情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

개인정보 유출 시 통지·신고 프레임워크 및 가이드라인

이 충 훈,† 고 유 미, 김 범 수‡
연세대학교 정보대학원

A Framework and Guidelines for Personal Data Breach Notification Act

Chunghun Lee,† Yumi Ko, Beomsoo Kim‡
Graduate School of Information, Yonsei University

요 약

2011년 9월 시행되는 개인정보 보호법에 따르면, 개인정보처리자는 개인정보 유출에 대한 추가적인 법적 책임을 져야 한다. 특히 개인정보 유출 시, 개인정보처리자는 정보 주체에게 개인 정보가 유출된 사실을 의무적으로 통지를 하여야 한다. 본 연구에서는 미국 46개주에서 실시하고 있는 현행 유출 통지법과 기타 국가의 주요 사례를 분석하여, 유출 통지 프레임워크를 제시한다. 개인정보 유출통지 프레임워크는 (1) '통지의 대상이 되는 개인정보', (2) '통지 주체', (3) '통지 시점', (4) '통지 내용', (5) '통지 방법' 등 다섯 가지 중요 요소로 구성된다. 그리고 새로운 유출 통지 프레임워크에 기초하여, 향후 적절한 가이드라인을 수립하기 위한 방향을 제안한다.

ABSTRACT

Recent personal data breach incidences draw the public's attention to their privacy and personal rights. The new personal data protection law effective in September 2009 imposes additional legal responsibility on personal data controllers and processors. For instance, if a data breach occurs, this new law requires that the processors must notify individuals (data subjects) and data protection authorities of the nature of incidents. This research reviews the U.S. forty six state laws and related acts, and offers a framework for managing incidents. This framework includes five major components: (1) type of personal data required to be reported and notified, (2) the ultimate subject notifying data subjects, (3) event occurrence and notification time phases, (4) notification message details, and (5) direct/indirect communication media. Along with this framework, we also offer directions for effective/manageable guidelines on data breach notification act.

Keywords: Personal Data; Privacy; Data Controller; Data Processor; Personal Data Breach Notification Act; Data Breach Notification Framework, Guidelines

I. 서 론

정보통신 기술의 혁신적인 발전으로 정보 생산 및 유통, 그리고 이를 활용한 새로운 가치 창출 활동이 활성화 되었다. 하지만 민감한 개인정보들까지 무작위로 오·남용 되면서 개인정보에 대한 적절한 대안과 보호 방안의 필요성이 높아지고 있다.

지난 4월 H금융사는 고객 43만 명의 이름과 주민등록번호, 전화번호, 주소가 유출되었고, 이 중 1만 3,000명은 대출계좌번호와 비밀번호까지 해킹된 데 이어, 농협 전산시스템 마비 등 대형 보안 사고들이 연달아 발생했다. 그리고 한국인터넷진흥원(KISA)의 개인정보침해센터에 신고 된 상담 건수만 보더라도 2009년 3만 5,167건에서 2010년 5만 4,832건으로 무려 56%가 증가했다. 행정안전부의 자료에 따르면

접수일(2010년 7월 29일), 게재확정일(2011년 9월 27일)
† 주저자, goguming@gmail.com
‡ 교신저자, beomsoo@yonsei.ac.kr

2007~2010년 사이 무려 1억 건의 개인정보 침해사건이 일어났으며, 60여 건의 소송 제기에 총 소송가액은 2,100억 원에 달하는 것으로 나타났다[9].

이러한 개인정보보호 이슈 속에 정부는 개인정보를 보호하기 위한 현행 법제의 한계를 인식하고 공공부문과 민간부분을 아우르는 개인정보 보호법을 제정하기 위하여 지속적인 노력을 경주해 왔으며, 그 결과 올해 3월 국회에서 개인정보 보호법이 통과되었다. 특히 개인정보 유출 시 통지의무조항이 마련되어, 개인정보처리자는 유출사고가 발생했을 때 반드시 정보주체 및 해당기관에 통지해야 한다.

개인정보유출 시, 통지는 유출사고 후 추가적인 피해가 발생하지 않도록 하는 중요한 사후조치 사항이며, 개인정보처리자가 신속하게 정확한 통지를 할 수 있도록 체계적인 가이드라인을 제공하는 것이 중요하다. 그리고 통지는 사고분석과 동시에 내·외부 커뮤니케이션이 긴박하게 이루어지는 단계이기 때문에 세부 가이드라인 작업에 앞서 전체적인 통지 프로세스를 조망할 수 있는 통지프레임워크를 사전에 마련하고 운영하여야 한다.

국내의 경우, 개인정보 보호법이 제정되기 전까지 정보주체에 대한 통지는 의무 조항이 아니었고 해외의 경우에도 미국을 제외한 많은 국가들에서 권고사항이기 때문에 통지 프레임워크에 대한 국내·외 연구와 자료가 미흡한 실정이다. 따라서 본고는 2003년 캘리포니아 주를 시작으로 현재까지 대부분의 주에서 통지법을 시행하고 있는 미국의 주별 통지법을 분석하였다. 또한, 전문 기관들의 실제 적용 사례 및 문헌 연구를 바탕으로 국내 실정에 맞는 통지 프레임워크를 도출하였다. 이렇게 도출된 유출 통지 프레임워크는 향후 만들어질 개인정보 유출통지 제도 가이드라인의 방향을 설정하고 수립하는데 기초 자료로 활용할 수 있다.

