법무법인(유) 린

Tech Legal Insights

AID (Artificial Intelligence Decoding) Vol. 13

2026. 01

고영향 AI사업자의 위험관리방안과 사이버보안의무

2026년 1월 22일부터 시행되는 '인공지능발전과 신뢰기반조성 등에 관한 기본법' (이하 "AI 기본법"으로 칭함)은 고영향 AI사업자의 책무 중 첫번째로 '위험관리방안의 수립, 운영'을 들고 있습니다(제34조). 관련 고시(안)는 이를 ①위험관리정책 수립 및 이행, ②위험관리 조직체계 수립 및 운영이 포함되어야 한다고 설명합니다.

후자의 위험관리 전담조직, 인력 등 내부 거버넌스 문제는 차치하더라도 전자는 사업자로 하여금 AI사용으로 인한 위험을 식별, 분석, 평가하고 이에 따른 위험을 처리하는 적절한 조치, 그리고 이에 대한 확인까지 하도록 광범위하게 요구하고 있습니다. 비록 법 규정은 사업자가 자발적으로 준수하도록 권고하는 형식을 취하고 있지만 최소한 '기록관리체계의 정비'를 요구하고 있고, 사이버보안의무 또한 핵심적 의무 내용으로 들어가 있습니다.

최근 쿠팡 사태로 사이버보안에 대한 국민적 관심이 높아진 상황에서, 고영향AI 사업자에게 '위험관리방안의 수립·운영'은 가장 시급하고 중요한 법률 과제입니다. EU AI법 제9조에 규정된 대로 고위험AI시스템에 대한 이러한 '위험관리방안' (risk management system)의 수립, 운영은 고위험 AI시스템의 전 수명주기 (life cycle)에 걸쳐 있는 법적 의무이며 우리의 기술고시(안) 역시 이 점을 분명히 확인하고 있습니다.

한편, EU는 2024년 10월 18일부터 사이버보안에 대한 일반 법인 NIS (Network and Information Security) Directive 2 (2022/2555)를 회원국 국내법을 통해 본격적으로 강제 시행함으로써 사이버보안이 IT기술팀의 문제가 아니라 경영진의 책임문제로 (이사회의 안건화) 전환을 시킨 바 있습니다. 더욱이 에너지, 교통, 금융은 물론이고 플랫폼, 데이터 처리 기업 등도 다 적용 대상에 포함시킴으로써 EU시장에 대한 국내 수출기업 대부분이 규제 대상으로 되어 버렸습니다.

Related Areas

[AI · 플랫폼 · 테크놀로지 부문]
AI법, EU CRA, 사이버보안

Contact

구태언 변호사
T. 02-3477-8695
E. tekoo@law-lin.com

방석호 미국변호사
T. 02-3477-8695
E. shbang@law-lin.com

여기에 더해 EU는 2024년 12월부터는 'Cyber Resilience Act'라는 이름으로 (Regulation 2024/2847; 이하 "CRA"라 칭함) 종전의 'Cybersecurity Act' (Regulation 2019/881; 이하 "CSA"라 칭함)를 보완하는 전혀 다른 차원의 사이버보안법을 시행중이고 이미 시행중인 AI법상의 고위험AI시스템에 대한 사이버보안요구(제15조)를 고려한 특별규정도 둠으로써 (CRA 제12조) 사이버보안에 대해서는 EU차원에서 일관된 관리와 규제를 하고 있습니다.

이하에서는 우리 AI기본법상 고영향사업자의 책무 가운데 첫번째로 부과되는 '위험관리방안'과 그 안에 담겨야 할 사이버보안요구를 중심으로 관련 법들을 분석, 국내 사업자들에 대한 적절한 준비 가이드라인을 제공하고자 합니다.

Ⅰ. AI 법상의 위험관리방안

1. EU AI법 제9조는 고위험(High-Risk) AI 제공기업에 위험관리방안을 핵심 의무로 규정하며, 일회성 체크리스트가 아닌 전체 생애주기에 걸친 지속적·반복적 프로세스를 요구합니다. 우리 AI기본법도 동일합니다. 즉 고위험 (고영향) AI시스템의 기획, 설계, 개발부터 시장 출시 후, 모델의 수명이 다할 때까지 진행, 유지되어야 하는 반복적이고 동적인 과정이라고 할 수 있습니다.

