Deloitte Insights

Oct 2024

인공지능(AI) 시대의 새로운 국면, AI 규제와 기업 리스크 관리 전략

Deloitte Insights

Deloitte.

Download on the App Store
GET IT ON Google Play

'딜로이트 인사이트' 앱에서
경영·산업 트렌드를 만나보세요!

목차

AI 기술은 인류에게 많은 편의를 제공하며, 다양한 산업 분야에서 새로운 사업 기회를 창출하는 데 기여해왔다. 그러나 AI의 급속한 확산은 기본권 침해를 비롯한 여러 사회적 및 윤리적 문제를 동시에 야기하고 있다. 최근에는 생성형AI의 등장으로 개인 데이터의 처리, 고용, 의료 등 여러 분야에서의 AI 활용이 증가하면서, 이에 대한 규제의 필요성이 더욱 커지고 있다. 예컨대, 생성형AI 기술을 활용한 딥페이크는 지난해 미국에서 무려 3,000%나 증가했으며, 딥페이크 사기로 인한 손실액은 연평균 32% 증가해 2027년에는 55조 규모에 달할 것으로 전망되고 있다.[1] 이에 대응하기 위해 각국 정부는 인공지능 기술의 올바른 활용과 관리를 위한 규제 마련에 주력하고 있으며, 규제 대응을 위한 기업들의 고민도 깊어지고 있다.

지난 8월 1일에는 유럽연합(EU)에서 제정한 인공지능법(European Artificial Intelligence Act, 이하 EU AI 법)이 공식 발효되었다. 이는 인공지능(AI) 기술의 발전에 따른 인간의 기본권 침해 및 윤리적 이슈를 해결하기 위한 첫 포괄적 규제의 시작을 알리는 중요한 이정표로 평가된다. EU는 해당 법안 도입으로 AI 기술의 사회적 부작용을 최소화하면서도 기술 혁신을 촉진할 수 있는 균형 있는 규제를 마련하고자 했다.

앞으로 정부의 AI 규제는 더욱 확대될 것으로 예상되며, 이로 인해 기업들은 새로운 도전에 직면하게 될 것이다. AI의 도입이 거부할 수 없는 흐름이 되면서, 조직 내에서 AI를 어떻게 활용할 것인지에 대한 논의 이전에 'AI 규제 대응'을 먼저 고민해야 하는 새로운 국면에 접어들었다. 딜로이트가 2024년 업계 리더를 대상으로 실시한 설문조사에서도 AI 기술을 비즈니스에 도입할 때 가장 큰 장애물로 AI 관련 규제 준수와 리스크 관리의 어려움, 그리고 AI 거버넌스 모델의 부재 등을 선택한 것으로 나타났다.[2]

기업들이 고민하는 이유는 규제를 준수함과 동시에 책임감 있는 AI 활용으로 비즈니스 성과를 향상시키고자 하기 때문일 것이다. 본 리포트에서는 EU 등 각국의 AI 규제 동향을 개괄하고, 신뢰할 수 있는 AI 활용으로 성과를 창출하기 위한 기업의 대응전략을 살펴보았다.

그림 1. 생성형AI 툴 및 애플리케이션의 성공적인 개발과 도입을 가로막는 주요 장벽-규제준수

Q **귀사에서 생성형AI 툴 및 애플리케이션의 성공적인 개발과 도입을 가로막는 주요 장벽은 무엇입니까?**

규제 준수에 대한 고민	리스크 관리의 어려움	AI 거버넌스 모델의 부재
36%	30%	29%

자료: 딜로이트(2024)

01 세계 최초 AI 규제법, 유럽 연합의 인공지능법[3]

현대 사회에서 AI 기술의 중요성이 커짐에 따라, AI 기술의 사용으로 인한 인간 기본권 침해와 관련한 리스크에 대한 우려가 증가했다. 이에 EU는 시민의 안전성을 보장하고 윤리 침해를 막기 위해 다양한 조치를 모색했다. EU는 2018년 'AI 전략'을 발표하며 AI 개발과 관련된 여러 원칙을 설정하며 규제 초석을 다지기 시작했다. 2021년 AI 법안 초안 발표로 AI 기술이 안전하고 윤리적으로 사용될 수 있도록 하는 법적 틀을 마련했으며, 2023년 12월 유럽 의회와 이사회는 EU AI 법안에 대한 합의를 도출했다.
EU AI 법은 AI 시스템이 인권과 안전, 그리고 기본적인 민주적 가치를 보호하면서도 혁신을 지원하는 것을 목적으로 하고 있다.

잠재적 위험에 따른 4단계 차등 규제

EU AI 법은 위험 기반 접근방식을 기반으로 하며, AI 잠재적 위험과 영향 수준에 따라 위험도를 4단계로 나누어 차등 규제하고 있다.

1단계: 최소 위험(Minimal risk)

최소 위험에 속하는 AI 시스템은 시민의 기본권이나 안전에 영향이 없는 AI기반의 추천 시스템 및 스팸 필터 등 거의 모든 AI 시스템이 이 범주에 속한다. 해당 범주의 시스템은 추가적인 법적 의무 없이 기존 법률에 따라 개발 및 사용 가능하며, 기업은 자발적으로 추가 행동 강령을 채택할 수 있다.

2단계: 투명성 위험(Specific transparency risk)

인간과 상호작용하는 챗봇, 콘텐츠를 생성하거나 조작이 가능한 딥페이크와 같은 AI시스템으로, AI시스템 사용자에게 기계와 상호작용하고 있다는 사실을 투명하게 공개해야 한다.

3단계: 고위험(High risk)

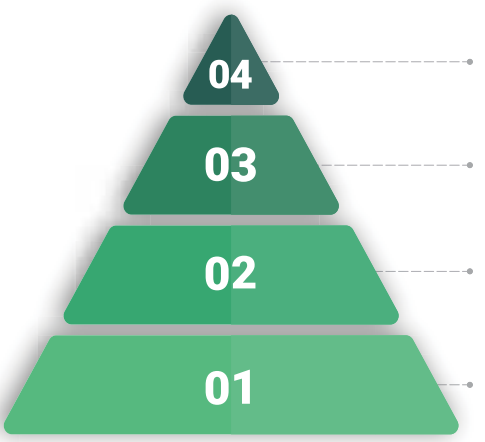
사람들의 안전 또는 EU 기본권 헌장에 보호된 기본권에 부정적 영향을 미칠 수 있는 AI 시스템으로, AI 기술의 발전에 따라 해당 위험 수준은 조정 가능하다. 의료서비스를 포함한 필수 공공 지원 혜택 및 서비스에 대한 자격 평가에 사용하기 위한 AI시스템, 신용도 평가에 사용하려는 AI시스템(금융 사기 탐지 목적 제외), 기소 과정에서 관련 지침에 따른 프로파일링을 위해 사용하려는 AI시스템, 범죄 피해자가 될 위험을 평가하기 위해 사용하려는 AI 시스템이 이에 속한다. 해당 시스템은 위험 완화 시스템, 고품질 데이터, 명확한 사용자 정보, 인간의 감독 등의 엄격한 요구 사항을 준수해야 한다.