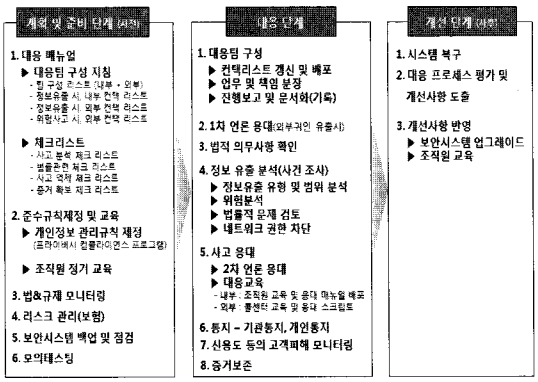
II. 기업대응 프로세스

개인정보가 유출됐을 때, 중요한 기업 대응단계 중 하나인 통지단계에서는 선행된 조사 및 분석단계를 통해 구체화된 사고개요와 대응방안을 바탕으로 내·외부 커뮤니케이션이 이루어지게 된다. 따라서 통지 프레임워크 도출에 앞서, 기업대응 프로세스의 각 세부단계에 대한 기본적인 이해가 필요하다. 앞에서 언급했듯이 통지의 목적은 사고개요와 대응방안을 정확하게 정보주체에게 전달하여 추가 피해를 예방하는데 있다. 통지 시, 중요한 구성요소인 사고개요와 대응방안은 정보유출분석, 사고 응대 등의 대응 단계를 통해서 구체화되고 명확해지게 된다. 그리고 기업대응 프로세스 중, 대응단계 외에도 계획 및 준비 단계 또한 통지와 밀접한 관련을 가진다. 사전 준비단계라 할 수 있는 계획 및 준비 단계에서는 개인정보유출을 대비한 통지문, 통지방법 등 법률적 요구사항이 반영된 사전 매뉴얼을 준비하여 사고가 발생했을 때 신속하고 체계적인 통지가 이루어질 수 있도록 한다. 따라서 통지와 관련된 구체적 방법인 프레임워크 도출에 앞서 일반적 방법인 기업대응 프로세스에 대한 이해가 선행될 필요가 있다.

개인정보 유출 사고는 기업의 비용 손실 외에도 이미지 실추까지 가져올 수 있는 기업의 위기 요소이다. 따라서 기업대응 프로세스 연구는 위기관리 관점에서 관련 자료들을 조사·분석하는 것이 적합하며, 위기관리 모델을 참고하여 기업대응 프로세스 프레임워크를 도출하였다.

많은 학자들이 다양한 위기관리 모델을 제시하고 있으나, 이 중에서 보편적으로 사용되는 Coombs[3]의 위기관리모델은 위기관리 단계를 위기 전 단계(Pre-crisis), 위기단계(Crisis Event), 위기 후 단계(Post-crisis)의 3단계로 구분하고 있다. 본 연구에서는 Coombs의 위기관리 모델을 반영하여 기업의 개인정보 유출의 대응 절차를 '계획 및 준비 단계(사전)', '대응 단계', '개선 단계(사후)'의 3단계로 나누었으며, [그림 1]과 같다.

기업대응 프로세스 프레임워크의 첫 번째 단계는 '계획 및 준비 단계'로써, 유출사고가 발생했을 때 효과적인 대응을 위해 사전에 구체적인 대응 계획을 수립하고 대응 매뉴얼을 준비한다. 그리고 정기적인 법·규제 모니터링을 통해 개인정보관리 시 나타난 취



[그림 1] 기업대응 프로세스 프레임워크

약점을 조기에 식별하여 법률 위반사항을 사전에 방지할 수 있다.

두 번째 단계는 유출사고가 발생했을 때, 사고를 수습하는 '대응 단계'이다. 대응 매뉴얼에 따라 신속히 대응팀을 구성하여 정확한 사고조사 외에, 루머확산 방지 및 기업이미지 실추를 최소화하기 위한 1차 언론 응대를 수행한다. 그리고 수집 된 정보들을 바탕으로 2차 언론 응대뿐만 아니라, 정보주체와 해당기관에 대한 통지 및 콜센터 운영을 통해 대응 커뮤니케이션을 실행한다.

마지막 단계는 유출사고가 수습된 이후 사후단계로써 '개선 단계'이다. 사고로 인하여 손상된 시스템을 복구하며, 대응절차에 대한 객관적 평가를 통해 개선사항을 도출하여 반영함으로써 대응프로세스를 고도화한다.

개인정보처리자는 개인정보 유출사고를 대비하여, 계획 및 준비 단계, 대응단계, 개선단계로 구성되는 대응프로세스를 구축·운영하는 것이 중요하다. 그 중, 개인정보유출이 발생했을 경우 실제적으로 대응조치가 이루어지는 대응단계는 사고에 대한 정확한 분석을 바탕으로 내·외부 응대 및 문제 해결 등이 긴박하게 이루어지는 핵심단계라고 할 수 있다. 특히, 대응단계에서 정보주체와 커뮤니케이션이 이루어지고 대응조치가 공유되는 통지는 개인정보유출로 인한 피해를 최소화하는 주요 조치사항 중에 하나이다[1,5,10,11,15,17].

III. 유출 통지 프레임워크

3.1 미국의 데이터 유출 통지법 사례

미국에서는 각 주별로 데이터 유출 통지법(Data Breach Notification Law)을 시행하고 있다. 대표적으로 캘리포니아 주는 2003년 보안위반정보법(Security breach information Act, 2003년 7월)을 시행하였고, 현재 미국에서 Alabama, Kentucky, New Mexico, South Dakota 4개 주를 제외하고 유출 통지법을 시행하고 있다. 각 주별로 통지법을 분석한 결과 주요 다섯 가지 영역인 '통지대상이 되는 개인정보', '통지주체 및 대상', '통지시점', '통지방법', '통지내용'으로 구분할 수 있으며, 각 영역별 자세한 항목은 [표 1]과 같다[2,8].

먼저, 통지대상이 되는 개인 정보를 광의의 의미로 기술하기 보다는 이름과 조합되는 개인식별번호와 금융정보로 대부분의 주에서 구체적으로 명시하고 있다.