특히 고위험 AI활용으로 인한 위험 관리를 위한 구체적 단계로 EU AI법이 제시한 4단계 프로세스는 우리의 AI기본법 고시(안)도 답습하고 있을 정도의 기본적 틀이라고 할 수 있고, 구체적으로는 ①위험 식별 및 분석 ②평가 ③사후 데이터반영 ④대응조치 채택의 4단계입니다.

첫번째로 제시된 위험의 식별 및 분석 단계는 기술적 차원의 안전성 확보만을 위한 체크가 아니라 고위험의 개념 정의에 따라 '기본권침해여부'까지 포함하여야만 하기에 사업자 입장에서는 EU AI법 제27조, 우리 AI 기본법 제35조에 규정된 기본권영향평가와 연계하여 준비할 수밖에 없어 보입니다.

다만 EU AI법에 명시되어 있는 바와 같이 기본권영향평가는 AI 모델개발자(provider)가 아닌 이용사업자(deployer)의 의무이고 적용 대상 또한 3가지로 법에 한정되어 있지만 우리의 시행령과 고시(안)은 고영향AI이용사업자뿐 아니라 모든 AI사업자로 하여금 자율적으로 영향평가를 수행, 실천하도록 장려하고 있습니다.

EU AI법은 구체적으로 첫째, 공공기관이 고위험AI를 사용하는 경우, 둘째, 교육, 보건 등의 공공서비스를 제공하는 민간이 고위험 AI를 사용하는 경우, 그리고 마지막으로 부록(Annex III)에서 개인신용평가 내지 신용점수 산출, 생명과 건강보험에서의 위험평가와 보험료율 책정에 사용되어질 때에 기본권영향평가를 받도록 한정하고 있습니다. 특히 마지막 세번째의 금융, 보험에서의 '배제, 차별' 위험으로 인한

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

기본권영향평가 세부지침은 결국 AI법상의 감독기구인 EU AI Office가 만들어서 시행하여야 될 것으로 보입니다.

한편 고위험(영향)AI시스템은 모델개발자(provider)에게 개발 단계부터 위험관리 의무를 부과하지만, 이용 단계의 잠재적 위험 관리를 위해 이용사업자(deployer)에게도 기본권영향평가를 의무화합니다. AI를 어떤 맥락에서 어떻게 사용할 것인지 (intended purpose)가 중요할 수밖에 없고, 따라서 기본권영향평가는 '첫 사용'(first use) 전에 시행하게끔 하고 있습니다.

우리 AI기본법은 기본권영향평가 제35조를 사업자가 지키도록 노력하는 정도의 주의 규정으로 정하고 있고 동 조 제2항은 "국가기관등이 고영향 인공지능을 이용한 제품 또는 서비스를 이용하려는 경우에는 영향평가를 실시한 제품 또는 서비스를 우선적으로 고려하여야 한다"고 함으로써 EU AI법처럼 기본권영향평가가 제한적으로만 적용되어질 수 있는 여지가 있음을 보여주고 있습니다.

또한 다양한 기본권에 발생할 수 있는 '합리적으로 예측 가능한 위험'을 파악하고 이를 반영하는 실무적 조치를 지원할 기본권영향평가 전담기관으로 정보통신정책연구원(KISDI)이 지정되어 있습니다.

