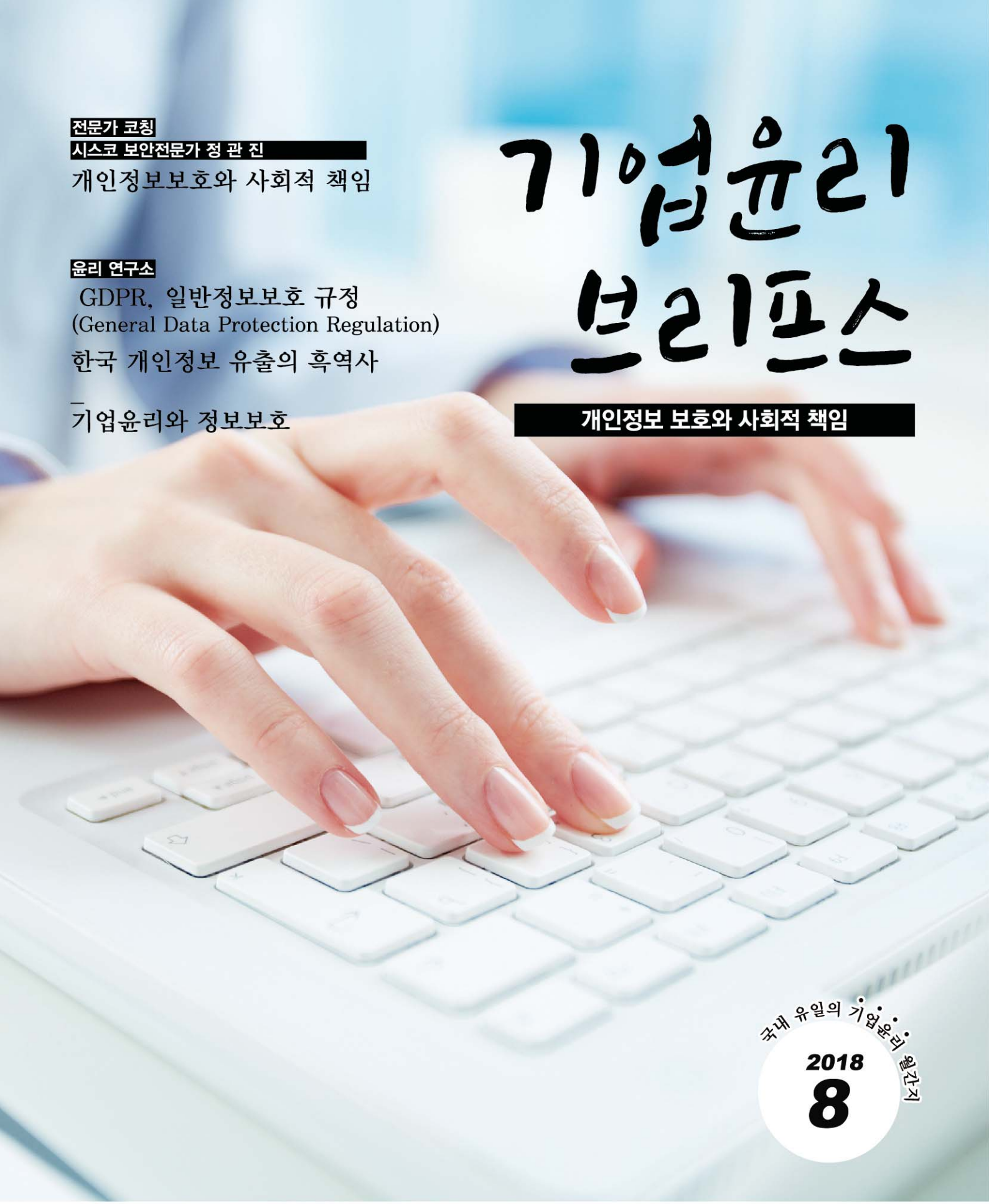


기업윤리 브리프스

개인정보 보호와 사회적 책임

전문가 코칭
시스코 보안전문가 정 관 진
개인정보보호와 사회적 책임

윤리 연구소
GDPR, 일반정보보호 규정
(General Data Protection Regulation)
한국 개인정보 유출의 흑역사

기업윤리와 정보보호

국내 유일의 기업윤리 월간지

2018 8

국민권익위원회

110 정부민원안내 부패·공익신고

▶ 국민권익위원회 홈페이지에서 자세한 내용을 보실 수 있습니다.
www.acrc.go.kr ▸기업윤리 브리프스

발행일 2018년 8월 1일 (매월발행, 통권68호, 비매품) **발행인** 박은정
발행처 국민권익위원회 **구독 신청** 044-200-7166
주소 30102 세종특별자치시 도움5로 20 정부세종청사 7동 민간협력담당관실

전문가 코칭 개인정보보호와 사회적 책임

정 관 진
시스코 보안전문가

Q1. 기업윤리와 개인정보보호는 어떠한 관련성이 있나요?

현재 우리 사회는 디지털사회로의 진입이 가속화되고 있으며 인공지능, 빅데이터, 사물 인터넷, 5G는 일반인들에게도 익숙한 단어가 되었습니다. 매일 일상처럼 사용하는 디지털 정보는 누군가의 데이터베이스에 차곡차곡 정보로 축적될 것이고, 기업은 해당 정보를 기반으로 개인 맞춤화된 서비스를 제공하거나 빅데이터 분석을 통하여 마케팅, 홍보, 제품 개발 등에 활용하고 있습니다.

기업에게 중요한 자료가 되고있는 이러한 정보의 활용은 기업의 '윤리'에 달려 있다고 할 수 있습니다. 정보를 전달받은 시점부터 어떻게 안전하게 저장하고 접근을 인가하며, 해당정보를 어떠한 방법으로 활용할 것인지는 기업의 몫이기 때문입니다. 물론 정보 주체자가 동의했다고 해서 이 정보가 기업의 자산이 되는 것은 아니며, 어디까지나 정보 주체자는 제공한 사람입니다. 그러므로 기업은 개인정보를 안전하게 보호해야 할 책임과 의무가 있습니다. 이것은 현 시대의 흐름, 즉 기업이 영속하기 위해서는 당연시 되어야 할 기업윤리의 하나가 된 것입니다.

기업은 현 디지털 시대에 정보를 기반으로 더욱 성장할 수 있는 발판이 될 수도 있지만, 그 반대에 처할 수도 있습니다. 즉, 데이터도 기업에 이롭게 사용하면 큰 득이 되지만 도덕적 해이(Moral Hazard)에 사용된다면 반드시 그 책임이 뒤따름을 잊지 말아야 합니다.

Q2. 개인정보보호의 중요성과 이를 위해 우리 기업이 해야 할 일은 무엇인가요?

빠르게 성장하고 있는 디지털 시대에 맞춰 많은 나라들이 개인정보보호 규정을 강화하고 있습니다. 일례로, 올해 5월25일부터 유럽연합(EU)의 경우 시민의 데이터 활용 시 GDPR(General Data Protection Regulation, 일반정보보호 규정)을 준수해야만 합니다. 그 동안 개인정보 이용과 관련해 사회적으로 논란이 되었던 내용들을 반영하고 개인정보에 대한 통제권을 정보 주체인 시민들에게 돌려주는 것을 골자로 하고 있습니다. 이번 GDPR이 유럽연합 국가들뿐만 아니라 전세계 기업들에게 영향을 주고 있는 만큼 글로벌 서비스를 하는 국내 기업 또한 대상이 됩니다. 여기서 중요한 것은 정보의 통제권이 주체인 개인에게 있고 주체의 권리를 강화한 만큼 크고 작은 변화가 예상되고, 이에따라 기업의 책임은 더욱 거세게 요구되어 질 것입니다. 기업은 이제 개인정보보호의 중요성을 회사 내의 중요한 과제로 인식해야 하며, 개인정보를 안전하게 보호하기 위한 정보보안 전략이 필요합니다. 디지털 시장이 커지면서 개인정보 유출의 빈도와 대상이 넓어지고 있는 것이 현실입니다. 하지만 크고 작은 개인정보 유출이 발생할 때 마다 지금껏 그래왔듯이 개인정보 유출 관련 사과 안내 공지문 하나 게시하고 책임을 다하는 경우도 많았습니다.

