



처음 발표자로 나선 (주)빅스 오제민 부장은 자사의 개인정보 취급자에 대한 정례적 교육 및 개인정보 관리지침에 의한 체계적인 개인정보 관리 사례를 발표하였다. <박스 참조>

이어서 개인정보보호에 대한 다양한 사례들을 중심으로 참여사들의 토론이 이어졌다.



# 진단! CPO(개인정보관리책임자)들이 보는 개인정보보호

협회 정보화 기획팀은 지난 4월 2일 개인정보관리책임자 협의회 운영위원 25개사를 초청하여 개인정보보호에 대한 우수 사례 발표와 아울러 각종 방안에 대한 토론의 시간을 가졌다. 이날 간담회는 옥선의 탁수신 위원장을 좌장으로 하여, (주)빅스 오제민 부장의 '개인정보보호 우수사례' 발표에 이은 다양한 사례별 진단 및 대처 방안에 대한 토론으로 이어졌다. 갈수록 그 비중이 커져가는 '개인정보보호' 그 최전선에 서 있는 CPO들의 진솔한 이야기들을 들어 보자.

먼저 실명확인절차의 의무화 방안 마련에 대한 토론에서는 옥선이 '실명확인절차에 관한 법적 근거가 미비하여 개인정보 도용사례 속출이 예상되므로 실명확인절차의 법제화 및 가이드라인 마련이 요구되고 있다' 라고 의견을 개진하였으며, 이에 대해 KISA는 '대부분의 사업자의 경우, 주민번호 수집 및 확인을 통한 실명확인절차를 실시하고 있으나 주민번호의 노출 위험성이 커져가는 추세라는 점에서 실명확인절차를 위한 주민번호 수집은 제한돼야 한다' 고 밝혔다.

이에 반해 빅스는 '주민번호 수집 없는 실명확인

방법은 사실상 불가능하며 오히려 사회적 문제를 야기시킬 것으로 예상된다'고 말했으며, KTF도 '주민번호 뒷자리 정도의 수집마저 제한될 경우, 실명확인 곤란 및 민원의 증가가 예상된다'고 말했다.

않는 사례도 있으므로 이 점을 이용자에게 충분히 고지할 필요가 있다'고 답했다.



이러한 의견들에 대해 KISA는 '향후 사업자의 의견을 수렴하여 주민번호 수집제한 여부 및 실명확인절차의 제도화 여부를 검토하겠다'고 마무리했다.

두 번째 주제로는 '유료 결제 시 이메일 통보 의무화 방안 마련'이었다.

이에 대해 옥선은 '현재 결제금액에 따라 이메일 통보의무를 부과하고 있으나, 유료 결제시 금액의 정도에 관계없이 이용자 이메일로 결제내역을 발송하는 것이 건전한 거래질서 확립에 필요하다'고 밝혔다. 백선은 '이메일로 결제내역을 발송해도 이용자의 스팸 메일 차단 프로그램의 설치로 도달되지

세 번째로는 요즘 화두가 되고 있는 '공인인증 의무화 및 유료화에 대한 대책 마련'에 대한 토론이 있었다. 공인인증 의무화의 경우 소비자의 불편을 초래해 온라인 결제를 기피하게 할 수도 있다는 점과 개인정보 도용 사례의 근본적인 차단을 내세우는 입장이 엇갈리면서 다양한 토론이 이어졌다.

하나로드림의 경우 'Online상의 모든 거래에서 공인인증이 적용될 것으로 예상되는 상황이라는 점에서 공인인증 사용 유무보다는 저렴한 비용으로 사용할 수 있는 방안을 마련하는 게 중요하다'라는 입장을 밝혔으며, 드림오피스도 '결제자 중 8% 정도가 불법행위를 하고 있는 실정인데, 모든 이용자를 대상으로 공인인증을 의무화하는 것은 불합리하다'라는 의견을 개진했다. 반면 KISA의 경우 '주민번호 생성프로그램을 이용하여 허위의 주민번호를



생성할 수 있을 뿐만 아니라 아이디, 비밀번호 도용 사건의 증가로 구체적인 대응 차원에서 개인정보 보호 방안으로 공인인증 실시가 된 것이다' 라고 본래의 취지를 밝혔다.

이렇게 본래의 취지와 사용자의 불편성에 대한 토론이 이어지자 옥선은 '차후에 구체적인 공인인증 절차를 검토해 보고 관련 가이드라인을 마련하기 위한 회의' 를 제안하였다.