4단계: 허용 불가능한 위험(Unacceptable risk)

사람의 기본권을 위협하는 AI 시스템으로, 이러한 시스템의 사용은 EU의 가치와 기본권을 심각하게 침해할 수 있으므로 다음과 같은 특정 용도로 사용 금지된다.

- **사회적 평점(Social Scoring)**
  소셜미디어(SNS) 등에서 개인과 기업 등의 사회적 영향력을 점수화하는 것으로 AI를 이용해 인터넷에서 사회적 인지도 조작 금지
- **특정 집단의 취약성 악용**
  사람이나 특정 집단의 연령, 장애 또는 특정한 사회적·경제적 상황으로 인한 취약성을 이용하여 사람이나 집단에 속하는 사람의 행동을 왜곡하거나 피해를 야기하거나 야기할 가능성이 있는 방식의 목적이나 효과를 가진 AI시스템은 금지
- **프로파일링을 이용한 범죄 예측(Predictive Policing)**
  AI 시스템이 개별 인물에 대한 프로파일링을 통해 범죄를 예측하거나 개인의 위험을 평가하고 조치를 취하는 AI 시스템은 금지
- **안면 인식 데이터베이스 수집**
  공공 및 민간 목적을 위해 인터넷 또는 CCTV를 통해 얼굴 이미지가 무차별적으로 수집되거나 데이터 베이스를 기반으로 확장하는 AI시스템 금지
- **직장/교육기관에서의 감정 추론**
  직장이나 교육에서 개인의 감정을 추론하기 위한 AI 기술의 사용은 의료적 또는 안전상의 이유를 제외하고는 허용되지 않으며, 이는 개인의 정신적 평화와 권리에 대한 침해로 간주
- **AI활용 생체 인식 분류 시스템**
  인종, 정치적 견해, 노조 가입, 종교적 또는 철학적 신념, 성적 지향 등을 추론하기 위해 생체 데이터 분류 금지(단, 법 집행 영역에서 합법적으로 수집된 데이터의 레이블링이나 필터링은 허용되지만, 기본적인 개인 권리를 침해하는 방식으로는 사용 불가)
- **실시간 원격 생체 인식 신원확인**
  법 집행 기관이 공공 장소에서 실시간으로 개인의 생체 정보를 원격으로 인식하는 것은 개인의 사생활 보호를 위해 금지

그림 2. EU AI 법, 잠재적 위험에 따른 4단계 차등 규제



허용 불가능한 위험 (Unacceptable risk)
사회적 평점, AI 생체 인식 분류 시스템, 안면 인식 데이터 수집, 원격 생체 인식 등 기본권을 위협하는 AI 시스템

고위험 (High risk)
대출, 공공지원 혜택 자격평가 AI 시스템 등 안전과 기본권에 영향을 미칠 수 있는 AI 시스템

투명성 위험 (Specific transparency risk)
챗봇, 딥페이크 등 인간과 상호작용하거나 조작이 가능한 AI 시스템

최소 위험 (Minimal risk)
기본권과 안전을 침해하지 않는 AI기반 추천 시스템, 스팸필터 등 기타 거의 모든 AI 시스템

자료: Deloitte Insights 재구성

EU AI법의 위반시 벌금

EU AI 법은 위반시 상당한 벌금이 부과되며, 벌금은 위반 유형에 따라 다르게 적용된다.

벌금 규모

- **AI 법의 위반** 또는 **데이터 관련 요구사항 미준수** 시, 최대 **3,500만 유로** 또는 **전세계 연간 매출의 7%**의 벌금 부과할 수 있다.
- **규정의 기타 요구사항** 또는 **의무를 준수하지 않는 경우**, 최대 **1,500만 유로** 또는 **전세계 연간 매출의 3%**의 벌금이 부과할 수 있다.
- 요청에 따라 신고 기관 및 국가 관할 당국에 **부정확, 불완전** 또는 **오해의 소지가 있는 정보를 제공한 경우**, 최대 **750만 유로** 또는 전세계 연간 매출액의 1.5%를 제재로 부과할 수 있다.

위반의 유형 및 심각성에 따른 차등 적용

- 각 위반 범주에 따라 벌금의 구체적인 금액은 위반 유형과 심각성에 따라 다를 수 있다. 스타트업을 포함한 중소기업에 대해서는 규정된 금액 중 낮은 금액이 기준이 되며, 기타 기업의 경우에는 높은 금액이 기준이 된다.

벌금 부과 외에도 특정 규제를 심각하게 위반하는 경우, 해당 AI 시스템의 사용을 즉각 중단하라는 명령을 받을 수 있다. 또한 부적절하게 수집된 데이터나 불법적으로 처리된 데이터는 즉시 삭제 명령도 가능하며, 데이터 처리 과정에서 사용자 동의를 확보하지 못한 경우에도 데이터 삭제 명령을 받을 수 있다.

EU AI법의 시행시기

EU AI법은 2년 후인 2026년 8월 2일부터 역내에서 활동하는 인공지능개발자에게 전면 적용될 예정이다. 또한, EU 내 각 국가별로 법률 체계에 통합하는 과정이 진행될 것이다. 법안의 전면 시행 전에 기업과 개발자들은 AI 시스템을 점검하고 필요한 변경 사항을 미리 준비하는 것이 중요하다.

EU AI 법은 유럽연합 내 모든 AI 기업에 적용된다. EU에 서비스를 제공하거나, EU 시민들을 대상으로 하는 글로벌 기업들은 모두 규제 준수가 필요한 상황이다. 다만 EU에 진출한 기업만이 규제의 영향을 받는다고 할 수 없다. EU AI법안은 세계 최초의 포괄적 AI 규제로서 글로벌 표준으로 작용할 가능성이 크다. 기업들은 AI 규제의 시작 신호탄이 된 EU AI 규제를 숙지하고 자사의 대응전략을 선제적으로 준비해야 할 시점이다.