물론, 그때마다 정보보안의 중요성이 부각되지만, 개인정보보호를 위해 보안 제품을 도입했다는 것만으로 책임을 다했다고 할 수는 없습니다. 현재의 지능화되어가는 보안 위협을 막기에는 분명 한계가 있기 때문입니다. 보안 제품의 도입부터 프로세스, 정책, 운영, 개선 등의 더 많은 요구가 뒤따라야하는 것입니다. 보안이라는 것은 보이는 그대로를 믿는 것이 아니라 지속적으로 의심하고 관리해 나가야 하는 것입니다. 뒤늦은 후회는 개인의 피해뿐만 아니라 기업의 신뢰 하락과 경영의 어려움을 가져다 줄 수 있기 때문입니다.

실례로, 작년에 미국 3대 크레딧 평가기관인 에퀴팩스(Equifax)는 해킹으로 인해 1억 4,300만 명의 이름, 생년월일, 사회보장번호, 운전면허, 신용기록 정보 등을 유출했습니다. 기업의 신뢰도 하락은 말할 것도 없고, 기업 가치를 보여주는 주가 또한 크게 떨어졌습니다. 또한 데이터 침해를 인지하고도 공개적으로 발표까지의 시간이 길었던 점(GDPR 은 데이터 유출시 72시간 내에 고지해야 할 의무가 있음)과 고위 임원들이 침해 사실을 알리기 전 주식을 내다 팔았다는 점에서 도덕적 문제와 기업의 윤리를 다시 한번 생각해 볼 수 있습니다.

현재의 개인정보가 갖는 의미는 과거의 그것과 달라지고 있습니다. 기술의 급격한 발전에 따라 정보는 그 가치 이상의 의미를 주고 있어 앞으로의 정보 활용 가능성은 더욱 커질 것이며, 이에 따라 기업이 개인정보를 들여다보는 시각도 달라져야 하는 것입니다. 보안은 완벽할 수는 없습니다. 그러나 개인정보보호를 위한 인식을 달리하는 그 시작점이 바로 중요한 전환점이 됩니다. 보안은 인식의 전환으로부터가 시작입니다.

ISO 37001 Study

Ch 7.

ISO 37001 요구사항 [DO, 실행단계②-b]

부패리스크는 조직이 통제하는 조직뿐만 아니라 비즈니스 관련자로부터 야기될 수 있다. 이에 따라 조직은 통제하는 조직과, 통제하지 않는 조직 모두로부터 발생할 수 있는 부패를 방지 할 수 있는 노력이 필요하다.

Q. 한국상사 OO실장은 다음과 같은 의문이 들었습니다.
"협력업체나 사업 관련자와 같이 예상치 못한 곳에서 발생하게 되는 부패리스크는 어떻게 예방할 수 있을까요?"

[DO, 실행단계] 중 8장 운용은 부패방지경영시스템의 (1)실행을 위해, (2)실행과정 중에, (3)실행한 후에 수행해야하는 가이드라인을 제시하고 있습니다. 이번 호에서는 8장 운용 중 '통제받는 조직과 비즈니스 관련자의 부패방지 관리 시행', '부패방지에 대한 의지 표명', '선물, 접대, 기부 및 유사한 편익' 편에서 요구하는 사항들을 살펴보도록 하겠습니다.

7장 지원

8장 운용

①운용 기획 및 관리 ②실사 ③재무적 관리 ④비재무적 관리
⑤통제받는 조직과 비즈니스 관련자의 부패방지 관리 시행
⑥부패방지에 대한 의지 표명
⑦선물, 접대, 기부 및 유사한 편익
⑧부패방지 관리의 부적절성에 대한 관리
⑨문제/우려사항 제기
⑩부패의 조사 및 조치

[DO 8장. 운용]

조직의 자회사, 대리인, 공동 프로젝트를 수행하는 협력사 등을 비롯한 이해관계자들로부터 발생하는 부패위험은 예측하기도, 예방하기도 어려울 것입니다. ISO 37001은 이러한 위험을 감소시키기 위한 요구사항을 다음과 같이 소개하고 있습니다.

⑤통제받는 조직과 비즈니스 관련자의 부패방지 관리 시행

조직은 자회사와 같이 충분한 영향력을 행사할 수 있는 회사에게는 ISO 37001을 실행하거나 자체적으로 부패방지를 위한 액션을 요구해야 합니다. 한편, 통제할 수 없는 기업에게서 부패 발생의 위험이 높게 감지될 경우에는 부패방지를 위한 관리 수단을 보유하고 있는지, 부패방지시스템 실행을 요구할 상황인지를 파악해야 합니다. 만약 부패방지 수단이 있는지 알 수 없고, 자체적인 노력을 요청하기 어려운 기업이라면, 기업 평가 시 이를 고려하고 해당 기업으로 인해 부패에 연루될 위험이 존재함을 염두에 두어야 합니다.

Tip. 밀접한 거래관계나 많은 업무를 함께 수행한다는 것이 기업을 통제하고 있음을 의미하지 않습니다.

⑥부패방지에 대한 의지 표명

통제할 수 없는 중간이상의 부패위험을 야기하는 비즈니스 관련자를 대상으로 부패방지에 대한 의지표명을 받아내야 합니다. 관련자로 인해 부패가 발생할 경우 거래관계의 종결을 요구할 수 있는 절차가 마련되어 있어야 하며 의지표명은 가능한 한 서면으로 확보해야 합니다. 그러나 거래관계 특성상 이러한 사항을 요구할 수 없는 경우, 의지 표명이 없음은 부패리스크 평가와 실사 수행 시 반영되어야 합니다.

⑦선물, 접대, 기부 및 유사한 편익

주는 자나 받는 자 모두 뇌물을 의도하지 않았다 할지라도 선물, 접대, 기부 및 기타 편익을 제 3자(경쟁자, 언론, 검사, 판사)가 뇌물로 간주할 수도 있다는 것을 인지해야 합니다. 제3자가 합리적으로 뇌물이라고 판단할 수 있는 모든 선물, 접대, 기부 및 유사한 편익의 제안, 제공 또는 수락을 방지하기 위한 절차를 계획하고 그에 따라 행동해야 합니다.
편익에는 다음을 포함할 수 있습니다

선물, 여흥 및 접대 / 정치적 기부금 및 자선 기부금 / 클라이언트 대표자나 공직자의 여행 / 홍보비 / 후원 / 지역사회 자선활동 / 훈련비 / 클럽멤버십/ 개인적 호의/ 기밀정보 및 특권정보

지금까지 ISO 37001의 DO 단계 중, 8장 '운용'의 일부 요구사항에 대해 살펴보았습니다. 다음 'ISO 37001 Study'에서는 '운용'의 나머지 요구사항들에 대해 알아보겠습니다.

사례돋보기

사이버테러를 대비하라

대한민국 주민등록번호는 공공재라는 말이 있다. 국내 IT 산업이 활성화된 이후 수천 만 단위의 개인정보 유출사건이 여러 번 터졌기 때문이다. 유출된 개인정보는 음성적으로 거래되기 때문에 추적해서 삭제하기도 여의치 않다. 때문에 우리나라에서 스팸 문자는 일상이 되었고 보이스피싱도 빈번하게 일어난다. 상황이 이러니 '내 주민번호는 사회 공공재'라는 우스개가 나올 법도 하다.

