개인정보 유출 판례 분석과 실무자 대응 방안

김일영 변호사

법률사무소 이웃
한국개인정보법제연구회(KADP)

유출사고 개관

	발생 시기	발생 원인	피해 규모(건)	적용 법률	민사 판결(원고 기준)			판결 주요 내용
					1심	2심	3심	
A사 오픈마켓	2008. 1	해킹	1,800만	정	×	×	×	고시 내 기술적 보호조치시 주의의무 위반 아니다(대법)
B 정유사	2008. 7.	수탁사 직원	1,100만	정	×	×	×	유출되어도 판매·유통되지 않으면 손해배상 의무 없다(대법)
C 포털 커뮤니티	2011. 7.	해킹	3,500만	정	○/×	○/×	×	고시 규정 없어도 기대가능한 보호조치 해야 한다(대법)
D 통신사 1차	2012. 7.	해킹	870만	정	○/×	○/×	×	개인정보처리시스템에 어플리케이션 포함(1,2심)
D 통신사 2차	2014. 2.	해킹	1,170만	정	○/×	×	-	개인정보처리시스템을 DB에 한정(1,2심)
카드3사	2010. 4 ~ 2013.12.	수탁사 직원	1억 400만	정/개	○(R사 2차×)	○(R사 2차×)	G사 : 10만	변환되지 않은 개인정보 제공, 수탁사 관리 미흡 위법(대법), 유출 후 유통되지 않아 손해배상 없음(R카드2차)
국내 마트 E 사	2014. 6.	내부원인	2,400만	개	○ 5/20만	-	-	대표이사, 임직원 형사 처벌(확정)
처방 정보 수집 및 판매	2014. 6.	내부원인	43억	개	×	-	-	-
해외 포털 사이트 F사	2014. 2.	내부원인	-	국제사법/정	일부 ○	-	-	글로벌기업에게 정보통신망법상 개인정보 제3자 제공 내역을 정보주체에게 제공할 의무 인정(1,2심)

2018년 주요 판결(대법원)

1. 대법원 2018. 1. 25. 선고 2015다24904 판결, 대법원 2018. 6. 28. 선고 2014다20905 판결

- **"고시를 준수하였더라도 기술 수준과 정보통신서비스제공자의 규모 등에 비추어 예상가능하고 사회통념상 기대 가능한 보호조치를 취하지 않았으면 주의의무 위반을 인정할 수 있다."**

- 과거 A사 사건 대법원 판결과 차이점 주목
  - A사 유출 사건 판결 : "**정보통신서비스제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다**(대법원 2015. 2. 12. 선고 2013다43994, 2013다44003)."

- **주의 : 관련 고시상의 보호조치 수준에 안심하지 말고 적절한 수준의 보호조치 강구해야 합니다**

2. 대법원 2018. 12. 28. 선고 2017다207994 판결

통신사 전산영업시스템 해킹 사건. 정보통신서비스제공자가 기술적 관리적 보호조치를 다하였다고 봄(원고들 패소)

2018년 주요 판결(대법원)

3. 대법원 2018. 12. 13. 선고 2018다219994 판결

카드 3사 유출 사건 중 피고 G카드와 K사(수탁사)에 대한 소송으로서 1심과 2심에서 손해배상 10만원을 선고되었던 사건. 대법원이 카드사와 수탁사의 상고 기각.

G카드에 대하여 : **"피고 카드사는 피고 K사의 개발인력들에게 카드고객의 개인정보를 제공하여 취급하도록 하는 과정에서 위와 같은 법령들을 위반하여 보안프로그램 설치 및 관리 · 감독의무, 암호화된 카드고객정보 제공의무, 접근권한 제한 등 보안조치를 취할 의무, 개인정보 처리업무 위탁 시 기술적 · 관리적 보호조치에 관한 문서약정의무, 단말기에 이용자 정보를 보관 · 공유하지 않을 의무를 다하지 않았다."**

