Samil PwC Governance Center Online Library

리스크관리와 내부통제 :

데이터와 개인정보 보호를 위한 이사회 역할

삼일 PwC 거버넌스센터

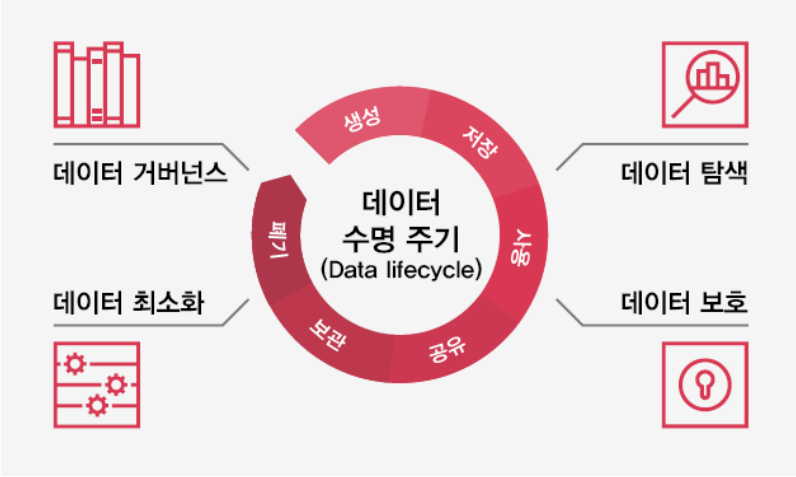
pwc 삼일회계법인

오늘날의 사업 환경에서 데이터는 힘이다. 방대한 양의 데이터를 수집하고 사용하는 능력은 기업에 경쟁 우위를 제공할 수 있다. 그러나 이러한 기회에는 개인정보를 보호해야 하는 위험과 의무도 따른다. 이것이 바로 이사회의 감독이 필요한 이유이다.

데이터는 경쟁 환경을 변화시키고 있다. 이제 기업들이 사용할 수 있는 방대한 데이터 양은 '기업이 효율성을 높이고, 신제품을 개발 및 타겟팅하고, 고객에 대한 통찰력을 얻고, 운영을 최적화하며 이전에는 불가능하다고 생각했던 방식과 속도로 사업 전략을 조정할 수 있음'을 의미한다. 그러나 데이터를 수집하고 사용하다 보면 데이터가 오용되거나 위협 행위자가 데이터에 접근할 위험도 발생한다. 데이터를 윤리적이고 안전하게 기업의 가치로 전환하는 것은 향후 10 년간 사업에 필수적인 과제이다.

데이터의 "수명 주기(Lifecycle)" 전반에 걸쳐 데이터를 효과적으로 관리하는 기업은 성공할 수 있는 가장 좋은 기회를 갖게 될 것이다. 관련된 기회와 위험을 고려할 때, 이사회는 반드시 그 과정에서 핵심적인 역할을 해야 한다.

데이터 수명 주기(lifecycle) 이해하기



• **데이터 탐색:** 우리 기업은 어떤 유형의 데이터를 수집하는가? 어떤 데이터가 가장 중요한가? 가장 민감한 데이터는 무엇인가? 데이터는 어떻게 사용되며 윤리적으로 사용되는가?

• **데이터 보호:** 어떤 데이터를 보호해야 하는가? 보호해야 할 다른 데이터는 무엇인가? 데이터를 보호하기 위해 어떤 절차가 마련되어 있는가?

• **데이터 최소화:** 수집되지만 사용되지 않는 데이터는 무엇인가? 더 이상 사용하지 않고 제거할 수 있는 오래된 데이터가 있는가? 현재의 기능이나 가치를 유지하면서 기업의 데이터 수집 및 관련 위험을 최소화할 수 있는 방법은 무엇인가?

• **데이터 거버넌스:** 데이터를 관리하고 컴플라이언스 및 개인정보 관련 요구사항을 충족할 수 있는 적절한 인력, 정책 및 절차, 기술이 있는가? 어떻게 개선할 수 있는가?