개인정보 유출 수습은 쉽지 않다. 신용카드를 해지해야 하고 핸드폰 번호도 바꿔야 한다. 주민등록번호는 이마저도 쉽지 않다. 한 번 유출되면 바꿀 수 없는 홍채나 얼굴, 지문 같은 생체 정보의 디지털화는 더 문제가 되고 있다. 정부는 물론 기업과 개인이 합심하여 정보보안에 대한 중요성을 인지하고 관련 시스템의 수준과 사회적 인식을 높여나가야 하는 이유다.

개인정보보호에 실패한 기업들

이름만 대면 알만한 IT 공룡들마저도 개인정보 유출 사태로 인해 뭇매를 맞고 있다. 고객들의 개인정보를 안일하게 취급해왔다는 사실이 드러난 것이다.

공룡기업의 곤욕, 페이스북

올해 3월, 세계 최대 소셜 네트워크 서비스인 페이스북의 개인정보 유출 사건이 터졌다. 사태는 경위가 밝혀지면서 더욱 심각해졌다. 2014년 알렉산더 코건 박사가 페이스북 플랫폼에 배포한 성격 검사 어플리케이션이 페이스북 사용자들의 개인정보를 수집했는데, 이것이 2016년 미국 대선 당시 후보인 도널드 트럼프 캠프에 판매되었기 때문이다. 페이스북 사용자들은 트럼프 선거 캠프에서 5천 만 건에 달하는 개인정보 데이터를 정치적 목적으로 활용했을 것이라며 분개했다. 온라인에서는 페이스북 삭제 캠페인(#DeleteFacebook)이 번졌고 테슬라와 스페이스X의 CEO인 엘런 머스크는 500여만 명의 팔로워를 지닌 페이스북 페이지를 삭제해 버렸다. 영국과 미국 언론은 페이스북에 집중포화를 쏟아부었고 CEO인 마크 주커버그는 미국 의회 청문회까지 참석하며 곤욕을 치렀다.

페이스북의 개인정보 유출 사건은 기업 신뢰도의 추락에서 끝나지 않았다. 주가는 14% 급락했고 시가총액 약 40조 원이 증발했다. 아마존, 애플, 넷플릭스 등 같은 IT 기업들의 주가도 1.5% 이상 동반 하락했다. 대형 IT 기업들 조차도 개인정보를 제대로 보호하지 못할 것이라는 불신이 시장 전체로 확산 된 것이다. 유니레버, P&G 등 세계 최대 광고주들이 속해있는 영국광고주협회(ISBA)는 정보 유출 사태에 대한 페이스북의 해명이 만족스럽지 못할 경우 광고를 전면 중단할 것이라고 경고했다. 수세에 몰린 주커버그는 페이스북의 실수를 인정하고 재발방지를 위해 노력하겠다며 영국과 미국 주요 일간지에 "죄송하다"는 사과 성명을 냈다.

정보유출 사태와 경영위기, 타깃

타깃은 미국의 대형 유통 업체다. 2013년 추수감사절, 해커들은 타깃 매장의 POS 단말기에 악성코드를 유포하여 신용카드, 계좌, 보안코드, 유효기간 등이 담긴 개인정보를 유출시켰다. 무려 4천만 여건에 달하는 막대한 양이었다. 이름, 이메일, 전화번호, 사회보장번호 등을 포함하면 거의 1억 1천만 여명의 개인정보가 새나간 것이었다.

당시 CEO였던 그렉 스타인하펠과 CIO(최고정보관리책임자)였던 베스 제이컵이 이 사건에 대한 책임을 지고 사퇴했다. 타깃은 피해 복구액으로 1억 6천만 달러, 피해보상액으로 1천만 달러를 지출했다. 법률비용과 피해배상액을 포함해 무려 1억 7천만 달러, 한화로 약 1,908억 원에 달하는 거액을 고객 정보 유출 사태 수습을 위해 지출한 셈이다.
타깃은 해킹 사건 이후 고객 신뢰 추락으로 장기간 실적 부진에 시달렸다. 비용절감을 위해 1,700여 명을 구조조정하고 1,400개의 일자리를 없애겠다고 발표했으며 첫 해외 진출지였던 캐나다에서는 실적 부진으로 시장 철수까지 하게 된 것이다.

보안 업체의 정보유출, E사

E사는 종합 소프트웨어 기업이다. 바이러스와 악성코드 등으로부터 PC를 보호하는 프로그램으로 유명하다. 지난해, E사의 고객 정보 유출 사태가 있었다. 유출된 개인정보는 16만 건이었다. 역대 개인정보 유출 사건에 비하면 피해 규모는 작았지만 시사하는 바는 컸다. 국내 대표적인 보안 업체에서의 유출사고는 개인정보보호에 대한 우리 기업들의 안일한 인식 수준을 방증하고 있기 때문이다.
E사의 해킹 사건은 취득한 개인정보를 불법적으로 판매하는 데서 끝나지 않았다. 해커는 빼돌린 E사의 A프로그램 등록정보로 이용자가 가입한 포털 사이트에 접속해 이용자가 저장한 주민등록증, 신용카드, 사진을 확보한 뒤 가상화폐 거래소에

서 가상화폐를 출금했다. 개인정보 유출이 실제 금전 피해로 이어진 것이다.
방송통신위원회는 E사가 이러한 위험을 방지하기 위한 개인정보 보호조치 규정조차 준수하지 않았다며 과징금 1억 2천만 원, 과태료 1,000만 원을 부과했다.
E사의 A프로그램(가입제 커뮤니티·포털 사이트 ID 및 암호를 기억했다가 재방문시 자동으로 로그인해주는 프로그램. 2012년 4월 4일 서비스가 종료)이 보관 중인 개인정보는 수천 만 건에 이른다.
이와 같은 사건이 또 일어난다면 피해 규모는 상상할 수 없을 정도다. 개인정보 보호를 위한 철저한 규약과 시스템 개발이 시급한 이유다.

정보보호 리스크 대응

한국은 IDI(ICT 발전지수. 국가 간 ICT 발전경로, 디지털 격차, 성장 잠재력 등을 평가하는 것이 목적) 기준으로 전세계 1, 2위를 다툴 만큼 IT 수준이 높은 나라다. 고도의 정보통신서비스가 일상화되어있는 만큼 개인정보 유출 사고가 터졌을 시 예상되는 피해 규모도 크다. 하지만 아직까지도 사용자들은 특정 인터넷 서비스 이용 시 이메일 주소는 물론 생년월일, 전화번호 등 예민한 개인정보를 모두 제공해야만 한다. 게다가 이 개인정보를 제3자에게 제공하거나 위탁해도 된다는 조항에 동의해야만 해당 서비스를 온전히 이용할 수가 있다. 사용자 입장에서는 불안한 것이 사실이다.

이러한 상황에서 대두된 것이 GDPR (General Data Protection Regulation, 일반정보보호 규정)이다. 2년 전 EU의회에서 통과돼 지난달 25일부터 시행된 GDPR은 인터넷 사용자 보호에 방점이 찍혀있다. GDPR이 적용되면 인터넷에서 신상정보가 이용될 때 그 정보의 제공자는 해당 정보가 어떤 방식으로 왜 사용되어야 하는지 설명을 요구할 수 있고, 일정 목적에 쓰인 정보의 삭제를 요청할 수도 있다. 개인정보를 제공했더라도 다른 업체로 정보를 이전하거나 정보처리 방식에 이의를 제기할 수도 있다. EU의회는 EU국가에 사업장을 보유한 업체는 물론 EU거주 시민에게 온라인 서비스를 제공하거나 시민의 행동을 모니터링하는 기업이라면 예외 없이 GDPR 준수를 요구하고 있다. 이에 따라 GDPR 준수를 위한 소프트웨어를 출시하는 등 기업들의 대응도 발 빠르게 전개되고 있다.

