국민권익위원회

청렴윤리경영 브리프스

3

디지털시대의 영업비밀보호와 청렴윤리경영

2022 March | VOL. 111

국민권익위원회

www.acrc.go.kr 국민권익위원회 청렴윤리경영 브리프스
국민권익위원회 홈페이지에서 자세한 내용을 보실 수 있습니다.
발행일: 2022년 3월 1일(매월발행, 통권 111호, 비매품) 발행인: 전현희
발행처: 국민권익위원회 구독신청: 044-200-7166
주소: 30102 세종특별자치시 도움5로 20 정부세종청사 7동 민간협력담당관실

COVER STORY

기업이 경쟁회사의 영업비밀을 침해하는 행위는 기업의 청렴윤리경영에 정면으로 반하는 행위입니다. 모든 정보가 디지털화되어가는 시대에 기업의 고유자산에 대한 외부접근성이 높아지는 만큼, 기업은 이를 어떻게 보호하고 관리해야 하는지 고민해야 합니다.

이번 호에서는, 디지털시대의 기업이 고유의 영업비밀을 보호하기 위해 어떤 노력을 기울여야 하는지, 이것이 청렴윤리경영과 어떻게 맞닿아 있는지 살펴보겠습니다.

디지털시대의 영업비밀보호와 청렴윤리경영

전문가 코칭

최 희 정
법무법인 별 변호사

Q1. 기업의 영업비밀보호가 중요한 이슈인 것처럼 경쟁상대 기업의 영업비밀 침해와 관련하여 기업이 내부적으로 어떤규범을 수립해야 하며 이와 관련하여 준수해야 할 내용은 무엇일까요?

경쟁회사의 영업비밀을 침해하는 행위는 법률에 저촉되는 행위일 뿐 아니라 윤리준법경영에 정면으로 반하는 행위이다. 법정 다툼에 소요되는 비용만 하더라도 상당하기 때문에 이러한 일이 발생하지 않도록 사전에 예방하는 것이 필요하다. 예방비용은 방어비용보다 훨씬 저렴하며, 방어비용에는 회복할 수 없는 기업 이미지가 포함될 수 있는 만큼 그 비용은 실로 어마어마할 수 있기 때문이다. 그러므로 기업의 대표 및 임직원이 이러한 내용을 깊이 인식하고 기업 내부 규범과 행동지침을 마련해야 한다.

우선 기업 내부적으로 준법경영방침을 수립해야 한다. 회사의 기본경영지침에 준법경영을 규정하고 준법경영지침에 영업비밀침해 금지에 관한 내용을 포함해야 한다. 영업비밀보호를 위한 특별한 규범이라고 어렵게 생각할 필요는 없다. 준법경영이 모든 것을 포괄하기 때문이다.

영업비밀보호에는 우리 자신의 영업비밀뿐 아니라 타인의 영업비밀을 침해하지 말자는 것도 포함된다. 기업경영을 하며 다양한 상황을 접하다 보면 너무나 당연한 기본 윤리를 지키지 못하는 상황에 처하게 되는데, 회사의 경영방침에서 준법을 선언하고 확인하고 있다면 갈등의 상황에서 고민의 여지가 없다.

원칙을 수립했다면 이제 구체적인 행동강령을 마련해야 한다. 'Dos and Donts'와 같은 사례를 수집하여 임직원에게 전파할 필요가 있다. 구체적인 행동요령 없는 원칙선언은 실제 실행력을 담보할 수 없기 때문이다. 법률은 추상적 규범이고 그것이 구체적으로 사례화 되었을 때 '어떻게 해야 하는 것이구나'하는 느낌이 오게 마련이다. 그러므로 무엇보다 사례발굴 및 전파 활동이 필요하다. 이렇게 정의된 영업비밀 준수에 관한 기본지침 및 행동강령은 기업의 최고 책임자가 반복적, 주기적으로 선언하고 전파해야 한다.

Q2. 기업의 영업비밀 노출에 따른 내부보안유지를 위해 어떤 노력을 기울여야 할까요?

기업은 각자 고객을 관리하는 방법, 고유 자산, 특허 등 여러 가지 정보와 자산을 가지고 고유의 영업활동을 한다. 그러나 회사가 이것이 우리의 영업비밀이라고 정의한다고 해서 법에 따른 보호를 받는 것은 아니다. 법이 인정하는 영업비밀은 '공공연히 알려져 있지 않은 것', '독립된 경제적 가치가 있는 것', '회사가 비밀로 관리한 것' 이라는 요건을 모두 갖춘 것을 의미하는데, 이때 회사가 비밀로 관리하지 않은 정보라는 이유로 법에 따른 영업비밀보호를 받지 못하는

판결사례가 많기 때문에 비밀관리성을 인정받는 것은 매우 중요하다.

비밀관리성을 인정받기 위해서는 우선 기업에서 생성하는 각종 자료에 '비밀'표시를 제대로 해야 한다. 진정으로 영업비밀에 해당하는 것에 '비밀', '극비' 등의 표시를 함으로써, 그 정보를 다루는 자에게 주의를 주는 것이 필요하다. 또한 비밀정보를 다루는 임직원으로부터 비밀유지서약서를 받는 것, 외부 협력업체에 정보를 전달할 경우 비밀유지계약서를 반드시 체결하는 것도 필요하다. 이때 비밀유지서약서는 매년 갱신하는 것이 좋다. 이에 더해 회사에서는 정보에 대해 1급–2급–3급 등으로 등급을 매기고 접근 권한자를 차등적으로 지정하고, 파일 등의 정보는 암호를 설정해 관리해야 한다.

