보안공학연구논문지 *Journal of Security Engineering*
Vol.11, No.5 (2014), pp.399-416
http://dx.doi.org/10.14257/jse.2014.10.02

한국내 글로벌 외국법인의 개인정보보호 전략에 관한 연구 - C사의 개인정보보호 TFT 운영사례를 중심으로 -

이대영[1], 정진홍[2]

A Study on Strategy of Global Foreign Company in Korea to comply Privacy Information Protection; Focused on TFT Operation Case of C Corporation

Dae-Young Lee[1], Jin-Hong Jeong[2]

요 약

본 논문은 국내의 외국법인 수가 1,500개를 넘어서는 비즈니스 환경 속에서 개인정보보호를 위한 글로벌 외국법인인 C사의 개인정보보호 TFT 운영 사례 연구를 통하여 모범적인 개인정보보호 전략을 제시하고자 하였다. 1930년대부터 국내에서 영업활동을 시작한 C사의 경우 2011년 상반기부터 개인정보보호법과 관련하여 주기적인 모니터링을 실시하여 왔으며 안전행정부와 한국인터넷진흥원에서 실시하는 개인정보보호 전문가 교육에 사내 전산부서 담당자를 파견하여 지속적으로 대응준비를 하여왔다. 외국법인의 특성으로 인해 한국 본사와 아시아 지역 본부 및 미국 본사 법률 팀과의 연계가 필수적이었으며 임원회의 결과에 따라 2011년 하반기부터 개인정보보호 TFT 활동을 수행하였다. C사는 국내 법 준수를 위해 다각적인 업무 프로세스 및 IT 시스템 개선작업 등을 통하여 성공적인 개인정보보호 규정, 조직, 시스템 구축 등을 이루었으며 지속적인 직원 교육 및 감사프로세스를 통하여 실질적으로 운영되는 개인정보보호 시스템을 구축·운영하고 있다. 따라서 본 연구는 C사의 TFT 운영 시의 산출물과 이메일기록 및 TFT 리더와의 면담을 통하여 조직 내의 전반적인 TFT활동 내역을 점검하여 국내 기업뿐 아니라 글로벌 외국법인들의 국내 개인정보보호법 준수를 위한 10가지 전략과 4가지 제언을 제시하였다.

핵심어 : 개인정보보호, PIMS, 보안정책, 보안조직

Abstract

In this paper, The best practice for implementing of Personal Information Protection TFT which is operated in global foreign C Corporation is presented in to other companies in more then 1,400 foreign companies. C Corporation has been operated the business in Korea from 1930s. They monitored new Personal Information Protection Law in Korea and trained IT specialist for it in special course which are opened by Ministry of Public Administration and Security, Korea Internet and Security Agency. From 2011 year, They operated Task Force Team for implementing strategy and organization for Personal Information

접수일(2014년06월09일), 심사의뢰일(2014년06월10일), 심사완료일(1차:2014년06월17일, 2차:2014년10월13일)
게재일(2014년10월31일)

[1]120-808 서울시 서대문구 대현동 67-7, 서울과학종합대학원 산업보안전공.
email: gaesalgu@korea.com
[2]120-808 서울시 서대문구 대현동 67-5, 서울과학종합대학원대학교.
email: jhjeong@assist.ac.kr

ISSN: 1738-7531 JSE

Protection Law. As C Corporation is a global foreign company in Korea, there are lots of gaps between local regulation and internal corporate policy. They have been cooperated with local legal team and corporate legal team to find out proper strategy and organization to comply. They improved business process and IT system and consequentially accomplished to build strategy, policy, organization and audit process. From the result of this case study of C Corporation's TFT activities and outputs, 10 strategies and 4 recommendations are presented to not other local companies but also global foreign companies in Korea.

Keywords : Privacy Information Protection, PIMS, Security Strategy, Security organization.

1. 서론

1.1 연구 목적

국내 개인정보보호법은 2011년 3월 29일 공포되고 6개월 후인 2011년 9월 30일 시행이 되었으며 이듬해인 2012년 3월 29일을 마지막으로 유예기간(계도기간)이 만료되어 실질적인 법 강제력이 시행되었다. 이 법 시행 이전에는 공공기관 및 정보통신서비스사업자, 신용정보회사 등 일부 사업분야의 약 50만 사업자에게만 개인정보보호의 의무가 선별적으로 적용되었었으나 새로운 법의 공포로 인해 공공 및 민간분야를 망라하여 약 350만 이상의 개인정보처리자가 법의 적용 대상으로 확대되었다. 이에 따라 각 기업들은 개인정보보호법 준수를 위해 다양한 조치를 취하고 있으나 기업 내 개인정보보호 전문가 부재 등으로 인해 실질적인 대응체계 구축에 어려움을 겪고 있다.

안전행정부 및 인터넷진흥원에서 이러한 기업 내 전문가 부재 문제를 해결하고 지원하기 위해 다양한 "개인정보보호 전문가 양성" 프로그램 등을 운영하고 있으나 홍보 부족 등으로 인해 기업들이 적극적으로 활용하지 못하고 있다. 또한 현재 안전행정부나 인터넷진흥원의 기업 지원 방식이 법규 준수를 위한 법령 가이드 및 지침 수준에 머물러 있으며 실질적인 개인정보보호 준수를 위한 기업 맞춤 컨설팅이나 실질적인 업무 지원을 하기에는 예산 및 인력부족 등으로 인해 어려움을 겪고 있다. 때문에 각 기업들의 개인정보보호 대응전략구축은 기업의 몫으로 남아있다. 이러한 환경에서 기업들은 개인정보보호법 대응활동에 대한 성공 모델이 필요한 상황이다.

2014년 7월 국세청 통계에 따르면 국세청에 신고 된 외국법인 수는 2012년 기준 1,513개이며 법인세 신고액은 7,694억 원에 달하며 그 수는 지속적으로 증가할 것으로 보인다. 이러한 외국법인들은 외국법인들의 조직 특성상 기업 운영에 필요한 IT시스템들이 해외에 설치되어 있거나 Cloud SaaS(Software as a service) 형태로 운영되고 있다. 이러한 IT시스템에 직원, 거래처, 소비자 등의 개인정보를 처리함에 있어 국내 "개인정보보호법"에 의한 규제 대상이기 때문에 이에 대한 적절한 대응 방안을 마련하여야 하나, 현재까지 외국법인들이 국내 법인들과는 다른 대응전략을 구축하여야 하는지, 추가적인 대응전략에는 어떤 것이 있는지 구체화 된 기업 지침이 없는 상태이다[1].

본 연구는 국내 외국법인의 성공적인 "개인정보보호법" 대응전략 사례에 대한 연구로서 본 연구 결과를 다른 외국법인들에게도 공통적으로 적용할 수 있도록 기본 워크프레임을 구축하고자 하는데 그 목적이 있다. 본 사례 연구의 대상인 외국 글로벌 기업 C사의 경우 2011년부터 사내에 개

인정보보호 전문가를 양성하며 체계적이고 성공적인 개인정보보호 대응 TFT를 운영하여왔다. C사의 개인정보보호법 대응 TFT 활동 내용에 대한 사례연구를 통하여 국내 기업 뿐 아니라 외국 기업들도 참조할 만한 성공 사례를 소개하고 이 사례를 PIMS(Personal Information Management System) 모델로서 설명하여 기업의 실질적인 대응전략을 제시하고자 한다.

