국내 유일의 기업윤리 월간지

기업윤리 브리프스

2016 Nov
11

국민권익위원회 Monthly Business Ethics Briefs

▶ 국민권익위원회 홈페이지 www.acrc.go.kr ☞ '기업윤리 브리프스'에서 자세한 내용을 보실 수 있습니다.

전문가 초청

정보보호, 사람에 주목하고 좋은 거버넌스 만들어야

권 헌 영
고려대학교 정보보호대학원 교수

질문 1 기업의 정보보호에서 가장 염두에 두어야 할 사안은 무엇인지?

단연코 사람이 제일 중심이다. 정보보호에서 가장 중요한 부분은 결국 누군가가 지키고자하는 '정보', 즉 '내용(contents)'이다. 기업 차원에서는 '영업비밀'과 '고객정보'이고, 국가 차원에서는 '국가기밀'과 '국민정보'라고 할 수 있다. 전자는 정보보호(정보보안), 후자는 개인정보보호라고 일컫는다. 그동안 이를 보호하기 위해서 시스템 보안 투자를 꾸준히 늘려 왔다. 하지만 안타깝게도 열심히 정보보호 관련 투자를 하는 기업에서도 보안사고가 반드시 터지게 마련이다. 왜냐하면 기술투자를 하면서도 이 시스템에 접근하는 '사람'에 주목하지 않았기 때문이다. 최근 정보보호에서 '인적 보안'을 다시 주목하고 있는 이유가 바로 여기에 있다. 이제는 '어디'가 정보보호에 취약한가를 살피는 것과 동시에 '누가' 잠금장치를 파괴할지 살피는 경영이 더욱 요구된다.

최근 전 국민을 놀라게 하고 아직도 관련 재판이 진행 중인 신용카드사 정보유출 사건이 있었다. 범인은 자신의 처지나 처우에 대한 비관 때문에 스트레스가 쌓이고 화가 나서 욱하는 마음에 정보유출 범행을 행동으로 옮기게 되었다는 취지의 범행 동기를 밝혔다. 이 범인은 시스템 전산 쪽 전문가로 개발 작업에 참여한 사람이었지만 신용카드사 입장에서는 외주업체의 직원에 불과했다. 경영자 입장에서는 거의 관심의 대상이 아닌 일용직 근로자에 해당할 만한 이가 어떻게 신용카드사의 가장 중요한 고객 정보에 접근하고 심지어 그걸 통째로 몇 년 동안에 걸쳐 빼돌릴 수 있었을까? 아무도 이 '고객정보'가 이러한 '위험'을 초래할 수 있는 경영 리스크인지 몰랐기 때문이다. 인적보안은 누가 우리의 중요한 '정보'에 접근하는 '사람' 인지를 먼저 살피고 그 위험을 분석하는 일에서 출발해야한다.

질문 2 경영자 관점에서 정보보호 리스크를 효과적으로 관리하는 가장 좋은 방법은?

은행 · 증권 · 보험 등 금융기관이나 통신회사와 같은 기업 입장에서 고객 정보는 곧바로 돈이 된다. 그 내용이 구체적이고 실시간 정보일수록 더욱 가치가 있다. 이런 정보는 해커나 내부자가 경제적 이유로 유출하게 된다. 이런 일을 막으려면 기업이나 기관의 모든 구성원이 함께 나서야 한다. 그런데 어떻게 하느냐가 문제이다.

'새로운 문제'에는 '새로운 답'을 찾아야 한다. 좋은 거버넌스를 만드는 게 핵심이다. 당장 정보보호책임자를 경영자나 기관장 직속 임원으로 설치하면 된다. 직속으로 만들기 어려우면 적어도 2인자의 직속 임원은 되어야 한다. 미국의 정보보호협회에서는 재무담당이사 직속에 정보보호책임자를 둘 것을 권고하고 있다. 기업에서는 재무이사가 실질적으로 2인자이기 때문이다. 이제는 '정보보호'가 경영 리스크의 최상위에 올랐다는 의미이기도 하다. 이미 금융기관에서는 이를 제도화했다. 빅데이터 시대에는 금융기관뿐만 아니라 가전회사, 자동차 회사, 에너지 회사가 모두 고객정보 유출 사고 때문에 바로 망할 수도 있다.

거버넌스를 잘 만든 후에는 모든 구성원이 정보보호 리스크를 이해하고 보안 활동을 실천하게 하는 일이 중요하다. 최고경영진에서 외부 고객까지 이해관계자가 모두 동참해야 하는 일이다. 역설적이지만 '청탁금지법'이 좋은 사례이다. 불만은 있지만 모르는 사람이 없고, 어렵지만 모두 실천하고 있다. 기관 내 보안정책도 시끄러울 정도로 오랫동안 함께 만들고 지속적으로 홍보하고 시행하면 어렵다 할지라도 못할 일은 아닌 것이다.