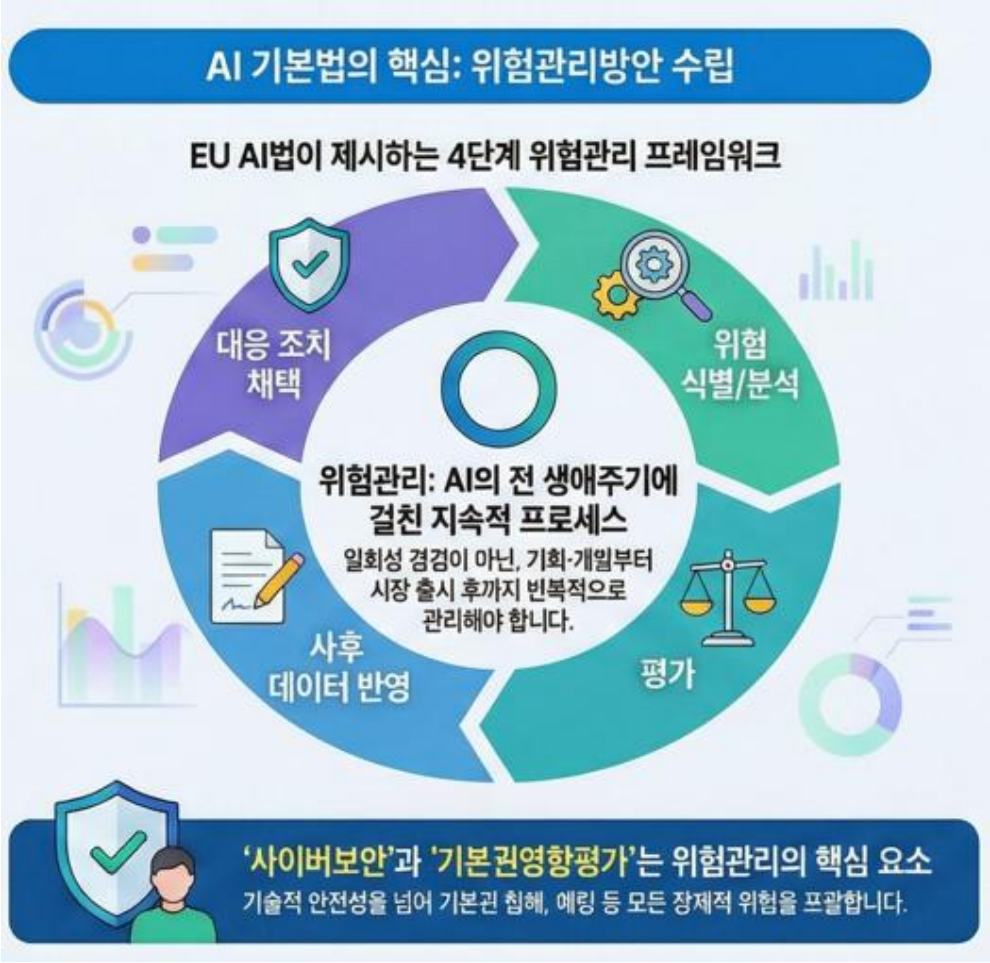
2. 위험관리방안의 둘째 단계로 제시된 '평가'는 사용자의 의도와 다르게 사용된 오용(misuse)도 당연히 포함되기 때문에 해킹, 불법 접속 등과 같은 사이버보안사고 역시 포함됩니다.

즉 EU AI법 제9조에서의 '위험'(risk)은 기본권에 가해지는 위험은 물론이고, 고위험 시스템 자체에 가해지는 위험 (오작동, 조작, 악용 등)도 포함되기 때문에 제15조에 규정된 '정확성, 견고성, 사이버보안'은 독립된 규정이라기 보다는 제9조의 위험에 대한 구체적 예시규정으로 이해하는 것이 타당합니다. 따라서 실무적으로는 제9조의 위험관리방안의 수립, 체계화 작업 시 제15조의 사이버보안에 대한 부분도 포함되도록 만드는 것이 필요합니다. 또한 제27조의 기본권영향평가와도 연계되어 체크되어질 수 있기 때문에 고위험 AI 영역의 서비스나 제품의 사업자 (모델제공자와 이용사업자 포함)는 제9조의 상위 우산속에서 일어날 고위험관리 방안에 대한 다양한 세부 체크리스트를 미리 준비하여야만 함은 우리 사업자들도 동일합니다.

다시 말해, EU AI법 제9조는 고위험AI시스템의 사용시 발생하게 되는 위험에 대한 원칙적 상위 규정이고 구체적 위험관리는 제15조, 제27조에서 추가로 정하고 있고 관련 사업자들에게 이를 분담시키는 구조이며, 우리 AI기본법 시행시 동일하게 해석될 수 있습니다.