[표 1] 미국의 데이터 유출 통지법 분석표

구분			United States	
			HITEC	California
Actual(A) or Proposed(P) or Guidelines(G)			A	A
개인정보	개인식별번호		Y	Y
	이름		Y	Y
	운전면허번호			Y
	금융계좌정보		Y	Y
	신용/직불카드 정보			Y
	신용/직불카드 비밀번호			Y
	생년월일		Y	
	주소		Y	
	기타		장애코드	
	데이터암호화 여부			Y
	공적 정보 제외여부			Y
통지대상	정보주체		Y	Y
	해당기관		Y	Y
통지방법	기본통지	-서면고지	Y(등기)	Y
		-전자고지		
		-전화통지		
	대체통지기준	-비용($)		25만
		-피해인원(명)	500	50만
		-불충분한 연락정보를 가진 경우	Y	
	대체통지방법	-email		Y
		-웹사이트	Y	Y
		-주 영역포괄 가능한 미디어 매체	Y	Y
통지시점	한계시점		60일	
	합리적 지연 허용여부		Y	Y
통지내용	사고경위기술		Y	Y
	유출된 개인정보 설명		Y	Y
	개인정보보호 추후 조치 방법		Y	Y
	수신자 부담 문의 연락처		Y	Y
	법적구제기관/해당기관연락처		Y	Y
	신용평가회사정보			Y

대체적으로 사회보장번호, 운전자등록번호, 주정부발급번호, 신용 및 직불카드 정보, 금융계좌 정보를 지정하고 있다. 미국 건강정보기술법(Health Information Technology for Economic and Clinical Health Act: 이하 'HITEC')에서는 의료정보에 특화되어 이름을 포함한 사회보장번호, 운전자등록번호, 생년월일, 주소, 장애코드 등을 개인정보로 지정하였다.

둘째, 대부분의 주에서 통지대상과 주체를 명시하였다. 통지대상은 정보주체와 해당기관으로 구분된다.

유출된 개인정보 소유자인 정보주체는 물론 추가 피해 확산방지를 위해서 개인정보보호 관련 담당 기관에 통지하여야 한다. 통지주체는 일반적으로 개인정보처리자이지만 개인정보를 위탁하거나 제3자에게 제공했을 때에는 대부분의 주에서 수탁자 또는 제3자가 개인정보처리자에게 통지해야 하는 것으로 명시하고 있다.

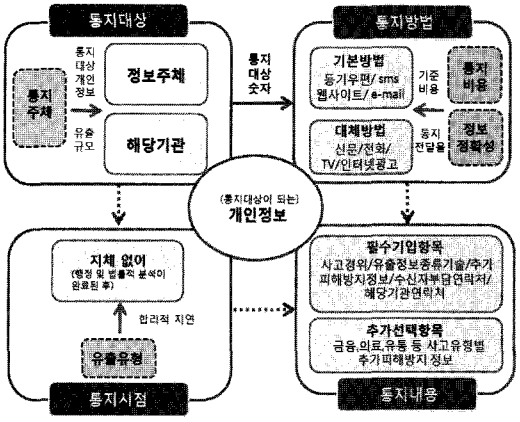
셋째, 통지방법은 통지대상 숫자와 통지비용, 연락처의 불충분함에 따라 기본방법과 대체방법으로 이원화 하였다. 기본통지 방법에는 주로 서면통지, 전자통지, 전화통지를 지정하였고, 대체적으로 통지대상 규모가 50만 명 이상이거나 통지 비용이 25만 달러 이상일 때, 그리고 통지대상의 연락처가 불충분할 시에는 대체 통지를 허용하였다. 대체통지 방법에는 인디애나 주를 제외한 거의 모든 주가 주를 포괄하는 미디어, 웹사이트 공지, e-mail을 모두 사용하도록 하였다.

넷째, 통지시점에 대하여 대부분의 주에서는 "without unreasonable delay(불합리한 지연 없이)", 또는 "in the most expedient time possible and without unreasonable delay(불합리한 지연 없이 가능한 조속한 시기에)" 로 명시하고 있다. 다만, 범죄 조사, 국가적인 보안 침해 등과 같이 신중한 조사가 필요할 때, 그리고 시스템의 무결성 복구 시에는 합리적 지연을 가능하도록 하였다. 반면에 HITEC에서는 유출 사고 인지 후 60일 내로, 플로리다 주 역시 사고 발생시점이 아닌 사고 인지 후 45일 이내로 통지 한계시점을 조항으로 제시하였다.

마지막으로 유출 사고의 구체적 사고경위와 유출된 개인정보 유형 및 추가 피해방지를 위한 조치 등 통지문에 필수적으로 포함해야 할 내용을 제시하여 정보주체는 유출사고에 대한 정확한 정보를 습득하고 개인정보처리자는 통지문 작성 시 혼돈이 없도록 하였다.

3.2 유출 통지 프레임워크

개인정보 보호법이 시행되기 전까지 국내에서 개인정보 유출사고에 대한 통지는 법적 의무사항이 아니었다. 정보통신기반 보호법 제13조, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조에 나타난 바와 같이 기존의 국내 유사 법제에서는 일정 요건을 충족할 경우에 한하여 해당기관에 통지하도록 하였으나, 정보주체에게 반드시 통지하도록 하는 조항은 없었다[13]. 그러나 개인정보 보호법이 발효되면서 개인정보 유출 시에 그 사실을 정보주체에게 정확하게 통지



〔그림 2〕 개인정보 유출 시 통지 프레임워크

하도록 함으로써 정보주체의 권익을 보장하고, 개인정보처리자 또한 적극적인 조치를 취하게 함으로써 개인정보 관리의 투명성 제고 및 신뢰를 구축할 수 있게 되었다.

국내보다 앞서 통지법을 시행하고 있는 미국의 사례를 조사·분석하여 일련의 통지 프로세스가 '통지대상 개인정보', '통지주체', '통지시점', '통지내용', '통지방법'의 다섯 가지 핵심 요소로 구성됨을 밝혔다. 이들 해외사례 분석을 바탕으로 국내 개인정보 보호법 및 실정을 고려한 프레임워크를 〔그림 2〕와 같이 도출하였다.

국내에서도 개인정보 유출사고가 발생했을 경우, 개인정보처리자는 개인정보 보호법의 통지 의무조항에 따라 정보주체에게 통지해야 한다. 이 때 활용 가능한 통지 프레임워크는 '통지대상이 되는 개인정보', '통지주체 및 대상', '통지방법', '통지시점', '통지내용'의 다섯 영역으로 구성되며 서로 긴밀한 관계를 가진다. 먼저 통지대상이 되는 개인정보가 유출 된 경우, 개인정보처리자는 정보주체에게 통지하고 해당기관에 신고해야 한다. 이때 통지방법은 기본통지와 대체통지로 이원화되며 그 기준은 통지대상의 규모와 통지 비용, 정보주체 연락처의 정확성이 고려된다. 통지시점에서는 개인정보처리자가 유출 사실을 인지한 '즉시'로 해석하기보다는 법률적·행정적 절차가 완료된 시점으로 해석하는 것이 적합하며 이와 함께 유출 사고의 유형에 따라 합리적 지연 여부가 고려된다. 마지막으로 통지시점에 따라 통지내용의 구체성과 정확성 여부가 달라질 수 있지만 법에서 제시된 내용은 반드시 포함하되, 유출유형에 따른 선택적 추가항목으로 구분될 수 있다.

