情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

개인정보보호 거버넌스의 목표와 프로세스에 관한 연구

황 수 하*, 김 정 덕**

요 약

오늘날 개인정보는 개인의 권익에 관한 문제로 국한되는 것이 아닌 기업의 사활을 좌지우지하는 비즈니스 이슈이다. 특히 이러한 개인정보는 마케팅 부서, 고객지원 부서 등 현업에서 직접적으로 처리하기 때문에 단순히 정보처리 부서 차원에서가 아닌 전사적인 차원에서 관리해야 한다. 이를 가능하게 하는 것이 바로 거버넌스 개념이다. 따라서 본 논문에서는 개인정보보호의 특성 및 필요성 등을 통해 개인정보보호 거버넌스의 개념을 정립하고, 전사적 차원의 개인정보보호 관리가 가능하도록 개인정보보호 거버넌스 프레임워크 및 프로세스를 제안하고자 한다.

Ⅰ. 서 론

최근 정보화의 급속한 발전과 함께 다양하고 첨단화된 서비스를 제공하기 위해 개인정보에 대한 의존도 및 활용도가 높아지고 있다. 특히 오늘날 개인정보는 사회 모든 분야에서 없어선 안 되는 필수재 역할을 하고 있고, 이러한 이유로 개인정보보호는 단순히 개인의 권익에 관한 문제로 국한되지 않고, 기업의 사활을 좌지우지하는 비즈니스 이슈로 대두되고 있다. 이에 따라 최근 들어 개인정보 침해사례가 급증하고 그 심각성이 극대화되고 있는 등 개인정보보호의 중요성 또한 점차 증대되고 있다.

우리나라에서도 정부를 위시하여 개인정보보호법 제정과 한국인터넷진흥원의 '개인정보보호관리체계' 운영 등 법·제도적 뿐만 아니라 다방면으로 우리나라의 개인정보보호 수준제고를 위해 노력하고 있다. 하지만 이러한 노력을 무색하게 할 정도로 우리나라의 실제 개인정보보호 수준을 살펴보면 OECD 수준은 고사하고 중·후진국 수준에 불과하다고 할 수 있다. 왜냐하면 여전히 기술적 측면에서의 정보보호에 치중하였고, 비즈니스 차원에서의 정보보호 노력은 상대적으로 매우 미흡하였기 때문이다[1].

따라서 본 논문에서는 개인정보보호의 특성 및 필요성 등을 통해 개인정보보호 거버넌스의 개념을 정립하고, 전사적 차원의 개인정보보호 관리가 가능하도록 개인정보보호 거버넌스의 프레임워크 및 프로세스를 제안하고자 한다.

Ⅱ. 개인정보보호 거버넌스의 필요성

2.1 개인정보보호의 특성

개인정보란 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"이다[2].

이러한 개인정보의 특성을 살펴보면 크게 세 가지가 있다.

첫째, 개인정보보호는 전사적 차원에서 접근해야한다. 개인정보는 마케팅부서, 고객지원 부서 등 많은 현업부서에서 직접적으로 다루어지고 있다. 따라서 단순히 정보처리 부서 차원에서의 관리가 아닌 전사적 차원에서의 관리가 필요하다.

둘째, 개인정보보호는 이해관계자가 다양하다. 일반

* 중앙대학교 경영경제대학원 정보시스템학과 (shhwang@cau.ac.kr)
** 중앙대학교 경영경제대학 정보시스템학과 (jdkimsac@cau.ac.kr)

적인 정보보호의 관리 및 책임 주체가 내부의 이해관계자인 반면 개인정보보호의 경우 내부뿐만 아니라 조직 외부의 고객이라는 또다른 권리 주체를 대상으로 해야 하기 때문에 개인정보보호는 전통적인 정보보호의 범위를 포함하고 있으며, 보다 폭넓은 영역을 다루어야 할 필요가 있다.

셋째, 개인정보보호는 자기정보 결정권이 있다. 이는 개인정보보호의 권리 주체가 고객에게 있는 만큼 이용자 스스로 자신의 개인정보의 처리과정에 직접 참여할 수 있음을 나타낸다. 이 밖에도 이용자 개인정보의 오남용을 방지하고 필요 시 공개하여야 하는 특성 등이 있다[3].