데이터 수명 주기를 살피면, 이사회는 전반적인 데이터 전략을 더 깊이 이해할 수 있다. 기업이 고객, 직원 및 다른 사람들로부터 개인정보를 수집할 때, 해당 데이터를 안전하게 유지하고 소유자의 프라이버시를 보호해야 한다. 빠르게 증가하고 있는 개인정보 보호 법규는 이 중 일부를 규정한다. 그러나 데이터가 수집 대상이 되는 개개인은 기업이 보유하고 있는 데이터가 무엇인지, 그 이유는 무엇인지, 어떻게 사용되고 있는지를 알고 싶어 한다.

이러한 데이터를 보호하지 못하면 기업은 소비자와 직원의 신뢰를 잃을 수 있다. 또한, 브랜드 손상, 재무적 손실, 벌금과 규제 기관의 감사로 이어질 수 있다.

기업의 미래 성장과 혁신 능력은 해당 데이터를 얼마나 잘 사용하고 보호하는지에 달려 있다. 기업들은 데이터 및 개인정보 관련 전략을 탐색하고 있다. 따라서 이사회는 기업이 포괄적이고 이해관계자와 신뢰를 형성하며 관련 위험을 관리하는 전략을 개발하는지 확인해야 한다.

데이터 탐색

기본적으로 기업이 데이터를 수집 및 사용하고 보호하는 방법에 대한 질문은 사업 전략과 연관이 있다. 이사회가 이러한 연관을 결정하려면, 기업이 어떤 데이터를 수집하고, 어떻게 저장하고 사용하는지 이해하는 것부터 시작해야 한다.

수집된 데이터의 각 요소에 대한 사업 목적과 사용을 이해하려면, 재무, 사업부, IT, 마케팅, HR, 법률, 데이터 거버넌스, 데이터 분석 및 데이터 보호에 대한 전문지식을 갖춘 교차기능팀(Cross-Functional Team)의 보고가 필요하다. 기업에 따라 최고 정보 책임자(CIO), 최고 기술 책임자(CTO), 최고 데이터 보호 책임자(CDPO) 또는 데이터 전략을 감독하는 다른 고위 임원이 있을 것이다. 이사회는 이러한 전문성을 활용하여 데이터 전략의 전반적인 위험을 평가할 수 있다. 데이터가 합법적이고 윤리적인 방식으로 수집 및 사용되고 있는가? 데이터 소유자의 동의가 있는가? 데이터는 신뢰할 수 있고 편의가 없는가?

기업이 다양한 유형의 데이터를 수집하는 동안, 이사회와 담당 팀은 가장 철저한 데이터 보호와 규정 준수가 필요한 개인 및 민감 데이터 수집에 세심한 주의를 기울이는 것이 바람직하다.

개인정보에 각별한 주의를 기울일 것

개인정보는 직간접적으로 식별 가능한 사람과 관련된 정보이며 데이터 보호가 필요하다. 예로는 이름, 집 주소, 이메일 주소 등이 있다.

개인정보 보호법 제 2 조

"개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

다. 가목 또는 나목을 제 1 호의 2 에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용・결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

1 의 2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

민감정보는 개인정보의 대상이며 개인의 인종, 민족, 정치적 또는 철학적 견해, 종교적 신념, 노조 가입 여부, 범죄 기록, 건강 또는 성생활과 관련된 모든 데이터를 직간접적으로 드러내는 정보로 정의된다. 민감정보를 보관하려면 일반적으로 추가적인 보호 장치가 필요하다. 민감정보의 예로는 개인의 인종이나 종교, 건강 정보, 생체 정보 등이 있다.

개인정보 보호법 제 23 조

①개인정보처리자는 사상・신념, 노동조합・정당의 가입・탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다.

데이터 탐색에 있어 또 다른 중요한 점은 많은 글로벌 개인정보보호 규정이 개인에게 권한을 부여함에 따라, 자신의 정보에 접근하고 삭제할 수 있는 사용자가 증가하고 있다는 사실이다.