구체적인 시행 일정

- **2025년 2월 2일:** AI 리터러시와 관련된 금지, 정의 및 조항은 이 날 발효되며, 6개월 후에 적용
- **2025년 8월 2일:** 거버넌스에 관한 규정 및 범용 AI에 대한 의무가 발효된 후 12개월 후부터 적용
- **2027년 8월 2일:** 부속서II(유럽연합 통합 법률 목록, list of Union harmonisation legislation)에 명시된 고위험 AI 시스템에 대한 의무가 부여되며, 이는 법안이 발효된 후 36개월 후에 적용

02 주요국의 AI 규제 동향

AI 기술의 발전은 전 세계적으로 사회, 경제, 정치적 변화를 이끌고 있다. 이러한 변화에 따라 AI의 안전한 사용과 윤리적 적용을 보장하기 위한 규제 필요성이 높아지며 EU AI법안 발표 전부터 이미 각국은 발빠르게 움직이고 있었다.

미국, AI 규제를 위한 행정명령 발표[4, 5]

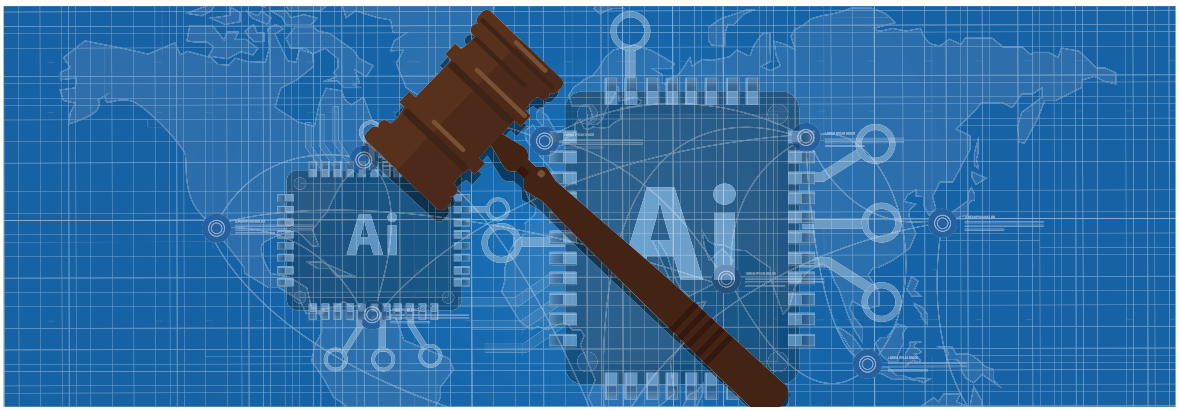
현재 미국은 연방정부 차원의 포괄적 규제 법률은 미비한 상황이다. 그러나 2018년에 인공지능의 정의 규정을 연방법에 명시한 바 있었으며, 연방의회는 2009년부터 지금까지 인공지능과 관련한 법률안을 지속적으로 발의해오고 있다.

2020년부터 2024년 5월까지 제정된 인공지능 관련 법률에는 「생성적 적대 신경망(GAN) 출력물 확인법」, 「정부인공지능법 2020」, 「국가 인공지능 구상법 2020」, 「미국인공지능진흥법」, 「미국 항공 분야 성장 및 리더십 확보법」 등이 있으며, 매년 국방수권법과 세출예산법 등의 법률에도 관련 조항이 포함되어 있다. 특히, 「국가 인공지능 구상법 2020」에 따라 백악관 과학기술처 소속으로 국가인공지능구상실이 신설되었고, 전문가로 구성된 국가인공지능자문위원회가 조직되어 다양한 정책 제안을 하고 있다.

바이든 행정부는 2023년 10월, 안정적이고 안전하며 신뢰할 수 있는 AI의 개발과 안전에 대한 행정명령(제14110호, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)을 발령했다. 이전 트럼프 행정부의 행정명령(Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government)이 신뢰성 있는 AI 사용 촉진에 집중했다면, 바이든 행정부의 행정명령은 AI의 위험성 완화 필요성을 언급하며 안전성, 보안성, 신뢰성을 중심으로 연방정부와 기업의 책임을 강화하는 내용을 담아 역대 가장 포괄적인 AI 규제 및 지침을 제시하고 있다.

이어서 바이든 정부는 2024년 1월 행정명령 발효 후 90일간의 진전사항을 담은 팩트시트(Vice President Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence)를 발표하며, 국립표준기술연구소(NIST) 내에 미국 AI 안전연구소(US AISI, The United States AI Safety Institute)를 신설할 계획을 밝혔다. 이 연구소는 사람에 의해 생성된 콘텐츠 인증, AI 생성 콘텐츠에 대한 워터마크 표시, 유해 알고리즘 식별 등에 관한 규칙을 제정하고 시행에 필요한 기술 가이드라인을 개발할 예정이다. 정부는 이 발표를 통해 AI 규제를 적극적으로 실행할 것임을 분명히 했다.

주(州) 차원에서도 자체적으로 인공지능 법률을 제정하고 있다. 전국주의회협의회에 따르면 2024년 5월까지 17개 주에서 인공지능 법률을 제정되었으며, 별도로 딥페이크 영상물을 규제하는 법률을 도입한 주도 17개에 달한다. 2024 회기 중에 인공지능 또는 딥페이크 규제 법률안이 발의되어 계류 중이거나 주지사의 서명 절차를 앞둔 주는 총 29개에 달해, 앞으로 더 많은 주에서 인공지능 법제를 도입할 것으로 예상된다.



중국, 생성형AI 잠정 관리 방법 공포[6]

중국의 AI 규제는 국가의 통제를 유지하면서 기술 혁신을 장려하는 방향에 중점을 두고 있다. AI 특허 보유량이 세계 1위로 음성 인식, 자연어 처리, 컴퓨터 그래픽 분야에서 선두를 차지한 것은 AI 발전을 장려하는 지원정책과 법률에 기반한 것으로 보인다.