1.2 연구 방법론

본 연구는 Yin의 정의에서와 같이 Real-Life context내에서 사례의 현상을 심층 깊게 연구하는 경험적 질적연구방법론(Qualitative Approach)인 단일사례연구 방법론을 사용하였으며[2] 이를 구체화하기 위해 Woods and Catanzaro가 제시한 현상의 배경, 상태, 상호작용 등을 심층적으로 조사 분석하는 연구 기법을 적용하여 전개하였고[3] 아울러 John W. Creswell의 저서 Qualitative Inquiry and Research Design 2E에서 내러티브, 현상학, 근거이론, 문화기술지 그리고 사례연구 방법론을 설명하는 Choosing Among Five Approaches 중에서 사례연구 방법론을 활용하였다[4]. C Corporation의 개인정보보호 준수 TFT 운영의 배경과 그 상세 활동 내용 등에 대해 TFT 활동 내용 위주로 사례를 분석하고, TFT 운영 이후 개선되어 적용된 주요 내용을 정리하여 10가지 전략과 4가지 제언을 개발 하였다. 본 사례와 관련된 자료는 개인정보보호법 대응 TFT 운영 회의록, TFT 멤버들의 이메일 내용, TFT 산출물 및 TFT 리더와의 인터뷰 내용 등을 정리하였다. 본 사례는 기업보안상의 특성으로 인해 기업의 실명 및 개인정보보호 TFT 구성 인원들에 대한 실명 등은 공개하지 않으나 사례의 전반전인 내용을 확인하여 모델로 삼기에는 문제가 없도록 구성하였다.

2. 이론적 배경

2.1 개인정보 유출과 개인정보보호법

개인정보보호 종합지원 포탈에 의하면 개인정보보호법은 세계 각국과의 FTA 대비 및 IT 강국으로서의 위상확보와 개인정보의 유출 및 오·남용 등의 근절을 통해 안전하고 신뢰받는 정보사회를 구현하기 위해 마련되었다고 선언하고 있다[8]. 2000년대 초반부터 급속도로 발전하기 시작한 국내 컴퓨터 통신이 기업의 주요 활동영역으로 자리 매김하면서 역 효과중 하나로 기업들의 무분별한 개인정보 수집과 기업들의 관리부주의 및 의도적인 개인정보 침해로 인한 정보주체의 피해를 막고 정보주체인 국민들을 보호하기 위해 2003년부터 관련법 제정이 논의되어 왔으나, 이후 여러 가지 이유로 인해 법 제정이 늦어지며 2008년 9월 GS칼텍스, 2010년 3월 신세계몰, 2011년 4월 현대캐피탈, 2011년 7월 SK컴즈, 2011년 12월 삼성전자, 2012년 7월 KT 등 여러 차례의 대규모 개인정보 침해 사건들이 발생 하였다. 개인정보 침해신고는 2007년 847건이던 것이 2011년 2,556건으로 증가하였고 상담 건수도 2007년 2만 5,118건에서 2011년 11만 9,659건으로 5배 이상 증가 하였다.

지속적으로 증가하고 있는 개인정보유출 사고는 기업의 주요한 보안위협 요소가 되고 있다. 이에 대해 한창희(2011)는 개인정보유출로 발생하는 경제적 피해규모에 대해 총 피해액은 유출사고 대응비용(시간당 인건비*총 인력 투입시간), IR 대응비용(브랜드 보호를 위한 광고비), 고객 감소로 인한 수익 손실(고객 1인당 수익 발생 측면 가치 * 이탈한 고객수), 유출된 정보의 가치(법적비용 + 보상받지 못한 개인의 정보가치), 관련 산업 파급효과(산업 연관표 중 유발계수를 이용한 산출) 등을 모두 합한 비용이라고 한다[5]. 이 경우 그 비용은 각 사례별로 다르겠지만 최근과 같은 대량 유출사고의 경우 기업의 존폐를 위협하는 비용이 될 수 있다. 김정연(2013)은 반복되는 개인정보 유출로 인해 상장기업의 주가에 대해 해당 사건이 기업에 부정적인 영향을 주고 있으며 일시적이나마 기업 가치에 음의 영향을 미치는 결과를 보여준다고 주장 한다[6].

이러한 개인정보침해에 의한 피해는 비단 우리나라만의 문제는 아니다. 국외 여러 다른 나라들도 우리와 비슷한 상황에 놓여있기 때문에 미국의 경우 2011년 3월 상원법안 761, 2011년 6월 세이프 데이터법, 2012년 1월 모바일 디바이스 개인정보보호법 등을 제정하였으며, EU역시 2012년 1월 정보보호법(잊혀질 권리) 개정안을 확정하였으며, 영국은 2012년 5월 개인정보보호 지침(E-Privacy)을 발효하였고, 중국은 2012년 4월 개인정보보호 가이드라인을 제시하였으며, 일본은 2012년 8월 스마트폰 개인정보보호 이니셔티브라는 지침을 추가적으로 제시하였고 캐나다는 2004년 1월 개인정보보호 및 전자문서법을 시행하고 있다[7].

우리나라의 개인정보보호법은 2011년 3월에 공포되었으며, 6개월 이후인 2011년 9월 시행되었고, 이듬해인 2012년 4월부터 유예기간 종료에 따라 법적 강제력을 발휘하게 되었다. 이 법의 시행으로 인해 분야별 개별법에 따라 시행되던 개인정보 보호의무 적용대상이 공공 및 민간부문 모든 분야에 걸쳐 확대 적용되었으며, 컴퓨터 등에 의해 처리되는 정보 이외의 각종 종이문서에 기록된 개인정보도 보호 대상으로 확대 적용되었으며 2013년 8월 법 일부 내용이 개정되어 개정된 내용은 2014년 8월부터 적용된다[8].

본 법의 세부 내용을 보면 고유식별정보(주민등록번호, 여권번호, 운전면허번호 등)의 처리를 원칙적으로 처리 금지토록 하였고, 또한 영상정보 처리기기에 대한 규제 내용도 추가 되었으며 개인정보 수집·이용 및 제공에 대한 상세 지침이 마련되어있고, 개인정보 유출 사고발생시 정보주체에게 유출 사실을 통지해야할 의무 및 관계기관에 신고해야할 의무 또한 기록하고 있다. 이러한 개인정보보호 및 처리에 대한 종합적인 일반법으로서 기존의 개별법에 의한 규제의 불합리성을 해소하고 실질적인 개인정보보호 활동을 강화하는 강력한 법령으로서 제정되었다. 법 시행이후 약 17개월 만에 관련법이 더욱 강화되는 개정안이 만들어졌고 이는 2014년 8월부터 강제력을 가지게 된다. 개정된 내용은 다음 같다.

개정안 변화1, 법 24조의 2(주민등록번호의 처리제한), 주민등록번호에 대한 처리를 위해 기존에는 정보주체의 동의가 있는 경우 처리가 가능하였으나 법 개정 이후 정보주체의 동의가 있더라도 다음의 3가지 경우가 아니라면 주민등록번호 수집 및 이용이 제한된다. 첫째 법령에 구체적인 근거가 있는 경우, 둘째 급박한 생명, 신체, 재산상 이익을 위해 명백히 필요한 경우, 셋째 안행부령

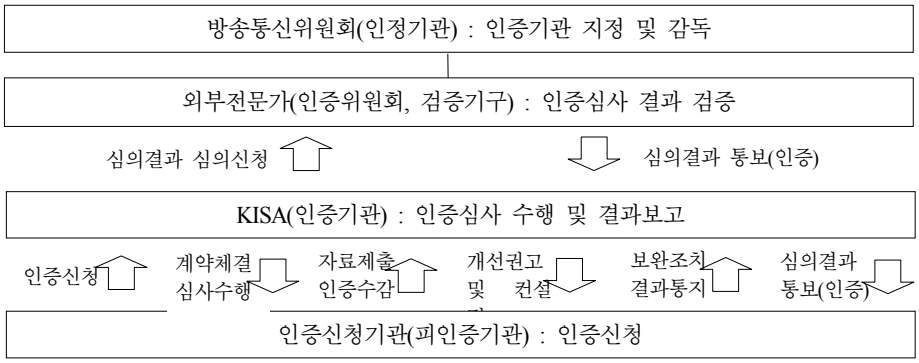
으로 정하는 경우. 또한 기존의 주민번호 수집금지 조항이 온라인에 국한되어 있었으나 이를 온라인 및 오프라인 모두에 적용하고 있다.

개정안 변화2, 법 제34조의2(과징금의 부과 등), 처벌 조항이 구체화 되고 과징금 상한선이 정해졌다. 주민번호 분실, 도난, 유출, 변조 및 훼손시 5억원 이하의 과징금을 부과, 징수 할 수 있게 되었다.