K사에 대하여 : **"피고 K사의 피용인 이 사건 유출자가 그 사무집행에 관하여 카드고객정보를 유출함으로써 원고 등에게 손해를 가하였고, 피고 K사가 유출자 등에 대한 지휘 · 감독을 다하였다고 보기 어려우므로 피고 K사는 유출자의 사용자로서 민법 제756조 제1항에 따라 피고 국민카드와 공동하여 원고 등에게 고객정보 유출로 인한 손해를 배상할 책임이 있다."**

판례 경향 분석

1. 해킹으로 인한 유출의 경우 기본적 보호조치를 취하면 손해배상 의무가 인정되지 않음

- A사 사건 : "정보통신서비스제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다(대법원 2015. 2. 12. 선고 2013다43994, 2013다44003)

- C사 사건 : "고시를 준수하였더라도 기술 수준과 정보통신서비스제공자의 규모 등에 비추어 예상가능하고 사회통념상 기대 가능한 보호조치를 취하지 않았으면 주의의무 위반을 인정할 수 있다(대법원 2018. 1. 25. 선고 2015다24904 판결)"

2. 유출 후 판매 또는 제3자에게 유통되지 않으면 손해배상 인정되지 않는 경향

- 2008년 정유사 사건 : 유출 직후 발각되어 저장매체가 회수되거나 폐기됨. 공범과 기자들만이 열람.

[대법원] **한정된 범위의 사람들에게 개인정보가 전달 또는 복제된 상태에서 범행이 발각되어 저장매체가 회수·폐기되었고 그 밖에 이 사건 개인정보가 유출된 흔적이 보이지 않아 위 사람들 외의 제3자가 이 사건 개인정보를 열람하거나 이용할 수 없어 보이는 점 등 (중략) 이 사건 개인정보의 유출로 인하여 원고들에게 위자료로 배상할 만한 정신적 손해가 발생하였다고 보기는 어렵다고 할 것이다**(대법원 2012. 12. 26. 선고 2011다59834)."

- 2013년 카드사 중 R카드사 2차 유출 사고 : 유출 직후 발각되어 제3자에게 유통되지 않음

판례 경향 분석

3. 개인정보 유출 행위자에게 징역형 선고

- 오픈마켓 유출 사고 당시 개인정보를 구매하여 회사를 협박한 자 : 징역 1년
- 정유사 수탁사 직원 및 공범 : 1년 ~ 1년 6개월
- 통신사 1차 해커 및 공범 : 1년 6개월
- 통신사 2차 해커 2년
- 카드 3사 수탁사 직원 : 3년

4. 재산상 이득을 목적으로 제3자에게 개인정보를 제공하는 경우 법인의 대표이사와 임직원 형사처벌 선고

2014년 국내 마트 임직원에게 6월 ~ 1년 선고(집행유예), 개인정보 제공받은 보험회사 임직원 벌금형

5. 기술적 보호조치 수준에 따라 손해배상 액수 인정

카드3사 사건에서 G카드사는 손해배상 10만원, R카드사는 7만원 인정한 고등법원 판결 참조

1. 2008년 A사 오픈마켓 사이트 해킹 사건

1) 사고 발생 경위

해커가 네 차례에 걸쳐 A사의 웹 서버인 E 서버에 침입
- 톰캣(tomcat) 서버로 운용되는 컴퓨터 시스템을 이용해 톰캣 서버의 관리자 페이지에 백도어 프로그램을 올린 후 IP 주소 등 시스템 정보를 획득하고 터미널 서비스를 가동

2) 주요 쟁점

쟁 점	판결 요지	관련 규정 변화
웹서버 보안조치 적절성 인터넷 통한 웹서버 접속 가능	서비스 특성상 외부접속 불가피. 인증·방화벽·접근 통제 조치 있음, 웹서버 침입은 상당인과관계 없음	-
DB에 주민번호를 암호화하여 저장하지 않음	주민번호 암호화 법적 의무 없음	주민등록번호 암호화 저장 명시(2009년 고시) cf. 2015년 개정 개인정보보호법시행령 : 주민등록번호 전자적 방법으로 보관시 암호화
과다 조회 탐지 및 경고(DB 서버에 정보요청 다량 발생, 웹서버 데이터 전송량 8배 증가)	실시간 탐지나 비정상적 조회 탐지 의무 없고 해당 시스템 갖췄으나 설정 기준에 미치지 못함	-
아이디 및 비밀번호 설정DB 서버 관리자 아이디에 회사명 포함, 비밀번호 쉬움, 톰캣 서버 아이디 초기설정 유지)	해커가 아이디와 비밀번호를 알아내 해킹했으므로 아이디와 비밀번호 설정이 쉬웠는지는 상당인과관계 없음	비밀번호 조합 방법 규정, 일정 길이 이상으로 설정, 추측하기 쉬운 번호 사용 금지, 반기별로 1회 변경(2009년 고시)