중국은 2023년 년 「생성형AI 잠정 관리 방법」이 공포되어 생성형AI 시장에 대한 체계적인 규제를 시작하였다. 이전에는 '인터넷 보안법'(互联网安全法), '데이터보안법'(数据安全法), '개인정보보호법'(个人信息保护法), '인터넷 정보 서비스 알고리즘 추천 관리 규정'(互联网信息服务算法推荐管理规定), '인터넷 정보 서비스 딥페이크 관리규정'(互联网信息服务深度合成管理规定, 이하 '딥페이크 관리규정')등을 통해 생성형AI 리스크를 관리해왔다.

중국의 생성형AI 서비스 관련 규정은 AI 서비스 제공자가 만드는 콘텐츠의 책임을 정확히 명시하고 있다. 생성형AI 서비스 제공자는 다음과 같은 법적 의무를 준수해야 한다:

알고리즘 훈련 관련 의무

- 적법한 출처 있는 데이터와 기본모델을 사용해야 함
- 타인의 적법한 지식재산권 침해 금지
- 개인정보와 관련된 경우, 개인의 동의를 받거나 법률 및 행정 법규에서 정한 기타 요건을 충족해야 함
- 훈련 데이터의 진실성, 정확성, 객관성, 다양성을 강화하여 품질 향상을 위한 효과적인 조치를 취해야 함
- 데이터 보안법', '인터넷 보안법', '개인정보 보호법' 등의 법률, 행정 법규의 기타 관련 규정 및 관련 감독 기관의 규제 요구사항을 준수해야 함

콘텐츠 관리 의무

- 콘텐츠 생성과 관련하여 본건 규정은 서비스 제공자가 생성내용의 적법성에 대한 책임을 지도록 요구하고 있다. 또한 서비스 제공자는 딥페이크 관리규정에 따라 해당 내용의 라벨화와 개인정보에 대한 보호의무 등에 유의하여야 한다.

사용자에 대한 의무

- 본건 규정은 서비스 제공자와 사용자 간의 권리의무관계 및 생성형AI가 사용자에게 미칠 수 있는 영향 등을 감안하여 서비스 제공자의 관련 서비스 계약서 체결 의무를 규정하고 있다. 특히 미성년 사용자가 적절하고 적법한 선에서 생성형AI를 사용하도록 유도해야 하는 의무를 부과하고 있다.이 외에도 서비스 제공자는 사용자의 개인정보를 보호하고 불법 행위를 방지하기 위한 다양한 조치를 취할 의무가 있다. 위반 시, AI 서비스 제공자는 위법행위의 유형에 따라 '인터넷 보안법', '데이터 보안법', '개인정보 보호법', '과학기술발전법' 등 법령에 따른 법적 책임을 부담하게 된다. 중국의 AI 규제는 자국 내에서 지난 서비스를 제공하는 외국 기업에도 적용된다. 본 규정을 위반할 경우 국가 기관이 기술적 조치를 취할 수 있으며, 외국 기업은 중국법에 따른 컴플라이언스 절차를 미리 준비해야 한다.

일본, AI 가이드라인 제시[7]

일본 경제산업성과 총무성은 G7 히로시마 정상회의에서 논의된 '히로시마 AI 프로세스'를 기반으로 2024년 1월 「AI 사업자 가이드라인」을 발표하였다. 이 가이드라인은 기업 및 정부 기관의 AI 개발자, 제공자 및 사용자를 대상으로 하고, 비업무용 사용자는 제외된다. 데이터 취급 책임은 개발자와 제공자에게 있으며, 따라서 데이터 제공자는 포함되지 않는다. 가이드라인은 5개 장으로 구성되어 있으며, AI 개발자, 제공자, 이용자를 위한 10개 원칙을 제시하고 있다.

그림 3. 일본 2024년 1월 AI 사업자 가이드라인 발표

가이드라인의 기본 이념

- 인간 중심의 AI 사회 원칙에 따라, ①인간의 존엄성이 존중받는 사회(Dignity), ②다양한 배경의 사람들이 다양한 행복을 추구할 수 있는 사회(Diversity & Inclusion), ③지속가능한 사회(Sustainability)를 실현

AI 거버넌스 구축

- AI를 안전하게 활용하기 위해, ①밸류 체인/리스크 체인 관점에서 연계성 확보, ②국경을 초월한 자유로운 데이터 유통 보장, ③경영진의 의지에 의한 각 조직의 전략 등을 고려한 적절한 AI 거버넌스를 구축

'AI 개발자'에 관한 사항

- AI 개발자는 AI 모델을 직접 설계하고 변경할 수 있기 때문에 AI가 제공·활용될 때 어떤 영향을 미칠지를 사전에 최대한 검토하고 대응책을 마련하는 것이 중요

'AI 제공자'에 관한 사항

- AI 제공자는 AI의 운영과 적절한 활용을 전제로 한 AI 시스템 및 서비스 제공을 실현하는 것이 중요

'AI 이용자'에 관한 사항

- AI 이용자는 AI 제공자가 의도한 범위 내에서 적절하게 이용하고 AI를 필요에 따라 효과적으로 활용하기 위해 필요한 지식을 습득하는 것이 중요

자료: Kotra(2024)

그림 4. 일본, AI를 활용한 모든 사업자를 대상으로 한 10대 원칙 제시

①	(인간중심) 인간 존엄과 개인 자유를 존중	⑥	(투명성) 데이터 수집방법 등을 대외에 공개
②	(안전성) 인간에 의한 컨트롤을 확보	⑦	(설명책임) AI에 대한 이념, 사상을 공표
③	(공평성) 부당한 차별을 최소화	⑧	(교육·리터러시) 올바른 지식을 보급
④	(개인정보보호) 개인정보보호법에 기초해 대응	⑨	(공정경쟁확보) 이해관계자에 유리하지 않게 대응
⑤	(시큐리티확보) 시스템 기밀성을 유지	⑩	(이노베이션) 사회전체의 기술혁신에 공헌

자료: Kotra(2024)

고급 AI 분야의 사업 행위자는 모든 AI 행위자를 위한 히로시마 프로세스 국제 지침 원칙과 고급 AI 시스템을 개발하는 조직을 위한 히로시마 프로세스 국제 행동 강령을 준수할 것을 권장한다. 또한 고급 AI 시스템 개발자는 고급 AI 시스템을 개발하는 조직을 위한 히로시마 프로세스 국제 행동 강령을 준수해야 한다.