개정안 변화3, 법 제65조 2항(고발 및 징계권고), 법규 위반시 책임 있는 자 징계를 권고 할 수 있도록 되어 있었으나 이를 책임 있는 자(대표자 및 책임 있는 임원)징계를 권고 할 수 있도록 수정하여 기업의 대표자와 관련 임원의 책임을 더 강조하고 있다. 앞으로도 본 법과 관련하여 더 많은 논의들이 수행되고 실무적인 지침 역시 강화될 것이다[9].

2.2 개인정보 관리체계(PIMS : Personal Information Management System)

PIMS(Personal Information Management System)는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위해 필요한 관리적, 기술적, 물리적 보호활동에 대한 표준을 제시하여주고, 이에 따라 기업 내 개인정보보호활동이 정상적으로 이루어지고 있는지 정부가 확인해 주는 인증제도이다. 인증제도의 객관성 및 신뢰성 확보를 위해 인정기관, 인증위원회, 인증기관을 분리하여 운영하고 있으며, 인증제도를 관리·감독하는 업무는 방송통신위원회가 직접 수행하고 산업계·학계·정부의 전문가로 구성된 인증위원회를 구성하여 인증결과를 심의하고 있고, 한국인터넷진흥원을 인증기관으로 지정하여 심사의 객관성을 확보하고 있다. 인증체계 구성은 [그림 1]과 같다[10].



[그림 1] PIMS 인증체계 구성

[Fig 1] PIMS Authentication Scheme

PIMS는 기업이 자율적으로 심사를 신청하도록 하고 인증기관이 일정 수준 이상의 기업에게 인증을 부여하는 제도로서 “정보보호관리체계 인증 등에 관한 고시(제2010-3호)”를 준용으로 운영되고 있다. 따라서 본 인증 제도는 기업이 반드시 따라야 할 법적 구속력은 없으나, 본 인증을 받는

과정에서 기업 내 개인정보보호 관리체계가 법적 요건을 충족할 수 있는 기반을 구축할 수 있다. 또한 인증을 득한 기업에서 개인정보 사고 발생 시 과징금 및 과태료를 경감 받을 수 있다.

PIMS 심사 기준은 개인정보보호를 체계적이고 주기적으로 수행하고 있는지 점검하는 항목으로서 관리과정 요구사항(정책수립, 범위설정, 위험관리, 구현, 사후관리)항목과 개인정보를 안전하게 보호하기 위한 관리적, 물리적, 기술적 보호조치를 점검하는 보호대책 요구사항(정책 및 조직, 개인정보분류, 교육 및 훈련, 인적보안, 침해사고 대응, 기술·물리보호조치, 내부검토 및 감사)항목 그리고 개인정보 생성에서 파기까지의 법률준수 여부를 점검하는 생명주기 요구사항(수집, 관리 및 파기, 이용 및 제공)항목이 있으며 이 3개 항목에 대해 118개의 통제항목과 325개의 세부점검 사항으로 구성되어 있다. PIMS의 구성요소를 간략히 정리해 보면 [그림 2]와 같다[10].

관리과정 요구사항	개인정보보호를 체계적이고 주기적으로 수행하고 있는지 점검하는 항목
보호대책 요구사항	개인정보를 안전하게 보호하기 위한 관리적, 물리적, 기술적 보호조치를 점검하는 항목
생명주기 요구사항	개인정보 생성에서 파기까지의 법률준수 여부를 점검하는 항목

[그림 2] PIMS 구성요소

[Fig 2] PIMS Components

김정덕(2008)은 “개인정보보호를 위한 관리체계와 거버넌스”에서 체계적인 개인정보보호 관리의 필요성에 대해서 ‘방화벽, 안티바이러스 등 보안기술 솔루션이나 정책서, 지침 등 문서의 존재 및 작동 유무를 확인하는 정보보호 통제 중심의 접근방법이라기 보다는 정보보호가 지속적인 경영활동의 하나로서, 정보보호 프로세스 중심의 접근방법이라는 점이다.’라고 주장한다[11].

심미나(2010)는 ‘효율적인 개인정보관리체계(PIMS) 인증제도 도입방안 연구’에서 PIMS 인증제도는 개인정보보호를 위한 PIMS가 일회적 보호조치가 아닌 체계적이고 지속적인 관리활동이 가능하도록 하는 체계를 구성하는지와 동시에 국제적인 개인정보보호 원칙과 국내외 개인정보보호 법률 및 규정의 요건 충족, 이에 부합하는 관리적, 물리적, 기술적 보호조치를 포괄하는지에 대한 적합성 평가를 수행하고 이를 보증하는 것‘이라고 의미를 부여하고 있다[12].

서영수(2012)는 ‘A Study on the Factors Affecting the Establishment of Personal Information Management Systems(PIMS)’에서 PIMS를 기업에 적용하는 활동이 기업의 영업성과를 향상시키고, 기업의 조직 능력과 자원이 PIMS를 구축하는데 주요한 요소이며, PIMS를 구축하는데 수반되는 어려움들도 기업이 마다하지 않고 있다고 파악하며 이제는 PIMS를 활용한 기업 내 개인정보보호 활동이 각 기업의 주요 현안으로 부각되고 있다고 주장한다[13].

전진환(2013)은 '개정 고시에 따른 개인정보보호 관리체계(PIMS)인증의 주요변화'에서 2013년 9월 방송통신위원회의 의결을 통한 개정 [개인정보보호 관리체계 인증 등에 관한 고시]에 대해 연구하여 인증기관 지정 및 인증 취득을 준비하는 개별 기업의 이해를 돕고자 설명하고 있다[14].

박은엽(2011)은 '개인정보보호 관리체계 인증제도 구축 사례 연구'에서 국·내외의 주요 개인정보보호 관리체계 동향을 비교·분석하고 국내 환경에 적합하도록 개인정보보호에 특화된 개인정보보호 관리체계 인증제도를 소개하고 구축에 필요한 방법을 사례를 들어 설명하고 있다[15].

박대하(2013)는 "클라우드 서비스 환경의 개인정보 위탁을 위한 개인정보보호 관리체계 통제 연구"에서 클라우드 서비스 제공자들에게 개인정보의 처리를 위탁하고자 하는 처리자 들이 국내 개인정보보호법 준거 여부를 파악할 수 있도록 PIMS를 비롯한 각국의 다양한 개인정보보호 인증 시스템에 대한 연계 개발이 필요하다고 주장하고 국제표준 인증시스템 필요성에 대해 역설하고 있다[16].

여러 연구자들이 다양한 각도에서 PIMS 및 기타 개인정보보호 통제 및 인증제도에 대해 연구결과를 발표하며 각 기업들의 PIMS 활용의 필요성에 대해 언급하고 있다. 나아가 자발적인 인증 취득 노력이 결과적으로 기업의 개인정보보호 활동에 긍정적인 영향을 주며 실질적인 업무 개선을 이룰 수 있다고 주장하고 있는 것이다. C사의 경우 직접적인 PIMS인증을 수행하지는 않았지만 PIMS의 인증기관인 한국인터넷진흥원에서 2011년 개발한 개인정보보호 수준 자가점검표를 활용하여 자가 진단을 수행하여 C사의 개인정보보호 TFT 업무 활동을 검증하였다.