▶ 발행일 2016년 11월 1일(매월발행, 통권47호, 비매품) | 발행인 성영훈 | 발행처 국민권익위원회 | 주소 30102 세종특별자치시 도움5로 20 정부세종청사 7동 민간협력담당관실 ▶ 구독신청 044-200-7167

윤경萬里

:: 국 내

1. 공공기관 임직원, 2시간 이상 반드시 부패방지교육 받아야

국민권익위원회는「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」과 시행령 개정에 따라 9월30일부터 중앙행정기관, 지방자치단체, 공직유관단체 등 공공기관 소속 임직원이 매년 1회, 2시간 이상 부패방지 의무교육을 받아야 하고 신규 공직자나 승진자 등에게는 반드시 대면 교육을 실시해야 한다고 밝혔다. 또한 재직 중 부패행위로 300만 원 이상의 벌금형을 선고받은 퇴직공직자는 취업이 제한되며, 이를 위반하면 2년 이하의 징역이나 2천만 원 이하의 벌금에 처해질 수 있다고 밝혔다.

참고 http://www.yonhapnews.co.kr/bulletin/2016/09/30/0200000000AKR20160930074000001.HTML?input=1179m
http://news.heraldcorp.com/view.php?ud=20160930000152

2. 준법지원인 안 뽑은 상장사 40% 넘어

10월17일 공개된 금융감독원 자료에 따르면, 올 6월 말 기준으로 준법지원인을 선임해야 하는 상장회사 311곳 중 183곳만 준법지원인을 두고 있는 것으로 밝혀졌다. 하지만 이들 대상 기업이 준법지원인을 선임하지 않아도 마땅한 처벌 규정이 없는 상태이다. 준법지원인 제도를 따르지 않는 곳이 전체 대상 상장사의 40% 이상에 달했고 특히 골목상권 침해 논란이 잦은 유통업종이 다수였다. 이 결과는 상당수 기업들의 준법경영 의지가 여전히 부족한 상태임을 보여준다.

참고 http://biz.khan.co.kr/khan_art_view.html?artid=201610171700001&code=920100
http://thel.mt.co.kr/newsView.html?no=2016101710228273497

3. 개인정보보호 위반 정보통신서비스업체에 과태료 처분

10월20일 방송통신위원회는 개인정보 유출·노출을 자진 신고한 정보통신서비스 제공사업자 중 강원심층수, 대교에듀피아, 소울소프트, 아시아나항공, 예스24 등 5개 업체에 시정명령과 과징금 236만원, 과태료 총 7500만원을 부과했다고 발표했다. 이 업체들은 개인정보처리시스템에 대한 접근 통제를 하지 않았거나 개인정보를 암호화해 보관하지 않는 등 기술상·관리상 보호조치를 하지 않은 것으로 나타났다.

참고 http://www.yonhapnews.co.kr/bulletin/2016/10/20/0200000000AKR20161020114600017.HTML?input=1179m
http://it.chosun.com/news/article.html?no=2825472

:: 해 외

1. 미국 웰스파고, '유령계좌' 200만 개 스캔들

9월초 미국 4대 은행 중 하나인 웰스파고가 2011년부터 고객명의를 도용해 '유령계좌' 200만개를 만들어 부당이득을 챙긴 사실이 적발돼 큰 파문을 일으켰다. 미 연방소비자금융보호국(CFPB)은 웰스파고에 1억8천500만 달러의 벌금과 고객 환급액 500만 달러를 부과했다. 웰스파고 직원들은 계좌개설 할당량을 부여받고 이를 달성하지 못하면 해고 등 불이익을 받기 때문에 강압에 못 이겨 유령계좌를 만든 것으로 알려졌다. 10월12일 존 스텀프 회장은 스캔들의 책임을 지고 사임을 발표했다.

참고 http://www.yonhapnews.co.kr/bulletin/2016/10/13/0200000000AKR20161013043500009.HTML?input=1179m
http://news.joins.com/article/20717162

2. '반(反)부패' 강화하는 중국, 한국의 청탁금지법에 주목

반부패 사정드라이브를 강화하고 있는 중국 시진핑 체제는 한국의 부정청탁 및 금품등 수수 금지에 관한 법률(청탁금지법)의 시행에 큰 관심을 보이고 있다. 시진핑 지도부는 "부패에는 관용도 성역도 없다"는 단호한 자세로 부패 공직자를 연이어 적발하여 처벌하고 공직사회기강 확립을 위해 각종 조처를 단행하고 있다. 최근 중국 공직사회는 공무접대 과정에서 음주를 엄격히 금지하는 '금주령'까지 확산하는 분위기다.