IV. 프레임워크의 주요 요소

4.1 통지대상 개인 정보

개인정보에 대한 보호는 기업이 소유권을 갖고 있는 자산을 직접 관리·보호하는 것과 그 성격을 달리한다. 일반적으로 기업 자산은 비즈니스 활동의 결과물로써 유출 또는 손실되어도 기업의 피해로 귀결된다. 그러나 개인정보는 기업이 정보주체로부터 정보의 발급부터 관리, 폐기에 이르는 일련의 과정에 대한 권리를 위임받은 것이다. 따라서 기업은 정보주체로부터 수집한 개인정보를 적극적으로 보호 할 의무가 있다.

정보기술이 발전하고 비즈니스 영역이 확대됨에 따라 보호되어야 할 개인정보의 범위 또한 확장되었다. 개인을 식별할 수 있는 정보에서 개인의 사생활을 침해할 수 있는 정보로까지 확대됨으로 인해 관리 대상 개인정보 유형이 매우 복잡해졌다. 개인을 설명하는 동일한 성격의 정보라 하더라도 시대와 환경이 변화하면서 개인정보의 의미와 영역도 변화되고, 어떤 상황에 놓이느냐에 따라 중요도 또한 달라진다. 따라서 개인정보는 개인의 성향, 성격, 경험 등과 같은 개인적 측면과 장소, 시간, 대상, 관계 등과 같은 사회·환경적 측면에 따라 개인정보 분류 체계가 달라지고 복잡해진다. 그러므로 법적 강제성이 부여되는 통지대상 개인정보의 경우에는 법 적용 대상자의 혼란을 최소화하고 법률 집행의 실효성을 고려하여 그 적용 범위를 최대한 한정할 필요가 있다.

개인정보 보호법에 따르면 개인정보는 살아 있는 개인에 관한 정보로서 성명, 주민등록번호, 영상 등을 통하여 개인을 식별할 수 있는 정보와 해당 정보만으로는 특정 개인을 확인할 수 없더라도 다른 정보와 쉽게 결합하여 식별할 수 있는 것까지 포함하는 것으로 정의된다. 그러나 개인정보 유출 사고가 발생했을 때, 정보주체에게 통지해야 할 개인정보는 광의의 의미로 기술하기보다는 정보의 민감성과 중요도에 따라 그 범위를 제한할 필요성이 있다. 유출된 개인정보의 종류에 따라 프라이버시 침해 여부나 2차 피해의 위험수준이 달라질 수 있기 때문이다. 일부 개인정보는 특정 정보와 결합하여 개인을 식별할 수 있어도 유출됐을 경우 명의도용, 금전적 피해 등을 일으킬 확률이 현저히 낮을 수 있다. 그러므로 정보주체를 설명하는 모든 개인정보들이 유출 사고 후 추가적인 피해를 야기하지는 않는다. 또한 통지대상 개인정보 범위가 광범위 할 때, 과다한 통지비용 발생과 잦은 통지로 인한 정보주체의 집중도가 현저히 저하될 수 있는 가능성도 함께 고려되어야 한다. 따라서 통지대상 개인정보는 개인식별정보, 금융정보 등과 같이 유출될 경우 제2차 피해의 우려가 높은 민감한 정보로 한정할 필요가 있다. Retzer[6]에 따르면 유출된 개인정보로 인해 추후 명의도용, 금융사기와 같은 추가 피해가 우려되거나 실직 또는 구직 기회 상실 위험을 초래할 경우에는 통지하여야 한다고 하였다. 미국 대부분의 주별 통지법에서도 개인정보는 이름과 개인식별번호, 그리고 금융 및 신용정보로 그 대상을 제한하고 있다.

통지대상이 되는 개인정보를 정리하면 [표 2]와 같이 유출된 개인정보의 추가 피해 정도를 고려하여 의무통지와 개인정보처리자의 자발적 통지가 가능한 정보로 구분된다. 먼저 의무통지 개인정보에는 온·오프라인에서 단일 정보만으로도 개인을 식별할 수 있는 정보들이 포함된다. 고유식별정보에는 성명 및 주민등록번호와 운전자등록번호, 여권번호, 외국인등록번호가 해당된다. 이 때, 성명은 다른 식별 가능한 정보와 결합하여 개인을 식별하는 기본 정보이다. 또한 인터넷 환경이 발달함에 따라 최근 주요 유출 정보인 온라인 계정정보가 추가된다. 온라인 계정정보는 온라인상에서 개인을 식별할 수 있고 전자상거래나 인터넷뱅킹 등이 활성화됨으로 인해, 유출 됐을 때 제2차 피해 우려가 높은 개인정보이다. 여성구[14]에 따르면 온라인상에서의 개인 식별자(아이디)가 웹 애플리케이션과 조합되어 개인의 식별, 성향, 상태 등을 나타낼 수 있다고 하였다. 그리고 임규철[16] 역시 온라인상에서는 익명의 아이디로 활동할 경우 개인식별 가능 유무로 보호법익을 결정하는 규정에 따라 당연히 개인정보에 포함된다고 하였다. 금융 및 신용정보는 유출 될 경우 금융사기 및 금전적 피해의 위험이 높기 때문에 의무통지대상에 포함하였다. 또한 개인정보 보호법 제23조와 시행령(안) 제22조에서는 개인의 사상·신념, 노동조합·정당의 가입 및 탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력자료 등에 관한 정보는 정보주체의 사생활을 현저히 침해할 수 있는 민감정보로 규정하고 있다. 이들 정보는 별도의 동의 없이는 처리할 수 없으며, 만약 이들 정보가 유출 될 경우 개인정보처리자는 반드시 통지하여야 한다.