기본적인 보호조치 주의!

1. 2008년 A사 오픈마켓 사이트 해킹 사건

3) 관련 고시 변화

쟁 점	고시 변화
해킹 시점과 해킹 인지 시점 사이에 차이가 발생하여 접속기록 장기간 보관 필요성 대두	개인정보취급자 개인정보시스템 접속 기록 보관(기간통신사업자 2년, 그 외 사업자 6개월 이상)(2009년 고시) - 기존 개인정보 처리 시스템 월 1회 이상 확인·감독 의무 외에 추가로 규정된 것
고시 규정에 있는 보호조치만 준수하면 되는지 여부	2015년 5월 개정된 고시는, 제1조 고시의 목적 사항 중 정보통신서비스 제공자가 지킬 보호조치의 "구체적인 기준"을 규정한다는 점을 개정하여, "최소한의 기준"을 정하는 것으로 규정하고, 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다는 점을 명시

2. 2008년 B사 개인정보 유출 사건

1) 사고 발생 경위

B사 보너스카드 회원들의 개인정보 DB 관리를 위탁받은 N사의 관리팀인 소외 1은 시스템 및 네트워크 관리 업무를 담당하는 자로서 고객센터 DB에 접근할 권한을 가지고 있던 중 동료인 소외 2와 고객 정보를 판매하거나 집단 소송을 할 변호사에게 판매하기로 모의.

소외 1은 업무용 컴퓨터의 데이터베이스 원격관리 프로그램에 접속하여 고객 정보를 자신의 업무용 컴퓨터로 전송받아 엑셀파일로 DVD에 저장하였고 소외 2는 이를 편집.

이들의 지인인 소외 4는 법무법인 사무장에게 개인정보를 유출하려 했으나 집단 소송을 위해서는 먼저 개인정보유출사실이 언론에 보도되어 사회문제가 되어야 한다는 이야기를 듣고 기자들과 PD 등을 만난 자리에서, "도심 쓰레기 더미에서 B사 고객정보가 담긴 DVD를 주웠다."는 취지로 말하며 위 사람들에게 샘플 CD와 DVD를 교부. 언론에 이 내용이 보도됨.

언론보도가 된 2008. 9. 5. 소외 1, 2, 3이 검거되었고, 다음날 소외 4가 검거되었으며, 소외인들이 소지했던 CD, DVD, USB, 외장형 하드디스크, 작업에 사용된 컴퓨터, 노트북 등은 모두 압수되었거나 폐기되었고 기자들에게 제공된 자료는 전량 임의 제출됨.

2. 2008년 B사 개인정보 유출 사건

2) 대법원 판결 요지

- 소외 1과 공범들 및 기자들이 개인정보를 열람하였을 뿐 이 외의 제3자가 개인정보를 열람하지 않은 사안

- 대법원 판결 취지 : **유출 직후 저장매체 등이 회수되었고 공범과 기자 외의 제3자가 개인정보를 열람하지 않았으며, 공범들은 개인정보를 편집하는 과정에서 열람하였을 뿐이고, 기자 등은 유출 사건의 존재 등을 확인하기 위해 열람한 것일 뿐으로서 개인정보의 구체적 내용을 인식하였다고 볼 수 없음. 이 사건의 경우 원고들에게 손해가 발생했다고 볼 수 없음**

3) 관련 고시 변화

- 유출한 개인정보를 DVD에 저장하여 유출

물리적 접근 방지 규정 신설(2015년 고시)
-개인정보가 포함된 서류, 보조저장매체(외장하드, USB, CD 등) 등을 잠금장치가 있는 안전한 장소에 보관 의무, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책 마련 의무