참고 http://www.yonhapnews.co.kr/bulletin/2016/09/30/0200000000AKR20160930084300083.HTML?input=1179m
http://news.kbs.co.kr/news/view.do?ncd=3353739&ref=D

3. 인도, 검은돈 엄벌 경고에 은닉자산 10조 자진신고

10월2일 탈세 목적으로 은닉한 자산을 4개월간 자진신고 받은 결과, 모두 6만4275명이 6천525억 루피(10조8천120억원)의 은닉자산을 신고했다. 인도 정부는 내년 9월까지 자진신고로 약 5조원의 세수를 확보할 것으로 전망하고 있다. 신고기한이 지나 은닉자산이 드러나면 검은돈 방지법에 따라 엄벌하겠다고 경고한 모디 총리는 "탈세 자진 신고가 성공적이었고 경제 성장과 투명성에 크게 기여할 것"이라고 말했다. 하지만 인도중앙수사국은 스위스 등 해외 조세피난처에 5천억 달러(약552조원) 규모의 은닉 자산이 있을 것으로 보고 있다.

참고 http://www.yonhapnews.co.kr/bulletin/2016/10/02/0200000000AKR20161002022600077.HTML?input=1179m
http://news.chosun.com/site/data/html_dir/2016/10/02/2016100200792.html

Q 우리 회사 정보를 지키기 위해 임직원 개인이 할 수 있는 일은 뭐가 있죠?

A 과거의 해킹은 전문 해커가 회사의 방화벽이나 보안 시스템의 허점을 노려 악성코드를 심고 정보를 빼내갔다면, 오늘 날의 해킹은 임직원을 공략하는 경우가 많습니다. 해커가 임직원의 방심을 노려 정보를 빼내는 만큼 임직원 개개인의 정보보안을 위한 노력이 중요합니다.

회사의 PC로 업무와 무관한 사이트, 신뢰성이 입증되지 않은 사이트에 접속하는 것은 지양해야 하며, 보안프로그램은 항상 최신버전을 유지해야 합니다. 특히 메일이나 메신저, USB 등에 담긴 파일은 꼼꼼히 살펴보고 수상한 파일은 절대 받지 않도록 해야 합니다.

웹보안 외에 정보보안을 위해 실천해야 할 것은 또 무엇이 있을까요? 가장 중요한 것은 회사의 정보보안 관련 규정을 준수하는 것입니다. 편의와 효율이란 이유로 보안절차를 건너뛰거나 자료를 함부로 반출하는 등의 행위는 회사 보안을 위협할 수 있음을 명심해야 합니다.

정보를 수집·처리할 때에는 목적에 맞게 최소한의 범위에서 적법, 정당하게 이를 수집·활용해야 하며, 외부에 정보를 제공하는 경우, 정보주체의 동의가 필요합니다. 목적에 맞게 활용하고 난 정보는 반드시 파기하여야 유출 사고가 발생하더라도 피해를 줄일 수 있습니다.

정보에 대한 접근·처리 권한을 다른 사람에게 양도해서는 안 됩니다. 아이디와 패스워드를 써서 책상에 붙여두거나 자동로그인을 설정해두는 것은 타인에게 나의 권한을 마음대로 이용해도 된다고 말하는 것과 같다는 것을 꼭 기억하세요!

윤리연구소

애플 사태를 통해 생각하는 개인정보보호

아이폰은 현재 7억 대 이상 팔린 세계적 상품이다. 그런데 한 대의 아이폰 때문에 애플과 미국 연방수사국(FBI) 간 세기의 '프라이버시' 전쟁이 시작돼 아직까지 법정 공방전이 벌어지고 있다. 지난해 말 샌버나디노에서 무슬림 부부의 끔찍한 총기난사사건이 발생해 14명이 죽고 22명이 부상당했다. 미 FBI는 애플 측에 테러범이 사용한 아이폰 5C의 '잠금 해제'를 요구했다. 하지만 애플 회장 팀 쿡은 고객의 개인정보를 위협하는 FBI의 월권행위에 맞서 고객정보를 끝까지 지킬 것이라며 대법원까지 가는 장기전을 불사하고 있다.

애플이 FBI 협조를 거부하는 이유

애플은 FBI 협조를 위해 10명의 엔지니어와 직원이 4주가량 매달려야 하고, 향후 벌어질지 모를 소송에 대비해 전체 개발과정을 일일이 기록해야 한다고 주장한다. 무엇보다도 법원의 협조 명령이 떨어질 때마다 이런 개발 및 폐지 작업을 반복할 경우 자사 부담이 더욱 가중되고, 정부 요청을 다루는 새로운 '해킹' 전문 부서를 설치해 수사 요청이 있을 때마다 매번 잠금장치를 해제하는 새로운 백도어(보안 장벽 우회로) 소프트웨어를 개발하는 상황이 벌어질 것이라 밝히고 있다. 강압적인 FBI의 협조 명령이 제약회사에게 독약을 만들고, 범죄수사의 미끼로 사용하기 위해 언론사에 허위기사를 작성하도록 지시하는 것과 다를 바 없는 상황이기 때문에 FBI 요구를 받아들일 수 없다는 것이다. 또한 애플은 테러용의자의 아이폰에 저장된 데이터와는 아무런 상관이 없으므로 개별 아이폰에 대한 책임을 질 하등의 이유가 없다고 항변한다.

