

August 27, 2026

영업비밀 침해 규율의 사각지대 보완 - 브로커·해킹 및 부정취득 영업비밀의 사용·누설에 대한 규제 강화

I. 부정경쟁방지 및 영업비밀보호에 관한 법률 개정 배경

2026년 8월 20일 「부정경쟁방지 및 영업비밀보호에 관한 법률」(이하 “부정경쟁방지법”) 일부개정법률안이 국회 본회의를 통과하였습니다.

최근 영업비밀 침해는 임직원이 직접 자료를 반출하는 전통적인 형태를 넘어, 기업의 핵심인력을 경쟁사로 이직시키면서 영업비밀 유출을 유도하거나, 해킹을 통하여 정보를 탈취하고, 이를 다시 제3자에게 전달·유통하는 등 그 수법이 다양화·고도화되고 있습니다. 이번 개정은 이러한 현실을 반영하여 영업비밀을 직접 취득하는 행위뿐만 아니라 침해를 소개·알선·유인하는 행위와 부정취득 이후의 사용·누설행위까지 규율을 강화하였다는 점에 의의가 있습니다.

개정법은 공포 후 6개월이 경과한 날부터 시행될 예정입니다.

II. 주요 개정 내용

1. 영업비밀의 부정취득 방법에 ‘해킹’을 명시

현행 부정경쟁방지법은 영업비밀의 부정취득행위를 “절취, 기망, 협박, 그 밖의 부정한 수단으로 영업비밀을 취득하는 행위”로 규정하고 있습니다.

이번 개정은 제2조 제3호 가목의 부정취득 방법에 ‘해킹’을 명시적으로 추가하였습니다. 이에 따라 해킹을 통하여 타인의 영업비밀을 취득하는 행위가 영업비밀 침해행위에 해당하고 처벌 대상이 된다는 점이 법문상 더욱 명확해졌습니다.

기존에도 해킹이 ‘그 밖의 부정한 수단’에 해당할 수 있었으나, 이번 개정을 통해 사이버 공격을 이용한 영업비밀 탈취행위가 법률상 명시적으로 규율됨으로써 해킹에 의한 기술유출에 대한 법적 대응의 명확성이 한층 강화될 것으로 예상됩니다.

한편, 중대범죄수사청 조직 및 운영에 관한 법률(중수청법)의 적용대상이 되는 중대범죄의 한 유형으로 「산업기술의 유출방지 및 보호에 관한 법률」 및 부정경쟁방지법의 기술유출 등 국가핵심기반 공격에 해당하는 사이버범죄를 규정하고 있는데, 해킹 사고에 의한 영업비밀침해행위의 형사처벌에 있어서는 중수청과 지식재산처의 중첩적인 수사대상이 될 수 있다는 점을 주목할 필요가 있습니다.

2. 영업비밀 침해행위의 '소개·알선 또는 유인' 행위를 독립적인 침해행위로 신설

이번 개정에서 특히 주목할 부분은 영업비밀 침해행위를 "소개·알선 또는 유인하는 행위" 자체를 새로운 영업비밀 침해행위의 유형으로 규정하였다는 점입니다(개정법 제2조 제3호 사목).

종래 기술유출 사건에서는 경쟁사 등이 기업의 핵심인력을 이직시키는 과정에서 중개인 또는 이른바 '브로커'가 개입하여 영업비밀 유출을 적극적으로 유도하거나 관여하는 사례가 문제되어 왔습니다. 그러나 실제 영업비밀을 취득·사용한 자가 아닌 중간 알선자에 대해서는 영업비밀 침해행위 자체를 이유로 직접적인 책임을 묻기가 쉽지 않았습니다.

이번 개정으로 이러한 규제의 공백이 상당 부분 해소될 것으로 보입니다. 특히 개정 조문의 문언은 특정한 형태의 이직 알선에 한정되지 않고, 부정경쟁방지법상 영업비밀 침해행위를 소개·알선하거나 유인하는 행위 전반을 대상으로 하고 있습니다.