이처럼 회사가 정보를 비밀로 관리한 노력이 인정되어야만 그 정보가 영업비밀로 법적인 보호를 받는다는 점을 반드시 기억하여 소중한 회사정보의 가치를 높여 나가야 할 것이다.

사례돋보기

기업 자체 노력의 성과, 영업비밀보호

기업은 태생적으로 이윤을 극대화하기 위해 광고 등으로 자신의 정보를 의도적으로 노출하면서도 연구결과 등 중요 정보에 대해서는 철저히 보안을 유지한다. 반면 각자의 입장에서는 타사의 중요한 정보를 취득하기 위해 때로는 불법적인 방법까지 동원하는 경향이 있다. 이처럼 기업이 중요 정보를 비밀로 유지하는 이유는 중요 정보가 타사와의 관계에서 경쟁 우위적 위치를 점할 기회를 제공해 주기 때문이다. 자사의 정보 노출을 최소화하면서 타사 정보를 최대한 많이 수집하려는 기업의 이중적 태도를 무조건적으로 비난할 수는 없지만, 이는 취득방법이 합법적이라는 조건으로 제한되어야 할 것이다.

이번 사례돋보기에서는 오랜 기간 동안 소비자의 신뢰를 한 몸에 받고 있는 기업들의 사례를 통해 영업비밀보호를 위한 기업의 자체 노력이 기업의 성장과 소비자 신뢰도 형성에 얼마나 중요한지 살펴보고자 한다.

코카콜라

코카콜라는 1886년부터 현재까지 130년 이상 독특한 제조법을 영업비밀로 간직하고 있다. 오랜 기간 동안 자사의 정보를 비밀로 유지할 수 있었던 비결은 무엇일까? 코카콜라의 맛의 비법은 'Merchandise 7X'라는 성분으로 이 제조법이 담긴 문서는 애틀랜타의 한 은행금고에 보관되어 있었다. 현재는 위 제조법이 코카콜라 박물관에 보관되고 있는 것으로 알려져 있을 정도로 철저한 보안을 유지하고 있다. 이 뿐만 아니라 미국의 특정 공장 3곳에서만 제품을 생산하고 콜라를 병에 담는 생산자도 별도 지정하여 관리하고 있는 것으로 알려져 있다. 2016년 당시 세계지적재산권기구(World Intellectual Property Organization, WIPO)의 중소기업 프로그램 기획조정관이었던 패트리샤 시마오 사토리어스는 코카콜라가 영업비밀 유지에만 수백만 달러를 쓰고 있다고 밝힌바 있다. 이렇듯 코카콜라는 자신의 영업비밀을 지키기 위해 맛을 결정하는 재료 배합 등 제조법을 극소수의 임원에게만 허락하고 제조법이 담긴 문서와 생산자를 철저히 관리하며 100년 넘게 보안을 유지하는 등의 노력을 하고 있다. 물론 이 과정에서 펩시콜라를 비롯한 경쟁사와 화학자들이 맛의 비밀을 알아내려 노력 해왔던 일도 있었다. 2006년 인도에서 살충제 성분이 검출되어 제조법 공개라는 초유의 위기에 직면하기도 했지만, 아직까지 코카콜라는 맛을 결정하는 1% 미만의 구성요소와 배합비율을 영업비밀로 유지하고 있다. 다시 말해 코카콜라가 100년 이상 영업비밀을 보호할 수 있었던 비결은 유출에 따른 사후관리가 아닌 사전적 예방으로 유출을 억제하고 있는 것이고, 이 과정에서 영업비밀 서약 및 전직금지 서약 등 기본적인 기업정보 관리방법(영업비밀 컴플라이언스 절차)을 이행하고 있는 것이다.

KFC

글로벌 치킨 프랜차이즈 KFC는 11가지 비밀 허브 및 향신료의 배합으로 독특한 맛을 내는 것으로 유명한데, 이는 코카콜라의 재료 배합 등 제조법과 더불어 식품 산업의 양대 영업비밀로 통한다. 오늘날 오리지널 레시피라고 알려진 KFC의 배합비는 설립자인 할란드 샌더스 대령(colonel, 공을 이룬 이들에게 켄터키 주에서 수여하는 비공식 명예 칭호)이 1940년에 완성한 것으로 현재까지 약 80년가량 비밀이 유지되고 있는 것이다. 영업비밀로 유지되고 있는 KFC의 독특한 제조법 역시 위 코카콜라의 사례와 마찬가지로 KFC 본사의 금고에 보관되어 있는 것으로 알려져 있다. 최근 유트브를 통해 50만개가 넘는 KFC 카피캣(copycat, 모방품)이 넘쳐나고 있지만, 그들만의 맛이 비결은 여전히 비밀 진행 중이다.