최근 우리 정부 역시 개인정보 유출 피해를 전보다 심각하게 인식하고 있다. 올해 5월 28일, 정보통신망법이 일부 개정되면서 금융회사나 신용정보회사에만 요구됐던 정보유출배상책임보험 의무 가입이 정보통신서비스 사업자에게도 적용된 것이다. 이에 따라 정보통신서비스 사업자들은 손해배상을 위해 보험 또는 공제에 가입하거나 준비금을 적립해야 한다. 이를 이행하지 않을 경우에는 2천만 원 이하의 과태료를 내야 한다.

행정안전부는 개인정보 유출사고를 막기 위한 방책으로 6가지 당부사항을 제시했다.
첫째, 공공기관장, CPO(Chief Privacy Officer, 개인정보보호책임자) 등은 개인정보보호 마인드를 제고한다.
둘째, 안전한 개인정보 보관·관리를 위해 적극적인 투자를 한다.
셋째, 개인정보보호 전담 인력을 배치·교육하고 전문성을 높인다.
넷째, 개인정보 유출 사고의 주요 원인인 해킹 방어에 힘쓴다.
다섯째, 개인정보가 유출됐을 때는 정보주체에게 알린다.
여섯째, 법령 및 고시 제·개정 사항을 지속적으로 모니터링한다 등이다.

정보보호, 개인의 보안 윤리의식과 시스템이 함께 가야

자물쇠를 달면 도둑으로부터 보다 안전해진다. 하지만 열쇠를 챙겨야 한다는 불편함이 생긴다. 보안성과 편리성은 반비례한다는 의미다. 최근 홍채, 지문, 얼굴 인식이 보편화되면서 보안성과 편리성을 둘 다 만족시키는 기술이 나오고 있지만, 디지털화된 생체 정보 유출에 대한 위험성도 함께 대두됐다. 생체 정보는 유출됐을 경우 삭제하고 다시 생성하는 게 불가능하다. 한번 유출되면 평생 불안 속에 살아야 할지도 모를 일이다. 기술이 발전할수록 정보보호 관련 시스템 및 규약도 철저해져야 하는 것이다.

대부분의 개인정보 유출 사건은 보안에 취약한 시스템이나 해커의 공격으로 발생한다. 하지만 내부 혹은 위탁 직원의 고의, 관리 부주의로 일어나기도 한다. 시스템의 강화, 정부 정책의 수립 등도 중요하지만 개인정보를 보호하려는 보안 윤리의식 강화야 말로 디지털 시대에 고객의 정보를 지키는 첫걸음일 것이다.

윤리연구소 - 인사이트+

GDPR, 일반정보보호 규정 (General Data Protection Regulation)

페이스북의 개인정보 유출 사건은 주목할 만한 이슈였다. 내로라하는 글로벌 IT 기업의 안일한 보안의식도 실망스러웠지만 유출된 개인정보를 사들인 곳이 당시 미국 대선 후보였던 도널드 트럼프 선거캠프였다는 것은 충격이었다. 불법 개인정보가 보이스피싱, 스미싱* 등의 금전 탈취를 넘어 개인의 정치 성향을 분석하기 위한 용도로 쓰였기 때문이다.

오늘날의 SNS는 개인의 취향, 가치관, 소비 패턴, 사소한 일상까지도 전부 보여주고 있다. 소수의 지인들과 계정 주인만 보기위해 업로드한 비공개 데이터도 엄청나다. 바야흐로 디지털 개인정보가 곧 개인의 삶의 궤적이 되기 시작한 것이다. 정치권에서도 인터넷 여론을 모니터링 하는 오늘날, 디지털 개인정보는 더 이상 금융재산에 접근하기 위한 인증수단을 넘어 개인의 사생활 자체가 되었다. 유출됐을 경우 한 사람의 삶을 파탄 낼 수도 있는 폭탄이 된 셈이다. 정보보안 인프라의 취약점을 발견하고 반드시 개선해야 하는 이유다.

GDPR, 고객의 사생활 보호

개인정보 유출 사건 소송은 기업에 유리한 판례가 대부분이다. 문제를 일으킨 기업들은 사과와 함께 피해 보상을 약속했지만 그간 국내 소송에서의 최대 보상액은 개인당 10만 원에 불과했다. 그나마 소송에 참여하지 않은 피해자들은 보상조차 받지 못했다.

외국의 상황도 크게 다르지 않다.
미국 유통기업 타깃의 경우 2014년 해킹으로 1억 건이 넘는 개인정보가 유출됐다. 타깃측은 피해 고객들에게 '신용 확인 절차를 무상으로 지원 했고 유출된 카드를 교체 해주는 서비스를 제공했다'며 앞으로 정보가 남용될 소지를 논하는 것은 '사실상의 피해 여부'에 해당되지 않는다고 주장했다. 2006년 판결난 민간 데이터 기업 액시엄의 16억 건 고객 정보 유출 사건 역시 '사실상의 피해 여부' 검열을 통과하지 못했다. 고객들은 사회보장번호, 전화번호 등의 개인정보가 유출돼 스팸메일과 스팸전화에 시달렸지만 주 연방법원은 이를 피해라고 보기 어렵고 명의 도용의 가능성 역시 피해라고 규정지을 수 없다고 판결한 것이다.

보다 실효성 있는 정보보호를 위해 유럽이 도입한 제도가 바로 GDPR(General Data Protection Regulation, 일반정보보호 규정)이다.
올해 5월 25일부터 발효된 GDPR은 유럽연합의 개인정보보호법이다.
기업이 고객의 정보를 사용하려면 동의를 얻어야 하고 권리를 침해한 경우 72시간 내에 감독기관에 알려야 한다. 이를 위반한 기업은 글로벌 매출액의 4% 또는 2,000만 유로(약 260억 원) 중 높은 금액을 벌금으로 내야 한다. EU회원국은 물론 EU에 법인이나 지점이 있는 외국기업, 유럽 시민에게 서비스 및 제품을 공급하는 외국 기업에도 적용된다.
GDPR은 정보 주체의 개인정보 자기결정권을 보장하기 위한 '개인정보 제공 사전 동의 규정'이 보강됐다. 프로파일링*에 의한 의사결정 거부권, 잊힐 권리, 자기정보 이전권 등이 그것이다. GDPR은 개인정보보호 외에 EU기업의 경쟁력 강화까지 목표로 하고 있다. 개인정보를 위탁 받아 서비스를 제공하는 업체를 선택할 수 있는 자기정보 이전권은 스타트업과 중소기업의 빅데이터 역량 고취에 큰 도움이 될 것으로 예상되기 때문이다. 즉 GDPR은 미래 사회 핵심자산인 데이터 선점 싸움에서 미국에 주도권을 뺏기지 않으려는 EU의 노력 중 하나이기도 한 것이다.

아이캔 – 에팍재판, 필요한 정보만 최소한 수집

GDPR이 발효된 지 4일 후인 5월 29일, 독일 본(Bonn)에서는 GDPR 적용 여부를 둘러싼 첫 재판이 열렸다. 원고는 세계 각국을 대상으로 IP주소 배급을 관장하는 비영리기구 아이캔(ICANN), 피고는 도메인*등록 대행업체이면서 아이캔의 서비스 사용자이기도 한 에팍(EPAG)이었다. 아이캔의 다양한 서비스 중 하나인 후이즈(WHOIS)는 인터넷 IP 보유자의 기본정보가 담긴 데이터베이스를 기반으로 서비스 이용자가 특정 IP주소 보유자의 정보에 대해 질문하면 답해주는 프로토콜이다. 이를 위해 후이즈는 IP주소를 등록하려는 사용자에게 이름, 주소, 전화번호, 이메일 등을 요구한다. 이때 IP 등록업체 대표뿐 아니라 관리자, 기술책임자, 연락처까지 제공해야 한다. 도메인을 받기 위해 이런 정보까지 다 제공해야 하나 싶은 사용자들이 분명히 있을 테지만 지금까지 별다른 이의를 제기하지 못하고 넘어갔던 것이다. 에팍은 후이즈 시스템을 사용해온 고객으로 EU국가 중 GDPR을 앞장서서 실천하고 있는 독일이 주된 시장이다. 따라서 에팍은 GDPR을 위반하면 엄청난 벌금을 물게 되는 만큼 관리·기술 책임자의 정보 수집을 못하겠다고 선언했고, 아이캔은 '에팍의 행동은 명백한 계약 위반'이라며 에팍을 독일 본의 지방법원에 고소하게 된다.