마지막으로 데이터를 수집하는 기업의 당면 과제는 많은 기술 플랫폼이 쿠키 사용 및 온라인 추적에 대한 제한을 강화하고 개인정보 공개에 대한 투명성을 강화하고 있다는 것이다. 이 모든 상황은 기업이 수집하는 정보와 수집하는 방식을 다시 생각하도록 만들고 있다.

데이터 보호

데이터 보호는 기업의 사이버 위험 관리 프로그램에 통합되어야 하고, 데이터 보호 전략은 이해관계자와 기업 간의 신뢰를 형성하고 강화할 수 있어야 한다. 사이버 보안과 개인정보 보호 정책 및 관행에 대한 임직원 교육을 실시해야 한다. 특히 원격으로 일하는 직원은 지속적으로 교육해야 한다. 암호화, 데이터 마스킹, 다단계 인증 및 강력한 암호와 같은 기술을 통해 사이버 보안 및 개인정보 보호를 위한 좋은 환경이 조성되어야 한다.

대부분의 기업은 수집하는 데이터를 지키고 보호하기 위해 노력하지만, 사이버 보안 사고의 급증은 이러한 노력이 쉽지 않음을 보여준다. 개인정보의 무단 공개와 관련된 위반을 포함하여, 법규에 따른 보고 의무가 있는

데이터 침해는 다양한 글로벌 사이버 보안과 데이터 보호 규칙 및 규정에 따라 적시에 공개해야 한다. 이러한 침해는 기업의 평판 손상, 재무적 비용, 위약금 및 신뢰 훼손을 초래할 수 있다. 디지털화, 원격 작업, 위협 행위자의 지능화가 갈수록 심화됨에 따라 데이터 손실 위험도 증가했다.

이사회는 무엇을 해야 할까? 경영진은 데이터를 보호할 책임이 있다. 따라서 이사회는 정보 보호 프로그램의 적절성에 대한 활발한 논의에 참여해야 한다. 논의 내용에는 통제의 효과성과 자원의 충분성도 포함된다. 또한 이사회는 회사에 적용되는 사이버 보안 및 개인정보 보호법과 주요 위반 사항을 확실히 파악할 필요가 있다. 이사회는 경영진으로부터 중요한 사이버 보안 사건, 개인정보 보호 요구사항을 준수하지 않은 사례 및 경영진의 대응 방식 등이 포함된 보고를 받아야 한다.

투명성 향상 – 우수한 데이터 보호 정책의 외부 공표

기업은 데이터를 사용하고 저장 및 폐기하는 방법과 소비자의 동의를 얻는 방법을 담은 최신의 데이터 보호 정책을 외부에 알릴 필요가 있다. 개인정보의 수집, 생성, 사용, 전송, 저장 및 폐기에 대한 세부 내용을 공시하는 것이 효과적이다. 또한 데이터가 명시된 목적으로 사용되었는지를 상세히 설명하고, 제 3 자의 개인정보 보호 인증을 받을 수도 있다. 무엇보다 고객과 주주들에게 기업이 정보를 어떻게 보호하고 있는지를 알려줄 수 있다. 이러한 공시는 종종 글로벌 개인정보 보호법을 준수하기 위해 이루어지기도 한다.

전세계에 흩어진 수많은 개인정보 보호법을 모두 탐색하는 것은 어려운 일이다. 현재 전체 194 개국 중 137 개국에는 데이터 보호 및 개인정보 보호를 위한 법률이 있는 것으로 파악된다.[1] 미국은 주마다 법률이 다르며, 50 개 이상의 데이터 보호 및 개인정보 보호 법안이 논의되고 있는 중이다.

데이터 최소화

이사회는 기업이 어떤 데이터를 수집하고 어떻게 보호하는지를 이해한 후에, 데이터에 대한 기업의 목표를 달성하면서 해당 데이터를 최소화할 수 있는 방법에 대해 경영진과 검토할 수 있다. 잘못된 결정이나 민감한 정보에 접근하는 악의적인 행위자 등으로 인해 거의 모든 데이터가 위험 요소가 될 수 있다. 기업은 데이터를 최소화함으로써 위험도 최소화할 수 있다. 필요한 데이터만 보호하고 나머지는 제거할 수 있다. 일반적으로 초안, 중복, 대체 데이터, 외부 데이터 및 불필요한 임직원 개인정보가 제거 대상이다.