위 사례에서 살핀 바와 같이 한 기업이 어떻게 수백 년간 자사의 중요 정보를 비밀로 유지해온 것인지는 정확히 알 수는 없다. 다만 비밀 유지를 위해 회사 금고나 박물관과 같은 중요장소에 극소수 사람에게만 정보를 공유하는 방법으로 보안이 유지되고 있다는 정도만 알려져 있을 뿐이다. 위 두 회사의 경우 영업비밀보호의 대표적 사례로 거론되지만, 글로벌 기업이라고 해서 모두 성공적으로 영업비밀을 보호하는 것은 아니다. 1992년 세계최초로 64M D램을 성공하면서 세계 반도체 시장의 강자로 발돋움한 기업, 바로 우리나라 삼성전자의 이야기이다. 오늘날 세계최고 글로벌 기업으로 성장한 삼성전자 역시 자사의 중요 정보를 비밀로 유지하기 위해 최고의 보안을 유지하는 것으로 유명하다. 특히 연구개발 영역으로 출입하기 위해서는 휴대폰의 지참을 금지하고 있는 것으로 알려져 있을

정도이다. 그러나 1998년 삼성전자의 64M D램 메모리 반도체 핵심기술이 대만으로 유출된 사례처럼 철통보안을 자랑하는 글로벌 기업도 완벽하게 영업비밀을 관리하는 것은 쉬운 일이 아니었다. 당시 유출된 기술이 반도체 분야에서 선도적 기술이었던 점을 고려할 때 1조원 이상의 손해를 야기한 것으로 추산될 만큼 피해는 적지 않았다. 이것이 바로 비밀보호가 중요한 이유이다. 이외에도 2003년 현대 LCD 직원이 경쟁사인 중국 트롤리사 한국지사인 비젼테크사에 핵심제조기술과 영업자료를 유출하려다 적발된 경우도 뼈아픈 유출 사례이다.

이쯤 되면 코카콜라와 KFC는 비밀유지를 위해 먼가 특별한 방법을 갖고 있는 것은 아닌지 의문이 들 수 있을 것이다. 그러나 지금까지 우리가 알고 있는 영업비밀 보안지침 외에 특별한 것은 없다는 것이 중론이다. 그 이유는 코카콜라 역시 다른 기업과 마찬가지로 퇴직자가 신제품의 제조방법과 샘플을 빼내려는 시도로 FBI의 수사를 받는 등 영업비밀 유출시도가 없었던 것은 아니었기 때문이다. 여기서 중요한 것은 이들 기업의 영업비밀보안 방식에 뭔가 특별한 방법이 있지 않을까라는 궁금증을 갖기에 앞서, 우리 기업은 기업정보 관리방법(영업비밀 침해 방지를 위한 컴플라이언스)을 구축하고 있는지, 그리고 그것을 잘 실행하고 있는지 되돌아보는 일일 것이다. 우리는 자사의 중요 정보를 영업비밀로 오랫동안 유지하는 기업일수록 소비자들의 무한 신뢰와 관심을 받는다는 사실을 잘 알고 있다. 기업의 가치는 기업 스스로가 만들어 가는 것인 만큼, 국가의 성장 동력이라고 할 수 있는 영업비밀보호를 위해 내부시스템을 강화하려는 노력이 필요하다.

보고서리뷰

영업비밀보호 관련 동향과 우리의 노력

■ 정민정, “미 바이든 행정부의 영업비밀보호 관련 입법·정책 동향과 시사점”, 국제경제법연구, 제19권 제3호(2021).

우리나라 국가 연구개발(R&D)에 투자한 비용의 60%(약 60조)가 영업비밀 유출로 빠져나가고 있다는 신문기사는 충격적이었다. 미국 역시 2021년 3월 전자 메일 및 캘린더의 플랫폼인 마이크로소프트 익스체인지(Microsoft Exchange)에 대한 해킹으로 MS와 전 세계 25만 명의 사용자, 그 외에도 지방 및 주정부, 기업, 로펌 등이 관리하는 지적재산권의 세부 정보가 노출되는 등의 피해가 발생했다. 지적재산권의 세부 정보는 영업비밀로 취급되는 사항도 있는 만큼 기업은 물론 국가적 비용 지출로까지 이어질 수 있는 심각한 일이었다. 전통적인 지적재산권(특허 · 상표 · 저작)과 달리 외부에 공표되지 않아 실질적 · 잠재적 · 경제적 가치가 더 우월하다는 평가를 받는 영업비밀이 국가의 성장 동력과 어떠한 관계에 있기에 유출시 국가적 비용까지 발생하는 것일까?

이번 보고서 리뷰에서는 침해에 따른 민형사상 조치 등에도 불구하고 한 번의 사고만으로도 사실상 피해회복이 불가능한 영업비밀 유출에 따른 사회경제적 비용에 대비하기 위한 우리의 노력으로써 영업비밀보호 현황에 대해 살펴보도록 하겠다.