교육 및 의료 서비스 제공업체의 생성형AI 사용과 같은 분야별 가이드라인도 발표되었다. 해당 규정은 법적 구속력이 없지만, AI 행위자가 준수해야 하는 기준을 제시한다.[8]

일본 정부는 AI 관리에 있어 개인정보보호법, 저작권법, 부정 경쟁 방지법 등 기존 법률을 활용하고 있다. 개인정보보호법을 통해 AI 데이터 수집과 처리에 관한 엄격한 규정을 두고 있으며, 개인의 데이터 보호를 권장하고 있다. 이러한 법안은 AI 기술이 각자의 권리를 침해하지 않도록 보장하는 데 집중되어 있다.

일본은 AI의 활용이 사회에 미치는 영향을 고려하여 정부와 업계의 지속적이 평가와 검토를 진행하고 있다. 일본의 AI 규제는 법적 구속력은 없지만 사전 예방적 가이드라인의 제시함으로 법적 분쟁이 발생할 경우 가이드라인의 준수 여부가 결과에 영향을 미칠 수 있다. 이러한 AI 규제에 대한 관망 전략은 기술에 대한 규제가 아닌 기술 발전을 촉진하는 방향으로 설정되어 있는 것으로 보인다.

한국, AI 규제 논의 활발

2019년 12월 인공지능 국가전략 발표를 시작으로, 한국은 2020년 12월 인공지능법, 제도 및 규제 개선 로드맵을 발표했으며, 2023년 5월에는 디지털 권리장전을 제정하는 등 AI 규제 환경 조성을 위해 적극적으로 나서고 있다.

국내의 AI법안은 2020년부터 발의되어 왔다. 인공지능 자체의 진흥이나 규제 등을 목적으로 발의된 법안은 총 9건)으로, 2023년에 발의된 2개 법안에는 교통, 의료, 서비스 등 인공지능이 일상 깊이 파고들며 다양한 분야에서 활용되는 환경을 고려하여 사업자의 책무와 이용자의 권리를 구체적으로 규정하는 내용 등이 포함되어 있었다.[9] 2022년에는 AI 기본법으로 '인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률안'(AI법)이 발의되었으나, 국가인권위원회와 시민단체의 반대 등 여러 이슈로 인해 기한 내 처리되지 못하고 폐기되었다. 그러나 한국의 이미 여러 법에는 AI 관련 사안을 규제하는 조항들이 포함되어 있으며, 총 23개의 법령이 AI 기술을 실질적으로 규율하고 있다.

그림 5. 인공지능에 관하여 규정하고 있는 법령(직제 제외)

법령명	내용
행정기본법	제20조(자동적 처분)
개인정보 보호법	제37조의2(자동화된 결정에 대한 정보주체의 권리 등)
공직선거법	제82조의8(딥페이크 영상등을 이용한 선거운동)
전자정부법	제18조의2(지능형 전자정부서비스의 제공 등)
정보통신망 이용촉진 및 정보보호 등에 관한 법률	제4조(정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련)
소재·부품·장비산업 경쟁력 강화 및 공급망 안정화를 위한 특별조치법	제36조(소재·부품·장비정보의 체계적 생산·관리 등)
항로표지법	제2조(정의), 제43조의2(항로표지 지능정보화 체계의 구축 등)
모빌리티 혁신 및 활성화 지원에 관한 법률	제2조(정의)
이러닝(전자학습)산업 발전 및 이러닝 활용 촉진에 관한 법률	제2조(정의)
바둑 진흥법	제12조(바둑문화산업의 융합 및 연계)
제약산업 육성 및 지원에 관한 특별법	제4조(제약산업육성·지원종합계획), 제19조(연구개발정보의 수집과 보급)
지방교육재정교부금법	제5조의3(교부금의 재원 배분 및 특별교부금의 교부에 관한 특례)
중소기업 스마트제조혁신 촉진에 관한 법률	제2조(정의)
공무원 인재개발법 시행령	제14조의4(지능형인재개발플랫폼의 운영)
대학설립·운영 규정	제2조의3(학과·정원 등의 증설·증원의 기준 및 자체조정·상호조정의 기준)
댐건설·관리 및 주변지역지원 등에 관한 법률 시행령	제3조(댐관리기본계획)
디자인보호법 시행령	제6조(우선심사의 대상)
산업교육진흥 및 산학협력촉진에 관한 법률 시행령	제8조(계약에 의한 학과 및 학부의 설치·운영 등), 제8조의2(계약정원의 운영)
벤처기업육성에 관한 특별조치법 시행령	제11조의16(벤처기업집적시설의 지정 요건 등)
전자정부법 시행령	제15조의2(지능형 전자정부서비스의 도입 및 활용)
특허법 시행령	제9조(우선심사의 대상)
중소기업 스마트제조혁신 촉진에 관한 법률 시행령	제8조(스마트제조혁신 촉진 지원)
학점인정 등에 관한 법률 시행령	제3조(평가인정 대상 교육훈련기관)

자료: 법제처 미래법제혁신기획단(2024)

예를 들어, 개인정보 보호법에서는 정보 주체가 완전히 자동화된 시스템으로 개인정보를 처리하여 이루어지는 결정이 자신의 권리 또는 의무에 중대한 영향을 미칠 경우 해당 결정을 거부할 권리를 제공하며, 자동화된 결정에 대한 설명도 요청할 수 있다. 공직선거법에는 선거운동을 위하여 인공지능 기술 등을 이용하여 만든 실제와 구분하기 어려운 가상의 음향, 이미지 또는 영상 등 이른바 딥페이크 기술을 활용한 영상 등의 제작·편집·유포·상영 또는 게시 행위를 금지하는 내용을 규정하고 있다.

22대 국회 개원 이후 AI 관련 법안 발의가 이어지고 있으며, 현재까지 발의된 AI 기본법 관련 법안은 총 10건에 이른다. 이들 법안은 안전하고 신뢰할 수 있는 AI 기술 및 정책의 제도적 기반을 조성하는 동시에, AI 기술 개발 및 산업 진흥을 위한 종합적인 정책 추진의 필요성을 공통적으로 제기하고 있다.[10]

한국의 AI 규제 환경은 다양한 법적 틀을 통해 AI 기술의 안전성과 공정성을 유지하며, 향후 AI 산업의 혁신적 발전을 도모하는 데 방향성을 가지고 있다. 기업들은 발생할 수 있는 규제 관련 정보를 사전에 수집하고 정책 향방을 살피면서 위험 관리 체계의 사전적 대비가 필요할 것으로 보인다.

