

보도자료

- 수 신 : 각 언론사 경제부, 사회부, NGO담당
- 발 신 : 경실련, 진보네트워크센터, 참여연대, 함께하는시민행동
- 문 의 : 진보네트워크센터 오병일 활동가 02-774-4551
- 일 자 : 2014. 2. 5(수)
- 제 목 : [카드사 개인정보유출에 대한 시민단체 공동입장]
대량 금융 개인정보 유출사고, 개인정보보호를 위한 근본 대책이 필요하다

대량 금융 개인정보 유출사고, 개인정보 보호를 위한 근본 대책이 필요하다

- 카드사 개인정보유출에 대한 시민단체 공동입장

주민번호 체제 근본적 개편 필요
금융지주회사 내 정보공유 금지
소비자 집단소송제도 마련
공인인증서 의무화 폐지
개인정보보호위원회의 독립성과 권한 강화

사상 최고의 기록을 또 한 번 경신했다. 1억 건이 넘는 개인정보, 개인당 20건에 이르는 민감한 정보가 유출됐다. 이미 우리는 대량 개인정보 유출에 익숙해져 이번 대번 금융 개인정보 유출이 새삼스럽지 않다. 이번 유출 사고를 금융기관의 '보안인식 부재'의 문제로만 돌리고, 처벌을 강화하면 되는 것일까? 그 동안 발생한 수많은 금융 개인정보가 유출됐을 때 마다 정부는 재발방지 대책을 내놨지만, 유출 사고는 끊이질 않아 왔다. 언제나 그렇듯이 이번 유출사고로 인한 정부 재발방지 대책 역시 개인정보 유출의 근본적인 원인은 건드리지 못하고 있다.

금융기관의 개인정보 유출이 빈발하는 근본 원인은 단지 '보안인식 부재'의 문제가 아니라, 보안 강화에 투자해야 할 동기가 부족하기 때문이다. 즉 개인정보 보유를 통해 얻는 이익이 개인정보를 보유함으로써 지는 부담보다 크기 때문이다. 개인정보가 유출되어도

정부는 숨방망이 처벌로 일관해왔고, 소비자들은 법원을 통해서 손해배상을 받기도 힘들다.

금융기관들은 더 많은 개인정보를 '강제적 동의'를 통해 수집했고, 정부는 금융지주회사법 등을 통해 정보주체의 동의 없는 개인정보의 공유를 부추겼다. 또한 공인인증서 의무화는 보안기술의 혁신과 더 나은 보안에 대한 투자를 방해했다. 나아가 대량 개인정보 유출의 단골메뉴인 주민번호는 불법적 개인정보 활용에 대한 매력을 높여 피해를 확산하는 주범이 됐다. 산업진흥과 개인정보 보호를 겸하고 있는 감독기구는 진흥에 방점을 뒀고, 그나마 2011년 만들어진 개인정보보호위원회는 권한이 별로 없는 심의기구일 뿐 개인정보보호를 위한 역할을 못하고 있다.

이와 같은 근본 원인을 치유하지 않는다면, 또 다른 영역에서 또 다른 방식으로 또 한번의 신기록을 갱신하게 될 뿐이다. 언제까지 소도 없고, 외양간도 방치할 것인가! 이제 개인정보 보호를 위한 근본적인 대책을 수립할 것을 정부와 국회에 촉구하며, 우리는 다음과 같은 제안을 하고자 한다.

첫째, 주민번호 체제를 근본적으로 개편해야 한다.

한국 사회에서 개인정보 유출로 인한 피해가 큰 것은 주민번호 때문이다. 주민번호는 다양한 개인정보를 통합하는 열쇠(key) 역할을 한다. 이는 개인정보에 대한 가치를 높여 해킹이나 내부자에 의한 개인정보 유출을 부추긴다. 전 세계적으로 거래되는 주민번호는 이제 '공공재'가 됐다. 더 이상의 '사회적 혼란과 비용'을 막기 위해서, 그리고 '신뢰'에 기반한 정보사회를 구축하기 위해서 주민번호 체제 개혁은 더 이상 미룰 수 없는 과제다.

당장 유출된 주민번호로 인한 피해를 막기 위해, 정부는 주민번호 변경을 허용해야 한다. 그리고 민간을 물론이고, 공공 영역에서도 최소한으로 사용되도록 주민번호 수집 및 이용을 제한해야 한다. 사회 각 영역에서는 주민번호가 아닌 고유 목적에 맞는 별도의 식별체계를 사용하고, 주민행정 목적으로 사용되는 주민번호는 재발급이 가능한 무작위 일련번호로 대체돼야 한다.

둘째, 금융지주회사 내 정보공유를 금지해야 한다.