3. C사의 개인정보보호 TFT 운영 사례연구

3.1 C사의 소개

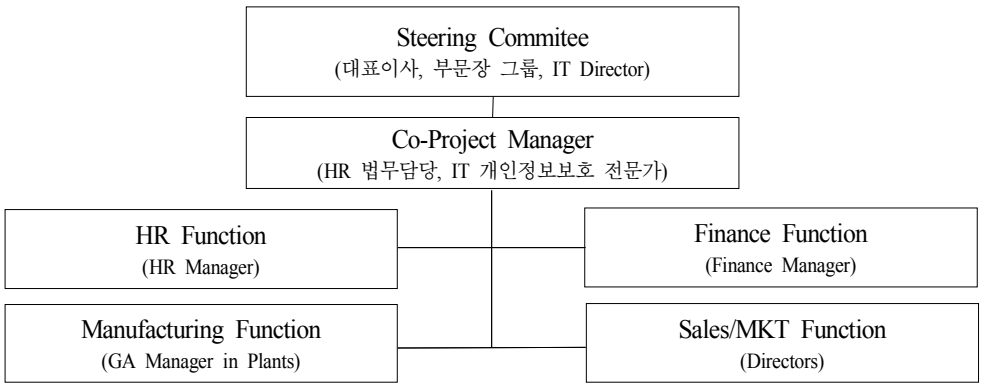
C사는 100여 년 동안 전 세계에 식품소재에 대한 솔루션과 혁신을 제공하여온 글로벌 다국적 회사이며 다양한 산업분야에 1차 원료를 공급하는 선도적인 소재기업으로 거듭나기 위해 노력하고 있는 회사로서 1908년 일리노이 주에서 세탁용 전분 제품을 출시하며 설립되어 졌다. 이후 1919년 캐나다 최대 옥수수 가공업체를 인수 합병하며 그 규모를 키웠으며 국내에는 1930년부터 영업활동을 시작하였다. 1940년 페니실린 원료 등 군수 및 민간용으로 서비스를 확대 하였고 1955년 제지산업에 널리 사용되는 양성전분을 출시하고 2009년에는 포브스가 선정하는 미국 내 가장 잘 관리되는 회사 5위로 선정되었으며 현재는 전 세계 30개 국가에 관련 회사를 운영하고 있고 이중 약 10여개 나라가 아시아에 위치하고 있다. 현재 국내법인은 직원 수 약 300명 정도이며 업종으로는 음식료품 및 제조업으로 등록되어 있고 비즈니스 형태는 1차 식음료 원재료를 가공업체에 납품하는 B2B형태로서 2012년 매출액은 약 3,300억 원 이다.

3.2 개인정보보호 TFT 운영 배경

2003년 전자정부 31대 과제 중 하나로 선정된 개인정보보호법이 우여곡절 끝에 드디어 2011년 3월 29일 공포되고 9월 30일 시행되었다. 이 법은 개인정보에 관한 일반법으로서 다른 법률에 특별한 규정이 있는 경우를 제외하고는 모든 개인정보처리자에게 적용된다. 이 법 시행 이전에는 공공기관의 개인정보보호법에 관한 법률 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 여러 개별 법에 따라 약 50만 개의 기관, 단체 및 사업자가 부분적으로 규율을 받았었지만, 이 법의 제정으로 인해 공공, 민간부문 및 온·오프라인을 포함하여 헌법기관, 민간사업자, 비영리단체, 개인 등 약 350만 여개의 개인정보처리자가 추가로 개인정보보호법의 제제 대상이 되었다. 이러한 시대적인 배경과 법규준수의 필요성에 따라 C사의 경우 2011년 상반기부터 관련 법규 내용에 대해 유의 주시하여 왔으며 하반기에 개인정보보호법 대응 TFT를 운영하기에 이르렀다.

3.3 개인정보보호 TFT(Task Force Team) 조직

C사는 2011년 상반기부터 관련법에 대하여 주기적인 모니터링을 실시하여 왔으며 안전행정부와 한국인터넷진흥원에서 실시하는 개인정보보호 전문가 교육에 사내 전산부서 담당자를 파견하여 전문가 과정을 수료하게 하였으며 여러 가지 배포 자료와 세미나 등을 통해 개인정보보호 전문가를 사내에서 지속적으로 육성하는 등 회사 임원들의 심도 있는 관심과 실질적인 지원 속에 개인정보보호법 준수를 위한 대응을 준비하여 왔다. 2011년 9월 29일 임원회의 결과에 따라 개인정보보호법 준수를 위한 TFT(Task Force Team)를 다음 [그림 3]과 같이 구성하였으며 TFT 활동을 통해 기업 대응 전략을 마련하게 되었다.



[그림 3] 개인정보보호 TFT 조직도

[Fig 3] Privacy Protection TFT Org

대표이사와 부문장 그룹 및 IT Director로 구성되어진 Steering Commitee의 적극적인 지원 아래 Co-Project Manager는 HR의 법무담당자와 IT부서의 개인정보보호 전문가 두 사람이 공동으로 맡게 되었으며 HR의 법무 담당자가 TFT 운영 일정 및 결과물 도출을 담당하였고 전산부서 담

당자는 개인정보보호법 지침해설 및 기술적 조치 사항에 대해 자문하는 역할을 담당하였다. TFT 활동 결과는 주기적으로 임원회의(Steering Committee)에 보고하여 회사 전반의 정책에 반영하였으며 모든 조직의 합의(Consent)를 도출하기 위해 각 Function에서 TFT 멤버들을 지정하여 TFT 활동에 참여하게 하였다. TFT 멤버들의 일정을 일률적으로 조정하여 활동을 하기에는 무리가 있어 화상회의 시스템, 이메일, 그룹웨어 시스템 등 사내 커뮤니케이션 툴을 총 동원하여 원활한 의사소통을 유지하도록 하였다.

3.4 개인정보보호 TFT 활동 내용

2011년 3월 29일 개인정보보호법 공포에 따라 IT 부서에서 관련 정보를 정보보안활동의 일환으로 기초 자료를 수집하기 시작하였으며 9월 30일 법 시행시기 이전까지 약 6개월 동안 보안담당자가 임원회의에 요약 자료를 주기적으로 보고하였다. 임원회의 검토에 따라 IT 보안담당자가 개인정보보호법 관련 상세 정보를 9월 법 시행이전까지 정리 요약하여 기업 대응 방안에 대한 1차 준비사항을 정리보고하기로 하여 인터넷진흥원, 안전행정부 등 기타 관련 기관에 문의하였으며 인터넷진흥원에서 운영하는 “개인정보보보 전문가”과정을 수료하여 상세 내용을 습득하였다. 9월 마지막 임원회의에 관련 자료를 요약 정리하여 보고하였으며, 이에 따라 임원 결정에 의해 개인정보보호를 위한 TFT를 운영하고 최종적으로 2012년 상반기까지 관련 대응책 마련과 관련 조직 운영을 시작하기로 하여 다음과 같은 실질적인 TFT운영 활동이 시작되었다.

2011년 10월 7일(금) 오후 5:30분경 HR 법무담당 매니저, IT 개인정보보호 전문가, 회계부서 매니저, 마케팅부서 매니저, 총무부서 매니저, 공장관리부서 매니저, 영업부서 매니저 등 7명이 참석하여 TFT Kick off Meeting을 수행하고 이후 운영 방안에 대해 논의 하였으며 상기 논의에 따라 각 부서별 활동이 이루어 졌다.

TFT운영 초기 가장 큰 첫 번째 과제는 TFT 멤버를 선정하는 것이었다. 초기 멤버는 각 부문 내 임원 1인과 담당자 1인으로 구성하여 운영을 시작하였고 TFT 리더는 개인정보보호법을 연구하고 임원회의 자료를 작성했던 IT 개인정보보호전문가와 HR부서의 법률관련 담당자가 함께 담당하기로 하였다. 그러나 TFT운영 과정 중 각 부서에서 직급이나 직책과 상관없이 실질적인 업무 내용 중 개인정보보호와 관련된 업무를 담당하는 담당자가 포함되어야 한다는 합의에 의해 임원은 TFT 운영 지원의 역할(업무조정, 업무시간 재배치 등)로 변경하고 실제 업무 담당자가 추가적으로 포함되었다. 이후 관련 멤버들은 주 1회, 주기적인 회의를 통해 관련 업무 진척 사항을 보고하는 방식으로 TFT활동이 이어졌다.

TFT 활동 중 주요 핵심 내용 중에 하나는 기존 업무 중 개인정보보호법과 관련 있는 내용을 파악하여 리스트 하는 것이었다. 기존의 각 부서 내 업무 내용 중 개인정보를 다루는 업무가 어떤 것들이 있는지 전체 업무 리스트를 나열하고 관련 업무 담당자가 누구인지 파악하여 관련법과 비교하여 필요 없는 부수적인 업무는 과감히 삭제하고 타 부서와 동일하게 수행되는 중복되는 업무

의 경우는 임원들의 합의를 거쳐 한 부서로 업무를 통합하였다. 예를 들면 신규 대리점 개설시 영업부서, 고객지원부서, 구매부서 및 회계부서 등에서 동일하게 관리하는 대리점 관련 정보 수집 및 계약서 관련 업무를 영업부서 한 곳으로 일원화 하는 등 개인정보를 다루는 업무 중 중복된 업무를 한 부서로 일원화 하였다. 부서별 주요 업무 내용은 다음과 같다.