통지대상 개인정보 외에 상대적으로 제2차 피해가 낮은 정보들은 자발적 통지대상으로 분류할 수 있으며 개인정보처리자가 제2차 피해 위험 수준을 고려하여 통지여부를 결정할 수 있다. 자발적 통지 개인정보에

〔표 2〕 유출 시 통지대상 개인정보

구분	항목	내용
의무 통지	고유 식별 정보	성명 및 주민등록번호, 운전자등록번호, 여권번호, 외국인등록번호 등
	금융 및 신용 정보	신용·직불카드 번호, 신용·직불카드 비밀번호, 신용등급, 계좌정보, 계좌비밀번호 등
	온라인 계정 정보	사용자 아이디(ID) 비밀번호, 이메일 등
	민감 정보	유전정보
		범죄경력자료 정보
		사상·신념
		노동조합·정당의 가입·탈퇴
		정치적 견해
		건강
		성생활 등
자발적 통지 (예시)	비민감 정보	인종, 습관 및 취미정보, 학력 및 훈련정보 등

는 인종, 습관 및 취미정보, 교육 및 훈련정보 등이 포함된다.

4.2 통지주체 및 대상

개인정보를 개인정보처리자가 직접 처리할 경우, 통지주체가 명확하지만 개인정보를 위탁하거나 제3자에게 제공했을 때 통지주체는 복잡해질 수 있다. 가이드라인(안)에서는 개인정보를 수탁 받거나 제공받은 제3자(수탁자)가 통지를 해야 한다고 제시하고 있다. 하지만 이럴 경우 개인정보의 최초 수집자인 개인정보처리자는 법 제18조, 제26조의 제3자 제공 및 위탁 시, 정보주체가 제공한 개인정보에 대한 관리의 책임이 있음에도 불구하고 직접적인 사고발생처가 아니라는 사실 때문에 사고 책임을 지지 않을 수 있다.

국내 판례(수원지방법원 2005. 7.29. 선고 2005고합160)에서도 개인정보처리자의 관리 소홀은 형사책임을 면할 수 없음을 확인할 수 있다. 개인정보처리자와 택배위수탁계약을 체결한 택배회사가 개인정보를 유출한 사건에 대해 법원은 택배회사가 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제66조에 정한 '법인의 사용인이 법인의 업무에 관하여' 위반행위를 한 것이고, 개인정보처리자는 위반행위를 방지하기 위하여 당해 업무에 대하여 상당한 주의와 감독을 하였다고 보기 어려워 형사책임을 면할 수 없다고 판결하였다.

미국의 대부분의 주는 수탁자 및 제3자가 개인정보처리자에게 유출사실을 즉시 통보해야 한다고 되어있지만 몇몇 주에서는 수탁자 및 제3자의 개인정보유출 시, 개인정보처리자의 관리 책임 이행을 요구하고 있다. 미국 애리조나 주의 통지법에서는 계약관계에서 별도로 통지에 관한 사항이 규정되어 있지 않으면 제3자(수탁자)가 개인정보유출 시, 개인정보처리자에게 해당 유출사실을 통보하고 개인정보처리자가 정보주체에게 통지하도록 되어 있다. 플로리다 주의 통지법에서도 개인정보처리자의 통지 책임을 부여하고 있다. 제3자가 개인정보유출 시, 개인정보처리자에게 통지를 하고 양쪽의 협의를 거쳐 정보주체에게는 하나의 통지만 갈 수 있도록 한다. 만약 통지에 대한 협의가 이루어지지 않을 때에는 정보주체와 직접적인 비즈니스 관계를 갖는 자가 통지를 하도록 되어 있다.

이처럼 유출 통지 시, 개인정보처리자가 관리적 책임을 이행할 수 있는 방향으로 가이드라인에도 반영되어야 한다.

4.3 통지시점

개인정보유출사고 발생 시 통지시점은 이해당사자들 간의 이해관계에 따라 복합적 시점을 아우르게 되는데, 사고발생시점, 사고인지시점, 통지시점으로 나누어 그 의미와 각 시점에 따른 통지대상이 달라질 수 있음을 이해할 필요성이 있다. 이는 개인정보 유출사고는 무형의 자산인 개인정보를 유출하는 것이므로 유형자산 손실로 인한 피해보다 인지하기 어렵기 때문이다. 단기간에 기업의 1차적 피해로 직결되지 않으므로 사고가 발생한 후 유출 사실을 인지하는데 시일이 소요되며, 사실 확인과 동시에 통지가 즉시 이루어지기 어렵다. 이처럼 개인정보 유출사고는 사고발생과 인지시점이 상이할 수 있고 악의적인 외부인에 의한 침입의 경우 즉시 감지하기 어려워 상당한 시일이 소요된 후 인지할 수 있으므로 시점의 세분화가 필요하다. 통지시점은 크게 세 가지 시점으로 구분할 수 있는데 이를 정리하면 〔표 3〕과 같다.

첫째, 고의적 또는 비고의적 목적을 가진 내·외부자에 의한 유출사고가 발생한 사고발생시점이다. 이 단계는 실제 사고가 발생한 단계로 유출사고의 진위여부는 확인 되지 않은 상태이다. 고의적 목적인 경우 내부자, 외부자로 나뉘는데 관련 사실에 대한 제보가 이

〔표 3〕 통지시점에 따른 구분

시점 구분	이해당사자		단계 내용
사고 발생 시점	고의적	내부자	특정 목적을 달성하기 위한 고의적 내부자의 부정행위가 발견된 시점
		외부자	특정 목적을 달성하기 위한 고의적 외부자의 부정행위가 발견된 시점 및 제보가 접수된 시점
	비고의적	내부자	사고 인지에 대한 유발요인이 없어 사고인지에 대한 자연적 지연 발생
사고 인지 시점	개인정보 처리자 (기업, 공공기관)		사고 조사 및 분석을 통하여 정확한 사고 개요를 바탕으로 기업 내부 보고
	수사기관		사고의 과학적 분석 및 범죄 수사를 위해 수사기관에 의뢰
	담당기관		사고 조사 후, 통지규모에 따라 해당 담당기관에 신고
	방송 및 언론매체		정보주체를 포함한 일반인이 방송 및 언론 매체를 통해 기본 사고 내용 인지
통지 시점	정보 주체		정보주체에게 정확한 사고 개요와 대응방안 통지

루어지지 않을 경우, 추후 자체적 내부 모니터링으로 부정행위가 탐지되는 등 즉각적으로 인지하기가 어렵다. 그리고 내부자가 비악의적인 목적으로 유출한 경우에는 사고 인지를 위한 유발 요인이 없어 앞의 경우보다 인지하기가 더 어렵고 자연적인 지연이 발생하게 된다.

