자체의 고지 절차를 운영하고 있고 이러한 절차가 동법의 시간 조건에 부합하는 경우, 별도의 고지를 의무화하고 있지 않음

IPPs)과 국가프라이버시원칙(National Privacy Principles: NPPs)에서는, 개인정보를 수집하여 활용하는 정부 및 조직들에게 합리적인 보안장치들을 마련하여 그들이 보유하고 있는 개인정보가오용, 분실되거나 허가받지 않은 접근, 수정 혹은 노출되지 않도록 방지하는 적절한 절차들을 이행할 의무를 부과하고 있다.

동법에서는 그러나 개인정보 보안 침해 문제(personal information security breach)가 발생하였을 경우 이러한 사실을 개인에게 고지할 의무를 명시적으로 부여하고 있지는 않다.

단지 호주 프라이버시위원회(Office of the privacy commissioner)가 2008년 8월에 발간한 '개인정보 유출 대응 지침(Guide to handling personal information breaches)에서 일반적으로는 이러한 침해 발생으로 인해, 치명적인 피해를 야기할만한 실질적인 위험이 존재할 경우, 피해 당사자에게 고지하는 것이 법의 취지에 부합하는 것임을 언급하고 있다. 또한 이를 통해 조직에 대한 신뢰와 투명성을 향상시키고 중요한 완화전략(mitigation strategy)로서 기능할 수 있음을 강조하고 있다.

동 지침은 조직이나 기관이 개인정보 보안 침해에 대응할 때 고려해야할 핵심 단계 및 요소들에 대한 일반적 지침을 제공하기 위해 발간된 것으로서 강제적인 규정은 아니다. 그러나 2008년 8월에 호주법개혁위원회(australian law reform commission)가 이러한 고지가 법에서 의무화되어야할 것임을 제안한 바 있는 등 개인정보 보안 침해 문제에 큰 관심을 가지고 있음에는 틀림이 없다.

동 지침에서는 개인정보보안 침해에 대응하기 위해 1) 우선 침해가 더 이상 일어나지 않도록 가능한 모든 수단을 동원하여 추가 침해 가능성을 봉쇄하고 현황을 파악하며 2) 침해와 관련한 위험을 평가하고, 3)고지 여부를 결정하며 4) 향후 동일한 피해가 발생하지 않기 위해 어떠한 행동이 취해져야 하는지에 대해 고찰하여야 한다고 언급하고 있다.

또한 고지가 매우 훌륭한 완화전략임에는 틀림없지만, 무조건 고지할 것이 아니라 아래의 몇 가지 요소들를 고려하여 고지하는 것이 나은지의 여부에 대해 결정할 것을 권하고 있다.

〔표 6〕 고지여부 결정에 고려되는 요인들

- 침해와 관련해 어떠한 위험이 존재하는가
- 만약 고지가 이루어졌을 경우, 정보주체가 잠재적 위험을 피하거나 완화할 수 있는 능력은 무엇인가
- 그러한 능력이 없다하더라도, 유·노출된 정보가 해당 정보주체를 창피나 당혹한 상황에 처하게 할 수 있는 성격의 것인가
- 고지하여야 할 법적 및 계약적 의무는 무엇이며, 고지의 결과는 무엇인가
- 해당 정보주체에게 고지하지 않았을 경우의 결과는 무엇인가

이러한 분석 등을 통해 일단 고지가 결정되고 난 후에는, 사건 경위와 발생 시기, 해당 개인정보 유형, 향후 계획, 지원 내용, ID도용과 같은 사건 발생을 방지할 수 있는 다양한 정보 혹은 그 정보를 제공할 수 있는 기관 등에 대한 정보, 연락처, 프라이버시 위원회 등 외부 기관에 고지되었는지의 여부, 법적 효력 및 민원(분쟁조정이나 상담) 관련 기구에 대한 정보 등을 포함하여 고지가 이루어져야 한다.