이에 따라 영업비밀 유출을 전제로 핵심인력의 이직을 알선하는 브로커 등에 대하여 금지청구 및 손해배상 등 민사상 책임을 물을 수 있을 뿐만 아니라, 형사처벌 규정도 적용할 수 있는 근거가 마련되었습니다.

3. 부정하게 취득한 영업비밀의 '사용·누설'에 대한 처벌 강화

개정 전에는 부정한 방법으로 영업비밀을 취득한 자가 해당 영업비밀을 이후 사용하거나 제3자에게 공개·누설한 경우, 그 후속 행위를 처벌하기 위해서는 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적이 있었다는 점이 별도로 문제될 수 있었습니다.

이번 개정은 부정한 수단으로 영업비밀을 취득한 자가 그와 같이 취득한 영업비밀을 사용하거나 제3자에게 누설하는 행위를 형사처벌 대상에 명시적으로 포함하였습니다(개정법 제18조 제1항 제2호).

이에 따라 일단 영업비밀을 부정한 방법으로 취득한 사실이 인정되는 경우, 그 이후의 사용·누설행위에 대하여 별도의 부정한 목적을 입증하여야 하는 부담이 완화되어 영업비밀 침해에 대한 형사법적 대응이 보다 용이해질 것으로 예상됩니다.

4. 침해 개입 사실을 알고 영업비밀을 전득한 자의 '누설'도 처벌

이번 개정은 최초 부정취득자뿐만 아니라 그로부터 영업비밀을 전달받은 전득자에 대한 규율도 강화하였습니다.

기존에는 영업비밀 침해행위가 개입된 사실을 알면서 해당 영업비밀을 취득하거나

사용하는 행위를 처벌 대상으로 규정하고 있었으나, 개정법은 이에 더하여 그 영업비밀을 제3자에게 누설하는 행위까지 명시적인 처벌 대상으로 추가하였습니다(개정법 제18조 제1항 제3호).

이는 부정취득된 영업비밀이 최초 취득자에게 머무르지 않고 여러 기업이나 관계자를 거쳐 유통되는 현실을 반영한 것으로, 향후 수사기관 역시 최초 유출자뿐만 아니라 영업비밀의 전달·유통 경로 전반을 보다 적극적으로 조사할 가능성이 있습니다.

III. 시사점

이번 개정은 단순히 새로운 침해수단 몇 가지를 추가한 것에 그치지 않습니다. 영업비밀 침해에 대한 규율의 초점이 '누가 직접 영업비밀을 빼냈는가'에서 '누가 침해를 유도·알선하였고, 취득된 영업비밀이 이후 누구에게 전달되어 어떻게 사용·유통되었는가'까지 확대되고 있다는 점에 주목할 필요가 있습니다.

첫째, 경쟁사 경력직 인력의 채용 과정에 대한 관리가 한층 중요해졌습니다. 특히 헤드헌터, 채용대행업체 또는 기타 중개인을 통하여 경쟁사 임직원을 영입하는 과정에서 종전 회사의 기술자료나 영업상 정보를 가져오도록 요구하거나 이를 전제로 이직을 제안하는 경우, 실제 자료를 취득·사용한 당사자뿐 아니라 그 과정에 관여한 자의 민, 형사상 책임까지 문제될 수 있습니다. 기업으로서는 채용 및 온보딩 과정에서 전 직장의 영업비밀을 반입하거나 활용하지 않도록 명확한 원칙과 절차를 마련할 필요가 있습니다.

둘째, 외부에서 유입되는 기술정보의 출처와 취득경위를 확인하는 절차가 중요해질 것입니다. 퇴직자, 협력업체, 컨설턴트 또는 사업파트너를 통하여 경쟁사의 기술자료를 제공받는 경우 그 정보의 출처와 제공권한을 충분히 확인하지 않은 채 기업 내부에서 사용·공유하는 것은 상당한 리스크를 수반할 수 있습니다. 특히 영업비밀 침해행위가 개입되었다는 사실을 인식하였거나 인식할 수 있을 수 있는 상황임에도 해당 정보를 계속 사용하거나 제3자에게 전달하는 행위는 형사책임으로 이어질 수 있으므로, 의심스러운 정보가 유입된 경우 즉시 사용과 전파를 중단하고 법적 검토를 거치는 체계를 갖출 필요가 있습니다.