프라이버시보호 vs. 국가안보

윤리경영은 고객의 프라이버시보호를 우선적으로 고려해야하지만, 국가안보라는 현실의 법리 논란 속에서 정부의 수사권과 프라이버시보호 사이의 균형을 어떻게 잡을 것인지 중요한 부분이다. 마이크로소프트 전 CEO 빌 게이츠는 애플 사태와 관련해 FBI의 주장에 제한적으로 찬성하며 올바른 안전장치를 둘 경우 테러방지 등 공공이익을 위한 정부활동에 협조할 수 있을 것이라는 의견을 냈다. 그러나 페이스북, 구글, 트위터의 CEO들은 데이터 암호화의 필요성을 강조하면서 고객정보보호를 최우선으로 생각해야 할 기업이 고객의 권익에 반하는 행동을 하도록 정부가 강요하고 있다고 주장한다. 미국 내 전반적인 분위기는 프라이버시보호 쪽 손을 들어주고 있는 것처럼 보인다. 어떤 결과가 나오든 애플 사태는 먼 나라의 분쟁이 아니다. 우리도 정부, 기업, 소비자 등 이해관계자들의 개인정보보호와 국가안보의 충돌 가능성을 염두에 두고 진지한 논의가 필요한 시기다.

프라이버시보호를 위한 비식별조치

데이터를 조합해 새로운 가치를 창출하는 빅데이터 시대에 미국 등 선진국은 프라이버시보호와 개인정보 이용 사이의 갈등을 없애는 데이터 비식별화 기술에 관심을 갖고 관련 사업을 진행하고 있다. 개인정보의 철저한 비식별 조치와 추후 재식별 방지 및 처벌 조치를 위한 지속적인 모니터링 등 사후관리를 강조하고 있다. 미국은 소비자프라이버시권리장전법(CPBRA), 의료개인정보보호법(HIPPA) 등 개별법규에서 비식별 조치를 완료한 데이터는 개인정보보호 범위에서 제외한다. 지난 4월 EU의회에서 통과된 개인정보보호법(GPDR)도 가명처리(Pseudonymisation)를 규정하고, 데이터의 가명처리 요건만 충족하면 개인정보사용동의 의무가 면제되어 최초 수집목적 외의 다른 용도로의 사용과 데이터 외부 제공 시 정보주체 통지의무의 면제 등을 허용하고 있다. 다만 공익, 과학적 연구, 역사연구, 통계 목적에 한정해서 가명정보를 동의 없이 처리할 수 있다. 국내에서도 7월 1일 행정자치부를 비롯한 관계 부처에서 '개인정보 비식별 조치 가이드라인'과 '개인정보 법령 통합 해설서'를 발표하는 등 빅데이터 활성화를 위한 개인정보 보호제도 개선을 단행했다. 비식별 조치를 사전검토, 비식별 조치, 적정성 평가, 사후관리 등 4단계로 나누고 각 단계별 조치 사항과 유의사항이 명시되어 있다. 빅데이터 시대를 주도하기 위해서는 정부와 학계, 기업과 소비자 간 개인정보이용에 대한 합의가 전제되어야 한다.

국경을 초월한 개인정보보호의 필요성

많은 기업이 개인정보보호가 허약한 나라로 데이터 센터를 이전하여 규제를 회피하고 있다. 타국 정부나 해외 기업이 자국의 온라인 정보에 수시로 접속하여 개인정보유출문제가 발생하기 때문에, 각국은 자국민의 개인정보보호를 위해 데이터의 무분별한 해외 이전을 제한하기 시작했다. 2000년 10월 EU와 미국은 '세이프 하버(Safe Habor)' 조약을 체결하여 미국기업이 협정 7개 원칙(고지, 선택, 제3자 제공, 접근, 보안, 정보통합, 법률이행)을 준수한다면 개인정보보호 조치를 취한 것으로 간주하고 EU지역에서 수집한 개인정보를 자유롭게 미국으로 이전 할 수 있도록 했다. 그러나 지난해 유럽사법재판소는 이 조약으로는 EU시민의 개인정보를 보호하기 어렵다는 이유로 체결 15년 만에 무효화를 선언했다.

