Privacy Report 2019.01

SOMANSA

2018년 국내외 5대 프라이버시 이슈와 2019년 5대 개인정보 보호 관련 변화

2018년 국내외 프라이버시 이슈 TOP 5

1. 페이스북, 2018년에만 4건 이상의 대형 유출사고
2. 유럽연합, GDPR 시행
3. 메리어트 호텔 5억명 개인정보 유출사고
4. 북한 해킹조직 히든코브라, ATM 해킹 공격의 배후로 밝혀짐
5. 구글 플러스 개인정보 유출로 서비스 조기 폐쇄

2019년 개인정보 보호 관련 변화 TOP 5

1. 가명정보의 개념 도입, 빅데이터 시대에서의 개인정보 활용과 보호
2. 금융권 클라우드 전면 도입, 개인정보 활용 가능
3. 2019 개인정보의 기술적 보호조치 개선 방향
4. 개인정보의 컨트롤 타워: 개인정보보호 위원회로 감독 기능 일원화
5. 정보보호최고책임자(CISO) 제도 확산

2018 이슈 TOP5

[이슈 1] 페이스북, 2018년에만 4건 이상의 대형 유출사고

2018년 3월 영국 데이터분석 기업인 케임브리지 애널리티카(CA)가 8천 7백만명의 페이스북 계정 정보를 무단으로 수집하여 미국 대선 캠페인 전략에 활용한 사실이 내부자 고발로 인해 밝혀졌습니다. 페이스북은 2014년 이전 앱개발자들에게 이용자 정보 접근을 허락하는 정책을 취하였는데 케임브리지애널리티가가 이를 악용하여 개인정보를 대거 유출한 것입니다.

페이스북의 개인정보 유출사고는 여기서 끝나지 않습니다. 지난 5월에는 포스팅된 게시물들이 이용자의 설정을 무시하고 자동으로 '전체 공개' 되는 결함이 발생해 1400만명이 피해를 입었으며, 9월에는 해킹으로 인해 전세계 5천만명(한국인 피해자는 3만여명)의 계정 정보가 노출되었습니다. 12월에는 API 버그로 인해 680만명의 이용자 사진들이 노출되었고, 같은달 뉴욕타임즈는 페이스북이 마이크로소프트, 넷플릭스 등 150개 기업에게 개인정보를 유통하였다고 폭로하였습니다. 미국 암호학 권위자인 폴 코처(Paul Kocher)는 페이스북이 정보 유출방지와 보안관점에서 회사를 운영해왔다면 이러한 유출사건이 없었을 것이었다며, 페이스북이 이익 추구를 우선시 하였기 때문에 발생한 사례라고 코멘트 하였습니다.

[이슈 2] 유럽연합, GDPR 시행

2018년 5월 25일 유럽 내 공통된 정보보호 및 프라이버시 기준을 다루는 GDPR이 시행되었습니다. GDPR은 시행 전부터 전세계 연매출액 4% 또는 2천만 유로의 과징금을 시사하며 그 악명을 떨쳐왔지만, 2만달러의 가벼운 벌금을 물은 크누델스(독일 채팅앱)를 제외하고는 아직까지 "천문학적인 벌금" 부과 소식은 없습니다.

4차산업 혁명을 앞둔 시점에서 GDPR은 전 세계 개인정보의 이용 • 활용 • 보호에 새로운 패러다임을 제시합니다. 개인정보의 가명처리(Pseudonymisation) 및 프로파일링(Profiling) 기법 등을 정의하고 정보주체의 권리를 침해하지 않는 선에서 목적에 맞게 시스템이 설계(Data Protection by Design) 되도록 요구합니다. 2019년에는 각국에서 GDPR을 모델로한 법안들이 출현될 가능성이 높습니다.

[이슈 3] 메리어트 호텔, 5억명 개인정보 유출사고

2018년 11일 30일 세계 최대 호텔 그룹인 메리어트 인터내셔널의 DB가 해킹되어 5억명의 고객정보가 유출되었습니다. 2013년 해킹사건으로 인해 30억건의 유출사고를 낸 야후 다음으로 가장 큰 피해규모입니다. 메리어트는 쉐라톤, 웨스틴, 르메르디앙, 리츠칼튼, 포포인츠, 알로프트 등 30여개 브랜드를 보유하고 있으며 전세계 6700개가 넘는 호텔을 운영 중입니다.