예를 들어, 금융기관 AI 신용평가 시스템 해킹으로 특정 계층이 불이익을 받으면 제9조(위험관리), 제15조(사이버보안), 제27조(기본권평가)는 물론 CRA, NIS 2(Network and Information Security; EU Directive 2022/2555)까지 연계되어 위반이 입체적으로 검토되므로 우리 AI기본법 시행에 따른 국내 사업자들의 대응체제도 같은 맥락에서 준비할 필요가 있습니다. 결국, 사이버보안사고가 발생함으로써 기본권침해가 발생하게 되고, 위험관리방안에 따른 대응조치가 자동 작동되는 연결구조인 셈입니다.

麟
서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com



Ⅱ. 사이버보안요구

1. 2016년에 제정된 EU NIS 1법은 사이버사고에 대비한 적절한 보안조치, 사고발생시 보고를 규정한 선언적, 기술중심의 광범위한 사이버보안법 (Directive)이었다면 2022년의 EU NIS 2법은 경영진의 책임을 통해 조직 차원의 사이버 보안 거버넌스를 강제하는 법이라고 할 수 있습니다.

즉 구체적으로 사업자는 위험관리를 위해 조직에 맞춘 적절하고 비례적으로 위험분석 및 보안정책, 사고대응계획, 취약점관리, 암호화, 접근 통제 등의 보안조치를 취하여야만 하고 사이버사고 발생시 24시간 이내 초기 통지, 72시간 이내 상세보고, 1개월 이내 최종보고를 하여야만 하며 무엇보다도 보안의 문제가 경영진의 책임으로 규정하고 있으며, 위반에 따른 제재의 정도 또한EU GDPR에 유사할 정도로 강하게 규정하고 있습니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

법적으로 NIS 2는 Directive이기 때문에 EU에 수출을 하고 있는 한국 기업의 본사 자체에는 적용되지 못하고 EU 회원국내에 설립된 법인, 사업장과 같은 사업적 존재가 있거나 서비스 공급체계 (supply chain)에 편입되어지면 한국 기업도 당연히 NIS 2에 따른 규제대상이 됩니다.

그러나 EU에 의료AI 기기를 수출하는 한국 기업은 '민사계약'을 통해 위험관리, 사고대응, 백업, 복구, 취약점 관리, 사고통지 의무 등을 요구받아 사실상 NIS 2 준수의무를 지게 됩니다. 따라서 EU시장을 타겟으로 하는 제품공급망에서의 보안이 미흡하게 되면 결과적으로 NIS 2법 위반이 되고 결국 EU역외의 한국 수출기업이라도 계약해지와 손해배상 책임으로 묶이게 되는 결과가 됨을 유의해야 합니다.

더욱이 디지털AI 의료기기처럼 고영향AI 영역의 사례라면 EU AI법 (Regulation)과 디지털제품에 대한 보안을 별도로 규정하고 있는 CSA(Regulation)에 따른 직접 책임 역시 질 수 있음도 유의해야 합니다.

따라서 EU 역내에 어떤 형태의 사업거점 (자회사, 지점, 대리인 등)을 갖고 있고, 한국 본사와의 책임분장을 어떻게 하고 있으며, AI모델의 업데이터와 관리는 어떻게 하고, 국내 위험관리체계는 어떻게 하며, AI 모델 탑재제품의 제조관리(하도급 유무) 방안은 어떻게 하고 있는지 등의 다각적 체크리스트가 전문적으로 준비되어야만 합니다.

2. EU의 NIS 2 법은 서비스를 제공, 운영하는 사업자의 보안 책임에 초점을 맞추었지만 기업들이 사용하는 제품 자체의 취약점으로 인해 서비스가 마비되면, NIS 2법으로는 해결할 수 없는 규제의 공백이 발생하게 됩니다.

이런 점에서 사이버보안에 대한 근원적 처방을 담은 EU CRA의 제정은 서비스를 안전하게 운영하기 위해 필요한 기본적인 도구(제품)의 안전성을 제조업체가 보장하도록 강제함으로써 디지털 제품의 사고예방의 효과적 개입 모델을 제시한 획기적인 것이라고 평가할 수 있습니다.

특히 종전의 CSA(Cybersecurity Act)가 EU 역내에서의 자발적 사이버보안인증 프레임을 수립, 시행하려 했던 한계를 뛰어 넘어 CRA은 사이버공격으로 인해 SW공급망 보안이 중요해지고 SBOM(Software Bill of Materials)이 필수요소로 등장함에 따라 모든 디지털제품에 대한 최소한의 보안 요구사항을 의무적으로 부과(Annex I)하고 있음을 주목해야 합니다.