한국기업들도 EU국가의 개인정보를 그 밖의 지역에서 사용할 수 있도록 '개인정보보호적합성평가추진단'을 통해 국가차원에서 EU의 개인정보보호적합성평가를 추진하고 있다. 지금까지 한국은 국가차원의 적합성 평가를 받지 않아 국내 기업이 개별국가의 심사를 거쳐야 개인정보를 국내에 전송하고 처리하는 것이 가능했다. 앞으로는 정보의 자유로운 유통을 보장하지만 무분별한 사용을 제한하고 개인프라이버시를 보호할 수 있는 방안에 대한 협의가 본격적으로 이루어질 것이다. 개인정보보호정책이 강력하게 적용되는 유럽에서 사업을 하려면 민감한 정보와 그렇지 않은 정보를 따로 구분하는 것이 사내 문화로 완전히 정착되어야 하며, 그렇지 않으면 엄청난 벌금을 물게 될 수 있다. 윤리경영을 표방하는 기업이라도 해외 각국의 정보이전 시스템을 체계적으로 파악하지 않으면 정보보호스캔들의 주역이 될 가능성을 배제할 수 없기 때문에 정보보호에 각별한 관심이 요구된다.

윤리경영 스터디

2016 정보보호 10대 이슈

한국인터넷진흥원(KISA)이 발표한 「2016 정보보호 10대 이슈」 보고서는 정보보안의 중요성을 이해하는 데 큰 도움을 줄 수 있다. 정보보호 10대 이슈 가운데 윤리경영과 직접적인 관련성이 있는 내용을 중심으로 살펴보고자 한다.

기반시설 및 공공부문 클라우드 보안의 중요성 증대

전력, 물, 가스 등 주요 기반시설 사고는 세계적으로 2014년 245건으로 2010년 대비 600% 증가했고 취약점은 2010년 18건에서 2014년 159건으로 800% 증가했다. 작년 6월 미 연방 인사관리처가 해킹당해 연방 요원 400만 명의 신상정보가 유출되는 사건이 발생했다. 국내에서도 한국수력원자력 해킹 공격으로 원전 관련 설계도면 유출('15.7), 한국철도공사 네트워크 망구성도 등 주요 정보통신 기반시설 공문서 유출('15.9) 등 기반시설에 대한 해킹 사례가 발생했다. 따라서 기반시설 해킹 사전 방지대책마련은 물론이고 신속한 사고처리, 복구 등 체계적인 사후 대응 시스템 구축이 필요할 것으로 전망된다.

미국, 영국 등 주요국에서는 보안성 강화를 통해 공공부문의 클라우드 도입을 촉진하고 있다. 영국은 2014년 이미 정부의 클라우드 사용을 위한 'G-클라우드'인증제도 시스템을 구축하여 데이터 보안체계를 개편했다. 우리는 약 1만 5,000여 곳의 공공기관에 클라우드 도입이 가능하지만, 보안 시스템의 제도적 기반 및 보안 기준 부재로 도입 및 활용이 현재 어려운 상황이다. 국내 클라우드 시장도 앞으로 매년 20%에 가까운 성장세를 이어갈 것으로 보이고, 작년 9월 시행된 '클라우드발전법'에 따라 공공기관의 클라우드컴퓨팅 확산이 본격화되면 보안 신뢰성 제고를 위한 정책의 중요성도 강조될 전망이다.

프라이버시 침해 가능성 및 방지책 마련의 중요성

핀테크 차세대 인증수단으로 신체 일부를 활용하는 생체인증(FIDO) 기술이 부상하고 있고, 표준 수립을 위해 관련 협의체를 신설하는 등 정부와 민간기업의 관심이 높아지고 있다. 안드로이드페이 삼성페이 등 간편 결제서비스를 중심으로 생체인증 기술이 이미 활용되고 있다. 하지만 개인 생체 정보를 활용한 기기, 서비스의 보급이 확대되면서 시장 혼란, 프라이버시 침해 방지를 위한 표준화 및 제도적 보완을 요구하는 목소리도 높아질 것이다.

한편, 드론시장도 연평균 28% 성장해서 2023년 22억 달러에 달할 것으로 보이지만 무분별한 사진 및 동영상 촬영으로 인해 프라이버시를 침해하는 사례가 증가하고 있다. 이런 점을 감안해 미국, 일본 등 주요국은 드론 활성화 정책과 함께 프라이버시 보호 방안을 마련 중이다. 지난해 미국 캘리포니아주는 no-fly zone을 지정(8월)했고, 연방항공청은 개인드론등록을 의무화(11월)했다. 드론 사용이 증가함에 따라 프라이버시 침해 논란도 확대될 것이며, 주요 시설물에 대한 드론 공격 위협에 대응하기 위해 드론 탐지 레이더, 식별 카메라, 전파 교란 장치 등 드론 방어 체계 관련 기술의 실용화가 이루어질 전망이다.