메리어트는 국내에도 20여개의 호텔체인을 운영하고 있어 우리나라 국민의 개인정보 또한 대거 포함되었을 가능성이 매우 높습니다. 유출된 정보에는 이름, 주소, 생년월일, 전화번호, 이메일 주소, 여권 번호, 성별, 카드정보 등이 포함되어 해커의 손에 악용된다면 2차 피해가 클 것으로 예상됩니다.

[이슈 4] 북한 해킹조직 히든코브라, ATM 해킹 공격의 배후로 밝혀짐

2018년 10월 美 국토안보부(DHS)와 연방수사국(FBI)가 2016년부터 지속된 ATM 기기 현금 탈취사건의 배후로 북한 해킹조직 히든코브라를 지목하였습니다. 미국 정부는 히든코브라가 2016부터 지금까지 아프리카와 아시아 등지의 은행들을 해킹하여 수천만 달러를 탈취하였으며 앞으로도 이와 같은 사이버 공격을 감행할 것이라고 경고하였습니다. 북한의 해킹조직인 히든코브라는 2014년 소니픽처스 해킹, 2016년 방글라데시 중앙은행 해킹의 배후로도 지목되었습니다.

라자루스(Lazarus), 평화의 수호자(Guardians of Peace) 등의 가명으로 불리우는 이 단체는 올해 4월 한국소비자원과 한국공정거래조정원을 대상으로 사이버공격을 감행하기도 하였습니다. 국내 금융권을 타겟으로한 공격 또한 배제할 수 없어 각별한 주의가 요망됩니다.

[이슈 5] 구글 플러스 개인정보 유출로 서비스 조기 폐쇄

2018년 9월 구글의 SNS 서비스인 구글 플러스에 API 버그가 존재했으며 이로 인해 50만명이상의 이용자 정보가 노출되었던 것으로 밝혀졌습니다. 문제는 구글이 이 사실을 인지하고도 의도적으로 묵인해왔다는 것입니다. 구글은 실제 유출된 증거가 없어 아무런 문제가 없다고 반박하였으나 올해 12월 두번째 API 버그로 인해 5천만명의 이용자 데이터가 추가로 유출되면서 서비스의 문제점을 인정하였습니다. 이로인해 구글은 지난 7년간 운용해온 구글 플러스 서비스를 2019년 4월에 조기 폐쇄하기로 결정하였습니다.

어플리케이션과 데이터 보안에서 신뢰를 받아오던 구글 조차 두차례 연속 개인정보 유출사고에 휘말리면서 우리나라 국민을 대상으로 서비스를 제공하는 해외 IT기업에 대한 개인정보 침해 대책 마련이 시급한 실정입니다.

2019 개인정보 관련 변화 TOP5

[변화 1] 가명정보의 개념 도입, 빅데이터 시대에서의 개인정보 활용과 보호

2019년에는 가명처리된 개인정보를 활용할 수 있는 법이 시행될 전망입니다. 2018년 11월 15일 발의된 「개인정보 보호법」, 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」 및 「신용정보의 이용 및 보호에 관한 법률」 개정 법률안은 데이터 활성화를 위한 가명정보(추가정보 없이는 특정 개인을 알아볼 수 없는 정보)의 개념을 도입하였습니다. 또한 가명정보는 통계작성(상업적 목적 포함), 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의가 없더라도 처리할 수 있도록 정하고 있어 개인정보를 빅데이터 등에 활용할 수 있는 법적 근거를 마련하였습니다.

하지만 가명정보를 가지고 특정 개인을 알아볼 목적으로 처리하는 경우 5년 이상의 징역 또는 5천만원 이하의 벌금에 처할 수 있어 개인정보가 식별되지 않도록 주기적인 점검이 필요할 것으로 예상합니다.

[변화 2] 금융권 클라우드 전면 도입, 개인정보 활용 가능

2019년 1월 1일부터 국내 금융회사도 개인신용정보와 고유식별정보를 외부 클라우드 환경에서 활용할 수 있게 되었습니다. 금융위원회는 2018년 12월 5일 정례회의를 열고 클라우드 이용 확대방안을 위한 전자금융 감독 규정 개정안을 심의 • 의결하였습니다.

지금까지 금융권 클라우드 도입은 비중요 처리시스템(개인신용정보를 처리하지 않는 전산시스템)에만 국한되어 있어 적극인적 활용이 어려웠으나, 금융위원회가 이용 확대를 위해 규제를 완화한 것입니다. 금융권 클라우드의 전면 도입은 운용 비용절감과 신규 서비스 확대로 이어질 것입니다. 다만, 최근 클라우드를 도입한 글로벌 기업들(버라이존, 우버, 월마트 등)의 개인정보 유출사고가 빈번히 발생함에 따라 국내 금융 클라우드 서비스 내 개인정보 자산관리의 필요성이 대두됩니다.