2.2 개인정보보호 거버넌스의 필요성

최근 UN에서 190개국을 대상으로 하는 전자정부발전지수 및 온라인참여지수 평가에서 우리나라는 전자정부발전지수의 경우 2001년 15위에서 2010년 1위로 도약하였고, 온라인참여지수 또한 2010년 1위로 평가 받는 등 세계에서 우리나라의 정보화 수준은 높게 평가받고 있다[4].

이 밖에도 오늘날의 정보화 시대에 있어 가장 큰 이슈로 대두되고 있는 개인정보보호의 필요성이 증대되면서 2009년 한국인터넷진흥원에서 개인정보보호관리체계(PIMS)를 수립 및 운영 중에 있다. 또한 국가차원에서도 2008년 개인정보보호법을 발의하였고 약 3년만인 지난 3월 29일 제정되었으며, 오는 9월 30일에 시행될 것이다.

하지만 이렇게 정부를 위시하여 법·제도적 뿐만 아니라 다방면으로 우리나라의 개인정보보호 수준제고를 위해 노력을 하고 있지만 이에 반해 우리나라의 개인정보보호 수준을 보면 OECD 수준은 고사하고 중·후진국 수준에 불과하다고 할 수 있다. 왜냐하면 여전히 기술적 측면에서의 정보보호에 치중하였고, 비즈니스 차원에서의 정보보호 노력은 상대적으로 매우 미흡하였기 때문이다. 특히 개인정보보호의 경우 비즈니스 차원에서의 개인정보보호름과 유출 가능성 분석을 통한 대책 수립이 매우 중요하기 때문에 실질적인 개인정보보호 노력 또한 매우 미흡한 실정이다[5].

물론 앞서 설명한 개인정보보호관리체계의 수립 및 운영과 개인정보보호법의 재정 및 시행을 통해 앞으로 국가 정보보호 인식과 수준을 한층 높이는데 많은 역할을 할 것으로 기대가 되고 있고, 이 둘이 존재한다는 것 자체로 우리사회에서 개인정보를 적절히 보호 및 관리하고 안전하게 사용해야 한다는 인식과 환경이 조성되는데 크게 기여할 것으로 판단된다. 하지만 아직 시행 초기단계이고 제대로 정립된 상태가 아니기 때문에 많은 시행착오가 있을 것으로 예상된다.

따라서 2.1 에서 언급된 개인정보보호의 특성을 고려하고, 개인정보보호법과 개인정보보호관리체계의 조기 정착 및 효과적인 적용을 위해서는 우선 개인정보보호를 비즈니스 차원의 전사적인 관점에서 다루어야 하고, 이를 위해선 거버넌스 개념의 도입이 필요하다. 현재 개인정보보호 거버넌스에 대해 몇몇 전문가나 관련 기관에서 언급하고 있으나 아직 제대로된 정의가 내려지지 않았고 실현되고 있지도 않다. 따라서 본 연구에서는 개인정보보호에 대한 거버넌스를 알기 위해서 먼저 개인정보보호와 상당히 중복 관계가 있는 정보보호활동의 발전과정을 살펴봄으로써 많은 시사점을 얻고 이를 통해 개인정보보호 거버넌스에 대한 개념 정립을 하고자 한다.

Ⅲ. 개인정보보호 거버넌스의 목표와 프로세스

3.1 정의

Basie von Solms(2006)은 정보보호의 발전과정을 정보보호 기술, 정보보호 관리, 정보보호 조직화, 정보보호 거번너스의 4가지 패러다임의 변화로 구분하고 있다. 먼저 정보보호 기술 패러다임은 메인프레임에 대한 접근통제를 위한 보안기술을 중점적으로 연구하는 패러다임이고, 정보보호 관리 패러다임은 정보보호를 위한 기술적 솔루션의 한계를 인식하고, 이를 보완하기 위한 관리 활동에 초점을 맞춘 패러다임이다. 한편, 정보보호 조직화 패러다임은 효과적인 정보보호 구현을 위해 정보보호 표준 및 모범사례가 필요함을 인식하고, 정보보호 문화를 정착시켜 조직 구성원 전체의 정보보호 노력을 요구하는 패러다임이다. 끝으로 정보보호에 대한 최고 경영층 및 이사회의 역할과 책임을 강조하는 정보보호 거버넌스 패러다임은 최고 경영층 및 이사회를 정보보호와 관련된 법, 규정에 대한 준수, 그리고 정보보호에 대한 계획 및 의사결정의 주체로 명시하고 있다.