독일 법원은 이튿날인 30일에 판결을 내렸다. 'GDPR이 발효된 이상 향후 고객 정보는 꼭 필요한 것만 최소한으로 수집하겠다'는 에팍의 입장이 계약 위반이 아니라는 것이었다.
GDPR이 과연 얼마나 실효성을 가질까 하며 재판을 예의 주시하던 IT 서비스 업체들에게 보내는 경고 메시지였다.

국내 개인정보보호 강화

GDPR은 1995년부터 시행된 EU의 개인정보보호지침을 수정, 보완한 후 법령화한 것이다. 우리의 개인정보보호법은 EU의 개인정보보호 지침사항을 참조해 제정한 것이라 GDPR과 거의 비슷한 골격을 가지고 있다. 국내 개인정보보호법처럼 GDPR도 개인정보의 정의와 범위를 폭넓게 규정하고 있다. 다만 GDPR은 개인정보 처리의 동의를 필요할 때만 받게 돼 있고 개인정보 주체는 그 동의를 언제든 철회할 수 있다. 그래서 EU에서는 동의 여부에 근거한 개인정보 활용 빈도가 낮다. 동의를 개인정보 처리 원칙처럼 다루는 한국과는 상반된다.

개인정보 처리의 주체가 정보를 제공하는 사용자인 만큼 GDPR은 기업을 개인정보의 수탁자 개념으로 보고 있다. 기업이 위탁자의 업무와 책임을 상당 부분 대신하도록 규정하고 있는 우리 법하고는 다른 지점이다. 즉 GDPR은 개인정보에 대한 법적인 모든 책임이 행위의 주체에 있다고 보는 것이다.

우리 정부와 유관기관들은 지난 2년 동안 GDPR 발효에 철저히 대비해 왔다. 행정안전부는 한국의 개인정보보호법이 유럽의 것을 참고해서 만들어진 만큼 국내 법률을 성실히 준수해 온 기업이라면 EU의 개인정보보호 방침에서 바뀐 규정을 중심으로 대응하고, 현재 EU 집행부의 세부 가이드라인 수립이 늦어지고 있는 만큼 EU 집행부의 움직임을 지켜봐야 할 필요가 있다고 했다.

또한 정부는 관련 부처를 중심으로 GDPR 대응을 위해 기업 인식 제고, 교육 상담 등 다방면의 지원책을 내놓고 있다.

고객은 사생활을 보호 받을 권리가 있다. 고객의 사생활 보호를 위해 명쾌한 법적 기준을 제시하고 있는 GDPR은 보안 윤리의식이 낮은 우리 기업들이 글로벌 시장에서 성공적인 비즈니스 활동을 위한 주요한 지침이 될 것이다.

GDPR 관련 문의사항은 무역협회, KOTRA, 중소기업수출지원센터, 중소기업중앙회 등에서 운영하는 애로사항 접수창구를 이용할 수 있고 전문적인 상담은 한국인터넷진흥원에서 제공하는 상담 서비스를 활용하면 된다.

* 스미싱(smishing) : SMS와 phishing(민감정보 수집을 위한 사기수법)의 합성어로, 인터넷주소를 클릭하면 악성코드가 설치되는 휴대폰 해킹 기법
* 프로파일링(profiling) : 자료수집을 뜻하는 말
* 도메인(domain) : 숫자로 이루어진 인터넷주소를 알기 쉬운 영문으로 표현한 것

역사속의 사례

[한국 개인정보 유출의 흑역사]

우리나라는 세계에서도 손꼽히는 IT강국이다. 금융부터 외식까지 대부분의 산업이 온라인 서비스를 제공하고 있다. 기업들은 원활한 고객관리를 위해 회원가입을 유도하고 동시에 개인정보를 요구한다. 소비자들은 별 수 없이 주민등록번호, 핸드폰 번호 등 예민한 개인정보를 기업에 넘긴다. 문제는 이렇게 고객들의 개인정보를 취합한 기업들의 보안 시스템이 허술하다는 데 있다.

업종을 가리지 않고 발생하는 유출 사고

거래 사이트의 개인정보 유출사건, 금융사 전산망 마비사건, 선거 관리위원회 시스템 디도스 사건 등을 봐도 정보보호 실패 사례는 산업과 업종을 가리지 않고 발생했다. 2005년부터 2018년까지 발생한 주요 보안 사고만 추려 봐도 무려 35건에 이른다. 피해 규모는 상상 이상이다. 피해 인원은 2005년을 시작으로 N사 50만 명, A사 1,863만 명, S사 3,500만 명, E사 400만 명, K사 5,300만 명, L사 2,600만 명, N사 2,500만 명에 이른다. 이쯤 되면 국내에는 개인정보 유출 피해를 안 본 사람이 드물 지경이다.

심각한 2차 피해

유출사고 피해자들은 스팸문자나 광고전화 같은 공해에 시달린다. 청소년들에게도 음란문자가 전송되고 스미싱으로 인한 피해도 빈번하다. 금전 피해도 발생하고 있다. 2011년 SNS 메신저 해킹 사건은 금전 피해로 이어졌다. 메신저를 통해 자주 대화를 나누던 지인이 급한 사정을 호소하며 돈을 요구하자 많은 사람들이 의심 없이 돈을 송금한 것이다.

2008년 이후 유출된 개인정보는 무려 9,800여만 건에 이른다. 피해 규모가 엄청났기에 오히려 개인정보 유출 피해는 일상화된 불편 정도로 여겨지고 있다. 그러나 기술이 발달할수록 정보보호 실패로 인한 피해 규모는 커지게 된다. 생체 정보를 포함한 개인의 모든 정보와 기록이 디지털화되고 있기 때문이다. 4차 산업혁명은 개인의 삶을 온라인 세계로 빠르게 끌어당기고 있다. 보다 정교한 정보보안 시스템과 규정, 개인의 보안의식 고취가 반드시 필요한 이유다.

윤리연구소 - 보고서 리뷰

기업윤리와 정보보호

우리는 환경 보존에 힘쓰고, 협력업체와의 상생을 위해 노력하는 기업들을 향해 착한 기업 또는 윤리적인 기업이라고 부른다. 착한 기업의 이러한 활동은 SNS를 통해 회자되며 기업의 평판과 신뢰는 한층 올라가게 된다. 디지털 경제시대를 보자. 고객의 개인 정보는 사고로 또는 의도적으로 유출이 되어 팔리고 있다. 고객의 소중한 개인 정보는 보호되어야 하는 권리임에 틀림없다. 개인의 권리를 보호하는 기업 활동이야말로 정보가 돈이 되는 시대에 착한 기업이 해야 하는 윤리적인 행동이 아닐까?
이번 보고서리뷰에서는 일리노이 대학 연구(University of Illinois Law Review) 저널에 2016년 게재된 '지속가능한 사이버안보: 사이버공격 관리에 녹색운동으로부터의 교훈 적용(Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks)'을 통해 기업윤리와 정보보호 간의 연결고리를 찾아보고자 한다.