둘째, 사고인지시점은 크게 기업, 수사기관, 담당기관, 일반인으로 구분된다. 사고 발생 후 내부조사결과, 유출사고라 판단되면 기업은 내부보고절차를 거쳐 사고를 인지하게 된다. 그 후, 과학적 사고조사 및 범죄수사를 위해 수사기관에 수사를 의뢰하는 통지가 진행된다. 그리고 사고 조사 후 통지규모(국내의 경우 1만 명 이상)에 따라 해당 기관에 대한 통지(신고)가 발생할 수 있다. 앞의 세 가지 경우와 달리 보다 독립적으로 진행되는 시점은 방송 및 언론매체를 통해 정보주체를 포함한 일반인이 사고에 대한 기본적 내용을 인지하게 되는 시점이다.

셋째, 개인정보처리자가 추가 피해를 막기 위해 정보주체에게 사고개요와 대응방안을 제공하는 통지시점이다. 통지시점과 관련하여 가이드라인(안)에서는 개인정보처리자가 개인정보 유출을 인지한 때로부터 '지체 없이' 정보주체에게 통지하도록 명시하였다. 그러나 '지체 없이'라는 의미를 단순히 '사고 인지 후 즉시'보다는 '통지 전, 필요한 법적·행정적 절차 이행 완료 후 즉시'라는 관점으로 이해할 필요성이 있다. Debix, Inc.〔4〕는 '통지속도보다 정확한 사고분석이 더 중요하다'라고 제안한다. 즉 앞에서 제시한 기업대응프로세스의 대응단계에서 통지이전의 단계들에 대한 이행이 중요하다고 할 수 있다. 왜냐하면 통지의 목적은 정보주체가 정확한 사고인지와 대응방안에 대한 이해를 통해 추가 피해를 최소화하는데 있기 때문에 통지의 속도보다는 정확한 사고분석을 바탕으로 한 적합한 대응조치 수립이 선행되어야 한다. 또한 사고유형에 따라 법률적으로 요구되는 사항들이 통지에 포함되어야 한다. 따라서 '지체 없이'는 '행정적·법률적 절차가 완료된 즉시'로 해석하는 것이 맞다.

그리고 앞에서 제시한 사고분석 외에 오히려 통지를 했을 경우 문제해결에 심각한 장애가 발생할 때에는 통지의 지연을 가능하게 하여야 한다. 미국 대부분의 주에서는 불합리한 지연 없이 통지하되, 합리적 지연 사유를 명시하고 있다. 크게 세 가지로 국가보안을 위협하거나 범죄수사를 할 경우, 유출범위 조사 시, 시스템의 무결성 복구 시에 통지를 지연 가능하도록 하고 있다.

위의 논의와는 다르게, 해석이 다양할 수 있는 '지체 없이'라는 문구 대신 구체적으로 통지 한계시점을 제시하는 것에 대해 고려해 볼 수 있다. 한계시점을 법으로 제한할 경우 기업의 통지 이행에 대한 책임을 강화할 수 있다. 하지만 개인정보 유출 사고 유형이 다양해지면서 일괄적으로 동일 기간을 적용하기에는 현실적인 어려움이 있다. 대신 한계시점을 적용할 경우, 정해진 기간 내에 통지가 불가능하면 해당기관에 보고·승인을 거쳐 추가적으로 기간을 연장하는 제도를 통해 현실적 문제점을 보완할 수 있을 것이다〔7〕.

4.4 통지내용

정보주체에게 통지하는 통지문의 내용에는 법조항 및 가이드라인(안)에서 제시하는 '유출된 개인정보의 항목', '유출된 시점과 경위', '추가 피해 방지를 위한 정보', '개인정보처리자의 대응조치 및 피해구제절차', '상담 및 신고할 수 있는 연락처'의 5가지 필수항목이 포함되어야 한다. 통지문의 내용 구성 순서도 위에서 제시한 순서처럼 정보주체의 관심도가 높은 정보가 먼저 나올 수 있도록 해야 한다.

유출 통지문은 먼저 육하 원칙에 따라서 유출된 개

인정보항목과 경위를 정보주체가 이해하기 쉽도록 일목요연하게 작성하고 추가 피해 방지를 위한 효과적인 대응이 가능하도록 유출로 인해 발생할 수 있는 피해와 최소화 방법을 구체적으로 제시해준다. 그리고 정보주체의 혼란을 최소화하기 위해 사건 해결을 위한 대응조치와 피해구제절차도 상세히 알려줘야 한다. 마지막으로 사건에 대한 추가정보 확인과 피해발생 시, 신고할 수 있는 담당부서 및 연락처를 명시해야 한다.

가이드라인(안)에서는 담당부서 및 연락처를 통지내용에 명시할 것을 간단하게 제시하고 있지만 이 부분은 미국처럼 더 자세한 연락처 정보가 추가되어야 할 것이다. California Office of Privacy Protection에서는 개인정보처리자의 연락처 외에 정보주체가 추가피해에 대한 모니터링을 할 수 있도록 미국 3대 신용평가회사 연락처와 법률관련 문의가 가능한 법집행기관 연락처, 개인정보유출에 관한 추가적인 정보 확인을 할 수 있는 California Office of Privacy Protection의 웹사이트를 기재하도록 권고하고 있다. 또한 정보주체의 혼선을 줄이기 위해 연락처는 수신자부담 번호를 기입하고 콜센터 운영시간까지 명시하도록 제시하고 있다.