그림 6. 주요국의 AI 규제 동향

*CESI: China Electronics Standardization Institute / **FTC: Federal Trade Commission
*** CDEI: Centre for Data Ethics & Innovation / **** IEEE: Institute of Electrical & Electronics Engineers
*****Nist: National Institute of Standards & Technology

03 미래를 위한 준비: AI 규제와 기업 리스크 관리 전략

인공지능 기술의 발전은 기업의 운영 방식에 혁신을 가져오고 있지만, 동시에 법적 및 윤리적 리스크를 동반하고 있다. 인공지능 연구·개발자, 임원 설문 응답 결과 응답자의 68%가 인공지능이 편향성을 가질 수 있다고 염려하고 있었으며, 66%는 책임과 배상의 범위 및 한도가 불분명하다고 답했다.[11]

특히, EU AI 법이 발효되면서 기업들은 새로운 규제 환경에 적응해야 할 필요성이 커지고 있다. AI 규제가 전 세계적으로 강화되는 현 시점에 기업은 법적 책임을 다하고 윤리적 기준을 준수하는 동시에, AI의 혁신적인 잠재력을 최대한 활용해야 한다. 이에 따라 기업은 통합적이고 구조화된 리스크 관리 방안을 수립하는 것이 필수적이다.

AI 거버넌스의 중요성

AI 규제 리스크 대비 전략의 핵심은 AI 거버넌스의 구축이다. AI 거버넌스는 조직 내에서 AI의 책임 있는 개발과 배포를 보장하는 프레임워크를 의미한다. 이는 법적 요구사항, 윤리적 기준 및 기업 목표에 부합하는 정책, 구조, 프로세스를 포함한다. 최근 AI를 활용한 비즈니스가 확대됨에 따라 각 국가별로 기업들에게 가이드 준수를 요구하고 있어 AI 거버넌스 확보에 대한 수요가 증가하고 있다. AI 거버넌스는 규제 준수뿐만 아니라 윤리적 책임의 기반을 마련해 기업의 신뢰를 확보할 수 있다.

AI 거버넌스가 체계적으로 마련되어야만 이들 각 요소가 원활하게 작동하고, 실제로 기업의 리스크를 효과적으로 관리할 수 있게 된다. 결국, AI의 혁신 잠재력을 최대한 활용하기 위해서는 AI 거버넌스의 체계적이고 명확한 구축이 필수적이다. 이는 단순한 규제 준수를 넘어, 기업의 지속 가능한 성장과 경쟁력 강화를 위한 전략적 투자로 자리잡을 것이다. 기업이 이러한 거버넌스 체계를 통해 탄탄한 리스크 관리 체제를 마련한다면, 급변하는 AI 환경에서도 그 안정성과 신뢰성을 확보할 수 있다.

규제 준수	EU AI 법과 같이 AI에 대한 규제는 갈수록 강화되고 있다. 기업은 AI 의사결정의 투명성 확보, 데이터 프라이버시 보호, 그리고 차별 방지와 같은 복잡한 요구사항을 충족해야 한다. AI 거버넌스는 이를 준수할 수 있는 체계를 마련함으로써 규제 리스크를 줄일 수 있다.
윤리적 책임	AI는 의사결정 과정에서 편향성을 가질 수 있으며, 그로 인해 사회적 및 윤리적 문제가 발생할 수 있다. 또한 개인정보 침해, AI 설명가능성 문제등으로 사회적 규범과 가치 침해 사례가 발생하고 있다. AI 거버넌스를 통해 기업은 편향성 방지, 윤리적 AI 사용을 장려하고, 사회적 책임을 다할 수 있는 기반을 구축할 수 있다.
신뢰 확보	AI 시스템이 더 많이 사용될수록 소비자와 사회의 신뢰가 중요해진다. AI의 객관성, 정확성, 공정성의 문제로 인해 AI 오류에 대한 문제가 대두되는 요즘, AI 예측 결과의 정확성에 대한 신뢰가 확보가 그 어느때보다 중요하다. 투명하고 책임 있는 AI 거버넌스는 기업이 신뢰를 얻고, 시장에서의 경쟁력을 유지하는 데 중요한 역할을 할 것이다.

AI 거버넌스 구축 기대효과

AI 거버넌스 구축은 AI의 잠재력을 극대화하면서도 신뢰성을 확보하고, 법적, 윤리적 문제 발생을 예방하고 규제 변화에 신속히 대응할 수 있다. 가장 핵심적인 기대효과는 다음과 같다.

법적 리스크 감소 및 컴플라이언스 확보

- AI 규제가 강화됨에 따라, 이를 준수하지 않을 경우 기업은 막대한 벌금이나 법적 제재를 받을 수 있다. 기업은 AI에 관한 최신 법률과 규제를 지속적으로 모니터링해야 한다. AI 거버넌스 체계를 수립을 통해 규제 요구사항 준수를 보장하고 필요 시 정책을 수정하여 법적 리스크를 최소화해야 할 수 있다.

신뢰성과 브랜드 가치 제고

- AI 거버넌스 구축은 기업이 책임감 있게 AI 기술을 사용한다는 신호를 소비자, 투자자, 규제 기관에 전달한다. 이는 신뢰성과 브랜드 가치를 높이는 데 직접적인 영향을 준다. 또한 기업이 윤리적인 AI 사용을 명시적으로 보장함으로써 사회적 책임을 다하는 기업으로서 이미지를 강화할 수 있다. 신뢰를 구축한 기업은 AI 기반 제품 및 서비스 출시 시 소비자와 투자자들의 긍정적인 반응을 유도할 수 있다.

AI 모델 성능 향상 및 혁신 기회 증대

- AI 거버넌스는 데이터 품질 관리, 알고리즘의 공정성 및 투명성 확보 등을 통해 AI 시스템의 성능을 지속적으로 개선하는 기반을 마련한다. 모니터링과 피드백을 통해 시간이 지나면서 환경 변화에 따라 성능이 저하되는 모델 드리프트 같은 문제를 조기에 발견하고 해결할 수 있어, 장기적으로 AI 시스템의 효율성과 신뢰성을 보장한다.