3.3 영국

영국의 정보보호법(Data Protection Act 1998)의 7번째 원칙에서는 모든 정보 관리자들은 그들이 보유하는 개인정보의 적절한 보호를 보장하도록 의무화하고 있다.

영국의 경우도 호주와 마찬가지로, 개인정보의 유출, 훼손, 분실 등과 같은 개인정보 침해가 발생하였을 경우 이를 정보 관리자가 보고할 법적 의무는 부재하다. 그러나 영국의 개인정보보호 위원회(information commissioner's

office)는 심각한 침해의 경우 위원회에 보고할 것을 제안하고 있으며 이러한 침해에 대처하는 관리법에 대한 지침(Guidance on data security breach management)을 제공하고 있다.

동 지침에서도 호주의 지침과 마찬가지로 이러한 보안침해(Security breach)가 발생하였을 경우 조직이 고려할 필요가 있는 4가지 중요한 요소에 대해 언급하고 있으며 내용은 거의 동일하다.

1) 차단 및 회복(containment and recovery)
2) 위험평가(assessment of ongoing risk)
3) 고지(notification of breach)
4) 평가 및 개선(evaluation and response)

특히 동 지침에서는 고지의 경우 고지 자체가 중요한 것이 아니라 동 고지를 통해 피해받을 가능성이 있는 주체가 적절한 보호 수단을 취할 수 있는지 혹은 규제기구가 불만에 대응하고 상담을 제공할 수 있는 그들의 기능을 적절히 수행할 수 있도록 하는지와 같은 명확한 목적이 있어야 한다고 언급하고 있다.

〔표 7〕 영국의 정보보호법 8원칙

1. 개인정보는 공정하고 합법적으로 처리되어야 하며, 특히 아래의 경우가 아니면 처리되어서는 안 된다.
(a) schedule2에서의 조건 중 적어도 하나가 충족되어지고, 그리고
(b) 민감정보의 경우, schedule 3에서의 조건 등 하나 이상 또한 충족시켜야 함.
2. 개인정보는 하나 혹은 그 이상의 특정하고 합법적인 목적을 위해 획득되어져야 하며, 그러한 목적들에 부합하지 않는 형태로 처리되어서는 안 된다.
3. 개인정보는 그들이 처리되는 목적과 관련하여 적합하고, 관련 있어야 하며 과해서는 안 된다.
4. 개인정보는 정확해야 하고, 필요할 경우, 최신성을 유지하여야 한다.
5. 특정 목적을 위해 처리된 개인정보는 동 목적을 위해 필요한 이상 보관되어져서는 안 된다.
6. 개인정보는 동법에 따른 정보주체의 권리에 부합하게 처리되어져야 한다.
7. 개인정보를 처리하는 조직은 개인정보의 사고로 인한 손실, 훼손, 파괴나 불법적이거나 허가받지 않은 처리로부터 적절히 보호할 수 있는 적절한 수단들을 보유하여야만 한다
8. 개인정보가 EEA(European Economic Area)를 벗어난 지역이나 국가로 이전되어지기 위해서는 동 지역이나 국가가 개인정보처리와 관련하여 정보주체의 권리와 자유를 적절한 수준으로 보호되어짐을 보장해 줄 수 있어야 한다.

또한 누구에게 어떠한 내용을 어떠한 통신 수단으로 전달할 것인지에 대해서도 고려할 필요가 있다고 언급하고 있다.

영국 개인정보보호 위원회가 제시하는 고지여부를 결정할 수 있는 몇 가지 질문은 다음과 같다.

