情 報 保 護 學 會 誌
第22卷 第6號, 2012. 10

개인정보보호 신규 제도와 정책 변화

최 광 희*, 정 연 수**, 이 재 일***

요 약

최근 해킹 등으로 인한 대량 개인정보 유출 사고로 인한 계속됨에 따라 개인정보보호 법제도 측면에서 변화가 시작되고 있다. 지금까지는 사고원인을 분석하여 기술적, 관리적으로 미흡한 부분을 보완하는 기업의 보호조치의무를 강화하는 방식이었으나, 최근에는 보다 근본적으로 개인정보 수집을 최소화하고 사고를 적극적으로 예방하려는 다양한 신규 제도가 만들어지고 있다. 따라서 새롭게 도입되는 개인정보보호제도의 의미와 주요 내용을 살펴보고 기업이 새로운 제도에 대응하는 전략을 고찰하고자 한다.

Ⅰ. 서 론

대량 개인정보 유출 사고가 계속됨에 따라 기업의 개인정보보호체계를 강화해야한다는 사회적 공감대가 형성되었다. 하지만 종전처럼 기업에게 암호화나 방화벽 도입 등의 보호조치 구축 의무만을 강화하는 방식으로는 점점 지능화되고 고도화되는 개인정보 유출 위협에 효과적으로 대응하기는 어렵다. 따라서 정부는 2011년 8월 '인터넷상 개인정보보호 강화방안'을 발표하면서 보다 근본적인 개인정보 유출 사고를 예방하기 위한 제도 도입을 추진하였다. 그 결과 "정보통신망이용촉진 및 정보보호에 관한 법률(이하 정보통신망법)" 개정으로 올해 8월 18일부터 지금까지 정책과 성격이 다른 다수의 신규제도가 도입되었다. 그러나 아직까지 많은 사업자들이 신규제도의 의미와 정부 정책의 변화를 이해하지 못해 새로운 제도 도입에 많은 어려움을 겪고 있다. 따라서 본 논문에서는 현재 개인정보보호 체계 문제점과 새로운 제도의 주요 내용을 살펴봄으로써 사업자들이 신규제도를 효과적으로 도입할 수 있는 방안을 모색하고자 한다.

Ⅱ. 기존 체계의 문제점

2.1 과도한 주민등록번호 수집 및 이용

국내 웹사이트의 대부분은 회원가입시 본인인증을 수행하고 있으며 대표적인 방식이 주민번호와 성명을 입력하는 실명확인 방식을 사용하고 있다. 이로 인해 많은 웹사이트가 모든 회원들의 주민번호를 보유하고 이를 통해 고객을 고유하게 식별하고 관리하게 된다.

하지만 주민번호는 그 자체로 많은 개인정보를 포함하고 있으며, 취약한 위조검증방식, 영구성, 유일 식별성 등의 문제를 가지고 있다. 따라서 개인정보보호법에서는 주민번호를 수집할 때에 이용자에게 별도 동의를 받거나 타 법령에서 요구된 경우만 수집·이용할수 있도록 한정하고 있다[1][2]. 주민번호 수집시 동의 규정을 만든 취지도 수집·이용을 최소화하고자 하는 의도였으나, 실제는 대부분의 기업이 별도 동의를 획득하는 과정을 신설하고 이용자도 신중한 확인 없이 동의를 하고 있어 무분별한 주민번호 수집·이용 관행이 개선되지 않고 있다.

2.2 개인정보보호조치 구축에 소극적

개인정보보호관련 법률에는 기업이 수집한 고객의

* 한국인터넷진흥원 개인정보보호기획팀장(khchoi@kisa.or.kr)
** 한국인터넷진흥원 개인정보보호단장(meet@kisa.or.kr)
*** 한국인터넷진흥원 정보보호본부장(jilee@kisa.or.kr)

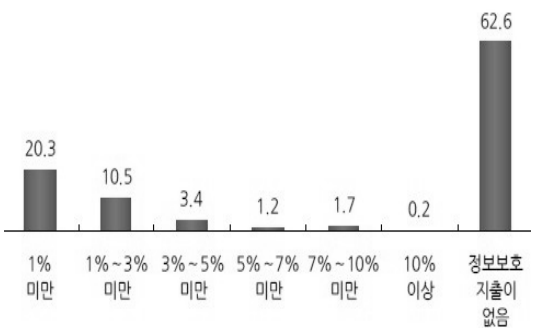
개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 적절한 안전성 확보조치를 수립하고 이행하도록 의무화 하고 있다.