기업을 바라보는 관점의 변화

본 논문에 등장하는 아비-요나(Avi-Yonah) 교수는 로마시대 이후 기업형태가 네 단계에 걸쳐 진화해 왔음을 주장한다. 그에 따르면, 14세기 이전, 기업은 공공의 이익을 증진시키기 위한 법인으로써 등장하였으며, 이후 영리를 추구하는 목적을 가진 조직으로, 분산된 소유구조를 보유하는 형태로, 한 가지 국적이 아닌 다국적 기업의 형태로 진화해 왔다. 형태뿐만 아니라 기업의 정의 또한 많은 변화를 거쳐 왔다. 불과 10년 전만 해도 많은 경영학서에서 기업을 '투입물(Input)과 산출물(Output) 사이의 블랙박스', '이윤극대화를 위한 존재'로 정의 했지만, 지금은 '계약으로 이루어진 유기체', '가치극대화를 위한 존재', '사회적 책임을 위한 존재'로 정의가 변화하고 있다.
이렇게 기업의 형태와 정의가 변해온 것으로부터, 기업에 대한 사회 구성원들의 기대 또한 그 관점과 범위 역시 변화해 오고 있음을 유추할 수 있다. 기업의 사회적 책임에 대한 이해관계자들의 날로 증가하는 요구에는, 기존의 '이윤 극대화'와는 달리 법인 또한 자연인과 같은 하나의 인격체로서 사회 구성원의 역할을 다해야 한다는 주장이 담겨져 있는 것으로 보인다.

이번 보고서 리뷰에서는 이러한 사회적 책임의 범위가 정보보호에까지 닿을 수 있는지 살펴보고자 한다. 일각에서는 사회적 책임 활동에 정보보호를 포함할지 논하는 것 보다 정보유출의 빈도, 시기, 위험 등을 아는 것이 더 시급하고 생산적일 것이라는 비판도 있다. 그러나, 기업의 사회적 책임이 강조되고 있는 현실 속에서, 기업이 정보보호의 실패로 얻게 되는 위험이 단순히 손해배상 차원의 금전적인 손실에만 그치지 않는 만큼 기업의 역할에 대해 다시 한 번 생각해 봐야 한다

법규 준수와 기업의 사회적 책임

이번 보고서리뷰의 논문은 환경으로부터 보안과 기업윤리의 연결고리를 찾을 수 있다고 주장하며, 미국에서는 잘 알려진 최악의 환경 재난사례인 'Love Canal'사건을 소개한다. 19세기 후반에서 20세기 초반 사이에, 미국 나이아가라 폭포 인근에서는 Love라는 사람의 운하공사가 경제공황 등으로 인해 중단되게 된다.

공사가 중단된 운하부지는 한 화학회사의 화학폐기물 매립지로 사용되었고, 약 10년간 축적된 화학폐기물이 묻힌 이 장소는 1달러에 나이아가라 시(市)에 매각되어 학교부지로 사용되었다. 덮혀진 매립장 위에 생겨난 마을의 주민들은 원인모르는 고통을 받아야했다. 아이들의 몸에는 화상 자국이 선명했고, 마을의 유산률과 암 발병률은 타 지역에 비해 월등히 높았다. 이 사건으로 인해 수많은 환경규제들이 생겨나게 되었고 당시 이 화학회사의 행동은 위법이 아니었지만, 기업이 했어야 할 사회적 책임을 다하지 못했다는 거센 비판을 받아야만 했다.

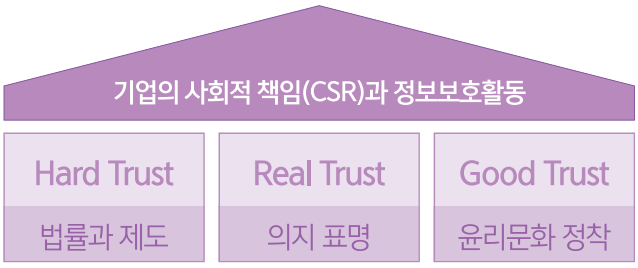
기업의 사회적 책임이란 위법 여부에 초점을 맞추지 않는다. 법의 그물망에서 벗어날 수는 있어도 신뢰에 돌이킬 수 없는 손상을 입게 된다. 정보가 행동을 결정한다는 주장이 나올 만큼 정보가 전부인 시대에서, 정보가 유출이 되었을 때 법적으로 큰 책임이 없는 만큼 정보보호에 애를 쓰지 않아도 될까? 데이터가 행동을 결정하는 정보화 시대에서, 이러한 행동이 이해관계자와의 신뢰를 저버리는 행동은 아닌지 진지하게 생각해 봐야 하는 것이다.

지속가능한사이버안보

기업윤리와 정보보호

정보보안의 중요성

본 논문에서는 신뢰를 크게 Hard trust, Real trust, Good trust 등의 세 가지로 분류하고 있다. 구체적으로, 사회 구성원들의 합의를 통해 도출된 법률과 같은 Hard trust, 기업이 외부에 비춰지는 이미지나 명성과 같은 Real trust, 마지막으로 내부 구성원의 행동을 이끌어낼 수 있는 Good trust가 신뢰를 분류할 수 있는 방법 중 한 가지라는 것이다.
기업의 정보보호 활동을 위의 3가지 신뢰측면으로 분류해 보자. 법률과 제도의 수립(Hard trust), 개인정보보호를 위한 의지표명 등 고객을 위해 헌신하는 이미지(Real trust), 회사 내부에 윤리문화 정착(Good trust) 등을 통해 신뢰를 구축해 나갈 수 있다.



지속가능한 정보보안

시스코의 전 CEO인 존 챔버스(John Chambers)는 다음과 같은 말을 했다고 한다. "세상에는 해킹을 당한 회사와 해킹을 당한지 조차 모르는 두 타입의 회사가 있다." 이를 기업 외부의 시선에서 바라볼 경우, 한 가지 더 치명적인 사실이 있다. "혹은 누출사실을 알리지 않은 회사." 최근 정보유출에 대한 많은 제도와 판결들이 기업을 우선시했던 과거와는 달리 개인을 중요시하는 판결로 바뀌고 있다. 아직 완전히 드러나지 않은 심각한 문제들을 위한 대비책 마련의 필요성이 점차 강조되고 있는 것이다.

예측할 수 없는 내/외부의 다양한 공격에 대응해야 하는 정보보호 활동은 매우 어려운 일임에 틀림없다. 하지만 사고가 발생했을 때, 앞서 제시한 세 가지 신뢰구축을 위해 노력한 기업과 그렇지 않은 기업을 바라보는 사회 구성원들의 시선에는 극명한 차이가 존재할 것이다.

본 논문은 지속가능한 정보보안을 위한 즉, 기업의 신뢰를 위한 정보보안의 여섯 가지 원칙을 제시한다. 아래의 표를 통해 이러한 정보보안의 여섯 가지 원칙이 우리 기업에도 적용되고 있는지 검토해보길 권한다.