- 개인정보 처리업무 위탁시 수탁자에 대한 관리 · 감독

-개인정보 취급자에 대한 정기적인 교육 실시 의무 부과(2009년)
-개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독 사항을 내부관리계획 단계에서 고려하도록 함(2015년 고시)

3. 2011년 C사 커뮤니티 포털 서비스 해킹 사건

1) 사고 발생 경위

해커는 C사의 DB 기술팀 직원 컴퓨터에, 윈도우 예약작업을 이용하여 해커가 미리 설정해 놓은 임의의 도메인에 역접속을 시도하는 악성프로그램을 유포한 후 위 직원 컴퓨터에 원격으로 접속한 상태에서 C사의 포털 서비스와 커뮤니티 서비스 회원정보가 각 저장되어 있는 데이터베이스 서버에 침입하여 개인정보를 유출

cf. 해커가 내부 컴퓨터를 감염시켜 침입하여 계정을 얻은 후 인터넷으로 개인정보를 유출 - **망분리 의무 신설(2013년 고시)**

2) 쟁점 및 판결 요지

쟁 점	대법원 판결 요지	고시 변화
개인정보 유출 차단 및 탐지(실시간 모니터링 및 비정상적 트래픽 감시 의무 인정 여부)	**주의의무 위반 없음**	
개인정보시스템에 접속시 IP접근통제로 불법접근차단	IP 통제에 주의의무 위반 없음	
공개용 압축프로그램을 사용	**보안에 취약한 프로그램 사용하지 않을 의무 위반했으나** 이 사건 손해와 상당인과관계 없음(2014다20905 판결)	
FTP 서비스 사용	**FTP 프로그램 사용하지 않을 의무 위반이나** FTP 프로그램 사용과 이 사건 손해와 상당인과관계 없음	
퇴근시 로그아웃을 하지 않은 점 및 자동 로그아웃 미설정	**로그아웃 등 조치는 사회통념상 기대 가능한 조치이므로 의무가** 인정되나 이 사건 손해와 상당인과관계 없음	최대 접속시간 제한(2015년 고시)
개인정보 암호화가 MD5 방식의 해시함수이므로 충분하지 않다는 점	MD5 방식은 권고되지 않으나 80비트 이하의 보안강도를 가진 SHA-1도 현재 광범위하게 사용되고 고시 해설서에 안전성 유지기간이 2010년으로 되어 있으며, 암호화 방식은 해독 시간에만 영향을 줌(2014다20905 판결)	

4. 2012년 통신사 전산영업시스템 해킹 사건

1) 사고 발생 경위

컴퓨터 프로그래머인 해커는 휴대전화 기기 변경에 관한 텔레마케팅 사업을 하던 중 지인인 을의 제안에 따라 텔레마케팅 영업을 위해 개인정보를 해킹하는 프로그램을 제작. 해커는 D 통신사의 무선전산영업시스템에 통신사 대리점 직원의 계정으로 접속해 서버 패킷을 캡처하고 이를 이용하여 인증 기능이 있는 서버를 우회하여 개인정보가 보관된 서버에 접근할 수 있는 프로그램을 통해 고객 정보를 유출

2) 판결 경과

- 대법원 2017다207994호 판결 : 1심 원고들 승소(일부 승, 손해배상 10만원)한 후 2심에서 원고들이 패소 사건에 관한 원고들의 상고 기각
- 대법원 2017다256910호 판결 : 2심까지 원고들이 승소(일부 승, 손해배상 10만원)한 사건에서 원고들 패소 취지로 파기 환송

3) "개인정보처리시스템"에 관한 판시 사항

1, 2심 판결은 개인정보처리시스템에 DB 외에도 DB에 접근하기 위한 중계서버, 어플리케이션도 포함된다고 판시(대법원 판결은 판시하고 있지 않음).

참고로 이 사건 이후 발생한 2014년 D사 홈페이지 해킹 사건의 1, 2심은 개인정보처리시스템의 범위를 DB에 한정하는 것으로 해석하고 있음.