반드시 포함되어야 할 항목 외에 본문내용 작성과 관련하여 문비치 등[12]의 연구에서는 조직 위기상황에서의 사과광고 메시지 작성 시, 개인정보 유출 사고 원인이 외부귀인인지, 내부귀인인지에 따라 대중의 용서 정도에 차이가 있다고 제시하였다. '해킹'과 같은 외부귀인일 경우에는 감성적인 사과메세지가 효과적이며, '내부유출'과 같은 내부귀인일 경우에는 이성적인 사과메세지가 보다 효과적인 것으로 나타났다. 이는 통지문 서두의 사과내용을 작성할 시에 개인정보 유출 귀인 유형에 따라 메시지를 전략적으로 구성하는 것도 효과적인 통지문 작성방법이라 할 수 있다.

4.5 통지방법

통지의 목적은 정보주체가 개인정보유출 사고에 대한 정확한 인지를 바탕으로 2차 피해를 최소화하는데 있다. 그러므로 통지의 기본 목적에 부합하여 법의 실효성을 높이기 위해서는 정보주체에게 통지가 정확히 전달되어 통지내용에 대한 인지를 높일 수 있는 방법과 통지가 제대로 전달되지 못한 정보주체를 파악할 수 있는 방법을 함께 고려해야 한다. 따라서 통지방법은 포괄적이고 빠르면서 동시에 정보주체에게 전달여부를 확인할 수 있는 방법을 사용해야 한다. 또한 정보주체의 연락정보의 정확성에 따른 통지전달률 등을 고려한 대체통지도 마련해야 한다. 하지만 가이드라인(안)에서는 동시 다발적으로 연락이 가능한 수단을 선택하여 통지하라고만 되어있어 자칫 개인정보처리자가 통지의 목적과 다르게 통지 행위 자체에만 의미를 부여하여 법의 실효성이 떨어질 우려가 높다.

미국의 경우, 정확한 통지 전달을 위해 기본과 대체통지 구분을 두고 있으며 법률상 제시한 기준을 초과할 경우에만 기본통지 대신 대체통지를 하도록 되어있다. 기본통지는 대부분의 주가 서면, 전화, 전자적 방법(예: 팩스) 중 한 가지를 선택하여 통지를 하도록 되어 있고 '통지비용', '통지대상숫자', '불충분한 통지(연락)정보' 세 가지 중 한 가지가 제시된 기준을 초과할 경우 대체통지를 해야 한다. 대체통지는 이메일, 웹사이트 공지 그리고 해당 주의 미디어를 통한 통지가 모두 이루어져야 한다.

국내의 경우도 미국처럼 기본통지와 대체통지 구분을 두고 현실적인 대체통지 가능 기준을 제시하여 통지의 목적인 정보주체의 정확한 사고인지에 부합할 수 있도록 하여야 한다. 기본통지방법은 등기우편을 기본으로 하되, [표 4]에서 제시된 바와 같이 국내의 높은 인터넷 및 모바일 사용 환경을 감안하여 정보주체의 핸드폰 및 이메일 주소를 보유했을 경우 SMS와 이메일을 통한 통지도 동시에 이루어질 수 있도록 하여 통지의 정확성 뿐만 아니라 통지 속도까지 높일 수 있도록 한다.

또한 웹사이트를 운영할 경우에도 웹사이트를 통한 고지도 같이 이루어질 수 있도록 하여야 한다.

대체통지는 기업측면에서 현실적인 통지비용과 통지대상숫자에 대한 수치상의 기준을 제시하여 기준을 초과할 경우 대체통지가 가능하도록 하고 기업의 규모에 따라 기준을 달리 적용하도록 한다. 또한 기본통지 시, 불충분한 연락 정보로 인해 통지가 어려울 경우도 대체통지가 가능하도록 한다. 대체통지방법은 정보주체를 포괄할 수 있는 미디어를 활용하되, 효과적인 통지 전달을 위해 [표 5]에서 제시된 미디어 접촉률, 이용시간, 광고주목도, 신뢰도, 영향력 등을 고려하여 지상파TV, 케이블TV, 인터넷 등이 보다 적합하다.

[표 4] 2010년 이메일 및 이동전화 이용률[19]

구분	이용률(%)	비고
이메일	85.5	만 6세 이상 인터넷 이용자
이동전화	96.6	전체 가구 기준

〔표 5〕 미디어별 특성 비교〔18〕

구분	접촉률 (%)	이용 시간 (일평균/분)	광고 주목도 (%)	신뢰도 순위	영향력 순위
지상파 TV	77	163	71	1	1
라디오	23	90	76	4	5
신문	32	31	52	2	3
잡지	25	-	68	6	6
케이블 TV	36	87	65	5	4
위성 방송	2	103	72	9	6
인터넷	53	109	38	3	2
지상파DMB	4	30	56	8	8
IPTV	3	73	61	7	7

통지전달을 높이기 위한 잦은 통지는 오히려 부작용을 초래할 수 있으므로 주의해야 한다. 앞에서도 언급했듯이 과다한 비용 발생 외에도 잦은 통지로 인해 정보주체의 관심 저하를 가져올 수 있다. 그리고 피해가 미비한 사고를 통지함으로써 불필요한 법적 소송이 발생할 수 있다.

V. 결 론

개인정보 보호법이 처음 시행되고 많은 이해관계자들을 포괄하고 있기 때문에 적절한 가이드라인이 제공되어 법률적 의무사항들을 이행하는데 있어 혼란을 최소화하는 것이 중요하다. 특히 기업의 정보유출 대응 프로세스에서 통지와 관련된 부분은 유출 사고 시 정보주체의 프라이버시를 보호하고 정보주체 및 기업의 피해확산 방지를 위한 주요 조치 사항으로서 각별히 주의를 기울여야 한다.

적절한 통지 가인드라인 수립을 위해서는 먼저, 통지단계와 밀접한 관계를 갖는 기업대응 프로세스의 세부 단계들을 정확하게 파악해야 한다. 그리고 급박하게 내·외부 커뮤니케이션이 진행되는 통지단계의 전체적인 프로세스를 이해해야 한다.