HR부서에서는 임직원의 개인정보에 대한 대응책에 대해 TFT리더의 조언과 법률 검토를 통해 개인정보보호 조직 안을 마련하고 개인정보 내부관리계획을 제정하였으며 임직원의 개인정보 처리를 위해 신규사원 입사 시에 적용할 양식으로 "개인정보보호 활용 동의서", "개인정보 제3자 제공 동의서", "개인정보 해외제공 동의서" 등을 개발하였다. C사의 경우 글로벌 회사로서 모든 임직원의 정보가 해외에 있는 HRM(Human Resource Management) 시스템에 저장되기 때문에 개인정보보호법 제3장 개인정보의 처리, 제17조 개인정보의 제공, 제2항에 의해 "개인정보 해외제공 동의서"가 필요하였다. 이와 관련하여 아시아지역 본부의 HR부서 법무담당자와 국내 HR 법무담당자 간에 이메일 교신을 통해 관련 내용을 파악 및 조정하여 국내법 준수에 문제가 없는 내용으로 관련 동의서가 작성되었다.

영업부서에서는 영업활동과 관련한 대외 활동 중에 발생할 수 있는 개인정보처리 업무를 파악하여 필요 없는 활동은 과감히 폐기하기로 하였다. 예를 들면 영업사원들이 고객과 미팅을 수행하는 경우 일일 미팅 보고서를 작성할 때 고객에 대한 상세 개인정보까지 기록(개인의 성향 및 기타 관련 사항)하도록 되어 있었으나 고객의 개인 정보를 보고 내용에 포함하지 않기로 합의 하였다. 이는 C사와 같은 글로벌 회사의 경우 CRM 시스템의 서버가 해외에 위치하고 있기 때문에 고객관련 미팅 정보 중 국내법에서 제한하고 있는 개인정보제공동의 및 해외제공 동의를 받기 어렵기 때문에 반드시 필요한 미팅 내용 이외의 개인정보 부분은 포함하지 않기로 하였다.

구매부서 및 회계부서에서는 대리점 및 협력업체 정보 처리과정에서 개인사업자의 경우 개인사업자의 계좌정보를 포함한 개인정보를 수집할 수밖에 없기 때문에 관련서류에 "개인정보제공 동의서"를 추가하였다.

IT부서에서는 Intranet 시스템에 운영의 편의를 위해 임직원의 개인 정보를 활용하기 위해 여러 시스템에 나누어져 등록되어 있던 자료를 HRM 시스템 한곳으로 일원화하여 관리하여 개인정보보호의 해킹 위험성을 최소화 하였으며 임직원의 급여계좌정보, 주민등록번호 등 민감정보는 시스템에서 암호화(마스킹) 처리하도록 시스템 운영회사와 협의하여 개인정보보호법에 명시된 시스템 보안강화를 수행하였다.

2012년 상반기 조직 내 임직원 및 협력업체 직원을 포함하여 개인정보보호 사내 교육 수행을 완료하였으며 이후 신규 직원 채용 시 OJT(On the Job Training) 프로그램에 IT정보보안 교육 프로그램에 관련 내용을 추가로 진행하고 있다.

개인정보내부관리계획과 별개로 2013년부터 업무와 관련하여(감사 및 수사 등)필요시 개인정보(이메일, 개인폴더 등 포함)에 접근해야 하는 경우 아시아 지역 임원의 결재 및 IT보안부서, 본사 CIO(Chief Information Officer)의 결재를 득하여야 타인의 개인정보를 확인할 수 있도록 지침을

운영하고 있다.

2014년부터 HR 법무담당자가 필요시 내부 개인정보보호 업무지침 준수여부 파악을 위한 내부 감사를 수행할 수 있도록 개인정보 내부관리계획을 개정하였다. 개인정보보호 대응 TFT 주요 활동 내용과 이후 개인정보보호 조직의 주요 활동 내용을 일자 및 시간대 별로 정리하면 다음 [표 1]과 같다.

[표 1] 주요 활동 내용 요약
[Table 1] Summary of main activities

일자	주요 활동 내용 요약
2011년 10월 07일	TFT Kick Off Meeting, 개인정보보호법 요약 자료 공유 및 향후 TFT 운영 방안 협의
2011년 10월 10일	Kick Off Meeting 시 협의된 사내 개인정보보호법 체크리스트 공유
2011년 10월 17일	개인정보 수집 동의서 내용 공유 및 의견 수렴
2011년 10월 20일	2차 TFT 정규 모임, 개인정보보호 정규 조직안, 보고 체계, 취급자 업무 평가 방법, 직무리스트, 동의서 내용 등 검토 및 사내 교육 수행 방안 논의, Finance 개인정보보호관련 업무 Process 정리 및 보완점 논의, HR & GA, 외국에 있는 국내 직원들의 인사정보시스템 운영시 문제점 논의, 세법에 의한 원천징수 작업 시 직원 가족들에 대한 개인정보 수집과 관련된 Process 점검
2011년 10월 27일	개인정보 책임자 및 개인정보 취급자에 대한 법정 지정요건 검토
2011년 11월 03일	홈페이지 인사채용과 관련된 Data Privacy Statement에 대한 APAC 법무 담당자와 검토
2011년 11월 04일	홈페이지의 개인정보취급 방침 수정
2011년 11월 09일	개인정보보호법 조직 및 각 부서별 개인정보 취급자 선정 및 주요 직무와 감사 대비 준비 사항 논의
2011년 11월 10일	TFT 활동 멤버 수정 논의 및 TFT 활동 종료 시기 및 개인정보 책임자와 취급자에게 업무 이관 논의
2011년 11월 15일	개인정보 제3자 및 해외 제공 동의서 내용 검토 및 수정
2011년 11월 16일	임원회의 최종 보고자료 공유 및 검토
2011년 11월 30일	TFT 운영 산출물 최종 검토 - 각종 양식류
2011년 12월 01일	개인정보보호팀 신설 최종 검토
2012년 01월 30일	개인정보 내부관리계획 최종 검토
2012년 03월 14일	개인정보 내부관리계획 제정 및 개인정보보호 조직 운영
2012년 04월 10일 ~ 05월 04일	4차례에 걸쳐 전 직원 및 협력업체 직원을 대상으로 개인정보보호법 및 규정 교육 시행
2012년 06월 20일	개인정보보호 감사툴 도입 결정
2013년 08월 02일	개인정보보호관리규정 1차 개정

3.5 개인정보보호 TFT 운영 결과 지표

C사의 개인정보보호법 대응 TFT 활동은 공식적으로 2012년 3월 14일 개인정보보호 조직이 운영되면서 종료되었다. 상기 TFT운영에 대한 최종 결과는 개인정보보호 조직 운영 1년이 지난 2014년 2월에 진행된 개인정보보호 수준 평가 지표로 확인할 수 있다. C사의 경우 개인정보보호 TFT 활동 초기에 한국인터넷진흥원에서 개발하여 배포하였던 개인정보보호 수준평가 자가 검검표를 활용

하여 2011년 10월을 기준으로 자가 점검을 실시하였다. 상기 점검기준은 “개인정보의 수집 및 이용”, “개인정보의 제공 및 위탁”, “개인정보의 관리 및 파기” 그리고 “개인정보 주체의 권리보장”이라는 4가지의 영역에 대하여 23가지 질문 항목으로 이루어져있다. 2011년 자가점검 결과는 100점 만점으로 환산하여 약 25점을 득점하였다. 2012년 2월까지의 개인정보보호 TFT 운영 및 이후 이어진 개인정보보호 조직의 업무 시작 후 약 2년이 경과한 2014년 2월에 동일한 자가점검표를 사용하여 개인정보보호 실태를 조사하였다. 그 결과 100점 만점 기준에 약 69.25점을 득점하여 2년 전에 비해 많은 향상이 이루어졌으나 추가적으로 보완해야 할 항목들도 여전히 있는 것으로 확인되었다. 2차 점검 상세 내용 중 현재는 수행되지 않는 내용들 중 일부 시행 가능한 부분을 보완하면 최대 87.65점 까지도 점검결과를 상향시킬 수 있는 것으로 보고되었다. 아래의 자가점검표는 2011년 한국인터넷진흥원에서 개발한 질문지표로서 일반기업이 사내 개인정보보호 실태를 간단히 확인하여 볼 수 있는 가장 간단한 지표였으므로 C사는 앞으로 PIMS 등과 같은 좀 더 세밀하게 개발된 도구를 통해 지속적으로 사내 개인정보보호 업무 실태를 점검할 계획이다. 당시 사용되었던 자가 점검표 내용은 [표 2]와 같다.