〔표 8〕 고지여부 결정에 고려되는 요인들

· 법적 및 계약적 의무 존재 여부
· 고지를 통해 정보보호법의 7번째 원칙과 관련한 보안 의무를 충족하는데 도움이 되는지의 여부
· 고지가 개인에게 도움이 되는지의 여부
· 대중의 정보가 침해되었거나 피해가 심각한 경우
· 특정군(어린이, 노약자 등)에 적절한 고지방법에 대한 고려
· 몇 명의 개인정보가 침해되었는가

3.4 캐나다

캐나다의 개인정보보호및 전자문서법(Personal Information Protection and Electronic Documents Act, PIPEDA) 또한 개인정보보안 침해 발생 시 이를 고지하도록 의무화하고 있지 않다. 하지만 최근 들어 꾸준히 발생하는 개인정보 유출 사건 등으로 인해 고지의 중요성에 대한 사회적 공감은 충분히 형성된 분위기이며, 프라이버시 위원회(Office of the Privacy Commissioner of Canada)는 관련 조항을 법에 추가하는 사안에 대해 계속적으로 제안하고 있다. 이러한 과정의 일환으로 동 위원회는 이러한 프라이버시 침해가 발생했을 때 해당 기업의 대응에 도움을 줄 수 있는 지침을 제공하기 위해 문서를 작성하였다.

동 문서에서 정의하는 프라이버시 침해(privacy breach)란 개인정보의 허가받지 않은 접근, 수집, 사용 혹은 노출이 있을 경우를 말하며, 허가받지 않았다라는 것은 PIPEDA나 기타 유사한 지역적 프라이버시법에 반하여 일련의 활동이 발생할 경우를 말함으로써 우리가 흔히 의미하는 개인정보 유·노출이라 할 수 있다.

프라이버시 침해에 대응할 때 고려해야할 네 가지 주요 절차(steps)로는 1) 차단과 현황파악, 2)위협 산정, 3) 고지, 4)예방을 언급하고 있다.

물론 건별로 차별점을 두어 다루어져야 하겠지만 프라이버시 침해가 해당 개인에게 피해를 줄 위험이 있다면, 자신들을 보호할 수 있는 조치를 취할 수 있도록 동 사실을 고지해야만 할 것이며, 이러한 고지가 필요한지

의 여부는 해당 개인의 피해를 피할 수 있거나 완화할 수 있는지에 따라 결정하도록 하고 있다.

〔표 9〕 고지여부 결정에 고려되는 요인들

· 법적 및 계약적 의무 존재 여부 · 개인에게 끼치는 피해 위험 · ID 도용의 위험 존재 여부 · 신체적 피해 위험 · 개인의 명성에 피해가 가거나 굴욕적인지 · 잠재적 위험을 피하거나 완화할 수 있는 능력 보유 여부

일단 고지가 이루어져야 할 것이라 판단되면 신속히 고지가 이루어져야 할 것이지만, 법 집행 기관이 연루되었을 경우, 이러한 고지가 조사에 부정적인 영향을 미칠 수 있는지에 대한 논의를 통해 연기가 가능하다고 언급하고 있다.

이러한 고지의 방법으로는 전화, 편지, 이메일 혹은 대면적인 방법과 같은 직접적인 수단을 제안하고 있으며, 웹사이트에 고지하거나 매체를 통한 간접적인 고지는 직접적인 고지 방법이 추가적 피해를 가져올 수 있거나, 피해 대상을 알지 못하거나 비용적인 장애물이 존재할 경우에 사용될 수 있을 것이며, 둘 다를 활용할 수도 있다고 언급하고 있다.

이러한 고지에 포함되어야 할 내용으로는, 건별로 그리고 고지 수단에 따라 상이하겠지만, 일반적으로 1)사건 경위 및 발생 시간, 2)개인정보 종류, 3) 피해를 감소하거나 조절하기 위해 조직이 취한 것들에 대한 일반적인 설명, 4)조직이 피해 주체를 지원하기 위해 취할 행동들과 개인이 자신을 보호하여 추가적 위험을 감소하거나 회피하기 위해 취할 수 있는 절차들, 5)이러한 도움을 받을 수 있는 정보 소스, 6)개인을 상담해주거나 정보를 제공해줄 수 있는 개인이나 부서의 연락처 정보, 7)프라이버시 위원회에 고지했는지 혹은 그들이 이 사실을 알고 있는지의 여부, 8)프라이버시 위원회의 연락처 정보와 같은 내용들이 포함되어져야 할 것이다. 또한 동 문서에서는 조직이 이러한 프라이버시 침해를 처리함에 있어 적절한 고려를 했는지 확신할 수 있도록 체크리스트도 제공하고 있다.