글로벌 시장에서의 경쟁력 강화

- 각국의 AI 규제가 상이한 상황에서, 선제적으로 글로벌 규제를 준수하는 AI 거버넌스를 구축한 기업은 다양한 지역에서 사업을 확대할 때 유리한 위치를 선점할 수 있다. 또한 AI 기술의 잠재적 리스크와 기회를 조기에 인식해 조직의 목표와 전략을 변화하는 환경에 맞춰 조정할 수 있어 장기적인 경쟁력 확보에 기여할 수 있다.

결국 AI 거버넌스는 단순한 규제 대응 수단이 아니라, 사회적 신뢰를 높이고 혁신을 촉진함으로써 궁극적으로는 글로벌 경쟁력을 강화하는 중요한 전략적 기반을 제공한다. AI 거버넌스 구축으로 기업은 장기적 성장과 안정성의 보장이 가능하다.

기업의 AI 거버넌스 구축 프로세스

AI 거버넌스 구축 프로세스는 AI 기술의 책임성과 윤리성을 보장하기 위해 필수적인 단계이다. AI 거버넌스 구축을 위해서는 현황 분석에서 시작하여 향후의 로드맵까지 정의하는 일련의 절차가 필요하다.

첫 번째 단계인 현황 분석에서는 규제와 기술 동향 등 AI 외부환경과 조직 내 AI 활용과 데이터 관리 체계와 같은 내부환경을 평가하고, AI 진단 도구를 활용하여 현재 상황을 분석한다. 이를 통해 AI 거버넌스 체계의 필요성과 방향성을 설정하는 기초 자료를 마련하게 된다.

두 번째 단계인 AI 거버넌스 체계 수립에서는 AI 윤리 기준과 관련 규정을 정의하고, 조직 내 거버넌스 구조를 설계하여 명확한 역할과 책임(R&R)을 수립한다.

세 번째 단계인 AI 거버넌스 실행 방안 수립에서는 AI 개발 및 운영 전반에 걸쳐 표준 가이드를 마련하고, 위험 분석 및 관리 방안을 수립하여 성과 관리 체계를 구축한다. 이렇게 함으로써 조직은 AI 시스템의 일관성 있고 책임 있는 운영을 보장하게 된다.

네 번째 단계인 PoC 검증 수행에서는 서비스의 현재 상태를 기준으로 위험 요소를 식별하고 평가한 후, 대응 계획을 수립하여 리스크를 지속적으로 모니터링한다. 마지막으로 개선 과제 및 로드맵 정의 단계에서는 AI 거버넌스의 최종 목표와 비전을 명확히 하여 모든 이해 관계자가 동일한 목표를 향해 나아갈 수 있도록 한다.

이러한 AI 거버넌스 체계 구축프로세스를 통해 조직은 AI의 사회적 책임과 법적 요구를 충족시키며, 변화하는 환경에 신속하게 대응하고 지속 가능한 발전을 이룰 수 있는 기반을 마련할 수 있다. 이를 통해 궁극적으로 신뢰받는 AI 환경을 조성하는 데 기여하게 된다.

그림 7. AI 거버넌스 구축 프로세스

프로세스	주요 수행 업무	수행 내용
현황분석	AI 외부환경 분석	AI 기술의 발전 동향, 규제 환경, 사회적 요구사항 등 파악 및 분석
	AI 내부환경 분석	조직 내 AI 기술의 활용 상황과 조직의 데이터 관리 체계 평가
	AI 진단 툴(Tool) 기반 분석	AI 진단 툴(Tool)을 활용해 AI 시스템의 성능, 신뢰성 및 윤리적 이슈 분석
AI 거버넌스 체계 수립	AI 윤리기준 수립	AI 시스템의 설계 및 운영에서 준수해야 할 윤리적 기준 정의
	AI 관련 규정 수립	조직 내에서 AI 시스템 운영 시 필요한 규정 마련
	AI 거버넌스 조직 체계 수립	AI 관련 의사결정 및 관리 기능 수행 조직 설정
AI 거버넌스 실행방안 수립	AI 라이프사이클별 표준가이드 수립	AI 개발 및 운영 전반에 준수해야 할 표준 가이드 수립
	위험분석 및 관리방안 수립	AI 시스템 사용과 관련된 잠재적 위험 분석 및 관리 방안 수립
	성과관리 방안 수립	AI 프로젝트의 성과를 평가하고 관리하기 위한 지표와 방법론 설정
	R&R 조직 실행방안 수립	조직 구성원 개별 역할의 이해와 효율적 수행을 위한 R&R 구체적 정리
Poc 검증 수행	서비스 AS-IS 수립	현재 서비스의 상태를 명확히 기록하여 향후 개선의 기준점 수립
	위험 식별	서비스 제공 과정에서 발생할 수 있는 위험 요소 철저히 식별
	위험 평가	식별된 위험의 성격과 심각성 평가
	위험 조치 계획 수립	평가된 위험에 대해 구체적인 대응 계획 수립 및 책임자 설정
	위험 모니터링	서비스 실행 후 지속적으로 위험 요소를 모니터링하여 상황 변화 파악 및 대응
개선 과제 및 로드맵 정의	AI 거버넌스 엔드 이미지 제시	AI 거버넌스의 최종 목표와 비전을 명확히 정의하여 조직 내 공유
	AI 거버넌스 중장기 로드맵 수립	기술 발전과 규제 변화에 맞춰 유연하게 조정 가능하며, 단기, 중기, 장기 목표가 포함된 로드맵 수립

자료: Deloitte

참고 딜로이트의 AI 거버넌스 구축 서비스 DAAT

(Deloitte AI governance Assessment for Trustworthy)

[AI 전략·운영 원칙 수립부터 개발까지 End to End로 진단 및 로드맵 제공]

딜로이트는 국내 산업별 표준 및 글로벌 기준이 모두 반영된 진단 Tool을 이용하여 AI리스크 관리를 위한 최적의 전략 및 기준을 마련하고, 기업의 AI 기술에 대한 사회적 책임 및 신뢰성을 확보합니다.

AI 활용 기준·원칙 수립

기업이 AI 적용함에 있어
"What we do, What we don't" 를 정의함

산업별 기준의 유연한 적용

금융권 AI 가이드, 과기부 AI 개발 안내서,
EU 가이드 등 진단항목을 산업에 맞춰 Customize 가능

AI 국제 인증획득

글로벌 인증업체와 협력을 통한
ISO 42001 기준 준수 및 인증 획득 가능

효과적인 결함 개선

Best Practice를 기반으로 한
Quick-Win 개선 방안 제공

딜로이트의 AI 거버넌스 구축 서비스 DTTA는 글로벌 딜로이트의 Trustworty AI TM 프레임워크를 기반으로 국·내외 기준을 반영하여 6개 Core Attribute를 진단합니다.