구체적으로 CRA는 제조업체에게 제품의 전체 수명주기 (Lifecycle) 동안 SBOM을 생성, 유지, 보관토록 하며, 취약점을 처리하고, 사고를 신속하게 보고해야 하는 등 공급망 전체의 투명성 확보를 위해 보안 관련 법적 의무를 명시적으로 부여하고 있습니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

특히 스마트 TV, 스마트 장난감, 보안 카메라 등 IoT 장치의 확산은 사이버 공격의 가능성을 폭발적으로 증가시킴에 따라 이러한 인터넷 연결 디지털제품의 제조업체에게 '설계부터 보안(Security by Design)'과 '기본적으로 안전한 설정(Secure by Default)'을 강제, 소비자가 안전한 제품을 사용하도록 보장하는 책임을 지웠다는 점에서 EU CRA는 글로벌 사이버보안의 패러다임을 바꿨다고도 평가할 수 있습니다.

3. EU CRA는 2024년 12월부터 발효되고 있지만 대부분의 핵심 의무 사항은 36개월의 유예 기간을 거쳐 2027년 12월 11일부터 전면 적용될 예정이고, 고위험AI제품, 서비스 역시 법 적용대상에 당연히 포함됩니다.

특히 실무적으로 2026년 6월 11일부터 우리나라 수출기업을 포함, EU 역내에 디지털제품을 판매, 유통시키는 사업자는 자사 제품에서 발생하는 유럽사이버보안청(ENISA) 및 회원국 당국에 24시간 이내에 활발하게 악용되는(Actively Exploited) 취약점, 심각한 보안 사고(Severe Incidents)를 보고할 의무를 지게 되기 때문에 EU역내에 디지털제품을 수출하는 국내 기업들은 2027년 12월까지 기다려서는 안됩니다.

국내 기업도 24시간 이내 취약점 보고 프로세스와 실시간 모니터링 시스템 구축 등 '사고대응시스템'(incident response system)의 근본적 변화가 필요합니다.

EU CRA는 복원력(resilience)이라는 명칭처럼 디지털 제품 보안을 '일회성 방어'가 아닌 '지속적 관리' 문제로 보며, 소스 코드를 보유한 '제조업체'에 제품 수명 전반의 SBOM 작성·유지·관리를 통한 보안을 의무화합니다. 더욱이 EU 시장감독기관이 법 준수여부를 확인하기 위해 SBOM제출을 제조업체에게 요구할 수 있다는 점은 국내 수출기업들로 하여금 사이버보안이 사후에 사고대응차원에서 준비할 수 있는 것이 아님을 분명히 일깨워줍니다.

4. EU AI법 제15조는 사이버보안(cybersecurity)에 대해 규정하면서 고위험AI시스템에 내재된, 또는 운영상 발생하게 될 오류, 또한 외부에서의 불법 접속으로 인한 위험에 대해 "복원력이 있어야 (shall be resilient)"한다고 명시함으로써 CRA의 적용이 추가적으로 이루어지게끔 하고 있습니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

예를 들면, 디지털의료기기와 같은 고위험 AI 제품의 경우에는 사이버보안 사고 발생시 CRA규정이 당연히 추가 적용되어지는 식입니다.

제품 자체의 보안을 통해 사이버 보안사고의 근원적 차단을 목표로 하는 EU CRA와 AI시스템의 안전성, 신뢰성을 확보하기 위해 사sd이버보안 요구를 규정하고 있는 EU AI법은 비록 법 취지는 서로 다르지만 사업자의 준수 부담을 줄여주기 위해 고위험 AI시스템이 CRA상의 요구사항을 준수할 경우에는 AI 법상의 사이버요구조항 (AI 법 제15조)을 충족하는 것으로 간주(CRA 제12조)함으로써 사업자의 이중 평가부담을 줄여주고 있습니다.