Ⅳ. 결론

앞서 살펴본 대로, 미국과 영국, 캐나다, 호주와 같은 주요 국가들은 개인정보 유노출 등과 같은 침해사실이 발생할 경우, 이러한 사실을 즉각 통지하도록 법에서 의무화하거나 지침 등으로 적극 권장하고 있다. 특히, 해당 정보주체에게 심각한 피해가 갈 것이라 판단되는 침해 사건에 대해서는 거의 의무적이라 할 수 있다. 그만큼 개인정보 유노출 사건이 발생하였을 경우 정보주체에게 발생할 수 있는 피해를 미연에 방지하는 절차는 매우 중요한 것일 것이다.

한편 기업의 입장에서는 이러한 유노출 사건이 발생하였을 경우, 자발적으로 공개하기가 쉽지 않을 것이다. 앞에서도 언급하였듯이, 이러한 사건이 알려질 경우, 기업 이미지에 큰 타격을 줄 수 있기 때문이다. 따라서 강제적인 규정에 의해 공개하도록 하되, 무조건 비판의 대상이 되게하기 보다는, 실제 피해의 정도와 가능성 등에 대한 보다 철저한 조사와 판단에 기반하여 필요한 절차를 이행할 수 있도록 하는 체계적인 시스템이 필요할 것이다.

따라서 이번 정보통신망법 개정안에 유노출 관련 규정이 신설되어 추가된 것은 매우 의미있는 것으로 보여진다. 향후 대통령령이나 관련 지침 등을 통해 고지 방법, 시기, 절차 등의 세부적인 내용들이 시급히 마련되어 기업은 유출 사고를 현명히 대처할 수 있고, 이용자는 자신의 개인정보 및 프라이버시 침해를 최대한 효율적이고 효과적으로 보호할 수 있는 계기가 될 수 있었으면 한다.

참고문헌

[1] Notice of Security Breach State Laws, Consumers Union, Aug 2007,

[2] Notification of Data Security Breaches to the Information Commissioner's Office, Information Commissioner's Office(UK), Mar 2008

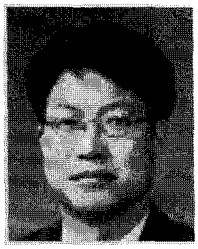
[3] Guide to handling personal information security breaches, Office of the Privacy Commissioner, Aug 2008

[4] Key Steps for Organizations in responding to Privacy Breaches, Office of the Privacy Commissioner of Canada

〈著者紹介〉

변 순 정(Soonjoung Byun)
1999년 2월 : 이화여자대학교 경영학과 졸업
2001년 2월 : 서울대학교 대학원 경영학과 마케팅 석사
2001년 3월~2002년 4월 : 유니레버 코리아 마켓 리서치 팀 근무
2002년 12월~현재 : 한국정보보호진흥원 개인정보보호기획팀 주임연구원
관심분야 : 개인정보보호

이 강 신(Gang Shin Lee)
정회원
1989년 8월 : 한양대학교 수학과 이학석사
2005년 8월 : 고려대학교 정보보호대학원 공학박사
1990년 7월~1992년 6월 : 데이콤 종합연구소 연구원
1992년 7월 ~ 2000년 8월 : 한국전산원 정보화표준부장
2000년 9월 ~ 현재 : 한국정보보호진흥원 개인정보보호기획팀장
관심분야 : 개인정보보호, 네트워크 보안, 정보보호아키텍쳐



박 광 진(Kwangjin Park)
정회원
1982년 2월 : 동국대학교 전자계산학과 졸업
1988년 2월 : 한양대학교 전자계산 전공 석사
1998년 : 광운대학교 컴퓨터과학과 박사과정 수료
1983~1988 : 한국전기통신공사
1988~1996 : 정보통신정책연구원 책임 연구원
1996~현재 : 한국정보보호진흥원 개인정보보호지원센터 센터장