1. 국가적 차원에서의 영업비밀보호 검토

우리나라의 경우 영업비밀은 「부정경쟁방지 및 영업비밀보호에 관한 법률」에서 규율하고 있으며, 보호를 위한 몇 가지 특성 중 비밀성의 입증이 가장 중요하다. 영업비밀은 조직의 혁신과 성장을 차별화한다는 점에서 유출 자체만으로도 천문학적인 금전적 손해를 불러올 수 있다. 따라서 기업은 유출에 대비하기 위해 스스로 엄격한 관리를 유지해야 한다. 그런데 관리의 필요성이 역설되는 더 중요한 이유가 있는데, 그것은 영업비밀 유출로 국제관계와 지정학적 시각에서 기업의 사유재산 개념을 넘어서는 훨씬 더 심각한 결과가 발생할 수 있기 때문이다. 다시 말해 영업비밀 유출은 국가가 보유한 사회 · 경제 · 정치 · 군사적 자산을 망라한 모든 자산의 탈취를 의미한다는 말로 이해할 수 있다. 실제로 정부의 사이버 인프라(ex, 에너지 공급)를 민간 기관에서 관리 · 운용하는 경우와 같이 민간이 운용하는 중요한 정보자원을 단순히 기업의 사유재산으로 치부하기에는 유출로 인한 피해 규모와 각 영역에 미치는 파장이 상당하다. 이러한 이유로 영업비밀보호를 위한 장려책으로 국가적 차원에서 관리가 필요하다는 논의가 제기되고 있다. 이렇게 함으로써 정부는 국가 경제와 세계 경제라는 측면에서 국가안보와 기술혁신 추진이라는 두 가지 정책을 모두 실현할 수 있다.

2. 디지털시대 영업비밀의 취약성, 사이버보안과의 연계

기업에서는 전 · 현직 임직원들에 대하여 업무 중 취득한 정보 등을 경쟁업체에 유출하지 못하도록 비공개조항에 대한 비밀유지의무 각서 작성 및 교육, 이와 더불어 퇴사 후 일정기간 동안 동종 또는 경쟁업체에 취업을 제한하는 내용의 전직금지 각서를 작성하게 하는 방법을 취하고 있다(다만, 헌법상 보장된 근로자의 직업선택의 자유와 근로권 등을 과도하게 제한하여 민법 제103조 위반일 경우는 예외로 함). 그럼에도 불구하고 불평등한 대우로 인한 불만과 고액 연봉의 스카우트 제의 등으로 이직을 결정하면서

영업비밀이 유출되고 있다. 이 과정에서 IT 기기 및 정보시스템이 유출의 주요한 통로로 활용되고 있다. 한편 IT 기기와 정보시스템에 영향을 받는 대형 인프라 시설의 경우 전체 링크 가운데 한 부분이 보안에 취약해도 영업비밀에 대한 백도어 액세스(back-door access)를 생성하여 전체 공급망을 위험에 빠뜨릴 수 있는데, 이점이 바로 영업비밀보호와 사이버보안이 연계되어야 하는 이유이다. 이러한 이유로 세계최고 기술선진국인 미국 역시 영업비밀을 사이버보안과 연계시키며 사이버공격과 이로 인한 영업비밀 유출을 최소화하기 위해 가능한 모든 역량을 쏟아 붓고 있다. 2021년 5월 미국 동부 지역 연료의 45%를 담당하고 있는 송유관에 대한 랜섬웨어 공격으로 이 지역의 연료공급에 차질을 빚은 것은 물론 파일 유출 및 암호화 피해가 발생한 사건은 영업비밀과 사이버보안에 대한 연계의 필요성을 다시 한 번 확인시킨 사례라고 할 것이다.

3. 미국의 영업비밀보호 현황

전 세계적으로 EU가 GDPR 제정으로 개인정보보호 영역을 주도한다면, 미국의 영업비밀보호 관련 입법례는 EU 등 타 국가에 모범사례로 여겨지고 있다. 영업비밀 등 미국의 첨단기술 유출방지 관련법으로는 컴퓨터사기 및 남용법(Computer Fraud and Abuse Act), 경제스파이법(Economic Espionage Act), 사이버정보공유 및 보호법(Cyber Intelligence Sharing and Protection Act) 등이 있는데, 주로 형사처벌의 강화에 방점이 찍혀 있다. 이는 국가 형벌권이 잠재적 유출자에 대한 사전 억제력과 사후 구제책 모두에게 효과적이라는 판단으로 비롯된 것이다. 한편, 지난 오바마 정부에서는 국가안보, 외교 또는 경제에 대한 심각한 위협으로 간주되는 해외로부터 시작된 사이버공격의 경우 연루된 개인, 단체, 국가에 대한 경제제재를 승인하는 행정명령을 공표한바 있다. 이는 영업비밀 유출 대응과 관련하여 중대한 정책 변경이 있음을 의미하는 것으로, 영업비밀은 국가의 안전보장과 국민경제 발전을 위해 해외 유출을 예방하고 관리해야 하는 공공재로서의 성격을 갖는 것으로 이해할 수 있다. 그러나 미국 내에서는 강력한 형사적 입법과 정부의 노력에도 불구하고 영업비밀보호의 한계를 지적하는 비판적 시각이 우세하다. 영업비밀 유출을 국부 유출로 바라보는 시각에서는 형사처벌과 더불어 경제제재 강화와 같은 다양한 법적 구제에도 불구하고 이들 모두 침해에 대한 본질적 해결 방안이 되지 못한다는 한계에 직면하게 된 것이다. 이런 한계를 극복하고자

능동적 사이버 방어행위로써, 사이버 공간에서 디지털 자구행위(Digital self-help)[1]를 법제화하는 방안과 영업비밀을 기업의 재화에서 공공의 재화(public goods)로 보는 전환적 시각 그리고 기업의 자발적 대응에서 의무적 조치로 하는 방안 등이 미국 내에서 거론되고 있다.