6개 Core Attribute 평가 및 개선을 위한 3단계 프로세스를 통해 사실에 기반한 정확한 진단 및 People, Process, Technology 관점에서의 개선안과, 이를 이행하기 위한 중장기 로드맵을 제공합니다.

01 공정성

- 윤리적으로 사회/경제에 부당한 영향을 미친 문제를 해결하거나 이해관계자 간의 우려를 해소한 상태
- 내/외부 점검을 통해 어플리케이션이 사용자 모두에게 공정한 결과물을 제공하는지 환경을 점검함

02 견고성

- AI가 외부의 간섭 및 극한적 운영 환경에서도 사용자가 의도한 수준의 성능 및 기능을 유지하는 상태
- AI 시스템은 사람 또는 다른 시스템으로부터 학습할 수 있으며, 일관되고 신뢰할 수 있는 결과물을 제공하고 있는지 점검함

03 투명성

- AI의 판단·예측 등 작동과정과 이를 구현하기 위한 구성요소를 사용자가 인지/확인 및 검사가 가능한 상태
- 데이터가 어떻게 사용되는지, AI 시스템이 어떻게 의사결정 하고 있고 이것을 확인 가능한지 점검함

04 프라이버시

- AI를 개발하고 활용하는 과정에서 개인의 정보를 보호하고 AI 전체 라이프사이클에 걸쳐 개인정보의 오용을 최소화한 상태
- 고객 데이터는 명시된 용도 외로 사용되지 않는지 또는 소비자의 데이터를 공유하지 않는지 점검함

05 책임성

- AI로 발생한 문제에 대해 책임의 주체가 명확해야 되며, 책임주체를 설정 및 추적함으로써 발생할 수 있는 피해를 최소화 할 수 있는 상태
- AI 시스템의 의사결정 결과에 대한 책임의 소재 또는 정책에 반영되어 시행되고 있는지 점검함

06 보안성

- 물리적, 디지털 피해를 초래할 수 있는 위험으로부터 보호되는 상태
- AI 시스템이 물리적 또는 디지털 손상을 야기할 수 있는 위험을 점검함

주석

1. 딜로이트 인사이트, 딥페이크 시대의 리스크 유형과 대응방안, 2024.09
2. 딜로이트 AI Institute, 기업의 생성형AI 사용 현황; 2024년 3분기 보고서, 2024.09
3. European Commission, Artificial Intelligence – Questions and Answers (https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683)
4. 세계법제정보센터, 미국 AI 입법 동향, 2024.06.24.
5. 법률신문, 미국과 영국의 AI 규제동향, 2024.02.29
6. 법률신문, 중국의 AI 관련 법률 규제 현황, 2024.6.10
7. Kotra, 일본의 AI 정책과 실제 사례, 2024.4.8
8. Asia Business Law Jornal, 기업을 위한 일본의 AI 규제, 2024.4.18
9. 법제처 미래법제혁신기획단, 인공지능(AI) 관련 국내외 법제 동향, 2024.7
10. 전자신문, 국회 발의 AI 법만 10건…속도론vs신중론 의견 엇갈려, 2024.9.22.
11. Deloitte AI Institute (2021) Investing in trustworthy AI.

딜로이트 산업 전문가

AI 서비스, TMT(통신·미디어·엔터테인먼트), 디지털 경영관리 서비스

딜로이트는 기업의 AI 활용과정에서의 문제를 해결하고, AI 혁신을 위한 거버넌스 체계 수립 및 고객 경험 개선 등의 서비스를 제공하고 있습니다. 기업 운영에 있어 AI의 효과적이고 신뢰있는 적용에 든든한 조력자 역할을 수행합니다. 딜로이트는 또한 통신·미디어·엔터테인먼트 분야에서도 기업들의 전략적 과제와 혁신을 함께해왔습니다. 다양한 배경을 가진 구성원들로 이뤄진 팀은 심도있는 인사이트를 제공하고 있습니다.

AI 서비스

정찬욱 파트너
Core Technology,
Data Analytics I 컨설팅 부문

02 6676 2732
chanjung@deloitte.com

정창모 수석위원
AI 서비스 I 컨설팅 부문

02 6676 3288
changjung@deloitte.com

김진숙 파트너
AI 혁신/거버넌스 리더 I
경영자문 부문

02 6099 4437
jessicakim@deloitte.com

이성호 상무
AI, Analytics I 컨설팅 부문

02 6676 3767
sholee@deloitte.com

TMT(통신·미디어·엔터테인먼트)

최호계 파트너
첨단기술·미디어·통신산업 전문팀 리더 I
감사 부문

02 6676 3227
hogchoi@deloitte.com

디지털 경영관리 서비스

조명수 파트너
디지털 경영관리 서비스 리더 I
컨설팅 부문

02 6676 2954
mjo@deloitte.com

앱

Download on the App Store

GET IT ON Google Play

카카오톡 채널

'딜로이트 인사이트' 앱과 카카오톡 채널에서
경영·산업 트렌드를 만나보세요!

Deloitte. Insights

성장전략부문 대표
손재호 Partner
jaehoson@deloitte.com

딜로이트 인사이트 리더
정동섭 Partner
dongjeong@deloitte.com

딜로이트 인사이트 편집장
박경은 Director
kyungepark@deloitte.com

연구원
김혜련 Senior Manager
hyerykim@deloitte.com

디자이너
박근령 Senior Consultant
keunrpark@deloitte.com

Contact us
krinsightsend@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

본 보고서는 저작권법에 따라 보호받는 저작물로서 저작권은 딜로이트 안진회계법인(“저작권자”)에 있습니다. 본 보고서의 내용은 비영리 목적으로만 이용이 가능하고, 내용의 전부 또는 일부에 대한 상업적 활용 기타 영리목적 이용시 저작권자의 사전 허락이 필요합니다. 또한 본 보고서의 이용시, 출처를 저작권자로 명시해야 하고 저작권자의 사전 허락없이 그 내용을 변경할 수 없습니다.

© 2024. For information, contact Deloitte Anjin LLC