〔표 1〕 개인정보보호관련 법령의 보호조치

법령	조항
개인정보보호법	제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
정보통신망법	28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

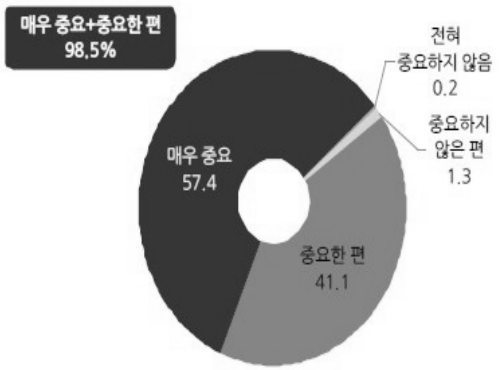
법률에 명시된 보호조치는 기업이 개인정보를 안전하게 관리하는데 필요한 최소한의 조치이므로 각 기업들은 법률에서 요구한 보호조치를 기반으로 위험분석을 통해 추가적인 보호조치를 구현해야 한다. 이를 위해서는 일정 수준 이상의 투자가 필요하나, 국내 사업자의 83%가 정보보호에 대한 투자가 전무하거나 정보화 예산 대비 1%미만의 투자를 하고 있는 상황이다[3].

현행처럼 개인정보유출 사고가 발생하면 원인을 분석하여 보호조치를 강화하는 방식으로는 지능화, 조직화되는 해킹기법에 효율적으로 대응할 수 없으며, 기업의 적극적 투자를 유도하기에도 어려운 상황이 지속될 수밖에 없다.



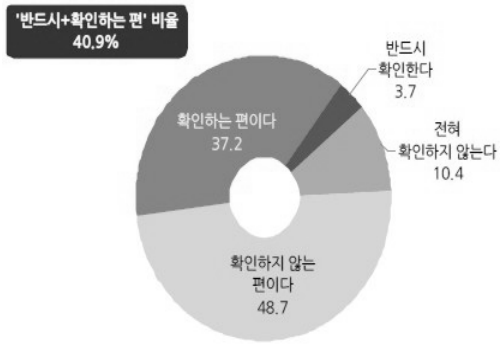
〔그림 1〕 정보화 투자 대비 정보보호 투자 비율(단위: %)

2.3 개인정보보호를 위한 이용자 참여 저조



〔그림 2〕 개인정보보호의 중요성 인식

한국인터넷진흥원에서 수행한 “2011 정보보호 실태조사”에 따르면 개인 인터넷 이용자중 98.5%가 평소 인터넷 이용시 개인정보보호의 중요성에 대해 공감하는 것으로 나타났다. 하지만 이와 반대로 기업이 개인정보보호 취급방침을 공개한다는 사실을 아는 이용자는 46.9%이고 이중 취급방침의 내용을 확인하는 사람은 40.9%에 그쳐 개인정보보호의 중요성에 비해 이용자의 인식 수준이나 보호활동은 상당히 미흡한 것으로 나타났다[3].



〔그림 3〕 개인정보취급방침의 확인 여부

정부가 모든 사업자를 관리·감독하기는 현실적으로 불가능하다. 따라서 기업의 지속적인 개인정보보호 활동을 유도하기 위해서는 이용자가 개인정보보호에 관심을 갖고 적극적으로 자신의 권리를 주장하는 환경을 만드는 것이 중요하다. 따라서 이용자가 개인정보보호 측면의 권리를 행사하기 편리한 법제도적 기반을 마련하