전문성을 갖춘 교차기능팀(Cross-Functional Team)은 더 많은 기능을 갖춘 소수의 데이터 저장소를 사용하여, 보다 효율적인 접근과 통제를 수행하는 방법에 대해서도 제안할 수 있다. 이는 대상과 위험을 제거하는 또 다른 방법이다.

[1] Source: United Nations Conference on Trade and Development

데이터 거버넌스

기업의 데이터 거버넌스는 데이터 수집, 전략적 사용, 보호 및 최소화와 같은 모든 영역에 영향을 미칠 것이다. 이사회의 역할은 경영진의 데이터 거버넌스를 감독하고 인력, 절차 및 기술이 효과적인지 확인하는 것이다.

어떤 기업은 기능별로 또는 사업 부서별로 데이터 통제를 설정한다. 그러나 중앙 집중식 데이터 거버넌스 프로그램은 잘못된 접근 및 규정 준수 오류의 위험을 줄이고 놓친 기회를 발굴하는 데 도움이 되므로, 데이터의 가치를 극대화할 수 있다. 물론 중앙 집중화의 이점이 항상 달성되는 것은 아니다. 국가 간 디지털 장벽을 유발하는 데이터 현지화 법률과 데이터 전송 제한이 증가함에 따라 이용에 제한을 받기 때문이다. 현재 전 세계 인구의 60%가 데이터를 현지에 저장해야 하거나 국경 간 데이터 흐름 제한이 적용되는 지역에 살고 있다. 이는 한국에 기반을 둔 다국적 기업이 더 이상 한국 기반의 인재, 인프라, 통제 및 절차를 사용하여 글로벌 데이터 운영을 지원할 수 없음을 의미한다. 다국적 기업들은 기업이 운영되는 각 국가에서 이러한 기능과 활동을 설정해야 하므로 운영 모델에 상당한 영향을 미친다.

데이터 거버넌스 절차 및 기술은 빠르게 발전하고 있다. 이사회는 경영진이 절차를 현대화·표준화·자동화할 기회를 모색하고 있는지 이해해야 한다. 이러한 변화는 효율성과 데이터 품질을 향상시키고, 현행 및 새로운 개인정보 보호법을 준수하는 데 도움이 될 수 있다. 또한 이사회는 기업이 이 중요한 영역을 관리하기 위한 적절한 자원(자금 및 인력 등)을 보유하고 있는지 확인해야 한다.

데이터 거버넌스에는 제 3 자 위험에 대한 고려 사항도 포함된다. 기업은 사업 운영을 지원하기 위해 다양한 제 3 자를 활용하며, 기업이 수집한 개인정보 또는 민감한 데이터의 일부를 이러한 제 3 자와 공유하거나 판매할 수 있다. 강건한 제 3 자 위험 관리 프로그램은 관련 당사자가 제기하는 위험의 범위와 운영되고 있는 통제 및 절차가 데이터를 보호하고, 개인정보보호 규정을 준수하기에 적절한지를 파악할 수 있게 해준다.

누가 데이터 및 개인정보 전략을 감독하는가?

전반적인 사업 전략에 맞춰 데이터 및 개인정보 전략이 조정될 수 있도록, 이사회는 이에 대한 주기적인 업데이트를 요청해야 한다. 사이버 보안을 감독하는 이사회 내 위원회는 데이터 보호와 법규 준수를 감독하는 역할을 할 수 있지만, 데이터 전략의 전체 범위를 감독하진 않을 수 있다. 이사회는 위원회의 접근 방식에 대해 논의하고 데이터 전략이 어떻게 다루어지고 있는지, 경영진 중 누가 적절한 정보를 제공하기에 가장 적합한 위치에 있는지를 명확히 해야 한다.

데이터 가치와 관련 위험을 다루는 전체적인 데이터 및 개인정보 전략을 신중한 거버넌스 접근 방식과 결합하면, 이사회와 경영진은 경쟁 우위를 확보하고 이해관계자와 더 큰 신뢰를 구축할 수 있을 것이다.