셋째, 해킹 등 사이버 침해사고에 대한 대응 역시 영업비밀 보호 체계와 연계하여 정비할 필요가 있습니다. 해킹을 통한 영업비밀 취득이 법문에 명시된 만큼, 향후 사이버 침해사고가 발생한 경우 단순한 정보보안 사고를 넘어 영업비밀 침해사건으로 민·형사상 대응이 이루어져야 할 가능성이 더욱 커졌습니다. 이에 따라 접근기록, 다운로드·전송기록 및 외부 접속기록 등 디지털 증거를 적시에 확보·보존할 수 있는 체계를 마련하는 것이 중요합니다. 동시에 침해된 정보가 법률상 '영업비밀'로 인정받기 위해 필요한 비밀관리조치 역시 지속적으로 점검하여야 합니다.

넷째, 영업비밀 침해 피해기업의 대응 범위도 확대될 수 있습니다. 향후에는 직접적인 유출자나 경쟁사뿐 아니라 영업비밀 유출을 기획·알선한 브로커와 부정취득된 정보를 전달받아 사용·유통한 관계자들까지 고려한 법적 조치를 신속, 정확하게 다각도로 마련해 두는 것을 고려하여야 할 수 있습니다. 따라서 침해사고가 의심되는 경우 관련자의 연락·이직 경위, 자료의 전달 경로, 외부 접속기록 등 영업비밀의 이동 경로를 조기에 파악하고 관련 증거를 확보하는 것이 더욱 중요해질 것입니다.

IV. 맺음말 – 기업의 대응 방향

이번 개정은 영업비밀 침해행위에 대한 규율을 침해의 유도·알선 단계에서부터 부정취득, 사용 및 제3자에 대한 누설·유통 단계까지 확장·구체화하려는 입법적 흐름을 보여주고 있습니다. 이에 따라 기업들은 개정법 시행 전의 준비기간을 활용하여 기존 영업비밀 관리체계를 다시 점검할 필요가 있습니다.

특히 이번 개정으로 기업은 한편으로는 영업비밀 침해의 피해자로서 보다 다양한 행위자에 대한 법적 대응수단을 활용할 수 있게 되었지만, 다른 한편으로는 경쟁사 인력의 채용이나 외부 기술정보의 수령·활용 과정에서 해당 기업이 의도하지 않게 영업비밀 침해의 유통과정에 관여될 수 있는 리스크에도 더욱 유의하여야 합니다.

따라서 개정법 시행에 앞서 영업비밀 관리규정만을 형식적으로 정비하는 데 그치지 않고, 실제 채용, 연구개발, 협력업체 관리, 정보보안 및 사고 대응 프로세스 전반에서 영업비밀의 유입·사용·반출 경로를 점검하고 관련 컴플라이언스 절차를 구체화하는 것이 바람직합니다.

법무법인(유한) 태평양은 개정 부정경쟁방지법에 따른 기업의 영업비밀 관리체계 점검, 내부 규정 및 계약서 정비, 핵심인력 채용 관련 리스크 검토 및 영업비밀 침해사고에 대한 민·형사상 대응과 관련하여 필요한 자문 및 분쟁 대응 업무를 신속, 정확하게 제공하고 있습니다.

관련 구성원

김지현

변호사

T 02.3404.0180

E jihyun.kim@bkl.co.kr

김정대

변호사

T 02.3404.6407

E jeongdae.kim@bkl.co.kr

윤택

변호사

T 02.3404.7450

E taek.yoon@bkl.co.kr

본 Legal Update는 유승엽 변호사가 함께 참여하였습니다.

법무법인(유한) 태평양의 뉴스레터에 게재된 내용 및 의견은 일반적인 정보제공만을 목적으로 발행된 것이며, 법무법인(유한) 태평양의 공식적인 견해나 어떤 구체적 사안에 대한 법률적 의견을 드리는 것이 아님을 알려드립니다. 뉴스레터와 관련된 문의사항이 있을 경우 위 연락처로 문의주시기 바랍니다.