기업의 신뢰를 위한 정보보안의 여섯가지 원칙	
Confidentiality (기밀유지)	인가되지 않은 사람으로부터 읽히거나 복사되지 않도록 보호
Integrity(온전성)	인가되지 않은 사람으로부터의 정보 변경 및 삭제 방지
Availability(유용성)	서비스가 손상되지 않도록 보호
Consistency(지속성)	이용자의 기대수준에 맞게 작동하도록 보장
Control(통제)	접근에 대한 규제
Audit(감사)	모든 활동에 대한 기록

> "세상에는 두 가지의 회사가 있다: 해킹을 당한 회사, 그리고 해킹을 당한지조차 모르는 회사 *(There are two types of companies: those that have been hacked, and those who do not know that they have been hacked)*."
>
> JOHN CHAMBERS
> Former CEO, Cisco

* 참고

'Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks', University of Illinois Law Review, 2016

뉴스클립 NEWS CLIP

▶ 국내동향

❶ 중소기업중앙회, 중소기업의 청렴 인식 조사

중소기업 10곳 중 7곳이 반부패·청렴의식 제고가 경제 활력을 회복하는데 도움이 될 것이라고 응답했다. 중기중앙회가 중소기업 306개 사를 대상으로 반부패·청렴의식 인식 현황을 조사한 결과, 표본기업의 약 70%는 경제 활력을 위해 중소기업의 청렴의식의 수준이 제고되어야 한다고 답한 것이다. 그러나 이러한 의식 수준 제고를 위한 중소기업이 도입한 제도 등을 조사한 결과, 약 60%의 기업이 별도의 제도를 운영하지 않는 것으로 나타났다. 이는 청렴문화 정착의 필요성은 인지하지만 중소기업 여건상 우선순위가 낮을 수밖에 없는 중소기업의 현실을 보여주고 있다. 중기중앙회 경제정책본부장은 '중소기업이 청렴 수준 제고에 더욱 힘쓸 수 있도록 정부 및 공공기관과 함께 사회 각 분야에 청렴문화가 정착할 수 있는 정책이 필요하다'고 말했다.

* 참고 – 중앙일보, 07.11
http://news.joins.com/article/22791761

❷ 과학기술정보통신부, 화이트 해커 양성 프로그램 개최

지난달 3일 '차세대 보안리더 양성 프로그램' 7기 발대식이 개최되었다. 과기정통부는 다양한 절차를 거쳐 선발된 160명의 고교, 대학(원)생들을 4차 산업혁명 시대의 정보보안 분야를 선도할 화이트해커로 양성할 것을 밝혔다. 과기정통부는 지난 6년간 본 프로그램을 통해 화이트해커 712명을 배출하였다. 선발된 인원은 관련 전문가들로부터 정보보안 각 분야별 최신 기술을 교육받고 실무 과업을 수행하게 된다. 현재까지 육성된 화이트해커들은 국제해킹방어대회에서 상위권에 입상하거나, 다양한 제품 및 서비스 취약점을 분석하는 등 정보보안 인재로서 다양하게 활동하고 있다. 과기정통부는 4차 산업혁명 시대, 정보보안 인력 수요에 대응하기 위해 우수 인력양성 프로그램을 보다 확대할 계획임을 밝혔다.

*참고 – 아이뉴스, 07.03
http://news.inews24.com/php/news_view.php?g_menu=020830&g_serial=1106088

❸ 대법원, SK커뮤니케이션즈 개인정보 유출 손해배상책임 판결

지난달 12일, 대법원은 2011년 SK커뮤니케이션즈(이하 SK컴즈)의 개인정보 유출 사건에 대해, 1심과 2심의 원고 일부 승소 판결을 파기하고 피고인 회사 측에 배상 책임이 없다는 취지의 판단을 내렸다. 이 사건은 2011년, 중국인으로 추정되는 해커가 SK컴즈의 운영사이트에 등록된 회원 3,500만명의 개인정보를 유출한 것으로부터 시작되었다. 당시 개인정보 유출의 피해자이자 변호사인 원고는 SK컴즈를 상대로 손해배상을 청구하였고, 1심과 2심은 개인정보 유출로 인한 정신적 고통에 대해 SK컴즈가 과실이 없음을 입증하지 못하는 것을 근거로 위자료 100만원 지급에 대한 판결을 내린 바 있다. 그러나 대법원은 사건 발생 당시 SK컴즈의 보호조치가 합리적으로 기대되는 정도의 보호조치가 아니었다고 인정하기 어렵다는 것을 근거로 회사의 배상책임이 없음을 밝혔다.

*참고 – 중앙일보, 07.12
http://news.joins.com/article/22793983

해외동향 ◀

❶ 영국, 페이스북 정보유출 사건 첫 유죄 판결

영국 의회 정보 위원회(ICO, Information Commissioner's Office)는 페이스북의 최대 8,700만 명의 개인정보 유출 사건에 대해, 개인정보를 안전하게 유지해야 한다는 1998년 데이터 보호법을 위반한 것이라고 밝혔다. 페이스북은 해당 개인정보 유출사건에 대해 잘못은 인정하지만 불법은 아니라는 입장을 취해오고 있다. ICO는 이번 사건에 법이 정한 최고 벌금인 50만 파운드(약 7억 4천만 원)가 부과될 수도 있다고 덧붙이며, 기존 절차에 따라 최종 결정을 하기 전 당사자에게 조사 결과에 대해 대응할 수 있는 기회를 허용한다고 전했다. 페이스북은 ICO의 발표에 대해 곧 입장을 내놓을 계획이라고 전한 것으로 알려져, 페이스북이 기존의 입장을 고수할 것인지에 대해 세계의 관심이 집중되고 있다.

* 참고 – 한국일보, 07.11
https://www.koreatimes.net/ArticleViewer/Article/111542

❷ 유럽 제약사, 부패방지경영시스템(ISO 37001) 적극 운영

한국제약바이오협회 국제반부패아카데미 연수단은 지난달 오스트리아에서 진행된 국제반부패아카데미(IACA, International Anti-Corruption Academy)의 연수일정을 마치며, 유럽 제약사들 역시 ISO 37001(부패방지경영시스템 국제표준)을 경영 시스템에 적극 반영하고 있다고 전했다. 2016년 제정된 ISO 37001은 국내 제약산업의 불법 리베이트 방지를 위해 많은 제약사들이 도입하고 있는 시스템으로, 현재 다양한 분야의 기업들이 부패 방지를 위한 의지표명 및 실천을 통해 ISO 37001 도입 인증을 받고 있다. 연수과정을 이끈 바바라 나이거(Barbara Neiger) 박사는 글로벌 제약사라면 ISO 37001도입이 타 국가와 신뢰를 쌓는데 있어 매우 긍정적인 영향을 발휘할 것이라고 전했다.

* 참고 – 코메디닷컴, 07.17
http://www.kormedi.com/news/news/drug_dist/1228298_2906.html

❸ 베트남, 출처 불분명 공직자 재산에 45%세금 부과

지난달 13일, 베트남 국회에서 공직자가 보유한 재산 중 출처가 불분명한 재산에 대해 높은 세율을 부과하는 방안에 대해 팽팽한 설전이 오갔다. 베트남 재정부 차관 및 검찰위원장 등은 '비정상적인 수입에 대한 체납'이고 '소득세의 납부가 무죄를 입증하지 않으며, 가장 현실적인 대안'이라며 찬성의 입장을 주장하였으나, 최고인민검찰원장 등은 '적법한 수입에만 부과하는 것이 세금'임을 주장하며 불법재산으로 밝혀졌을 경우에 발생할 문제들을 제시하는 것으로 반대의 입장을 밝혔다. 베트남은 국가권력 서열 1위인 응우옌 푸 쫑 공산당 서기관의 연임을 시작으로, 2016년부터 반부패 드라이브를 걸며 공직사회에 만연한 부패를 해결하기 위해 노력하고 있는 것으로 알려져 있다.