4. 2012년 통신사 전산영업시스템 해킹 사건

4) 주요 쟁점 및 판결 요지

쟁 점	대법원 판결 요지	고시 변화
접근 통제 서버 전반부인 포털서버와 인증서버에만 접근통제 기능을 두고 그 이후인 중계서버부터는 인증 기능이 설치되지 않음.	위반 아님 **- 인증서버에 접근통제조치가 되어 있으므로 고시를 준수하였음** **- 인증서버에는 계정 유효성 확인, 인증토큰 발급, 인증토큰 유효성 확인 및 접근 차단 등의 접근통제조치가 되어 있어 불완전하지 않음**	2016. 9. 1. <개인정보의 안전성 확보조치 기준> **개인정보처리시스템 개념** 확장 : "데이터베이스시스템 등"
퇴직자 계정 말소(해커가 퇴사한 자의 계정을 이용해 중계 서버에 접근한 것은 퇴직한 개인정보취급자의 접근권한을 말소하지 않았기 때문인지)	주의의무 위반 아님 **- 피고는 2011년 퇴직자의 ID를 인증서버에서 폐기함** **- 해커가 해당 직원 재직 중 인증서버를 우회하는 방법을 찾아내었으므로 계정 폐기 여부와 정보유출 사고의 인과관계를 인정하기 어려움(계정 폐기 여부로 인하여 정보유출사고가 발생했다고 볼 수 없음)** * 하급심 판결 비교	「개인정보의 기술적·관리적 보호조치 기준 해설서(2017. 12)」 다수 시스템의 경우 전부 말소하도록 하고, 해당 계정값을 이용해 우회 접근 가능한 경우 미조치 사례로 명시
접속기록 확인·감독(해킹프로그램이 개인정보를 일 10만건 조회하고 5개월간 탐지되지 않음. 인증 서서에 조회기록 탐지 기능이 있으나 이를 우회함)	**국내에서는 인증서버를 우회하는 방식의 해킹이 성공한 적이 없었던 상황에서 피고가 인증서버의 접속기록을 확인·감독한 이상 개인정보처리시스템의 개인정보처리 내역 등에 관한 확인·감독 의무를 게을리 하였다고 보기 어려움** * 하급심 판결 비교	2014년 <개인정보의 안전성 확보조치 기준>개인정보처리시스템의 **접속기록을 반기별로 1회 이상 점검**
개인정보 암호화 조치(전산영업시스템에서 개인정보를 전송하는 경우 주민등록번호를 암호화하지 않았고, 암호화한 개인정보에 관하여는 암호화키를 소홀히 관리했는지)	**피고는 개인정보 송·수신시 암호화를 하였고, 주민번호가 평문화되어 노출된 구간은 해당 고시에서 규정하는 암호화를 해야 하는 구간에 해당하지 않음**	-

5. 카드3사 수탁사 직원에 의한 유출 사건

1) 사고 발생 경위

카드사들은 각 K사에 카드사고분석시스템 업그레이드를 위탁하고 K사의 시스템 개발 업무를 위해 변형되지 않은 고객정보를 제공.
K사 직원 갑은 각 카드사에 파견되어 근무하던 중 일부 컴퓨터에 USB 쓰기 방지 보안프로그램이 설치되지 않은 점 및 업무용 외장하드를 카드사에서 직접 관여하지 않는 점을 이용하여 고객정보를 임의로 반입한 자신의 USB 또는 외장하드에 저장하여 유출. 그 후 위 개인정보는 대출중개업 등을 하는 을에게 제공하였고, 을은 위 정보를 다른 사람에게도 판매함.