정보보호관리체계 마련의 시급성

ICT 활용으로 인해 금융, 의료 등 비ICT 분야에서도 보안사고가 발생하면서 정보보호관리체계 도입이 증가하고 있다. 특히 금융사기, 불법 판촉, 보험·제약회사 악용 등 2차 피해 발생 가능성이 높은 금융, 의료 분야에서 개인정보 유출 사고 등의 위험이 크게 증가하고 있다. 미국의 경우 개인정보 유출 사고 42.5%가 의료 부문에서 발생하고 있다. 최근 5년간 국내 은행권에서 195건의 금융사고가 발생해 사고금액이 5,357억 원에 이른다. 그리고 국내 다국적 의료정보업체 대표가 25억 건의 의료정보를 미국에 유출시키는 사건이 일어나기도 했다.

국내외에서 금융·의료 부문의 보안사고로 사회적 비용이 발생하고 있어 정보보호관리체계 마련이 시급한 상황이다. 미국과 영국은 해당 분야를 대상으로 사이버보안프레임워크를 구축해서 정기적 훈련과 사이버 복원력을 테스트하고 있다. 한국도 사이버안전대진단을 통해 기업의 대응 능력을 점검하고 정보보호관리체계, 정보보호준비제도 등 인증 의무화를 추진하고 있다. 따라서 금융, 의료, 교육 등 비ICT 분야에서도 주요 정보 자산을 효율적으로 보호하고 관리하기 위한 정보보호관리체계 도입의 필요성이 높아질 것이다.

정보보호의 산업화와 전망

정보보호의 요구가 급속도로 커지고 있기 때문에 정보보호 시장의 수요와 공급이 활성화되어 선순환적인 산업 생태계가 조성될 것으로 전망한다. 전 세계 정보보호 산업의 높은 성장세에도 불구하고 국내시장은 성장세가 둔화되고 있다. 국내 정보보호 산업의 시장규모(14년 69억 달러)는 세계시장(1,900억 달러)의 약 3.6% 수준이고 최근 성장률(14년, 7.1%)은 이전 3년 평균 성장률(약 15%)에 비해 하락세를 보이고 있다.

국내기업은 윤리경영시스템에 대한 전반적 이해가 낮은 것처럼, 정보보호에서도 낮은 유지관리 요율 적용, 서비스 대가 불인정 등 덤핑식 저가 발주 관행이 정보보호 산업성장을 더디게 하는 악순환의 장애로 작용하고 있다. 따라서 선순환 정보보호 산업생태계 구축을 위한 법적 기반 마련이 필요했다.

지난해 국내 시장 가격의 왜곡을 해소하고, 정보보호 산업을 육성·강화하기 위해 정보보호 제품 및 서비스의 적정 대가 확보, 정보보호 공시 제도 등을 규정한 '정보보호산업의 진흥에 관한 법률'이 제정되었다.

기업의 자발적 정보보호 투자, 적정 대가 지급 등이 확대되어 정보보호 제품, 서비스 업체 및 컨설팅, 관제 등 국내 정보보호 산업이 활성화될 전망이다. 정보보호 관련 기술 개발, 표준화, 인력 양성 체계의 변화가 예상된다. 가격경쟁체제에서 기술경쟁체제로 전환되면서 정보보호 산업의 선순환 생태계가 조성될 것으로 전망된다. 윤리경영의 한 축인 정보보호가 역설적으로 산업화를 통해 더욱 강화될 전망이다.

윤리 it 수다

윤리적으로 정보 다루기

기업의 정보보안이 윤리경영과 무슨 상관일까? 회사의 자산인 정보를 올바르게 활용하고 보호하는 것이 당연하기도 하지만 이보다 중요한 것은 윤리적 리스크 절감과 윤리적 가치의 실현이다. 다양한 이해관계자의 정보를 다룬다는 것은 신뢰와 책임이 달린 문제이다. 최선을 다하여 이를 지키는 것이 바로 윤리적 기업의 역할인 것이다.

정보보호

기업의 정보는 곧 회사의 자산이자, 이해관계자들의 신뢰이다. 이를 제대로 지키지 못한 기업은 신뢰를 잃고, 비난과 질타까지 감내해야만 한다.

개인정보보호법 위반 기업 공개

행정자치부는 지난 2월, 2014년 개인정보보호법 위반으로 행정처분을 받은 5개 기업을 공개하였다. 가장 많은 정보 유출 원인은 해킹이었다. H사, H연합회, D사, P사 등은 해킹으로 인해 각각 53만 명, 29만 명, 22만 명, 19만 명의 정보를 유출하였고, A사는 위탁직원으로 인해 20만 명의 개인정보가 유출되었다. 이들 기업은 개인정보보호를 위한 안전성 확보 조치 위반, 또는 개인정보 유출 통지 위반 등을 이유로 과태료 4200만 원의 행정처분을 받았다.

