개인정보보호 교육 시리즈

개인정보 영향평가에 도전해 보세요

개인정보 유출사고에 대한 배상금 및 소송 판례들이 등장하기 시작했습니다. 이런 현상은 개인정보를 수집하는 기업이 향후 이용자들과 개인정보와 관련된 각종 분쟁과 민원에 더욱 자주 둘러싸이게 되는 것을 의미합니다. 때문에 국내 기업들은 깊은 고민에 빠져 있다고 합니다. 개인정보를 활용해 이익을 추구하는 한편, 그 활용방법이 합법적인지 또는 적정한 기준이 무엇인지 찾기 위해서 말이죠. 그런 의미에서 지난 호에 소개됐던 기술적 관리적 조치에 이어, 개인정보를 수집하는 기업에게 필요한 개인정보 영향평가 제도에 대해 알아보도록 하겠습니다.

정보보호뉴스 취재팀

기업이 보유한 개인정보는 대개 애플리케이션과 데이터베이스라는 형태로 수집·축적되고 있습니다. 최근 사례들을 통해 알 수 있듯, 각종 정보가 디지털 방식으로 저장됨에 따라 내외부 통제가 허술할 경우, 사회적 파장을 일으킬 만큼 엄청난 양의 개인정보가 유출될 수 있습니다. 기업들은 뉴스의 주인공이 되지 않기 위해 기술적으로, 또 관리적으로 보안정책을 강화하기 위해 분주하게 움직이고 있습니다. 사업자의 자율적인 조치 및 책임의식 고취, 사전 예방체계 도입 그리고 사고 발생 시 이용자의 피해를 최소화할 수 있는 긴급 대응방안 등을 마련하기 위해서죠.

개인정보 영향평가가 뭐죠?

개인정보 영향평가(PIA: Privacy Impact Assessment)는 이와 같은 사업자의 고민을 해결해 줄 수 있는 하나의 방법입니다. 개인정보 영향평가는 기업이 고객정보 침해나 유출로 인한 문제점을 사전에 예방하고 사후에 지속적으로 관리함으로써 서비스를 이용하는 고객정보의 안전성을 확보하는, 다시 말해 개인정보보호를 위한 일련의 위험관리체계를 의미합니다.

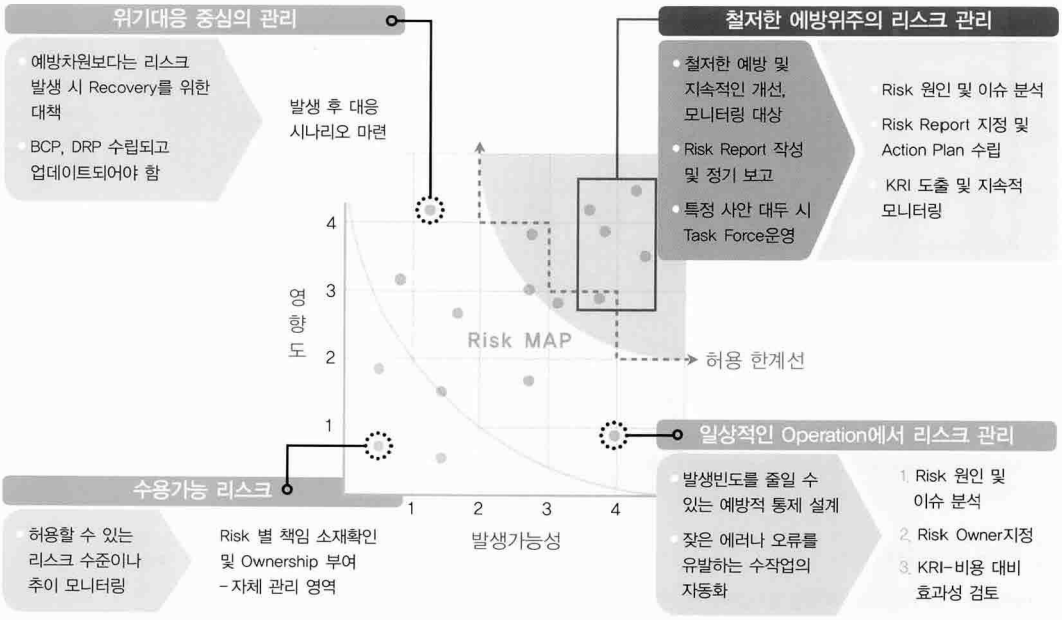
▲ 그림 1 개인정보 영향평가의 개념

미국과 유럽 등 선진국을 중심으로 이미 실시되고 있는 이 방법은 KISA가 국내 실정에 맞게 가이드라인을 제작한 이후, 이동통신사를 중심으로 포털 기업, 금융권, 공공기관 등으로 점차 확대되고 있는 중이죠. 개인정보 영향평가를 구성하는 요소는 그림 1에서 볼 수 있듯 크게 4가지 영역이 있으며, 영향평가의 궁극적인 목적은 각각의 영역이 시스템적으로 원활하게 정착됨과 동시에 개인정보를 위해 관리체계를 철저히 하는 데 있습

니다. 이를 위해서는 단계별 접근이 필요하게 되는데, 먼저 보호할 대상, 즉 개인정보의 식별, 점검표 작성, 기업 내 개인정보 취급 및 유통 패턴의 분석과정 등이 포함된 '사전준비단계'가 있으며, 위험 심각도 분석, 위험 발생 가능성 분석, 서비스별 위험 수준의 산출, 보안대책 등을 도출하는 '수행단계', 그리고 영향평가 체계를 정착시키는 '시스템화 과정'이 있습니다.

개인정보보호 위한 관리 시스템화

개인정보보호와 관련된 위험 요인이 매우 다양한 만큼 개인정보 영향평가 제도를 기업에 정착시키는 과정 또한 쉽진 않습니다. 아래 그림 2에서 볼 수 있듯, 개인정보와 관련된 프로세스와 데이터에 대한 위험관리가 정립되어야 하며, 각각의 정보에 대한 위험 분석이 수반되어야겠죠.



▲ 그림 2 위험도 관리방안의 예

각각의 과정을 통해 개인정보 영향평가 모델이 완성된다면 기업은 개인정보 관리에 있어서 효과적이고, 안전한 시스템을 확보할 수 있게 됩니다. 뿐만 아니라, 개인정보 영향평가를 실질적으로 확립할 경우, ISO 27001~2, ISO 22307 등과 같은 개인정보보호와 관련된 인증 획득의 기반을 다져놓는 효과도 거둘 수 있죠. 그러나 개인정보 영향평가는 보안부서 홀로 할 수 있는 것이 아닙니다. 개인정보 이용의 흐름을 분석하고 개인정보의 유통과 관리체계를 모든 부서와 직원들이 숙지하고 있을 때 가능하겠죠. 개인정보를 보호하고 고객들의 신뢰를 얻는 것이 결코 쉬운 일은 아닙니다.

아차! 개인정보 영향평가에 대한 보다 자세한 내용이 궁금하다고요? KISA 내 개인정보보호지원센터(www.1336.or.kr)를 방문하시면 개인정보 영향평가 적용을 위한 다양한 샘플과 절차를 보실 수 있을 것입니다. 이제, 개인정보 영향평가를 시도해 보실까요. **S**