4. 우리나라에 주는 시사점

과거 우리나라 전국 각급 법원에서 선고된 영업비밀 관련 사건을 분석해보면 최소한의 안전장치도 하지 않아 유출을 막지 못한 경우도 상당했다. 즉 합리적인 노력(비밀성 유지를 위한 보안조치)을 하였더라면 상당부분 예방할 수 있었던 안타까운 사건들이 많았다는 이야기이다. 앞서 미국의 형벌강화 입법의 경우와 같이 국가 형벌권의 작동으로 영업비밀 유출을 어느 정도까지는 억지할 수 있지만, 이것이 근본적인 해결책은 될 수 없다. 오히려 법경제학적 시각으로 보면 유출에 대한 형사처벌 강화는 형벌집행에 따른 비용을 증가시키므로 효과적이지 못하다. 잠재적 유출사범에 대한 처벌보다는 영업비밀 보유자(기업 등)로 하여금 보안조치에 더욱 만전을 기하도록 하는 것이 더 유익하다. 자본주의 기술고도사회로 발전함에 따라 영업비밀과 침해가능성은 비례적으로 증가 할 것이다. 그런데 많은 예산의 투입에도 불구하고 영업비밀 유출이 지속된다면 글로벌 기업도 혁신기술개발에 소극적일 수밖에 없을 것이며, 그 결과 보호기간 종료 후 기술을 공개해야 하는 특허로 옮겨갈 가능성도 배제하지 못할 것이다. 주지하다시피 특허보다는 존속기간의 만료가 없이 사실상 영구적인 영업비밀의 경우가 경쟁회사 간 우위를 점하기에 더 유리하다. 따라서 사후적인 처벌보다는 영업비밀 침해 방지를 위한 컴플라이언스 체계 구축을 통해 사전 예방할 수 있는 방안을 확고히 하여 오랫동안 기업 자체의 비밀로 유지하는 방안을 모색해야 할 때이다. 미국 역시 법적인 사후대응에 한계를 인식하고 영업비밀을 공공재로 바라보며 예방적 대응으로 보호의 방향을 전환하고 있음을 상기해야 할 것이다.

---

1) 김성용, "사이버 공간에서 디지털 자구행위(Digital self-help) 법제도화를 위한 해킹백(Hacking Back)에 관한 소고", 『법학논총』 제34권 제1호(2021), "능동적 사이버 방어 행위"는 현실세계에서는 상대 공격(이를테면 폭행에 대한 정당방위 등)에 대한 자위권적 대응으로 자구행위를 인정하지만, 사이버 공간에서는 이를 인정하고 있지 않기 때문에 나온 이론이다. 즉 진화하는 해킹기술과 그로 인한 피해에 적극적으로 대응해야할 필요성이 제기되면서 공격자(해커)를 식별하고 도난당한 데이터를 찾아오거나 파괴하는 등의 적극적 대응을 말한다.

영업비밀보호 컴플라이언스 체크포인트

1. 법원이 제시한 비밀관리성 기준

영업비밀은 실무에서 철저한 관리가 되어야만 비로소 영구적인 보호를 받을 수 있다. 이는 비밀유지에 철저한 관리가 뒤따르지 않는다면 비밀이 공개되어 더 이상의 비밀이 될 수 없는 영업비밀의 불안정성이라는 특징 때문이다. 따라서 기업은 영업비밀 요건에 맞는 보호기준을 준수하며 피해를 최소화 할 수 있는 내부통제체계를 마련해야 한다. 아울러 계약관계에 있는 상대와의 관계에서 영업비밀 탈취 혐의를 받지 않기 위해서 상대와의 비밀유지에 만전을 기해야 한다.

이에 법원이(판결문 또는 결정문을 통하여) 비밀관리성을 인정한 기준은 아래 〈표1〉과 같다.

<표1> 법원이 제시한 비밀관리성 인정 판단기준[2)]

①	입·퇴사 시 비밀유지계약서 작성·제출
①–1	퇴사 시 전직금지 및 비밀유지서약서 및 손해배상 이행각서
②	회사 내 중요시설에 대한 물리적 보안을 위한 출입통제시스템 설치
③	중요시설에 대한 회사 내부 인원 통제
④	회사 내 노트북이나 저장매체 반출의 엄격한 관리 및 통제
⑤	CCTV 등 영상장비를 통한 영업비밀 유출행위 감시
⑥	연구개발 사항에 대한 접근대상자의 제한 및 통제
⑦	회사 컴퓨터에 대한 해킹이나 자료유출 방지를 위한 백신프로그램 설치
⑧	직원들에 대한 정기적인 보안교육
⑧–1	비정기적이라도 직원들에게 외부 유출을 차단하기 위한 보안교육
⑧–2	이메일을 통해 정보유출 및 정보의 개인적인 사용을 경고
⑧–2–Ⓐ	발각 시 그에 따른 징계조치를 한다고 공지하는 등 비밀준수의무 부과
⑨	비밀문서임을 알리는 표시와 더불어 문서(정보)를 비밀로 적시하여 분류
⑩	문서나 파일 등의 정보자산에 대한 관리기준