애슐리 메디슨 해킹 사건

2015년 7월, 해커집단 '임팩트팀'이 웹사이트 애슐리 매디슨(ashley madison)에 해킹 사실을 알려왔다. 애슐리 매디슨은 기혼자들이 불륜 상대를 찾는 웹사이트로, 유출된 데이터는 3700만 건의 고객 기록과 취약 비밀번호 수백만 건이었다. 하지만 애슐리 매디슨은 해커들이 알려주기 전까지 해킹 사실조차 파악하지 못하고 있었고, 정보가 공개된 고객들은 정신적 고통을 호소하다가 결국 두 건의 자살 사건까지 발생하였다.

S사 직원의 기술정보 유출 시도

2012년, S사의 수석연구원 조 씨는 무려 1조 100억의 거금이 투입된 국가핵심기술 개발에 주도적으로 참여한 최고 전문가였다. 그는 '임원급 대우를 해주겠다'는 말에 함께 개발에 참여한 5명의 연구원과 경쟁사로 이직하여 1억 9천만 원에 기술관련 비밀자료를 넘겼다. 하지만 경쟁사 임원 입사가 무산되자 조 씨는 또다른 S사 전현직 연구원 5명과 함께 중국으로 해당 기술정보를 넘기려 하였다.
다행히 경찰이 먼저 이를 적발하여 해외로의 정보유출은 무산되었고 조 씨와 전현직 S사 연구원들, 경쟁사 임원 등 총 11명은 모두 검거되었다.

잘못된 정보 관리와 활용

정보의 보호만큼이나 기업신뢰를 좌우하는 것이 정보의 활용이다. 정당한 방법을 통한 수집, 정확한 활용목적 고지, 목적 외 용도로 활용하지 않는 것, 그리고 고지한 기간 및 사용 목적 달성 후의 폐기까지 모든 과정이 중요하다.

페이스북의 잘못된 정보수집

2015년, 브뤼셀 자유대학과 루벤대 연구진은 페이스북이 자사 회원 뿐 아니라 비회원들의 개인정보까지 수집했다는 보고서를 공개했다. 페이스북 자사 웹페이지를 방문한 모든 사람, 심지어 로그인을 하지 않은 사람이나 비회원의 정보도 수집되었으며, 페이스북의 웹 경로 추적 기능을 거부한 방문자들의 웹 경로까지 추적해온 것이다. 이는 EU의 개인정보보호법을 위배한 것으로 논란이 커졌고, 벨기에 법원은 페이스북에 비회원 유저에 대한 추적을 중단하라는 결정을 내렸다.

H사의 고객정보판매

H사는 2011년부터 2014년까지 경품행사를 통해 고객들의 개인정보 2천 400여만 건을 취득하였다. 이 정보를 보험사에 판매한 H사는 231억 원이 넘는 돈을 챙겼다. 지난 8월, H사는 무죄 판결을 받았다. 고객의 정보를 마케팅 용도로 활용한다는 것을 응모권에 표기했기 때문에 위법행위는 아니라는 것이다. 그러나 재판 결과와 재판부의 설명에도 불구하고 소비자들의 배신감은 누그러들지 않고 있으며, H사의 경품행사를 통한 고객정보판매는 소비자 기만이라는 주장이 계속되고 있다.

앞서 말한 바와 같이 기업의 정보보안은 소비자 신뢰와 책임에 대해 직접적인 영향을 미친다. 이는 법적인 문제를 넘어선 것이다. 법적인 책임을 다하는 것만으로 윤리적 책임을 다했다고 볼 수 없는 것과 마찬가지다. 고객을 지키는 마음으로, 회사와 동료를 지키는 마음으로 정보를 지키고 적확(的確)하게 활용해야만 우리를 믿는 고객과 이해관계자들의 믿음에 응할 수 있을 것이다.

카드뉴스

정보 블랙아웃을 막아라!

블랙아웃(Blackout, 대정전)은 어떠한 이유로 한 지역에서 발생한 정전을 의미하며, 마치 좀비와 같이 전력망을 타고 주변으로 퍼져나간다. 그렇기에 블랙아웃이 일어나기 전 그 원인을 막는 것이 중요하다. 정보보안 역시 그렇다. 단 한 명의 PC가 악성코드에 감염되면, 바이러스는 걷잡을 수 없이 퍼져 나가고 이는 곧 회사 전체의 피해로 확대된다. 그렇기에 정보보안을 위해서는 위기가 닥치기 전에 그 원인을 막는 것이 중요하다. 임직원 한 사람 한 사람이 정보보안을 철저히 하고 여기에 회사의 정보보안 시스템이 덧대어졌을 때, 우리의 정보보안은 하나의 철옹성으로서 우뚝 서있을 것이다.

청탁금지법 Q&A

공무수행사인의 범위

Q

(1) 청탁금지법상 공무수행사인의 범위는 어떻게 되나요?