개인정보보호 또한 이와 비슷한 관점으로 살펴 볼 수 있다. 특히 2000년대에 진입하면서 인식하기 시작한 중

요한 변화는 이사회나 상위 경영층의 정보보호에 대한 지원과 참여가 없으면 성공할 수 없다는 것이다. 따라서 본 논문에서는 기존의 IT 거버넌스와 정보보호 거버넌스 등의 정의를 바탕으로 다음과 같은 개인정보보호 거버넌스의 정의를 제시하고자 한다.

개인정보보호 거버넌스란 "기업의 비즈니스에 존재하는 개인정보와 관련된 위험을 평가 및 관리하고, 고객의 자기정보 결정권을 보장하기 위한 이사회와 최고 경영진의 역할과 책임을 명시하고 이를 바탕으로 조직 내에 개인정보보호 문화 형성을 도모하기 위한 조직, 프로세스, 관련 메커니즘으로 구성되어 있는 것이다."

〔표 1〕 IT/정보보호 거버넌스 정의

		정의
IT 거버넌스	ITGI	IT 부문의 리더십과 조직구조, IT 기획에서부터 구축, 운영, 관리를 위한 프로세스로 구성
	ISACA	조직의 전략과 목표에 부합하도록 IT와 관련된 자원 및 프로세스를 통제/관리하는 체계
정보보호 거버넌스	ITGI	기업 정보자산의 기밀성, 무결성, 가용성을 보장하기 위해, 경영층의 참여와 리더십, 조직 구조, 사용자 인식 및 참여, 정책, 절차, 프로세스, 컴플라이언스 집행 메커니즘으로 구성

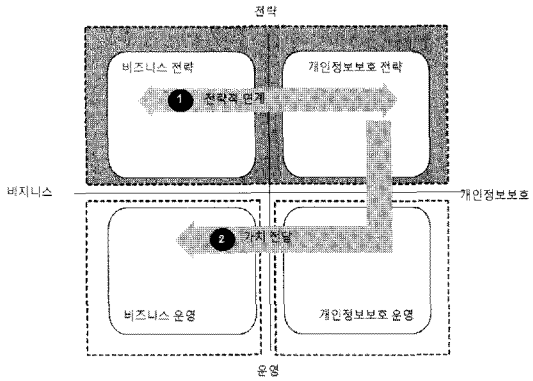
3.2 목표

개인정보보호 거버넌스의 개념을 이해하기 위해서는 우선적으로 개인정보보호가 달성해야할 목표를 정의해야 한다. 따라서 본 논문에서 제시하고자 하는 개인정보보호 거버넌스의 목표는 크게 두 가지이며 다음 [표 2]와 같다.

〔표 2〕 개인정보보호 거버넌스의 목표

목표	활동
전략적 연계	· 개인정보보호의 전략과 비즈니스 전략/목표와의 연계 · 높은 수준의 개인정보보호 운영위원회의 역할과 책임 명시 · 개인정보보호를 위한 보고라인의 간소화
가치 전달	· 거버닝 바디와 이해관계자에게 가치 전달 · 관련 국제표준과 모범사례에 기초하여 개인정보보호관리를 이행 및 운영 · 자금 계획/투자 통제 프로세스에 개인정보보호를 통합 · ROSI와 같은 척도를 사용하여 개인정보보호 투자를 최적화

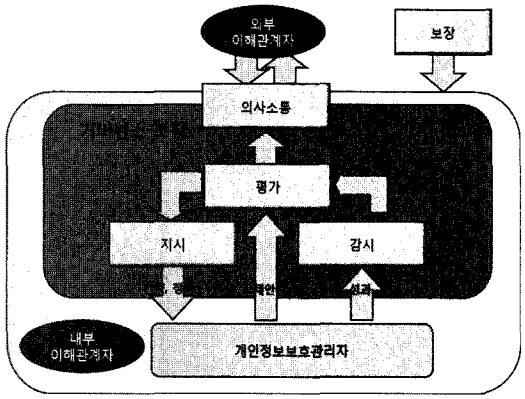
이러한 개인정보보호 거버넌스의 목표는 개인정보보호 활동을 비즈니스와 연계하는 것을 보장해 주는 것으로 단순히 비즈니스와 개인정보보호 분야와의 연계만 고려하는 것이 아니라 전략과 운영 분야와의 연계에도 초점을 맞추어야 한다. 따라서 본 논문에서는 개인정보보호 거버넌스의 목표를 정의하는데 다음 [그림 1]과 같은 프레임워크를 사용하였다. 본 프레임워크를 통해 비즈니스 전략, 개인정보보호 전략, 비즈니스 운영, 개인정보보호 운영의 4가지 측면에서 개인정보보호 거버넌스의 목표를 살펴보고자 한다.