2) 김성용·정관영, "법조(法曹)영역으로의 인공지능 도입에 대한 제언"–영업비밀 침해사건을 중심으로–, LAW & TECHNOLOGY, 서울대학교 기술과 법센터, 제15권 제2호(2019). 참조

⑪	보안규정 마련 및 보안담당자의 배치
⑫	정기적인 보안검사 실시
⑬	영업비밀로 관리하고 있던 정보 유출 후 그에 따른 신속한 법적조치
⑭	포괄적, 개략적, 추상적인 분류가 아닌 중요도에 따른 체계적 분류
⑮	취업규칙에 업무상 지득한 비밀의 누설을 금지

반면 법원이 비밀관리성을 부정하면서 그 이유에 대해 판결문 또는 결정문에 판시한 기준은 아래 〈표2〉와 같다.

<표2> 법원이 제시한 비밀관리성 부정 판단기준

Ⓐ	문서가 별도 관리되지 않고 혼재되어 보관된 점
Ⓑ	내부정보 유출방지시스템을 갖추지 않은 점
Ⓒ	퇴사 시 회사 내 소지물품 확인 및 삭제하는 등의 조치를 취하지 않은 점
Ⓓ	협업자들의 공유상태 파일을 다운로드 하는데 제한이 없었던 점
Ⓔ	회사에서 제공되지 아니한 저장매체로 회사 컴퓨터 이용이 통제되지 않은 점
Ⓕ	대외비나 비밀자료 표시가 없는 점
Ⓖ	사용자 계정과 비밀번호 설정 외 파일비밀을 위한 별도 보안장치가 없는 점
Ⓗ	중요도에 따라 비밀등급을 분류하거나 표시가 없는 점
Ⓘ	중소기업이라도 보안관리 규정의 제정 및 시행을 하지 않은 점
Ⓘ–1	보안담당부서 내지 보안담당자 지정하지 않은 점
Ⓘ–2	정기적인 보안검사 내지 보안교육 등을 실시하지 않은 점
Ⓙ	네트워크를 통한 물리적인 접근가능성
Ⓙ–1	접근할 수 있는 대상자나 접근방법을 제한하는 조치를 취하지 않은 점
Ⓚ	특허출원된 발명의 경우 출원된 내용 이외의 정보가 비밀로 관리되었는지

3) 영업비밀유지 의무를 부담시키고 또 그 비밀유지의무를 실질적으로 담보하기 위해 퇴직 후 일정기간 경업금지의무를 부담시키는 내용 포함. 단, 직업선택의 자유에 관한 헌법규정에 반하지 않는 범위에서.

4) 김성용·정관영, supra note 2.

2. 기업이 꼭 준수해야하는 기업정보의 관리방법(영업비밀 침해 방지를 위한 컴플라이언스)

기업은 자사의 영업비밀보호를 위해 크게 3가지 즉 ① 제도적 장치(ex, 관리규정 제정, 영업비밀 분류, 영업비밀 지정 및 표시, 접근권한자 지정) ② 물리적 보안 장치(ex, 보안시스템, 통제구역 설정, 컴퓨터 보안 및 통신 보안, 보안서류 표시) ③ 인적 장치(ex, 종업원 관리, 거래처 및 협력업체의 관리)와 같은 전략을 갖추어야 한다. 이를 항목별로 구체화 하면 아래와 같이 정리할 수 있다.

정보시스템 보안 강화 및 감시체계구축

- 메일의 송수신처의 제한
- web메일로의 접근제한
- web사이트 열람제한
- 로그 감시체계

비밀관리규칙 제정

- 모든 직원이 영업비밀의 존재를 인식할 수 있도록 교육하고 표시
- 영업비밀 '관리규칙' 또는 '문서관리규칙'을 제정하여 비밀로 관리하는 문서의 관리 및 분류, 파기 등의 절차를 명문화

접근통제 및 개발부서의 분리

- 기업기밀과 연관된 연구개발 및 생산공정은 장소적 분리 및 보안 필요
- 기업정보에 대해 특정 관계자 외의 접근 통제
- 출입 시 영업비밀 취급 부서의 회사 ID카드와 별도의 ID카드로 출입하도록 설정
- 내부 네트워크상 공유파일에도 영업비밀 표시

비밀유지의무 부과

- 내부적 정보를 다루는 모든 사원과 대외적 용역개발 모두 일정한 비밀유지의무가 발생함을 유의하여야 함(용역개발계약서에 비밀유지조항을 포함)
- 고용계약서 또는 서약서에 비밀유지의무를 명시(신입 직원에게는 전직 회사의 영업비밀을 의무기간 동안 비밀로 유지하도록 주의)필요

전직금지의무 부과

- 연구개발부서의 직원이 경쟁기업으로 옮겨 비밀을 유출할 것을 대비하여 당해 직원과 전직금지 계약 체결 필요(다만 과도한 기간 설정은 약정자체가 무효가 될 수 있으니 유의)