[표 2] 개인정보보호 수준 자가점검표

[Table 2] Self-Checklist of Privacy Protection Level

구분	질문항목
개인정보의 수집 및 이용 (25점)	개인정보 수집 시 정보주체들에게 동의를 받고 계십니까?
	개인정보 수집 시 기본정보(필수정보)와 추가정보(선택정보)를 구분하고 계십니까?
	개인과 관련된 민감한 정보(ex 유전, 범죄사실)을 수집하고 계십니까?
	정보주체의 고유식별정보(주민번호, 여권번호, 운전면허번호, 외국인 등록 번호 등)를 수집하고 계십니까?
	정보주체의 주민번호 이외의 대체수단(공인인증서, i-PIN 등)을 이용하여 본인확인을 하고 계십니까?
	수집된 개인정보를 동의 받은 수집/이용 목적 이외로 이용하고 계십니까?
개인정보의 제공 및 위탁 (25점)	수집된 개인정보를 제3자(다른 사업자)에게 제공하고 있습니까?
	제3자에게 제공할 경우 이에 대해 정보주체에게 고지 및 동의를 받고 있습니까?
	개인정보 관리 및 처리 시스템을 위탁하고 계십니까?
	개인정보 관리 및 처리시스템 위탁 시 이에 대해 해당 사실에 대하여 정보주체가 확인하기 쉽도록 공개하고 있습니까?
	개인정보 관리 및 처리시스템 위탁 시 위탁업체와의 계약사항에 안전 조치 의무 사항을 계약서에 포함하여 계약하고 있습니까?
개인정보의 관리 및 파기 (25점)	개인정보보호를 위해 개인정보보호 책임자를 지정하고 있습니까?
	개인정보 수집, 이용,제공, 파기 등의 내용이 담긴 개인정보 처리방침을 작성해 정보주체가 쉽게 확인할 수 있도록 공개하고 있습니까?
	개인정보 취급 시에 개인정보의 분실, 누출, 변조, 훼손을 방지하기 위한 기술적, 관리적 물리적 보호조치를 취하고 있습니까?
	개인정보보호를 위해 별도의 개인정보보호 내부관리계획을 수립해 이행하고 있습니까?
	내부관리계획에 준하는 개인정보보호 관리기준을 보유하고 있습니까?
	수집된 개인정보를 파기하는 시점이 별도의 절차를 통해 이뤄지고 있습니까?
	사내에 CCTV를 설치 운영하고 계십니까?

	CCTV 설치 시 정보주체가 쉽게 인식할 수 있도록 안내판을 설치하고 계십니까?
	CCTV 설치 운영시 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 안전성 확보 조치를 갖추고 계십니까?
개인정보 주체의 권리 보장 (25점)	정보주체의 권리를 보장하기 위해 열람요청, 정정요청, 삭제요청, 처리중지 요청 등의 절차를 갖추고 계십니까?
	만 14세 미만 아동의 개인정보 수집 시 이에 대한 법정대리인의 동의를 받고 계십니까?
	개인정보 유출 시 정보주체에게 알리는 절차가 마련돼 있습니까?

3.6 개인정보보호 TFT 리더와의 인터뷰 내용

2014년 2월 24일 오후 6시부터 8시까지 약 2시간 정도 서울특별시 강남구에 위치한 C사의 12층 소회의실에서 C사의 개인정보보호 TFT 리더와 인터뷰를 진행하였다. 상기 인터뷰를 통하여 TFT운영 관련 기록만으로는 판단하기 어려웠던 점이나 TFT운영 이후의 업무개발 계획 등을 판단할 수 있다. 외국인 회사로서 Compliance 관련하여 Legal Counsel 아시아 담당자와 국내 개인정보보호법 시행에 대해 상세 협의 과정이 오래 걸렸으며 그 과정에서 용어에 대한 영문 번역에 많은 시간이 투자되었음을 볼 수 있다. 또한 TFT운영 중반 이후부터 임원들의 좀 더 적극적인 지원이 필요했음을 확인할 수 있다. 인터뷰 전문은 다음 [표 3]과 같다.

[표 3] 인터뷰 내용
[Table 3] Interview

질문 : 회사와 본인에 대해 소개 부탁드립니다.
답변 : 는 C사의 HR&GA Function의 ***부장이라고 합니다. 저희 회사는 세계시장을 선도하는 100년이 넘은 회사로서 전 세계 약 40여 개국에 진출하였으며 약 11,100여명의 근로자가 근무하고 있고 본사는 미국 일리노이주의 웨스트체스터에 있습니다.
질문 : 개인정보보호 TFT 리더로서의 담당 업무 내용에 대해 설명해 주시기 바랍니다.
답변 : 2011년 당사의 개인정보보호 TFT리더 역할을 수행하였으며 주요 업무는 당사 개인정보보호 규정 제정, 조직 설계, 관련 업무 절차 구축 및 시스템 도입 등이었으며 TFT 종료 후 개인정보보호 담당자 업무를 지속하고 있습니다.
질문 : 개인정보보호 TFT를 운영하게 된 배경에 대해 설명 부탁드립니다.
답변 : 당시 사회적인 분위기에 따라 전반적인 개인정보보호법 제정 및 강제 적용 법규에 대한 인식은 공유되었으나 개인정보보호가 당사에 어떤 영향(비지니스)이 부여될지 정확히 파악하지 못하고 있었습니다. 그러나 최소한의 개인정보보호를 위한 제도적 장치가 필요하다는 공감대가 형성되었으며 CEO 및 임원들도 상기 내용에 대해 회사 차원의 대응 필요성을 느끼게 되어 '개인정보보호 TFT'를 운영하게 되었습니다. 당시 TFT의 주요 업무 목적은 법규 관련 대응 방안 및 시스템 도입의 필요성 등을 파악하고 '개인정보보호 조직'을 구축하는 것이었습니다. 당시 임원들은 개인정보보호 책임자가 되는 것을 기피하는 분위기였습니다. CEO의 경우 최소한의 요건만 갖추는 것으로 만족하는 정도의 수준이었고 당사는 카드사나 소비재를 다루는 회사와는 달리 B2B 회사로서의 특성으로 개인고객 정보가 많지 않았기에 임원들은 개인정보관련 리스크가 많지 않다고 판단하였습니다.

