개인정보보호 교육 시리즈

안 하면 안 되는 기술적, 관리적 조치

지난 호에서는 개인정보를 수집하는 기업이 기본적으로 취해야 할 조치에 대해 법률에서는 어떻게 규정하고 있는지를 살펴봤습니다. 그런데 많은 분들이 기술적 관리적 보호조치에 대해 보다 구체적인 사항을 요구하시더군요. 그래서 이번 호에서는 개인정보를 취급하는 기업이 준수해야 할 조치들을 소개해 드리고자 합니다.

정보보호뉴스 취재팀

개인정보를 취급하는 사업자가 준수해야 할 기술적·관리적 보호조치 사항에 대해서는 '정보통신이용촉진및정보보호등에관한법률(이하 정보통신망법)'을 통해 '개인정보의 기술적 관리적 보호조치' 기준이 이미 마련돼 있습니다. 지난 호에서도 언급된 바 있지만, 정보통신망 서비스를 제공하는 기업이라면 정보통신망법은 필독 대상입니다.

최소한 기본은 해야죠

정보통신망법에서 규정하는 기술적, 관리적 조치에 대한 두 가지 중요한 사항을 짚고 넘어가 보도록 하죠. 그 두가지란 개인정보의 분실·도난·누출·변조 또는 훼손되는 것을 방지하기 위한 필수적인 조치에 대한 내용과 위반시 부과되는 과징금 내용입니다.

개인정보의 기술적·관리적 조치 관련 법률 조항

정보통신망법 제28조(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.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

물론 개인정보를 법적으로 어떤 방식으로 보호해야 되는지 구체적인 내용까지 명시되지 않아 답답하실 수 있겠지만, 그 모든 사항마다 구체적으로 표기한다는 것은 불가능에 가까운 일입니다. 각 기업마다 독특한 조직구조와 규모를 갖고 있고, 특히 서로 상이한 IT 환경을 고려하지 않을 수 없기 때문이죠. 다만, 망법 내용 이외에도 KISA가 제공하는 '개인정보관리계획 모델'을 참고한다면, 각 기업이 고객정보를 보호하기 위해 어떤 활동을 펼쳐야 하는지 알 수 있습니다. KISA의 관리계획에는 개인정보관리책임자의 지정에서부터, 개인정보보호 교육, 개인정보 처리 시스템 접근 통제, 개인정보 취급 위탁업체 관리 등 총 21항목으로

구성돼 있어 이를 체크리스트로 활용한다면 기업의 개인정보보호 수준을 측정하는 데 매우 효과적인 수단이 될 수 있습니다.

개인정보보호 위반 시 배상금, 상상초월

기업이 수집하는 개인정보를 법률이 요구하는 수준에 맞추기 위해서는 그 규모에 맞는 예산을 편성해 투자하는 것이 필요합니다. 예산이 부족하다고요? 많은 분들이 그렇게 말씀하실 수 있겠지만, 개인정보보호를 충분히 해 내지 못한다면 오히려 발생할 수 있는 비용은 커지게 됩니다. 일례가 아래의 과징금 부과 항목입니다. 위반행위가 적발될 경우 작게는 1,000만원 이하지만 경우에 따라 최대 매출액의 100분 1에 해당하는 금액이 과징금으로 부과될 수 있도록 조항을 만들어 놓았죠.

과징금 부과 관련 조항

제64조의3 (과징금의 부과 등)

① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 전기통신사업자에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제6호에 해당하는 행위가 있는 경우에는 1억원 이하의 과징금을 부과할 수 있다.

6. 제28조제1항제2호부터 제5호까지의 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우

제73조 (벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자

제76조 (과태료)

① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

3. 제28조제1항제1호 및 제6호(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자

과징금의 문제뿐만 아닙니다. 최근 개인정보보호에 대한 법정 소송이 등장하기 시작하면서 법적 판결에 따라 수십억, 수백억의 보상금을 기업이 지출해야 하는 상황까지 이를 수 있어, 개인정보보호 조치는 각 기업들이 그야말로 사활을 걸고 고민해야 하는 화두로 떠오르게 됐습니다. 가령, 1,000만명의 개인정보가 유출된 상황에서 이중 100만명이 일인당 10만원씩의 피해보상금을 요구한다면 1,000억원이 보상금으로 지급되어야 합니다. 정말 어마어마한 금액이죠.

물론 개인정보보호에 대한 기술적, 관리적 조치는 하루아침에 이뤄질 일은 아닙니다. 정보보호에 대한 관심과 투자가 지속될 때에만 가능한 것이겠죠. 그 비용이 아까우시다고요? 그럴 때마다 개인정보 침해로 인한 보상금과 소송비용을 생각해 보시는 것은 어떨까요?