재직 종업원 관리

- 청렴윤리경영 가이드라인 수립 및 이에 대한 지속적인 교육
- Monitoring/Auditing
- 징계 기준 마련

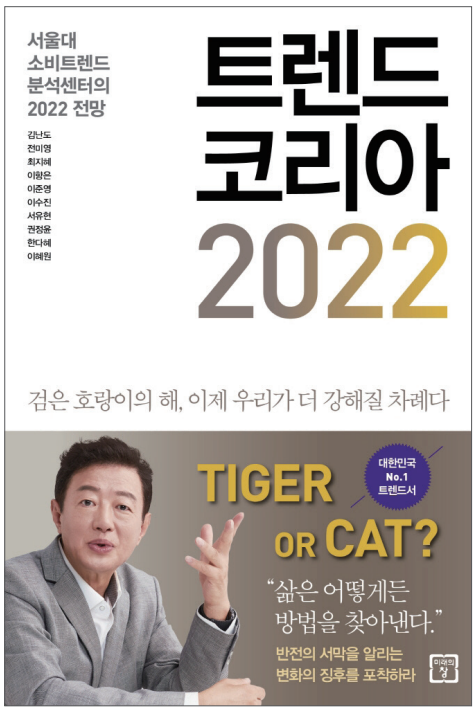
퇴사자 관리

- 연구개발부서의 직원 또는 영업비밀 관리부서의 직원이 퇴직 할 경우 영업비밀에 대한 인수인계를 철저히 한다.
- 영업비밀 관련 서류 및 프로그램 등 일체를 반납토록 하며 파일 삭제를 요구하여야 한다.
- 영업비밀유지 의무 또는 전직금지 의무 사항을 상기시켜 위반 시 처벌될 수 있음을 설명한다.

이상 살펴본 바와 같이 기업은 자사의 중요 정보를 소중하게 관리하기 위해 법원이 제시한 비밀관리성 기준과 기업정보의 관리방법을 참고하여 내부통제강화를 위한 자체시스템 확보에 최선을 다하여야 한다. 특히 벤처회사 등 소수의 인적구성과 끈끈한 신뢰를 토대로 운영되는 소위 '가족과 같은 분위기의 회사'는 비밀유지서약서 및 전직금지약정을 체결하지 않는 것이 문제이므로, 종업원 관리(서약서 및 지속적인 교육) 및 퇴사자 관리에 주의를 기울여야 한다.

문화 속
기업윤리

공감이 필요한 시대 기업에 필요한 변화 책, '트렌드 코리아 2022'



* 이미지 출처: 교보문고

트렌드 변화의 속도가 눈에 띄게 빨라지면서 우리 사회는 그에 맞는 대응방법을 놓고 고민하고 있다. 이에 책 '트렌드 코리아 2022'가 정의한 올해의 트렌드 10가지 중, '나노사회'와 '실재감테크'를 주요 키워드로 살펴보고자한다.

먼저 '나노사회'란 우리 사회가 극도로 미세한 단위로 분화되어 있음을 나타내는 말이다. 일상에 생각지 못하게 많은 제약이 생기면서, 공동체는 개인으로 흩어지고 공동체적 유대 역시 파편화되었다. 이러한 사회분화는 공공부문을 비롯한 민간기업이 사회적 기호의 흐름을 파악하기 어렵게 하고 있다. 이에 덧붙여 지나친 성취와 경쟁이 요구되는 사회 분위기 또한 사회분화의 원인으로 꼽힌다. 공정성이 담보되지 않는 사회가 우리를 더욱 치열하게 만들고, 사회구성원의 분열을 가속화하고 있는 것이다.

한편, '실재감테크' 키워드에서는 기술, 경영방식의 혁신이 강조된다. 실재감테크란 시공간의 물리적 한계를 극복하고 기술 이용자들이 완전한 실재감을 느끼게 만드는 혁신기술 전반을 의미한다. 코로나19의 장기화로 재택근무가 확대되면서 직원 간 결속력 저하를 우려하는 시선이 있는 가운데, 가상공간의 실재감을 높이는 것은 소속감, 유대감을 증대하는 데 필요한 기술로 각광받는다.

기술의 고도화와 공동체 결속력의 약화가 동시에 화두로 떠오른 지금, 이러한 변화의 흐름 속에 또 한 번 강조되는 것이 바로 공감력이다. 자신과 다른 의견에 '나는', '우리 때는' 그렇지 않다는 잣대를 들이미는 대신, '이해'라는 기본 가치를 지키면서 동시에 변화의 흐름을 파악하며 공감대를 넓힐 수 있어야 한다.

국내동향

뉴스클립

지난해 주식 불공정거래 혐의 70%가 '미공개 정보 이용'

유형별 혐의통보 실적 (단위: 건)

유형 구분	'19년	(비중)	'20년	(비중)	'21년	(비중)
부정 거래	28	23.3%	23	20.5%	10	9.2%
시세 조종	20	16.7%	33	29.5%	13	11.9%
미공개 정보 이용	57	47.5%	51	45.5%	77	70.6%
보고 의무 위반	3	2.5%	5	4.5%	4	3.7%
기타	12	10.0%	–	–	5	4.6%
총계	120	100.0%	112	100.0%	109	100.0%

[자료=한국거래소]

한국거래소가 발표한 '2021년도 불공정거래 심리실적 및 주요 특징'에 따르면 지난 2021년 적발된 주식시장 불공정거래의 70%가 '미공개 정보 이용'인 것으로 나타났다. 거래소 시장감시위원회가 지난 2021년 적발한 109건의 불공정거래 혐의사건 중 미공개 정보 이용이 77건으로 2020년 51건에 비해 크게 증가한 것으로 나타났다. 전체 불공정거래 혐의사건 중 미공개 정보 이용이 차지하는 비중도 2020년 45.5%에서 2021년 70.6%로 늘었다.