다만 제15조의 "정확성(accuracy) 및 견고성(robustness)에 관한 요건을 손상시키지 않는 범위 내"라는 단서가 있으므로, 국내 수출기업은 EU AI법 적합성 평가 절차를 밟으며 CRA 요구사항도 함께 확인받으면 됩니다. 물론 CRA는 제7조와 8조에서 규정하는 바와 같이 디지털제품이 부속서 III의 중요제품(important products), IV에 규정된 핵심제품(critical products)에 해당될 때에 별도의 인증절차를 밟도록 되어 있기 때문에 국내 수출기업입장에서는 해당 디지털제품에 대한 세밀한 성격 분석이 선행되어야만 합니다.

Ⅲ. 바뀐 사이버보안의 틀과 고영향 AI

EU의 CRA는 스마트폰, IoT 기기, 산업용 제어 시스템, 소프트웨어 등 '디지털 요소가 포함된 제품(Products with Digital Elements, PDE)'의 설계부터 폐기까지 전 주기에 걸친 사이버 보안 요구사항을 의무화하는 최초의 포괄적 법으로서 유럽 시장 내 소비자의 안전을 강화한다는 명분을 가지고 있으나, 전세계 기술시장을 주도하는 미국 기업들에게는 전례 없는 규제준수(Compliance) 부담과 시장 진입장벽이라는 반발을 불러일으켰습니다. 특히 CRA가 요구하는 24시간 이내 취약점 보고 의무, 소프트웨어 자재 명세서(SBOM)의 강제 등이 기술혁신을 저해하고 무역장벽을 형성할 수 있다는 강력한 우려를 표명하였지만 사이버보안의 중요성이 더욱 커짐에 따라 현재는 '사실상의' (de facto) 글로벌 보안표준으로 받아들여지고 있습니다.

이에 따라 사이버보안사고 발생시 사후적으로 서비스 제공자 내지 네트워크 사업자의 책임을 묻게 되는 기존의 법 관점에서 벗어나 디지털제품 제조업자의 의무부과 등을 통한 보안사고 사전 예방 및 설계에 의한 보안으로 사이버보안의 패러다임이 이동되었다는 엄연한 현실을 국내 수출기업들은 추가 준수 부담이 생긴 셈입니다.

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com

특히 고영향 AI의 영역이 의료, 에너지, 교통 등 사회 기반 시설은 물론이고 개인의 신체적 안전, 기본권에 직접적인 영향을 미치는 영역에 걸쳐 계속 확장되고 있기 때문에 우리의 AI기본법에서 요구하고 있는 사업자의 보안책무는 단순한 기술적 안전성 문제가 아니라 국가사회적 안전인프라의 핵심 요소로까지 부상했다는 점에서 법적으로도 사고발생후의 조치와 처리 중심의 수동적 '위험관리' 개념에 더 이상 안주해서는 안됩니다.

한편, 고위험 AI를 둘러싼 사이버보안 위험의 발생시 결국 법적 위반에 대한 판단기준은 당분간 EU AI법 제15조의 '정확성(accuracy), 견고성(robustness), 사이버보안(cybersecurity)', 우리 AI기본법 제35조의 '안전성, 신뢰성'이 될 수밖에 없어 보이기 때문에 '내부 조직체계와 문서관리시스템의 정비'와 같은 규제대응역량의 강화, 더 나아가 민사계약 단계에서 현지 사업자들과의 책임분담, 협상' 역시 국내 사업자들로서는 더욱 세밀한 주의가 필요합니다.

<올해 1월의 미국 CES(Consumer Electronics Show)는 'AI대전환'(AX)을 제품으로 선보이면서 소비자 선택을 본격적으로 받고자 하는 경연장이라고 할 수 있습니다. AI를 모르던 시대로 돌아가는 건 이제 불가능해 보이고 사이버보안에 대한 기대값은 더 커질 겁니다. AI국내외 법률이슈에 대해 매월 발간하는 법무법인 린 AI.플랫폼.테크(종전 'TMT'를 개명) AI산업센터의 뉴스레터인 AID에 대한 질문, 조언 등은 구태언 A.P.T. 그룹장 (tekoo@law-lin.com), 방석호 AI 산업센터장 (shbang@law-lin.com)에게 보내주십시오.>

麟 서울특별시 서초구 서초중앙로24길 10,13층, 14층(서초동, 316타워) | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com