본 연구에서는 위기관리 모델을 활용한 3단계(계획 및 준비 단계, 대응 단계, 개선 단계)로 구성되는 기업대응 프로세스 프레임워크를 제시하여 통지 이전 단계들의 업무내용과 통지단계와의 관계를 설명하였다. 그리고 통지 프로세스를 조망할 수 있도록 미국에서 통지법을 시행하고 있는 주와 다른 국가의 주요 사례를 분석하여, '통지대상 개인정보', '통지 주체', '통지 시점', '통지 방법', '통지 내용'으로 구성되는 통지 프레임워크를 도출하였다. 그리고 이렇게 도출된 통지 프레임워크는 적절한 가이드라인의 방향을 수립하는데 기초자료로 활용할 수 있다.

향후 공개될 '개인정보 유출 통지·신고 가이드라인'에서는 통지 프레임워크의 다섯 가지 구성 요소에서 다음의 내용들을 고려해야 한다. 먼저, 유효한 대응조치가 가능하도록 행정 및 법률적 분석이 기본이 되는 통지시점, 통지의 신속함과 정보주체의 정확한 수취가 함께 고려된 통지방법, 필수적인 통지내용 외에 콜센터 운영시간 및 신용 확인 연락처 등과 같은 정보주체의 편의성까지 고려되어야 할 것이다. 그리고 과잉 통지를 줄이기 위해 추가 예상 피해가 높거나 심각하게 사생활을 침해할 수 있는 개인정보들로 통지대상 개인정보를 제한하고 그 외의 정보들은 자발적 통지대상으로 분류하는 것이 적합할 것이다. 또한 법의 실효성을 높이기 위해 개인정보유출 상황에 따른 통지주체의 명확한 기준과 통지 여부가 아닌 통지 목적에 부합하는 통지 관리가 이행될 수 있는 방법들이 향후 배포 될 가이드라인에 추가적으로 반영되어야 한다. 그리고 개인정보 보호법 시행 후, 여러 변화가 예상되는 만큼 지속적인 업데이트를 통해 현실적으로 적용 가능한 방법들을 제시해야 할 것이다.

참고문헌

〔1〕 Affinion Security Center, "Data breach response guide," Apr. 2009, available at http://www.breachshield.com.

〔2〕 State of California, California Office of Privacy Protection, available at http://www. privacyprotection.ca.gov.

〔3〕 Coombs W. Timothy, "Ongoing crisis communication: planning, managing, and responding," Sage Publication, 2nd edition, Feb. 2010.

〔4〕 Debix, Inc., "Data Breach Incident," available at http://debix.com/workbook/index.php.

〔5〕 Fox Rothschild LLP, "Data security breaches: a first response checklist," available at http://www.foxrothschild.com.

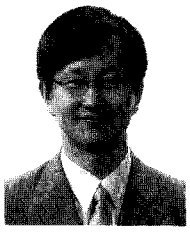
〔6〕 Karin Retzer, "Data Breach Notification: The Changing Landscape in the EU,"

Computer law review international, pp. 39-42 , Feb. 2008.
[7] Samuelson Law, Technology & Public Policy Clinic, "Security breach notification laws: views from chief security officers," University of California-Berkeley School of Law, Dec. 2007.
[8] National Conference of State Legislatures, State Security Breach Notification Laws in the USA, available at http://www.ncsl.org/default.aspx? tabid=13489.
[9] 강성주, "개인정보보호 어떻게 준비할 것인가," 한국CSO포럼, pp. 1-32, 2010년 12월.
[10] 권미진, "위기발생 및 해결과정에 있어서 사내커뮤니케이션적인 특성에 관한 고찰," 석사학위논문, 서강대 언론대학원, 2005년 8월.
[11] 김지윤, 성민정, "언론보도에 반영된 조직의 위기관리 전략 분석," 한국지역언론학회 언론과학연구, 9(3), pp. 37-69, 2009년 9월.
[12] 문비치, 이유나, "조직 위기상황에서의 사과광고 메시지 전략과 용서: 개인정보유출 사건을 중심으로," 한국언론학보, 53(6), pp. 354-378, 2009년 12월.
[13] 변순정, 이강신, 박광신, "개인정보 유·노출 등의 통지관련 국내외 법제 현황," 정보처리학회지, 18(6), pp. 35-42, 2008년 12월.
[14] 여성구, 심미나, 이상진, "웹 로그 데이터에 대한 개인정보 위협분석 및 보안 가이드," 정보보호학회 논문지, 19(6), pp. 135-144, 2009년 12월.
[15] 이정숙, "미국 증권회사 컴플라이언스 프로그램의 이론적 배경과 특징," 한국증권법학회, 5(1), pp. 221-254, 2004년 6월.
[16] 임규철, "개인정보와 법," 보명Books, 2009년 7월.
[17] 최진혁, "기업 위기관리(Crisis Management) 전략에 관한 연구 - 해외 Pandemic Planning 사례를 중심으로," 한국기업경영학회, 17(4), pp. 149-169, 2010년 12월.
[18] 한국방송공사, "2009 소비자 행태조사 보고서," pp. 31-52, 2009년 12월.
[19] 한국인터넷진흥원, "2010년 인터넷 이용실태 조사," 방송통신위원회, pp. 8-9, 2010년 9월.

〈著者紹介〉

이 충 훈 (Chunghun Lee) 학생회원
2005년 2월: 건국대학교 경제학과
2011년 3월~현재: 연세대학교 정보대학원 지식서비스보안과정 ASPN Research Fellow
〈관심분야〉 정보보호, 프라이버시, 개인정보

고 유 미 (Yumi Ko) 학생회원
2008년 2월: 연세대학교 문헌정보학과
2011년 3월~현재: 연세대학교 정보대학원 지식서비스보안과정 소만사 Research Fellow
〈관심분야〉 정보보호, 프라이버시, 개인정보



김 범 수 (Beomsoo Kim) 종신회원
1999년: 미국 University of Texas at Austin, Ph.D.
1999년~2002년: 미국 University of Illinois at Chicago, 조교수
2002년~현재: 연세대학교 정보대학원 교수
2011년~현재: 지식서비스보안과정 및 ITMS과정 주임교수, ISACA Korea 부회장
〈관심분야〉 정보보호정책 및 제도, 프라이버시 권리, 전자상거래, 정보경제학