참고: 아주경제. 2022. 02. 15

공정위, 5개사에 과징금 1천350억 원

공정거래위원회('공정위')는 공정거래법을 위반한 5개 빙과류 제조 · 판매사업자에 시정명령과 과징금 총 1천350억4천500만 원을 부과한다고 밝혔다. 공정위 조사 결과, 이 중에서 4개사는 2016년 2월 15일~2019년 10월 1일 아이스크림 판매 · 납품 가격 및 소매점 거래처 분할 등을 합의하고 실행에 옮겼다고 한다. 통상 제조사들은 납품 가격을 낮춰 소매점 거래처를 늘리고 유통업체들의 대량 매입을 유도하는 방식으로 경쟁하는데, 2016년 당시 아이스크림 주요 소비층인 저연령 인구가 줄고 소매점이 감소함에 따라 수익성이 악화하자 4개사는 담합을 시작한 것으로 조사됐다.

참고: 매일경제. 2022. 02. 17

해외동향

메타 얼굴인식 기술이 사생활 침해, 수천억 달러 피소

텍사스주 검찰총장은 메타의 얼굴인식 시스템이 개인의 생체 데이터를 보호하는 텍사스주의 사생활 보호법을 위반했다며 법원에 소송을 제기했다. 2015년에는 미 일리노이주가 주민의 생체 정보를 이용하려면 동의를 해야 한다는 주법을 위반했다며 유사한 소송을 제기했고, 메타(당시 페이스북)는 2020년 6억5000만 달러(약 7800억 원)를 지급하기로 합의한 바 있다. 국내에서도 이용자의 동의 없이 얼굴 정보를 수집했다며 지난해 개인정보보호위원회로부터 64억4000만 원의 과징금을 부과받았다.

참고: 동아일보, 2022. 02. 16

담배 회사 몰려있는 스위스도 광고 규제

스위스 국민투표 결과 과반수가 담배 광고 규제 강화 법안에 찬성하여 앞으로 스위스 공공장소에서 담배 광고가 사라진다. 이번 투표 결과에 따라 신문 · 인터넷 · 영화관 등 공공을 대상으로 하는 담배 광고 제한법 개정안이 2023년부터 시행된다. 스위스는 현재 스위스 내 담배 광고 대부분 합법적으로 다른 선진국에 비해 담배 관련 규제가 느슨하다는 평가를 받아왔다. 필립모리스인터내셔널(PMI)과 브리티시아메리칸토바코(BTC) 등 거대 담배 회사들이 스위스에 본사를 두고 있다.

참고: 매일경제, 2022. 02. 14

바로보는 기업윤리

웹툰

02. 당신의 메일함, 안전한가요?

날로 발전하는 스팸메일은 랜섬웨어 등의 바이러스, 해킹, 피싱 등을 동반해 기업의 주요 데이터관리에 위협을 끼칩니다. 출처가 불분명한 이메일 또는 첨부파일 이중 확인, 중요자료의 정기적인 백업, 백신 프로그램 설치 및 업데이트 등 개인과 조직의 더욱 세심한 관리가 요구됩니다.

행사소식

BIS (Business Integrity Society) Summit 2022

ESG 시대의 반부패 아젠다를 살펴보고 청렴한 비즈니스 환경 조성을 위해 기업들이 반부패 공동노력에 참여하는 컨퍼런스

주최 유엔글로벌콤팩트 한국협회, 한국사회책임투자포럼

일시 2022년 3월 25일(금) 09:30 – 16:00

장소 온라인/오프라인(광화문 포시즌즈호텔)

참고: http://unglobalcompact.kr/our-work/notice/?mod=document&uid=2196

ECI IMPACT Conference

다양한 영역의 윤리 및 컴플라이언스와 관련하여 전문가들과 조직의 대응, 실용적인 정보 및 리소스 등에 대한 통찰력을 공유하는 컨퍼런스

주최 Ethics & Compliance Initiative

일시 2022년 4월 19~22일

장소 Virtual Conference

참고: https://www.ethics.org/impact/

퀴즈

Q. 다음 중 기업의 비밀관리성 인정 판단기준에 해당하지 않는 것은?

① 입 · 퇴사 시 비밀유지계약서 작성 · 제출
② 대외비 또는 비밀자료 미표시
③ 직원들에 대한 정기적인 보안교육
④ 중요시설에 대한 회사 내부 인원 통제

지난 호 정답자는
김해용님, **이상준**님, **노명덕**님, **이민경**님, **강지숙**님입니다.
축하드립니다!!

정답 제출처 국민권익위원회 민간협력담당관실(mail@innocrew.co.kr)
성함, 연락처(휴대폰 번호)를 보내주세요(22일까지)

정답을 보내주신 분 중 5명을 추첨하여 모바일 기프티콘을 보내드립니다.
* 수집된 개인정보는 상품 발송을 위한 정보로만 활용되며, 추첨 이후 파기됩니다.