〔표 2〕 주민번호 수집·이용을 명시한 대표적인 법률

근거 법령		주요 내용
금융실명 거래법	법 제3조, 시행령 제3조	금융거래시 성명·주민등록번호 등으로 실지명의 확인
부가 가치 세법	법 제16조, 시행령 제53조	재화·용역을 공급받은 자에게 세금계산서를 교부하는 경우, 세금계산서에 공급받은 자의 주소·성명·주민번호 기재
	법 제17조의2, 시행령 제63조의2	사업자가 관할 세무서에 대손세액공제를 신고하는 경우, 신고서에 재화·용역을 공급받은 자의 주민번호 기재
	법 제33조, 시행령 제84조	납세관리인을 관할세무서에 신고하는 경우, 납세관리인 선정 신고서에 납세관리인(부가통신사업자)의 주민번호 기재
소득 세법	법 제145조, 시행령 제193조	원천징수의무자는 기타소득을 지급할 때 원천징수영수증을 발급해야 하며, 영수증에 주민번호 기재
	법 제164조, 시행령 제213조	기타소득 등에 대한 지급명세서를 관할 세무서에 제출 시, 기타소득자의 주민번호 기재
신용정보 보호법	법 제15조, 16조, 20조, 시행령 제13조, 17조	신용정보회사등은 일정한 제약조건을 준수하면서 신용정보를 수집할 수 있으며, 이 경우 신용정보주체를 식별하기 위하여 주민등록번호도 함께 수집할 수 있음
	법 제25조, 시행령 제21조	주민등록번호는 신용정보집중기관에서 집중관리 활용되는 신용정보의 하나로, 성명·주소와 함께 개인식별을 위한 key 값으로 사용됨
	법 제34조, 시행령 제29조	신용정보회사는 신용정보 제공·이용자로부터 본인의 동의를 얻은 뒤 주민번호 등 개인정보를 수집 가능
전자금융 거래법	법 제6조 시행령 제6조	금융기관 또는 전자금융업자는 전자금융거래를 위하여 주민등록번호를 포함한 개인정보를 통해 이용자 신원 확인
	법 제7조 시행령 제7조	금융기관 또는 전자금융업자는 전자금융거래의 거래내용 확인을 위해 주민등록번호를 포함한 상대방에 관한 정보 보존
	법 제16조 시행령 제11조	5만 원 이상의 전자화폐를 사용하고자 할 경우 실지명의와 연결하여 관리
전자상거래 소비자보호법	법 제6조	전자상거래 및 통신판매 사업자는 거래 기록 및 그와 관련한 개인정보를 보존
전자서명법	법 제15조, 시행규칙 13조의2	공인인증서 발급 시 발급자의 성명·주민등록번호 등으로 신원확인

는 것이 필요하다.

Ⅲ. 신규제도 도입

인터넷을 통한 대량 개인정보 유출 사고를 근본적으로 방지하기 위한 다양한 신규제도를 담은 정보통신망법이 2012년 8월 18일부터 시행되었다. 이번에 시행되는 인터넷상 주민등록번호(이하 주민번호) 수집·이용 금지와 이용자의 권리 행사를 강화하기 위한 새로운 정책적 내용을 포함하고 있다.

3.1 주민번호 수집·이용 금지

신규제도 중 가장 큰 정책적 변화는 인터넷 웹사이트에서 주민번호 수집·이용을 금지한 것이다. 행정 목적으로 발급된 주민번호는 편의성 때문에 공공과 민간 웹사이트에서 본인확인 수단으로 광범위하게 사용되고 있으며 국내 180만개 웹사이트 중 약 32만개 웹사이트에서 사용되는 것으로 추정된다[4][5][7].

최근 주민번호가 포함된 개인정보 대량 유출 사건이 빈발하여, 유출된 주민번호를 이용한 명의 도용, 신분증 위조, 보이스 피싱 등의 피해가 증가하여 사회적 불안감이 고조되고 있다.

이와 같은 대량 주민번호 유출 및 오남용 피해를 근본적으로 방지하기 위해서 인터넷상에서 불필요한 주민번호 수집·이용을 금지 하였다. 즉, 법률에 주민번호를 수집·이용할 수 있는 근거가 명시되어 있거나, 아이핀 등의 인증수단을 제공하는 본인확인기관만 인터넷상에서 주민번호를 사용할 수 있게 되었다.

또한 법률 시행이전에 수집하여 저장하고 있던 주민번호는 법 시행 후 2년 안에 모두 파기해야 한다[4][5][7].

제도 시행으로 사업자가 수집하는 주민번호가 줄어들게 되어 대량 유출 위험이 감소하게 되었으며, 인터넷상 주민번호를 사용하지 않는 환경이 조성됨에 따라 이미 유출된 주민번호도 악용되지 않는 효과가 예상 된다.

3.2 개인정보 이용내역 통지제도

지금까지는 이용자가 웹사이트에 자신의 개인정보 이용내역을 요구할 경우에만 사업자가 해당 기록을 제공하고 이를 통해 이용자가 삭제요청 등의 권리행사를 할 수 있었다. 하지만 이용자가 자신이 이용하는 웹사이트에 기록을 요구하는 경우가 많지 않아 실질적 권리행사가 되지 못하는 경우가 대부분이다. 따라서 기업이 개인정보를 제3자나 위탁 사업자에게 무분별하게 제공하는 관행이 쉽게 개선되지 않는 문제가 발생하였다.

