정보통신사업자의 개인정보 보호조치 의무와 과징금 처분 – 서울행정법원 2016. 8. 18. 선고 2014 구합 15108 판결, 서울고등법원 2016 누 64533 사건 진행 중

K사는 해킹으로 인하여 2013. 8. 8.부터 2014. 2. 5.까지 약 1천만명의 사용자들에 대한 개인정보를 유출하였습니다. 이에 대하여 방송통신위원회는 2014. 6. 26. 이 사건 해킹사고와 관련하여 KT가 구 정보통신망법 제28조 제1항 제2호, 그 시행령 제15조, 구 「개인정보의 기술적·관리적 보호조치 기준」(2015. 5. 19. 방송통신위원회 고시 제2015-3호로 개정되기 전의 것) 제4조 제2항, 제5항, 제9항을 위반하였다고 보아, 구 정보통신망법 제64조의3 제1항 제6호에 따라 과징금 7,000만 원을 부과하는 처분을 하였습니다.

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

시행령 제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다.

1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항

2. 개인정보취급자의 교육에 관한 사항

3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다.

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행

2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영

3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단

4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영

5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

③ 법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다.

개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제) ② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑨ 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

방송통신위원회는 다음과 같은 처분 사유를 지적하였습니다.

(1) 제1처분사유: 일단 로그인을 하면 타인의 고객서비스계약번호(9자리)를 입력하더라도 인증 단계 없이 타인의 정보(이름 등)까지 조회 가능(이 사건 고시 제4조 제5항, 제9항 위반)

(2) 제2처분사유: 특정 IP에서 일 최대 수십만 건의 개인정보를 조회하였음에도 비정상적인 접근을 탐지, 차단하지 못함(이 사건 고시 제4조 제5항 위반)

(3) 제3처분사유: 사내망에서 인가받은 자가 접근할 수 있는 웹페이지에, 해커가 인터넷망을 통하여 접속하였음에도 탐지·차단하지 못함(이 사건 고시 제4조 제5항 위반)

(4) 제4처분사유: 사용 중지된 퇴직자 ID로 8만 건의 개인정보를 조회하였음에도 비정상적 접근을 탐지, 차단하지 못함(이 사건 고시 제4조 제2항, 제9항 위반)

개인정보의 안전성 확보 여부에 대한 판단 법리에 대하여 대법원은 정보통신서비스제공자가 구 정보통신망법 제28조 제1항이나 정보통신 서비스이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상

의무를 위반하였는지 여부를 판단함에 있어서는, ① 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, ② 정보통신서비스 제공자의 업종·영업 규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, ③ 정보보안에 필요한 경제적 비용 및 효용의 정도, ④ 해킹 기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, ⑤ 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여, 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다고 보고 있습니다(대법원 2015. 2. 12. 선고 2013다43994 판결 등).

서울행정법원은 위 사건에서 정보통신망법 제64조의3에 의하면 방송통신위원회는 정보통신서비스 제공자 등의 위반행위에 대하여 과징금 부과 여부에 관하여 재량을 가집니다. 그런데 KT가 이 사건 고시 제4조 제2항을 위반하였으나 이 사건 고시 제4조 제5항, 제9항을 위반하였다고 볼수 없으므로, 법원은 KT가 이 사건 고시 제4조 제5항, 제9항도 위반하였음을 전제로 한 이 사건 처분은 재량권을 일탈·남용하여 위법하다고 판단하여 이 사건 처분을 취소하였습니다.

방송통신위원회는 위 판결에 대하여 항소를 하였고, 위 사건은 서울고등법원에서

2016누64533 사건으로 항소심이 진행 중에 있습니다. 위 사건에 대하여 항소심 판결이 나오면 다시 구체적으로 말씀을 드리겠습니다. 개인정보를 보관 사용하는 정보통신사업자에 해당하는 업체, 벤처, 중소기업 등은 위 사건에서 퇴직자들의 시스템에 대한 접근권한이 유지되지 않도록 유의하여야 할 것입니다.

정회목 변호사

ICT 연구개발 10년 경력 변호사/변리사, 특허심판소송, 회사소송, 계약분쟁, Claim 분쟁

T. 02-591-0657 E. hmchung@kasanlaw.com H. www.kasanlaw.com