질문 : TFT 운영의 주도적인 역할을 기업 내 어느 부서에서 수행하였는지 또 왜 해당 부서가 주도적인 역할을 수행하게 되었는지 본인의 의견을 부탁드립니다.
답변 : 당사의 경우 IT에서 선제적인 역할을 담당했다고 생각합니다. 당시 해당 분야에 대해 IT부서만큼 많이 알고 있는 부서가 없었다고 봅니다. 따라서 해당 IT담당자가 주도적인 역할을 수행하였습니다. 당시 당사의 여러 여건을 보았을 때 IT부서에서 시작한 것은 결과적으로 합리적인 판단이었다고 생각합니다.
질문 : TFT 운영의 전반적인 내용을 소개해 주십시오.
답변 : 우선 당사의 AS IS 파악을 위해 각 부서별로 TFT 멤버를 참여시켜서 '개인정보보호법' 및 '규제사항'들에 대해 설명하고 현행 업무 내용 중 개인정보 취급과 관련된 업무가 무엇이 있는지 확인하고 이에 대해 TO BE 대책을 세우고자 하였습니다. 이 과정 중 '개인정보보호법'에서 강제 규정하고 있는 관련 규제 사항들을 지키기 위해 '개인정보보호 최고책임자' 및 '개인정보보호 담당자'를 선정하였으며 관련 부서를 구축, 운영하였습니다. 아울러 각 현업부서에서 개인정보를 취급하는 취급자를 지정하여 취급자 교육을 실시하였으며 전 직원을 대상으로 '개인정보보호법' 규정 교육도 실시 하였습니다. 현재 개인정보보호 최고책임자는 당사의 CFO께서 겸임을 하시고 계시며 개인정보보호 담당자는 제가 맡고 있습니다. IT부서는 개인정보보호 관련 솔루션 도입 및 운영 지원을 맡고 있고 금년에는 사내 개인정보보호 관련 감사를 수행하고자 합니다. TFT 운영 당시 서울 본사와 양 공장이 지리적으로 떨어져 있었기 때문에 TFT 멤버들 간의 미팅은 화상회의와 Conference Call 툴을 통하여 주기적인 회의를 진행하였습니다. 분기별 전체 회의와 필요시 각 현업들과의 수시 미팅을 통해 TFT업무가 수행되었습니다.
질문 : TFT 운영 시 가장 힘들었던 내용과 이를 해결한 방법에 대해 소개해 주십시오.
답변 : 개인정보보호에 대한 전문적 지식의 부족과 조직원의 관련법에 대한 이해 부족이 가장 힘들었습니다. 전문적 지식에 대한 부분은 회사에서 개인정보보호법 관련 전문 교육을 이수하도록 하여 한국인터넷진흥원이 제공하는 '개인정보보호 책임자' 교육 등을 이수하여 일정부분 해소하였으나 그것만으로는 충분치 않다고 생각합니다. 또한 CEO 및 임원들의 개인정보보호법에 대한 인식 역시 초기에 많이 부족하다고 생각합니다. 이러한 사내의 개인정보보호관련 인식재고가 추가적인 해결 과제입니다.
질문 : 귀사는 글로벌 외국 B2B 기업으로 알고 있습니다. 글로벌 외국 B2B 기업으로서 개인정보보호법 준수에 어려웠던 내용과 해결 방법에 대해 소개해 주십시오.
답변 : 당사는 글로벌 회사로서 모든 임직원들의 직원 정보가 Global system(해외)에 저장되고 있습니다. 이렇게 HR에서 사용하는 개인정보를 글로벌 본사와 APAC에 제공하는 것이 "개인정보보호법"에서 규제하고 있는 '개인정보 제3자 제공 및 해외제공' 사항에 해당하기 때문에 법규 준수를 위해서 일반 회사와는 다른 추가적인 직원들의 동의서가 필요했습니다. 따라서 당시 전 직원들로부터 직원 정보의 '제3자 제공 및 해외제공(본사)'에 대한 내용을 상세히 안내해주고 별도의 개별 동의서를 전부 받아 놓았으며 이후 추가적인 입사자들에게는 입사 시에 근로계약서 작성하면서 추가적인 동의서를 받고 있습니다. 이 과정 중에 APAC이나 본사의 HR 부서에 상기와 같은 내용이 국내 규제법에 의해 신설되었다는 것을 알려주고 설명해야 했으며 관련 업무 중 '개인정보보호법'을 영어로 해당 부서에 소개하는 과정이 조금 어려웠습니다. 정부에서는 관련 내용에 대해 별도로 영문으로 제공해주는 서비스가 없었기 때문에 모든 작업을 회사 내부에서 직원들이 수행해야 했습니다. 이 과정 중 어려운 법률 용어에 대한 설명이 힘들었었다고 생각합니다.

질문 : 2010년 TFT운영 이전과 2014년 현재 TFT운영 이후를 비교한 성과에 대해 말씀하여 주시기 바랍니다.
답변 : 개인정보보호에 대한 기본적인 시스템을 구축하였고 이는 한국인터네 진흥원이 개발·제공하여 준 개인정보보호 점검 지표를 통해 개인정보 TFT 운영 전(25점)과 개인정보 TFT 운영 후(69.25점)인 점을 보았을 때 결과적으로 개인정보보호 개선이 이루어졌다고 생각합니다. 다만, 100점 만점의 지표임을 감안하면 아직도 추가적으로 보완해야 할 점이 많다고 생각합니다.
질문 : 개인정보보호를 위해 필요한 법과 제도 개선에 대해 말씀해 주시기 바랍니다.
답변 : 기업의 현실적인 사항에 대해 좀 더 구체적인 내용을 잘 확인하여 실무의 어려움을 충분히 투영할 수 있는 법 및 시행령 등을 개발하여 주셨으면 합니다. 아울러 당사와 같은 Global 회사의 경우 국내 업무 내용이 변경되거나 국내법 저촉사항이 발생하면 미국 본사에 보고하고 대응해야 하는데 정부에서 영어로 된 안내문 정도도 제공되지 않는 점이 많이 힘들었습니다. 국내에 저희와 같은 외국기업이 상당히 많이 있고 앞으로도 더욱 늘어날 것으로 생각되는데 정부에서 영문 서비스(규정 전체는 아니더라도) 구축에 신경 써주셨으면 합니다. 또한 개인정보보호책임자는 CEO 급의 임원(대표이사 또는 등기이사)으로 지정하여야 한다고 생각합니다.
질문 : 앞으로 귀사에서 개인정보보호법 관련 추가적인 보완작업이 있다면 어떤 것을 계획하고 있으신지 소개 부탁합니다.
답변 : 추가 적인 보완작업으로는 임직원들의 개인정보보호 규정에 대한 전반적이고 반복적인 재교육 수행 및 정기적인 내부 감사를 수행하고자 합니다. 현재 당사의 채용사이트는 개인정보보호법의 기술적 보안조치 상세 내용에 따라 이미 암호화 되어 운영되고 있습니다. 따라서 현재로서는 특별한 시스템적인 추가 조치 사항은 필요하지 않은 상태입니다.
질문 : 장시간 인터뷰에 응하여 주셔서 감사합니다. 마지막으로 이번 개인정보보호법 TFT 운영 경험이 귀사와 개인적으로 어떤 성과를 가져다주었는지 간략히 말씀 부탁드립니다.
답변 : 회사 입장에서는 개인정보 관리 수준이 현행법 위반이 없도록 개발 운영된 것이 큰 성과이고 개인적으로는 개인정보보호 업무를 수행하며 저의 역량과 업무 내용이 좀 더 풍성해 졌다고 생각합니다. 물론 업무가 많아져서 힘든 부분도 있지만 현재 뉴스를 떠들썩하게 하는 개인정보유출 사건들을 보고 있으면 미리 선제적인 조치를 취하고 회사 내에 개인정보보호의 중요성을 각인시키고 운영하게된 것에 만족하고 있습니다.

3.7 글로벌 외국 법인의 추가적인 조치 사항

본 사례의 경우 미국 본사에서 제정하여 운영하고 있는 Privacy Policy를 국내 법인에 그대로 적용하기에는 문제가 있어, APAC HR Function과 협의하여 국내법 준수에 문제가 되지 않도록 별도의 개인정보보호 규정 및 지침을 신규로 제정하고 개인정보보호 조직을 운영하고 있다. Global CRM(Customer Relationship Management) System, Global HRM(Human Resource Management) System에 저장되는 고객 정보 및 관련사 정보 및 직원 정보, 협력사 정보 등에 대해서는 국내지침을 준수하여 운영하기로 하였다. 국내 직원들의 개인정보 일부를 Global HRM system에 이관하는 과정에서 전 직원들에게 개인정보 '해외 제공 동의서'와 '제3자 제공 동의서'를 확보하였다[8]. 정기적으로 수행하는 Global Audit와는 별개로 국내 개인정보보호 사내 감사를 매년 1회 수행하기로 하였다. Global DLP(Data Leak Prevention) System 적용 시 개인정보 검출 및 보호기능을 추가하

거나 별도의 전용 시스템 운영을 추후 협의하기로 하였다.