개인정보 이용내역 통지 제도는 사업자등으로 하여금 수집한 이용자의 개인정보 이용내역을 해당 이용자에게 주기적으로 통지하도록 함으로써 이용자가 자신의 개인정보 이용내역을 정확히 알고 자기정보를 스스로 통제할 수 있도록 하기 위하여 도입되었다.

하지만 모든 사업자가 대상이 될 경우 개인측면에서는 다수의 웹사이트로부터 이용내역 이메일을 수신이 하게 되고, 사업자측면에서도 영세기업은 이용기록 보관 및 통지를 위한 설비 구축 등의 비용이 발생할 수 있어 적용 대상을 한정하였다.

즉, 개인정보 이용내역 통지제도 대상 사업자는 전년도 말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 경우로 한정되었으며, 이용자의 개인정보 이용내역는 연 1회 이상 해당 이용자에게 통지하여야 한다.

통지시 포함되어야 하는 정보는 첫째, 개인정보의 수집·이용 목적 및 수집한 개인정보의 종류, 둘째, 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 종류, 셋째, 개인정보 취급 위탁을 받은 자 및 그 취급위탁을 하는 업무의 내용이다.

통지방법은 전자우편, 서면, 팩스, 전화 등이 모두 가능하며 이용자에 정기적으로 발송하는 이메일이 있는 경우 이를 활용하여도 된다[6][7].

3.3 개인정보 유효기간제도

최근 발생하는 개인정보 누출 사고는 현재 정보통신서비스를 이용하고 있는 이용자의 개인정보 뿐만 아니라 장기간 미사용자의 개인정보도 상당부분 포함되어 있다. 이러한 경우에는 해킹으로 인해 자신의 개인정보가 유출된 사실조차 인지하지 못해 유출된 개인정보를 악용한 명의도용 등의 2차 피해 위험이 더욱 높아진다.

따라서 장기간 서비스를 이용하지 않고 방치되는 개인정보 유출로 인한 이용자의 피해를 방지하고 사업자의 불필요한 개인정보 보관을 최소화하기 위하여 3년간 서비스를 이용하지 않은 고객의 개인정보는 파기 또는 운영 DB에서 분리하여 저장하는 등의 조치를 취하도록 하는 개인정보 유효기간제가 도입되었다.

사업자들은 타 법률에 의해 개인정보를 일정기관 보관하도록 요구받는 경우나 이용자가 별도로 저장기간을 요청한 경우가 아니라면, 제도가 시행되는 2012년 8월 18일을 기준으로 3년이 경과한 2015년 8월 이후에는 해당 정보통신서비스를 이용하지 않는 기존 이용자의 개인정보를 파기하는 등의 조치를 취해야 한다.

개인정보가 삭제되어 발생할 수 있는 선의의 피해를 방지하기 위해 전자우편, 서면, 팩스, 전화 등의 방법 중 하나를 선택하여 개인정보가 파기 또는 분리 저장·관리 되는 사실과 일시, 개인정보 항목을 해당 이용자에게 유효기간 만료 30일 전까지 통지하여야 한다[6][7].

3.4 개인정보취급자의 인터넷망 분리

최근 발생한 농협, SK 컴즈 등의 개인정보 침해사고를 분석해보면 해킹 기법이 고도화, 지능화고 기업의 핵심 서비스 마비나 고객 정보 DB를 노리는 경우가 많아지고 있으며 핵심 시설에 접근하기 위해 관리자 PC을 우선 공격하여 통제 권한을 확보하는 경향이 나타나고 있다.

관리자 PC를 통한 개인정보처리시스템에 불법접근을 근본적으로 차단하기 위하여 외부 인터넷망의 분리가 의무화 되었다.

외부 인터넷망의 분리 역시 기업에게 과도한 비용 부담이 발생할 수 있으므로 전년도 말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 사업자만을 의무 대상으로 하고, 인터넷망을 분리 시켜야 하는 대상도 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템의 접근권한 설정을 변경할 수 있는 개인정보취급자 PC로 한정하였다. 또한 망분리 방식도 전송망, PC 등을 이원화하여 내부 업무망과 외부 인터넷망의 접근 경로를 차

단시키는 물리적 망분리와, 하나의 전송망이나 PC를 사용하지만 가상화 등의 방법을 사용하여 내부 업무망과 외부 인터넷망이 서로 접근할 수 없도록 구성하는 논리적 망분리를 모두 가능하게 하여 기업의 부담을 최소화 하였다[6][7].