*참고 – 매일경제, 07.16.
http://news.mk.co.kr/newsRead.php?sc=30000018&year=2018&no=446696

국내·외 행사 소식

▶ 국내행사

❶ 8월 경총포럼

4차 산업혁명 시대의 CEO에게 필요한 기업가 정신을 주제로 산업변화에 대한 대처방안 논의

주최 한국경영자총협회
일시 2018년 8월 23일
장소 서울, 조선호텔

❷ 2018 공학 기술자 윤리 포럼

성공적인 윤리교육사례 공유를 통한 공학 분야의 사회적 가치 실현

주최 한국공학교육학회
일시 2018년 8월 10일
장소 서울, 연세대학교

해외행사 ◀

❶ Gartner Security & Risk Management Summit 2018

정보환경의 최신 동향에 대한 소식 및 정보보안에 대한 위험 대책 공유

주최 Gartner
일시 2018년 8월 30일 ~ 8월 31일
장소 Mumbai, India

❷ International Conference on Contemporary Issue in Social Science, Business, CSR Strategic Marketing

사회과학, 경영, 기업의 사회적 책임 전략의 최신 이슈에 대한 논의

주최 Shanghai Academic Network
일시 2018년 8월 25일 ~ 8월 26일
장소 Shanghai, China

청탁금지법 Check!

<변화하는 대한민국>

제약사 영업방식의 변화

청탁금지법에 의해 가장 영향을 많이 받은 산업분야 중 하나인 제약업계에서 새로운 변화가 나타나고 있다. 지난 7월 한 조사기관의 연구결과에 따르면, 제약업계의 영업·마케팅 활동 방식이 전통적인 '대면'방식에서 정보통신기기를 활용하는 '온라인'방식으로 바뀌고 있는 것으로 나타났다. 구체적으로, 오프라인 영업·마케팅 활동인 '대면 디테일(의사나 약사에게 해당 의약품의 정보를 제공하는 일)', '오프라인 세미나', '샘플지급활동'의 비용 지출이 감소한 반면, '온라인 디테일', '온라인 세미나' 등과 같은 디지털 채널의 비용 지출이 증가하였다. 조사기관은 '대면 디테일'을 줄여나감에 따라 비용이 감소한 것인 만큼 제약업계의 영업·마케팅 트렌드가 기존의 관계중심에서 제품의 정보 제공 중심으로 변화되고 있음을 보여준다고 해석했다. 이러한 제약업계의 흐름은 다른 산업까지로 점차 확산될 것으로 전망된다.

청탁금지법의 평가 '긍정적'

곧 다가올 청탁금지법 2주년을 맞아 공공기관 및 지방자치단체는 설문조사를 실시했다. 시행 이후 우리사회에 미친 영향과 청탁금지법의 준수 정도 등에 대해 임직원 및 지역 주민들을 대상으로 조사한 것이다. 조사 결과, 경기도민의 10명 중 7명은 일상과 업무 등에서 우리사회가 긍정적으로 변하고 있다고 인식하는 것으로 조사됐다. 또한 청탁금지법이 공직사회의 부조리와 더불어 금품수수와 같은 부정청탁을 감소시켰다고 응답한 사람이 10명 중 8명인 것으로 나타났다. 한 공공기관의 임직원 대상 설문조사에서는 응답자의 99%가 청탁금지법으로 인해 사회 청렴성이 향상되었다고 인식하는 것으로 조사되었다. 이는 청탁금지법 적용 대상자의 답변이라는 사실이라 더욱 주목할 필요가 있다. 이들은 이러한 청탁금지법의 정착에 가장 크게 기여한 부분이 교육과 홍보라고 답하며, 시행 2주년이 가까운 지금에도 시행초기의 긴장감이 사라지지 않고 높은 준수 수준을 유지하고 있다고 응답했다.

지식 1g

정보보호 실천수칙 스마트폰 편

'우리나라의 스마트폰 이용률은 96%에 이릅니다.
일상 속 작은 실천이 스마트폰 해킹사고를 방지할 수 있습니다.

① 공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)의 앱 설치 제한하기
② 단문 문자(또는 SNS) 메시지에 포함된 URL 클릭하지 않기
③ 공인인증서는 USIM 등 안전한 저장장소에 보관하기
④ 스마트폰 운영체제와 모바일 백신을 항상 최신으로 업데이트하기
⑤ 스마트폰 보안 잠금(비밀번호 또는 화면 패턴)을 설정하여 이용하기
⑥ 루팅, 탈옥 등 스마트폰 구조를 임의로 변경하지 않기
⑦ 스마트폰 앱 설치 시 과도한 권한을 요구하는 앱은 설치하지 않기
⑧ 스마트폰 WiFi 연결 시 제공자 불분명한 공유기 이용하지 않기
⑨ 스마트폰에 중요정보 정리하기
- 매일 양치질하는 것처럼 매일 보안 소프트웨어 실행하여 PC, 스마트폰의 바이러스도 없애주세요.
- 주민등록증, 보안카드가 찍힌 사진 등은 보관하지 말고 깨끗하게 삭제하세요.

독자에게 물었습니다.

Q1. 기업윤리와 개인정보보호는 관련성이 있다고 생각하십니까?

C기업 K주임

윤리의 의미는 개인이든 기업이든 본인이 속한 사회 안에서 서로 의존하며 지켜야 하는 질서를 의미하는 것으로 알고 있습니다. 기업윤리는 기업이 사회 안에서 비즈니스 활동을 하는 데 지켜야 하는 질서인 것이구요. 그렇다면 기업이 비즈니스 활동을 영위하는 데 고객의 개인정보를 보호하는 것은 어떤 의미일까를 생각해 보았습니다. 나의 정보는 중요한 나의 자산인 만큼 본인의 정보를 보호받아야 하는 것은 고객이 누려야 하는 당연한 권리 입니다. 인권을 보호하는 인권경영이 윤리경영의 당연한 요건이 되는 것처럼 나의 정보를 보호받아야 하는 내 권리는 내 정보를 활용하는 기업이 지켜주어야 합니다. 그렇지 않다면 해당 기업은 질서를 지키지 않는 즉, 기업윤리를 다하지 않는 기업이라고 생각합니다.

Q2. 소속된 회사의 고객 개인정보보호를 위한 활동에는 어떠한 것들이 있나요?

F기업 J과장

어업이나 임업과 같은 1차 산업보다는 3차, 4차와 같은 서비스 위주의 산업에서 정보보호에 대한 관심이 더 많을 것으로 생각됩니다. 제가 다니고 있는 기업은 3차 산업에 속해있습니다. 가입된 회원들의 정보가 어떻게 저장되어있고 어떤 보안절차가 이루어져 있는지는 담당부서가 아니기 때문에 알 수는 없습니다만, 담당부서로부터 메일을 통해 주기적으로, 그리고 특정한 상황이 발생할 때마다 가이드라인을 자세히 제공받고 있습니다. 예를 들어, 보안을 위협하는 프로그램으로부터 내 PC를 보호할 수 있는 방법이나, 감염 시 증상 및 대처방안 등이 이에 해당됩니다. 저 역시도 그렇지만 담당자가 아니면 이러한 내용과 프로그램을 가볍게 여기게 되는 만큼 정보 유출의 심각성과 보안프로그램과 관련된 정기적인 교육으로 보안의식을 강화해 나간다면 더 좋지 않을까 합니다.

사례응모

이 기업을 추천합니다

- 기업윤리 브리프스에서는 독자의견을 수렴하여 윤리경영의 우수 사례를 발굴함으로써 많은 기업들의 귀감이 될 수 있도록 소개하고자 합니다.
- 하단의 담당관실 메일주소를 통해 추천하고 싶은 우수 기업과 관련 내용을 보내주세요.

독자퀴즈

Q. EU기업의 경쟁력 강화와 더불어 개인정보보호를 위해 올해 5월 25일 시행된 제도는?

① GAAP ② GDPR ③ GRDP ④ GCNK

정답 제출처

국민권익위원회 민간협력 담당관실(jykim5@ips.or.kr)
성함, 주소(상품권 수령지), 연락처를 보내주세요(22일까지)
정답을 보내주신 분 중 5명을 추첨하여 문화상품권을 보내드립니다.

▶ **지난 호 정답 : ④번** / 지난 호 정답자는 **김봉현**님, **박종규**님, **정세일**님, **최혜인**님, **추성호**님 입니다. 축하드립니다.