(2) 청탁금지법 제11조제1항제2호 · 제4호에 따라 법인 · 단체가 권한을 위임 · 위탁받아 공무 수행사인이 되는 경우, 해당 업무를 수행하는 직원도 공무수행사인인가요?

(3) 공무수행사인이 되는 경우, 수탁된 공무 외에 다른 업무와 관련하여서도 청탁금지법이 적용되나요?

A

(1) ① 각종 법령에 따라 설치된 위원회의 공직자등이 아닌 위원, ② 권한을 위임 · 위탁받은 법인 · 단체 또는 그 기관이나 개인, ③ 공무 수행을 위해 민간부문에서 공공기관에 파견 나온 사람, ④ 법령에 따라 공무상 심의 · 평가 등을 하는 개인 또는 법인 · 단체 중 어느 하나에 해당하는 자는 공무수행사인으로서 법 적용대상자에 해당합니다(제11조제1항제1호내지제4호).

(2) 권한을 위임 · 위탁받은 법인 · 단체 또는 기관의 경우, 대표자와 실질적으로 수임 · 수탁 업무 종사자도 공무수행사인에 해당합니다(제11조제1항제2호 · 제4호).

(3) 공무수행사인의 경우 '공무수행에 관하여' 부정청탁 금지 및 수수 금지 금품등 수수의 금지 규정을 준용하고 있습니다(제11조제1항).

Q

○○은행의 지점장급 간부 甲은 금융정책을 결정하는 중앙부처에 파견되어 부실금융기관 구조조정 업무를 담당하던 중, 부실금융기관으로 지정되어 공적자금 투입여부 심사를 받고 있던 A저축은행 대표 B를 만나 20만원 상당의 식사와 30만원의 백화점 상품권을 제공받은 경우, 甲, A, B는 청탁금지법상 어떤 제재를 받나요?

A

● 중앙부처에 파견된 ○○은행 지점장급 간부 甲은 청탁금지법상 공무수행사인에 해당합니다(제11조제1항제3호).

- 20만원 상당의 식사비는 음식물 상한액 3만원 초과, 30만원 상당의 상품권은 선물 상한액 5만원을 초과하며, 甲과 B 간의 관계 상 원활한 직무수행 등 목적이 인정되기도 어려울 것으로 보이므로, 이는 제8조제3항제2호의 수수 금지 금품등의 예외사유에 해당하지 않습니다.
- 甲은 직무와 관련하여 총 50만원 상당의 금품등(20만원 상당의 식사, 30만원 상당의 상품권)을 받았으므로, 수수 가액의 2배 이상 5배 이하의 과태료 부과대상에 해당하며(제8조제2항, 제23조제5항제1호), 징계대상에도 해당합니다(제21조).
- B는 총 50만원 상당의 금품등을 제공하였으므로, 금품 등 가액의 2배 이상 5배 이하의 과태료 부과대상에 해당합니다(제8조제5항, 제23조제5항제3호).
- A저축은행은 양벌규정에 따라 과태료 부과대상에 해당합니다(제24조).

※ 참고로, 법인의 대표자의 행위는 양벌규정의 면책 대상에서 제외된다는 것이 판례의 입장이므로, A저축은행은 대표 B의 위반행위를 방지하기 위해 해당 업무에 관하여 상당한 주의와 감독을 게을리 하지 않았다 하더라도 면책되기 어려움

행사소개

국내행사 | 국외행사

윤경SM포럼 정기모임 & CEO 클럽 정례모임

윤리경영 선진 우수사례 공유 및 이슈발굴을 통해 국내 산업계의 경쟁력 강화, 기업의 청탁금지법 올바른 이해 특강 등

- 주최 : 윤경SM포럼
- 일시 : 2016년 11월11일
- 장소 : 롯데호텔

First Green Business Forum for Asia and the Pacific (제1차 아시아 - 태평양 녹색 비즈니스 포럼)

실무자와 전문가들이 녹색 성장의 핵심 요소이자 원동력인 녹색 비즈니스의 최고의 생각과 경험을 공유하는 포럼.

- 주최 : Asian Development Bank
- 일시 : 2016년 11월 22~24일
- 장소 : Manila, Philippines

Basic Compliance & Ethics Academy Spain (스페인 컴플라이언스 & 윤리 기초 아카데미)

글로벌 기업들에게 미국을 벗어나 기초적인 컴플라이언스 & 윤리 아카데미를 제공하는 자리.

- 주최 : SCCE
- 일시 : 2016년 11월28일~12월1일
- 장소 : Madrid, Spain

4Th Annual Asia Ethics Summit (제4차 아시아 윤리 정상회의)

뇌물수수, 데이터 프라이버시, M&A 함정, 기업지배구조 및 이사회 참여, 기업가치 등이 메인테마로 다뤄질 예정.

- 주최 : Ethisphere
- 일시 : 2016년 12월 6일
- 장소 : The Fullerton Hotel, Singapore