2) 주요 사항 요약

구 분	시기	손해배상 의무		금액		유출 원인
		카드사	수탁사	1·2심	대법원	
M카드 1차	2012. 6.	○	○	10/50	-	PC에 Windows 대신 Unix 설치시 USB 쓰기 가능 고객 정보 저장된 PC에서 FTP 또는 터미널 접속 프로그램을 이용해 Unix설치 PC에 전송
M카드 2차	2012. 10.	○	○			디스크 증설 요청 이후 USB 쓰기 가능 PC 발견
G카드 1차	2013. 2.	○	○	10/50	**10**	USB 쓰기 가능 PC 발견
G카드 2차	2013. 6.	○	○			USB 쓰기 가능 PC 발견
R카드 1차	2010. 4.	○	×	7/10	-	업무용 하드디스크에 고객 정보 저장하여 사용 후 포맷하지 않고 반출
R카드 2차	2013. 12.	×	×			새로 PC 반입 후 고의로 보안프로그램 미설치하고 USB로 유출

* 유통되지 않아 손해배상 의무 인정 안됨

5. 카드3사 수탁사 직원에 의한 유출 사건

3) 쟁점 및 판결 요지

쟁 점	대법원 판결 요지	고시 변화
USB 쓰기 방지 보안 프로그램 미설치	USB 쓰기 방지 프로그램인 보안 프로그램을 설치하도록 지시하거나 실제 설치했는지 감독하지 않음	
보조저장매체 통제	• 저장매체 반입·반출에 별다른 개입을 하지 않거나, 반입을 보고받은 경우에도 정확한 수량 등을 파악하지 않음 • 반출시 직접 포맷을 감독하지 않음	개인정보보호법 고시에 보조저장매체 반입·반출 제한 규정 신설
접근 통제(변환되지 않은 고객정보가 저장된 컴퓨터에 대한 수탁사 개발자들의 접근 제한, 다운로드 · 공유 제한)	K사 직원들의 요구가 있을 때마다 개인정보를 제공하고, K사 직원들이 공유 폴더나 외장 하드 등을 통해 공유하는 것을 통제하지 않았으며, 개인정보처리시스템 접근이 가능한 컴퓨터에 K사 직원 접속 가능하도록 하였으므로 주의의무 위반	
암호화(수탁사에 변환되지 않은 개인정보 제공, 변환되지 않은 개인정보 저장)	암호화를 하지 않았고 부득이 변형되지 않은 정보를 제공할 필요가 있는 경우에도 필요한 작업시에만 제한적으로 제공하거나 직접 입회하여 감시 · 감독했어야 함	
개인정보 처리 위탁시 관리·감독	개인정보 처리 위탁시 기술적 · 관리적 보호조치를 문서화하여 약정하지 않음, 수탁사의 컴퓨터 및 보조저장매체 등 반입·반출과 보안프로그램 설치 등을 감독하지 않음	개인정보보호법 고시에 수탁사 관리·감독 강화

6. 국내 마트 개인정보 수집 및 판매 사건

1) 사고 발생 경위

국내 마트가 개인정보 판매 수익을 위해 경품행사를 기획하고 응모 고객의 개인정보를 보험회사에 판매한 사건. 응모권 등에 기재된 동의 및 제3자 제공 항목의 글자 크기가 약 1㎜ 에 불과

2) 관련 판결

- 행정 사건 대법원 판결 : "부정한 수단이나 방법", "기만적인 광고 판단 기준" 관련 법리 제시
- 형사 사건 대법원 유죄 취지 판결(파기환송심 확정), 1, 2심은 무죄 선고
- 민사 1심 선고 : 경품행사에 응모한 원고들에게 20만원, 사전필터링 위해 보험회사에 제공된 개인정보 주체인 원고들에 대해 5만원 지급하라는 취지

3) 판결 요지(형사 대법원, 민사 1심)

- 개인정보 부정 취득에 해당

- 중요 사항인 제3자 제공 대가로 경품을 제공하는 행사인지 여부를 숨겨 표시광고법 위반
- 개인정보 최소 수집 원칙 위반
- 제3자 제공에 동의하지 않았다는 이유로 재화 또는 서비스 제공 거부 : 개인정보 보호법 위반
- 동의 사항을 구분하여 명확히 인식할 수 없어 개인정보 보호법 위반

- 동의 없는 제3자 제공에 해당

① 사전필터링 대상 개인정보는 보험회사들의 마케팅에 필요한 정보, ② 필터링은 보험회사들의 업무이고 사전필터링도 온전히 E사 업무로 보기 어려움,③ 사전필터링에 E사의 감독이 없음