Ⅳ. 결 론

8월부터 시행되는 신규제도를 분석해보면 기존의 개인정보보호 정책의 변화를 찾아 볼 수 있다.

첫째, 인터넷상에 유통되는 개인정보를 최소화하는 정책의 시행이다. 지금까지는 기업이 보유하고 있는 개인정보의 유출이나 노출을 막기 위해 기업의 보호조치 구축 의무를 강화해 나왔으나, 인터넷상의 주민번호 수집・이용을 금지시키고 개인정보 유효 기간제를 도입하는 것은 지금까지 무분별하게 수집되고 이용되던 개인정보 자체를 줄여 대량 개인정보 유출이나 2차 피해를 근본적으로 줄여나가기 위한 정책이다.

둘째, 이용자의 적극적 권리 행사를 보장하기 위한 정책의 강화다. 이용자에게 개인정보를 어떻게 사용하였는지 그 해당 내역을 통지함으로써 불필요하게 제3자나 위탁 사업자에게 개인정보가 제공되는 문제를 최소화하고 이용자가 주기적으로 그 내역을 확인할 수 있게 됨으로써 회원 가입시 신중한 검토 없이 제공한 개인정보를 사후에라도 관리될수 있도록하는 정책이다.

앞으로 개인정보보호 정책은 이러한 두가지 새로운 방향성을 중심으로 개선되어 나갈 것으로 보인다. 이러한 정책 변환에 맞추어 기업은 개인정보를 활용하는 서비스를 점검하여 서비스 제공에 반드시 필요한 개인정보만을 수집하여야 한다. 또한, 이용자에게 수집한 개인정보의 종류, 이용 목적, 활용 내역 등을 명확히 알려주고 언제든지 이용자가 관련 정보를 삭제, 수정 할 수 있도록 필요한 기능을 제공하는 것이 중요하다.

참고문헌

[1] 이형효, “주민등록번호 대체수단 요구사항 연구” 2010 한국정보기술학회 하계학술대회 논문집.
[2] “개인정보 보호법령 및 지침・고시 해설” (2011), 행정안전부.
[3] “2011 정보보호실태조사” (2012), 한국인터넷진흥원.
[4] “인터넷 사업자를 위한 주민번호 사용 제한 정책 안내서” (2012), 한국인터넷진흥원.
[5] “인터넷 사업자를 위한 주민번호 사용 제한 준비 안내서” (2012), 한국인터넷진흥원.
[6] “개정 정보통신망법 개인정보보호 신규제도 안내서” (2012), 한국인터넷진흥원.
[7] “정보통신서비스 제공자를 위한 개인정보보호 법령 해설서” (2012), 한국인터넷진흥원.

〈著者紹介〉

최 광 희(Kwanghee Choi)
2002년: 중앙대 정보시스템과(석사)
2007년: 전남대 정보보호협동과정(박사수료)
2002년 1월~2009년 7월: 한국정보보호진흥원
2009년 7월~현재: 한국인터넷진흥원 개인정보보호기획팀장
<관심분야> PIMS, IDM, 정보보호거버넌스

정 연 수(Yeonsu Jeung)
1998년: 성균관대학교 행정학과(석사)
2003년: 중앙대학교 행정학과(박사수료)
1989년~1996년: 정보통신부
1996년 4월~2009년 7월: 한국정보보호진흥원 개인정보호팀장, 개인정보분쟁조정위원회 사무국장
2009년 7월~현재: 한국인터넷진흥원 개인정보보호단장
<관심분야> 개인정보보호, 이용자 피해구제, 잊혀질 권리

이 재 일(Jaeil Lee)
1988년: 서울대학교 계산통계학과(석사)
2006년: 연세대학교 컴퓨터과학과(박사)
1996년: 한국IBM
1996년 7월~2009년 7월: 한국정보보호진흥원 전자서명인증센터장, IT기반보호단장
2009년 7월~현재: 한국인터넷진흥원 정보보호본부장
<관심분야> 정보보호, 정보인증, 개인정보보호