4. 결론 및 제언

4.1 결론

C사는 2011년 상반기부터 운영하여온 개인정보보호 TFT활동을 통하여 기업 내에 개인정보보호 규정 제정, 조직 설계, 관련 업무 절차 신설 및 시스템 도입 등을 성공적으로 이루어내었다. 또한 외국 법인으로서 추가적으로 갖추어야할 법령 준수 사항에 대해서도 선도적으로 대응하였으며 이 과정에서 결과적으로 업무 프로세스 또한 향상되었다. 한국인터넷진흥원에서 제공하는 자가점검표를 활용한 자체 점검에서도 TFT활동 이전인 2011년에 25점에서 조직 운영 2년 후인 2014년에는 69.25점을 기록하며 믿을만한 지표에 의한 점검에서도 개인정보보호 수준이 향상된 것을 보여주고 있다. 이는 TFT 운영 과정에서 보듯이 대표이사와 임원들, 중간관리자, 현업 담당자 및 전체 조직원이 TFT운영 활동을 통해 개인정보보호의 중요성을 인식하고 세부 현업에서부터 관련 업무를 개선하고자 했던 노력이 결실을 맺은 것이며 이를 위한 기업의 인적, 물적, 시간적 투자가 얼마나 중요한가를 보여주는 좋은 사례이다.

본 사례연구 내용을 PIMS의 관리과정, 보호대책, 생명주기 요구사항의 주요 관리 항목을 기반으로 분류해 보면 다음과 같은 10가지 전략을 도출할 수 있다. 첫째(보호대책), 조직 내에 개인정보보호 전문가를 양성하여야 한다. 외부 컨설팅만으로는 지속적인 조직 내 개인정보보호 활동을 운영하는데 한계가 있다. 둘째(관리과정), 대표이사를 비롯한 임원들의 적극적인 지원(업무조정, 업무시간 재배치 등)이 반드시 필요하다. 셋째(생명주기), 조직 내 전 업무 프로세스에 걸쳐 개인정보보호 업무 프로세스가 녹아 있어야 한다. 넷째(생명주기), 국내법에 위배되지 않는 개인정보보호 내부 지침(규정)을 운영하여야 한다. 다섯째(생명주기), 개인정보보호 관리 IT시스템의 적절한 도입과 기존 시스템의 업그레이드가 필요하다. 여섯째(생명주기), 글로벌회사의 특성을 감안한 법률 검토가 반드시 이루어져야 한다, 일곱째(관리과정), 전 직원 및 협력업체의 긍정적인 이해와 동참(교육 수반)이 필요하다. 여덟째(관리과정), 지속적인 업무 연속을 위한 관련 조직의 구축 및 운영이 필요하다. 아홉째(관리과정), 정기적인 관련 업무 내부 감사 프로세스 구축 및 감사 툴 도입이 필요하다. 열 번째(보호대책), 개인정보보호최고책임자와 개인정보보호 담당자에게 적절한 직위와 권한을 부여하여야 한다.

4.2 제 언

본 사례연구 과정에서 보여 진 몇 가지 부족한 점을 제언으로 정리하면 다음과 같다. 첫째, 개인정보보호법과 관련한 정보에 대해 기업들은 손쉬운 접근을 하지 못하고 있다고 보여 진다. 이는

관련 정부 부처의 홍보 부족 및 기업인들의 의식 부족 등에서 비롯한 것이다. 관련 부서는 좀 더 홍보 및 교육에 필요한 예산, 인력, 시설들을 확보하여 좀 더 적극적인 활동을 하여야 하며 기업역시 사내 개인정보보호 전문가 양성에 투자하여야 한다. 둘째, C사에서 활용한 자가점검표와 같은 기업 내에서 활용할 수 있는 프로그램 들이 산업군 및 기업의 형태에 맞도록 좀 더 세분화되고 다양하게 개발, 배포 되어야 한다. 셋째, PIMS 인증에 대한 적극적인 홍보와 관련 인증을 취득한 기업에 대한 적극적인 지원과 혜택이 늘어나야 한다. 넷째, 관련 부처에서는 외국법인을 위하여 개인정보보호법 관련 기본적인 내용에 대한 다국어 지원 서비스를 시작할 필요가 있다.

본 사례연구 내용이 기타 기업들의 개인정보보호 활동을 시작하는데 의미 있는 기초 자료가 되기를 바라며 좀 더 많은 기업들로부터 긍정적인 사례들이 발굴되기를 바란다.

Reference

[1] http://www.index.go.kr/egams/index.jsp, June 1 **(2014)**.

[2] R, Yin, “The Case Study as a Serious Research”, Science Communication, **(1981)**, Vol.3, pp.97-114.

[3] N. Woods, and M. Catanzaro, Nursing Research. Theory and Practice. St, Louis, Washington DC, Toronto: The C.Y, Mosby Company, **(1988)**.

[4] Creswell, John W, Qualitative Inquiry and Research Design: Choosing Among Five Approaches 2E. Thousand Oaks, CA: Sage Publication, Inc, **(2007)**.

[5] Chang-Hee. Han, "A Quantitative Assessment Model of Private Information Breach", The Journal of Society for e-business Studies, **(2011)**, Vol.16, Issue.4, pp.17-31.

[6] Jeong-Yeon. Kim, "Analyzing Effects on Firms' Market Value of Personal Information Security Breaches", The Journal of Society for e-business Studies, **(2013)**, Vol.18, Issue.1, pp.1-12.

[7] Han-Na. You, “Analysis on Domestic and Foreign Privacy Information Acts to Suggest Directions doe Developing Korean Privacy Information Protection Act.”, Journal of Korea Institute of Information Security & Cryptology, **(2012)**, Vol.22, NO.5, pp.1091-1102.

[8] http://www.privacy.go.kr/, June 1 **(2014)**.

[9] http://www.law.go.kr/, July 23 **(2014)**.

[10] http://pims.kisa.or.kr/, June 1 **(2014)**.

[11] Jung-Duk. Kim, “Personal Information Protection management and Governance”, Review of Korea Institute of Information Security And Cryptology, **(2008)**, Vol.18, No.6, pp.1-5.

[12] M. N. Shim, “A study on the implementation methodology of the efficient PIMS certification system”, Korea University, **(2010)**.

[13] Young-Soo Seo, “A Study on the Factors Affecting the Establishment of Personal Information Management Systems(PIMS)”, Journal of information technology applications & management, **(2012)**, Vol.19, No.3, pp.31-47.

[14] Jin-Hwan. Jeon , “Major changes of PIMS Certification regarding updated official announcement of Information communications network Law, Review of Korea Institute of Information Security And Cryptology, **(2013)**, Vol.23 No.5, pp.20-23.

[15] Eun-Yeop. Park, "Case study on the Certification system of Privacy Information Management System", Journal of Korea Institute of Information Security & Cryptology, **(2011)**, Vol.21, No.5, pp.27-36.

[16] Dae-Ha. Park, “A Study on PIMS Controls for PII Outsourcing Mnagement under the Cloud Service Environment”, Journal of The Korea Institute of Information Security & Cryptology, **(2013)**, Vol.23, No.6, pp.1267-1276.

Authors

이대영 (Dae-Young Lee)

2002년 10월 ~ 현재 : Ingredion Korea, Regional Manager, IT Security & Compliance of APAC.
2013년 2월 ~ 현재 : 서울과학종합대학원대학교 경영학(산업보안전공) 박사과정
2013년 2월 : 서울과학종합대학원대학교 산업보안학과 석사
관심분야 : 산업보안, 개인정보보호, 기업보안, Data Leak Prevention, End Point Security, Physical Security.

정진홍 (Jin-Hong Jeong)

2009년 3월 ~ 현재 : 서울과학종합대학원대학교 산업정보대학원장
2009년 2월 : 국가정보원 산업기밀보호센터(처장/실장)
1996년 2월 : University of Iowa College of Law, Research Professor(LL.M.)
1993년 2월 : 한양대학교 법학 박사
관심분야 : 산업보안, 산업보안관리, 산업보안법령, 산업스파이