〔그림 1〕 4가지 관점에서의 개인정보보호 거버넌스의 목표

3.3 프로세스

앞서 제시한 프레임워크를 통해 개인정보보호 거버넌스의 목표를 정의하였다면 이제 정의된 목표를 어떻게 하면 효과적이고 효율적으로 달성할 수 있는지를 생각해봐야 한다. 그리고 그것을 가능하게 해주는 것이 바로 다음에 제시될 개인정보보호 거버넌스 프로세스이다 [그림 2 참조]. 본 프로세스는 누가, 무엇을 수행하는지에 초점을 맞추어서 각 프로세스 별로 '거버넌스 조직'과 '최고경영진'의 역할과 책임으로 구성되어 있다. 여기서 거버넌스 조직은 조직의 성과에 궁극적인 책임이 있는 사람들의 모임이라 할 수 있고, 최고경영진은 조직의 목표를 달성할 수 있도록 전략과 정책의 구현에 책임을 가지는 사람들로 거버넌스 조직에서 선출을 한다. 최고경영진에는 CEO, CFO, CIO 등이 모두 포함될 수 있다.



〔그림 2〕 개인정보보호 거버넌스 프로세스

3.3.1 평가

'평가' 프로세스는 거버넌스 조직이 조직에서의 현재와 미래의 개인정보보호에 관련한 대응태도를 판단하는 것으로 이를 통해 조직의 전략과 목표를 수립한다.

- 거버넌스 조직: 개인정보보호와 관련된 이슈를 고려한 비즈니스 이니셔티브를 보증하고 개인정보보호 성과 결과에 대응 및 요구되는 활동을 취해야 한다.
- 최고경영진: 새로운 개인정보와 관련된 위험들을 거버넌스 조직에 경보해야 한다.

3.3.2 지시

'지시' 프로세스는 개인정보보호 목표와 전략을 구현하는데 있어서 필요한 것들을 거버넌스 조직이 지시하는 것이다.

- 거버넌스 조직: 조직의 위험 성향을 결정하고, 개인정보보호 전략 및 정책을 승인하며, 적절한 투자 및 자원을 배치시킨다.
- 최고경영진: 개인정보보호 전략과 정책을 개발 및 구현하고 적절한 자원을 배치하여 지원하며, 긍정적인 개인정보보호 문화를 장려한다.

3.3.3 감시

'감시' 프로세스는 개인정보보호 관리 활동성과를 평가하는 것이다.

- 거버넌스 조직: 효과적인 개인정보보호 관리 활동을 평가하고, 내부 및 외부의 요구사항을 따를 것을 보증하며 변화하는 비즈니스 환경과 개인정보 관련 위험의 잠재적 영향을 고려한다.
- 최고경영진: 비즈니스 관점에서의 적절한 성과 척도를 선택하고, 거버넌스 조직에 개인정보보호 성과 결과에 대한 피드백을 제공한다.

3.3.4 의사소통

'의사소통' 프로세스는 거버넌스 조직이 내부 및 외부의 이해관계자들에게 그들이 요구하는 특정 개인정보 관련 정보들을 정확하고 시기적절하게 제공하는 것이다.

- 거버넌스 조직: 정보 분류 정책을 고려하여 비즈니스 본연에 상응하는 조직의 개인정보보호 수준을 외부 이해관계자들에게 보고한다. 또한 식별된 개인정보보호 이슈, 요구되는 교정활동 등을 포함한 여러 외부 검토 결과를 중역 관리자에게 고지하며, 내부 이해관계자들에게 개인정보보호의 상태와 그들에게 할당된 역할과 책임에 대해서 알린다.
- 최고경영진: 내부 이해관계자들에게 거버넌스 조직의 지시 및 의사결정을 돕기 위한 상세한 행동을 알려준다.