6. 국내 마트 개인정보 수집 및 판매 사건

4) 관련 고시 변화

- 개인정보 보호법 시행 규칙(2017년)

제4조(서면 동의 시 중요한 내용의 표시 방법)
글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게(제1호), 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시(제2호), 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시(제3호)

5) 시사점

- 개인정보를 영리 목적으로 제공한 경우 대표이사 등 임직원 형사 처벌 사례
- 검사가 추징을 구형한 사례 : 개인정보 판매대금에 관해 형법상 추징 인정하지 않았으나 (파기환송심 판결) 개인정보 보호법(2015년), 정보통신망법(2016)에 추징 규정이 신설되어 있음을 유의

7. 환자 동의 없이 처방정보를 수집 · 판매한 사건

1) 사고 발생 경위

H 법인은 약국관리프로그램인 P프로그램을 관리 및 배포 하던 중 2011. 1. 말경부터 P 프로그램에 개인정보 자동전송 기능을 포함시켜 업데이트되도록 하여 2011. 1.말경부터 전국 약 1만 8,000여개의 약국에서 P 프로그램에 입력한 환자들의 처방정보 및 의료진 정보 약 43억건을 수집하여 미국계 통계회사인 J사에 16억원을 받고 판매하고, J사는 이 정보를 통계화하여 국내 제약회사들에게 각 70억원을 받고 판매한 사건

2) 기간별 암호화 방식

구 분	기 간	암호화 방식
1기 암호화	2011. 1. ~ 2014. 6.	숫자와 알파벳 1:1 치환
2기 암호화	2014. 6. ~ 2014. 9.	SHA-512 방식으로 일방향 암호화
3기 암호화	2014. 10. ~ 2015. 1.	주민등록번호가 아닌 성명, 생년월일, 성별 등으로 특정 후 일방향 암호화

3) 주요 쟁점별 판시 사항(민사 1심)

- **동의 없는 개인정보 수집인지 여부** : 개인정보주체는 환자이므로 약국과 계약에 수집사실을 명시하였더라도 환자 동의 없는 수집은 불법
- **동의 없는 제3자 제공 및 이용에 해당하는지 여부** : 1기 암호화의 경우 충분하지 않아 제3자 제공이 개인정보법 위반이나, 2기와 3기 암호화는 충분하고 통계 목적으로 제공한 것이므로 개인정보 보호법 위반에 해당하지 않음
- **손해배상** : H법인 및 J사 외에는 유통되지 않았고 통계 목적 외 이용하지 않았으며 2차 피해가 없고 현재 해당 정보는 서버에서 삭제하였으므로 손해배상은 인정하지 않음

7. 환자 동의 없이 처방정보를 수집 · 판매한 사건

4) 민감정보 관련 규정 강화

- 안전성 확보 조치

개인정보처리자가 민감정보를 처리하는 경우 그 민감정보가 분실・도난・유출・위조・변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 하도록 하고(제23조제2항) 이를 위반하면 2년 이하의 징역 또는 2천만원 이하의 벌금(제73조 제1호) 및 3천만원 이하의 과태료 부과 (2016년 개정 개인정보 보호법 제75조 제2항 제6호)

- 민감정보 제공받는 자의 의무 강화

민감정보 처리자 또는 일정 규모 이상 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 3개월 이내에 일정 사항을 정보주체에게 알릴 의무를 신설(개인정보 보호법 제20조 제2항, 제3항)

8. 해외 포털에 개인정보 제3자 제공 내역 공개 청구

1) 사고 발생 경위

글로벌 포털사이트를 운영하고 있는 F사의 F메일(개인 메일) 또는 기업메일 서비스를 이용하고 있는 원고 6명은 정보통신망법에 근거하여 F인코퍼레이티드와 F코리아를 상대로 원고들의 "개인정보 및 이용정보를 제3자에게 제공한 내역"을 원고들에게 공개하고, 원고들에게 손해배상금으로서 각 50만원을 지급할 것을 청구