이밖에도 실무자들의 모임이니만큼 실무에서의 다양한 애로사항을 토로하였다.

코리아닷컴은 '실명인증 서비스를 받고 있는데, 동명이인의 경우에는 확인이 되지 않는 경우가 발생하여 곤란을 겪고 있다' 고 밝혔으며, NHN의 경우는 '주민번호 수집제한 문제는 검·경의 수사 요청 시 자료제공 문제와 관련된다는 점에서 향후 관

련회의 개최 시 수사기관 관계자 참여를 요구한다' 고 말했다.

실무자들의 모임이니만큼 다양하고도 실질적인 문제에 대한 토론의 시간이었다.

이 날 간담회에서는 이러한 토론의 결과로 '실명 확인절차의 의무화 방안' 은 회원사 의견수렴 및 KISA와 협의 후 제도화 여부를 결정토록 하기로 하였으며, '이용자의 유료 결제 시 결제내역을 의무적으로 이용자 이메일로 통보' 하는 방안에 참여 회원사가 합의했다.

또한 공인인증제도의 의무적 시행에 따른 가이드라인 마련을 위해 추후 CPO협의회 재개를 통하여 회원사의 의견을 수렴하는 자리를 가지기로 하였다.

## [1] 개인정보 취급자에 대한 교육

**개인정보의 관리 및 보호는 교육에 기초한다.**

개인정보의 유출로 인한 문제의 발단은 정보 취급자의 안일한 관리의식에서 시작되는 것이며 이에 대해서는 개인정보의 중요성을 인식시키는 개인정보에 대한 이해교육 및 정기적인 관리 교육이 필요하다.(개인정보보호 지침 교육, 정기적인 보안교육 등)

## [2] 개인정보 취급에 대한 업무규정

**개인정보 취급자들의 정보보호, 관리에 대한 의식교육이 이루어졌다면 확실한 업무처리 절차를 마련하여 취급자들의 이해력 차이로 발생할 수 있는 업무상의 오류를 최소화 시켜야 한다.**

●●● 1. 개인정보 취급자별로 정보의 열람, 수정권한을 단계적으로 설정 :

기초적인 정보만을 볼 수만 있는 기본 권한부터 수정, 삭제관련 권한이 배정되어 있는 상위 레벨의 권한을 두어 취급자별로 업무상황에 따른 기능만을 사용하도록 한다. (문제 발생의 빌미를 사전에 차단하는 기능 및 취급자별 이용기록을 남겨 내부적인 감사의 목적으로도 사용할 수 있음)

또 각 업무담당자별 계정권한에 따라 열람할 수 있는 항목을 최소화하고 각 담당자별 이용 상황에 대한 로그 파일을 저장하여 불필요한 정보열람에 대한 감사 및 문제발생에 대비한다. 주민번호, 주소, 전화번호, 비밀 번호 등을 암호화하여 관리한다.

●●● 2. 개인정보의 취급 시에는 제공 가능한 정보의 범위를 확실히 한다 :

개인정보의 제공 및 수정 등의 고객 문의 시에는 팩스나 주민번호 발급일자 등의 확인을 통해 본인여부를 확인해야 하며 혹시라도 잘못된 정보의 제공이 발생하지 않도록 내부적으로 취급 및 관리할 수 있는 범위 내에서 정보를 제공해야한다.

●●● 3. 개인정보책임자의 업무승인은 필수화

기본적인 정보취급자 이외에 내외부 부서에서 요청되는 개인정보 자료에 대한 제공은 CPO의 승인절차를 필수화 해야 하며 제공하는 정보, 목적, 제공 일자 등을 기록으로 남겨 불필요한 목적으로 사용되지 못하도록 관리하여야 한다.

●●● 4. 개인정보관련 클레임은 개인정보책임자나 이에 준하는 담당자가 처리

개인정보관련 클레임이 발생시에는 일반 취급자의 업무처리 권한 이외의 사항을 인식하고 개인정보책임자나 이에 준하는 담당자가 신속하게 고객에게 확실한 상담과 재결방안에 대한 안내를 하여야 한다.

●●● 5. 개인정보관련 서류의 관리 및 폐기담당자의 운영

고객의 문의를 처리하기 위해 접수한 서류 및 정보는 주어진 기간동안만 보관 및 관리를 해야 하며 관리 및 폐기는 꼭 특정 담당자가 확인하여 정기적으로 처리할 수 있도록 하는 것이 중요하다. 또한 폐기 시에는 처리기록을 남겨 CPO의 관리를 받도록 한다.