3.3.5 보장

'보장' 프로세스는 거버넌스 조직이 독립적이고 객관적인 감사, 검토 또는 인증 활동을 통해 얻는 것이다.

- 거버넌스 조직: 위원회의 독립적이고 객관적인 의견이 원하는 수준의 개인정보보호를 달성하기 위해 어떠한 책임성을 따르는지를 보장한다.
- 최고경영진: 위원회의 독립적이고 객관적인 의견이 2700x 패밀리나 COBIT® 등 국제 표준과 비교하여 어떻게 개인정보보호관리를 구현하고 운영하는지를 보장한다.

Ⅳ. 결 론

2009년부터 한국인터넷진흥원의 개인정보보호관리체계가 수립 및 운영 중에 있고, 2011년 3월 29일 개인정보보호법이 제정되었으며, 오는 9월 30일 시행을 앞두고 있는 등 우리나라의 개인정보보호의 수준제고를 위한 노력은 끊임없이 지속되고 있다. 하지만 이에 반해

실제 개인정보보호의 실태를 살펴보면 많은 문제점들이 도사리고 있는 실정이다. 이는 아직도 개인정보보호를 기술적인 이슈로 보고 있기 때문이라 할 수 있다.

앞서 살펴보았듯이 개인정보보호는 더 이상 기술적인 이슈가 아닌 비즈니스 이슈이다. 즉, 개인정보보호의 특성에 따라 전사적 차원의 관리가 필요하기 때문이다. 그리고 이를 가능하게 하는 것이 바로 거버넌스 개념이라 할 수 있다.

따라서 본 논문에서는 개인정보보호의 특성을 알아보고 이를 통해 개인정보보호 거버넌스의 목표 및 프로세스를 제시하였다. 하지만 아직 대내외적으로 개인정보보호 거버넌스에 대한 연구가 많이 부족한 실정이므로 지속적인 연구 활동이 필요하다고 사료된다.

본 논문을 기반으로 향후 연구에서는 더욱 정교한 프로세스 및 프레임워크를 개발하고 이를 통해 개인정보보호 거버넌스를 효과적으로 구현할 수 있는 핵심요인을 식별하고 이에 대한 분석을 수행 하고자 한다.

참고문헌

[1] 이강신, "국내 개인정보보호 법규 현황 및 방향," 한국인터넷진흥원, 2008.

[2] "정보통신망이용촉진및정보보호등에관한법률," 제2조 6호.

[3] 김정덕, "개인정보보호관리체계(PIMS) 국제표준화 이슈 및 전략," 한국인터넷진흥원, 2009.

[4] "국가정보보호백서," 한국정보화진흥원, pp. 1편1부 76, 2010.

[5] 김정덕, "개인정보보호 거버넌스의 ABC," 한국CPO 포럼, 2008.

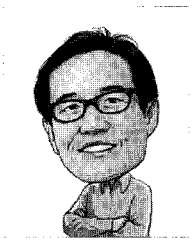
[6] Board Briefing on IT Governance, 2nd Edition., ITGI, Oct. 2003.

[7] Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, ITGI, Mar. 2006.

[8] J. Kim, K. Harada, and C. Provencher, "Information technology – Security technicques – information security governance framework," ISO/IEC 27014, Dec 2009.

[9] J. Kim, K. Harada, "Information technology – Security techniques – Governance of information security," ISO/IEC 27014, May 2011.

〈著者紹介〉



김 정 덕 (Kim Jungduk)
종신회원
1979년 2월 : 연세대학교 정치외교학과 학사
1981년 8월 : 연세대학교 경제학과 석사
1986년 5월 : University of South Carolina, MBA
1990년 12월 : Texas A&M University, Ph. D. in MIS
1995년 3월 : 중앙대학교 정보시스템학과 교수
<관심분야> 정보보호관리/거버넌스, 시스템감리, IT 전략/관리

황 수 하 (Hwang Sooha)
학생회원
2010년 2월 : 중앙대학교 정보시스템학과 학사
2010년 3월: 중앙대학교 정보시스템학과 석사과정
<관심분야> 정보보호 거버넌스, 시스템감사, 개인정보보호