[변화 3] 2019 개인정보의 기술적 보호조치 개선 방향

2019년에는 개인정보보호법 고시 '개인정보의 기술적 보호조치'의 '접속기록 관리' 부분이 개선될 예정입니다. 정부기관에 따르면 개인정보 접속기록 관리 부분에서 다음과 같은 개선사항이 검토 중에 있다고 밝혔습니다:

① **개선 필요**: 지자체 등 다수의 공공기관에서 관례적으로 의무 보관기관(6개월)이 경과한 접속기록을 삭제 조치하고 있음. 때문에 6개월이 지난 시점에서 발견된 침해사고는 접속기록이 없어 유출 원인을 추적하는데 어려움 발생

2019 개선방향: 개인정보 유출사고 발견 시점, 예산소요, 타 법의 사례 등을 고려해 접속기록 보관기관을 중요도에 따라 차등적 연장 검토
* 정보통신망법(개인정보의 기술적 관리적 보호조치 기준 제5조) : 기간통신사업자 2년,
* 신용정보보호법(신용정보업감독규정 제20조) : 1년 이상

② **개선 필요:** 접속기록에 정보주체에 대한 항목을 기록하지 않아 특정인의 개인정보 침해발생에 대한 추적이 곤란한 사례가 발생. 또한 대량의 개인정보를 다운로드하는 행위에 대한 접속기록 항목이 없어 대량으로 개인정보를 다운로드 및 유출해도 확인이 되지않아 침해사고 예방에 한계

2019 개선방향: 정보주체에 관한 사항(성명 또는 ID 등), 일정 규모(예 : 1천명) 이상 개인정보 다운로드에 대한 기록 항목 등을 구체화, 표준화할 예정

③ **개선 필요:** 접속기록 점검을 시스템 운영부서가 할 경우 동료 직원에 대한 엄격한 소명 확인 및 감사 기능이 위축될 우려가 있음. 반기별 1회 이상 점검할 경우 점검해야 할 기록이 방대하고 유출 발생 시 소명 확인이 어려운 사례 발생

2019 개선방향: 접속기록 점검 업무의 효율성을 확보하기 위하여 점검 주기와 점검 주체에 대한 기준 검토
* 정보통신망법(개인정보의 기술적 관리적 보호조치 기준) 및 신용정보보호법(신용정보업감독규정)은 자체 점검 주기를 월 1회 이상으로 규정

[변화 4] 개인정보의 컨트롤 타워: 개인정보보호 위원회로 감독 기능 일원화

2019년에는 방송통신위원회, 행정안전부, 개인정보보호위원회 등으로 나뉘었던 개인정보보호 감독기능이 개인정보보호위원회로 통합될 전망입니다. 개인정보보호법 개정 법률안(의안번호 16621호)에 따르면 개인정보보호위원회를 국무총리 소속 중앙행정기관으로 격상시키고, 현행법상 개인정보에 관한 행정안전부의 기능을 개인정보보호위원회로 이관하도록 하였습니다. 이에 따라 개인정보보호 인증, 개인정보 영향평가, 개인정보 유출 통지, 과태료의 부과, 열람청구, 고발 및 징계권고, 결과의 공표 등은 앞으로 개인정보보호위원회가 주관하며 개인정보보호의 컨트롤타워로 거듭날 예정입니다.

[변화 5] 정보보호최고책임자(CISO) 제도 확산

2019년에는 정보통신서비스 제공자의 CISO 지정 및 신고가 의무화 됩니다. 정보통신서비스 제공자는 임원급 CISO를 지정하고 과학기술정보통신부장관에게 신고하여 합니다(단, 대통령령으로 정하는 자산총액, 매출액 기준에 해당하는 경우에는 예외적으로 CISO를 지정하지 아니할 수 있습니다). 개정된 정보통신망법에서는 CISO의 업무 겸직을 금지하고 있어 정보화최고책임자(CIO) 또는 최고재무책임자(CFO)가 CISO를 겸하는 기업은 앞으로 별도의 CISO 임명해야 합니다.

국내 금융기관은 전자금융거래법에 따라 2012년부터 CISO 제도를 유지해왔습니다. 금번 정보통신망법 개정으로 CISO 제도가 금융 및 기업으로 확산됨에 따라 향후 공공분야에도 적용될 가능성을 배제할 수 없습니다.

(주)소만사 서울시 영등포구 영신로220 knk디지털타워 9층
TEL 02-2636-8300 | FAX 02-2636-8181 | Email privacy@somansa.com