이번 사건으로 유출된 KB국민카드의 고객정보 5,300만 명 중 1,150만 명은 해당 카드

사와 거래하지 않은 고객이다. 고객의 동의 없이 KB금융그룹 내에 개인정보를 공유하여 피해를 확산시킨 것이다. 이는 「금융지주회사법」에서 정보주체의 동의 없이 개인정보를 금융지주회사에게 영업상 이용하게 할 목적으로 제공할 수 있도록 규정하고 있기 때문이다.

이러한 문제에도 불구하고 정부는 ‘내부경영관리 목적으로만 한정’하고 ‘외부영업에 활용하는 경우 업무처리절차를 대폭 강화’하겠다고, 여전히 동의 없는 정보공유를 고수하겠다는 입장이다. 그러나 이 조항은 수집목적 외 사용금지, 정보주체의 동의 없는 제3자 제공금지 등 개인정보 보호의 국제적 원칙과 국내 개인정보보호 법제를 심각하게 훼손하고 있다. 헌법적 가치인 개인정보 자기결정권 보장을 위해 금융지주회사 내 정보공유는 금지되어야 한다.

셋째, 소비자들의 집단소송제도가 마련돼야 한다.

이번 대규모 개인정보 유출에도 불구하고 정부가 내놓은 ‘징벌적 과징금’은 기업에게 큰 부담이 되지 않을 뿐더러(‘관련’ 매출의 1%), 피해 당사자의 직접적 배상과도 무관하다. 유출로 인한 피해 당사자가 권리구제를 받기 위해서는 당사자 하나하나가 소송을 제기할 수밖에 없고, 이는 불필요한 사회적 비용을 발생시킨다.

현재 「개인정보보호법」에 규정되어 있는 소비자 단체소송은 유출로 인한 권리침해의 회복이나 손해배상이 불가능하다. 이에 개인정보 침해 피해자 1인 또는 수인이 법원에 소송을 제기하여 손해배상이 확정될 경우 동일한 피해자들에게 판결의 효력이 미치도록 하는 집단소송제도를 도입해야 한다. 이를 통해 기업이 보안에 투자하지 않았을 경우 감당해야 할 부담을 높이는 한편, 피해 당사자가 유출로 인한 직접적인 배상을 받을 수 있도록 해야 한다.

넷째, 공인인증서 의무화를 폐지하고 보안의 경쟁체제를 강화해야 한다.

현재 한국의 보안 환경은 전자금융거래 시 공인인증서만을 사용하게 하고, 이를 위하여 이용자의 PC에 Active X를 설치하도록 강제하고 있다. 이는 이용자의 PC 등을 해킹 위협에 노출시킬 뿐만 아니라, 금융보안 기술 시장에서의 경쟁을 제한해왔다. 특정 기술을 강제하는 것은 전체 사회적 차원에서도 보안 위협을 증가시킨다. 금융회사들이 공인인증서에만 의존하지 않고 자율적으로 금융 보안 수단을 결정하도록 해야 한다. 이를 통해

기업의 보안에 대한 책임성과 투자를 높일 수 있다.

다섯째, 개인정보보호위원회의 독립성과 권한이 강화돼야 한다.

국제적인 개인정보보호 규범은 각 국에 ‘독립적인 개인정보 감독기구’를 둘 것과, 개인정보 침해사건의 조정, 시정명령, 자료제출요구, 조사권 등 실질적인 권한을 보장하고 있다. 그러나 지난 2011년 제정된 현행 개인정보보호법에 의해 만들어진 개인정보보호위원회는 ‘심의’기능만 가지고 있을 뿐, 주요 기능은 안전행정부에 주어져 있다. 그러나 안전행 정부는 오히려 전자정부 추진이라는 미명 하에 국민의 개인정보를 생성, 수집하고 집적, 이용하는 부처로서 개인정보보호 업무에 부적합하다. 금융위원회와 금융감독원 역시 개인정보 보호에 대한 전문성도 의지도 없다. 방송통신위원회는 ‘공개된 개인정보’라는 황당한 개념으로 정보주체의 권리를 박탈하고 개인정보의 오남용을 부추기는 ‘빅데이터 개인정보보호 가이드라인’을 추진하여 사회적 물의를 일으키고 있는 것이 현실이다. 전 사회적인 개인정보 보호를 강화하기 위해서는 개인정보보호위원회의 독립성과 권한을 강화할 필요가 있다.

우리는 이와 같은 제안이 2월 국회에서 법안으로 발의되고 통과될 수 있도록 노력할 것이다. 이미 공인인증서 의무화 폐지를 위한 「전자금융거래법」 개정안과 개인정보보호위원회 강화를 위한 「개인정보보호법」 개정안이 발의되어 있는 상황이다. 우리는 정부와 국회에 개인정보 보호를 위한 근본적인 대책을 조속히 마련할 것을 다시 한 번 촉구한다.

2014년 2월 5일

경실련, 진보네트워크센터, 참여연대, 함께하는시민행동