2) 주요 쟁점 및 판결 요지

쟁 점		1심	2심
관할(F사)		**기업 메일 사용자 관할** 일반 메일 사용자 관할 인정 cf. 국제사법 제27조 제1항 : "당사자가 준거법을 선택하더라도 소비자의 상거소가 있는 국가의 강행규정에 의하여 소비자에게 부여되는 보호를 박탈할 수 없다." 이 규정은 소비자가 직업 또는 영업활동 외의 목적으로 '체결'하는 계약에 한함	기업 메일 사용자 관할 위반 **F메일 사용자 중 직업 활동 목적으로 가입한 자 관할 위반** F메일 사용자 중 직업 활동 목적으로 가입하지 않은 자 관할 인정
제3자 제공 내역 공개 의무	F사	의무 있음	의무 있음
	F코리아	의무 없음: 본사 보조적 역할만 하고 개인정보 수집 및 처리 하지 않음	**의무 인정(**위치정보서비스 관련 정보통신서비스 제공자로서 의무)
공개할 정보 범위		개인 정보 및 서비스 이용 내역 - 공개 의무 예외 : 안보 관련, 기타 법령에 비공개 의무 있는 경우	개인정보(**비식별정보, 위치정보,** 애플리케이션에 관한 정보 포함), 서비스 이용 내역 -공개 의무 예외 : 안보 관련(**기타 법령에 의한 공개 예외는 인정 안함)**
손해 배상		없음	없음

관련 판례

사건 구분	판례 번호
A 오픈마켓	대법원 2015. 2. 12. 선고 2013다43994, 2013다44003 판결
B 정유사	대법원 2012. 12. 26. 선고 2011다59834, 2011다59858(병합), 2011다59841(병합) 판결
C 포털 . 커뮤니티	대법원 2018. 1. 25. 선고 2015다24904 판결 대법원 2018. 6. 28. 선고 2014다20905 판결
D 통신사	대법원 2018. 12. 28. 선고 2017다207994 판결
카드3사 사고 중 G사	대법원 2018. 12. 13. 선고 2018다219994 판결
국내 마트 E사	행정] 대법원 2017. 4. 7. 선고 2016두61242 판결 형사] 대법원 2017. 4. 7. 선고 2016도13263 판결 민사] 서울중앙지방법원 2018. 1. 18. 선고 2015가합541763 판결
환자 동의 없이 처방정보 수집 . 판매	행정] 서울행정법원 2017. 6. 22. 선고 2015구합81803 적정결정취소처분취소 민사] 서울중앙지방법원 2017. 9. 11. 선고 2014가합508066, 2014가합538302(병합) 판결
해외 포털 사이트(F사)	서울중앙지방법원 2015. 10. 16. 선고 2014가합38116 판결 서울고등법원 2017. 2. 16. 선고 2015나2065729호 판결

관련 기사

[데일리시큐에서 연재 중]

1. [한국사회를 변화시킨 9대 개인정보 유출사고 판례 분석①] 2008년 오픈마켓 사이트 해킹 사건 : https://www.dailysecu.com/?mod=news&act=articleView&idxno=46254

2. [한국사회를 변화시킨 9대 개인정보 유출사고 판례 분석②] 2008년 수탁 회사 직원에 의한 개인 정보 유출 사건 : https://www.dailysecu.com/?mod=news&act=articleView&idxno=46734

3. [한국사회를 변화시킨 9대 개인정보 유출사고 판례 분석③] 2011년 커뮤니티・포털 서비스 개인정보 유출 : https://www.dailysecu.com/?mod=news&act=articleView&idxno=47218

4. [한국사회를 변화시킨 9대 개인정보 유출사고 판례 분석④] 2012년 통신사 전산영업시스템 해킹 사건 : https://www.dailysecu.com/?mod=news&act=articleView&idxno=48169

판례 분석집 출간 예정

「한국사회를 변화시킨 9대 개인정보 유출사고 판례 분석」 4월 말 출간 예정

- 한국개인정보법제연구회(대표저자 김일영), ㈜ 북랩.

Q & A

김일영 변호사

법률사무소 이웃

한국개인정보법제연구회(KADP)