





# 유럽연합 인공지능법: 주요 내용과 시사점

이해원(Haewon Lee)\*

\* 국립목포대학교 법학과 교수 / 법학박사(S.J.D., Civil Law), 변호사(Korean Bar).

2021년부터 추진되었던 유럽연합 인공지능법(‘EU 인공지능법’)이 3년 만에 제정되어 올해부터 단계적으로 시행될 예정이다. 마치 2018년 GDPR이 그러하였듯이 EU 인공지능법도 유럽연합 역내에 인공지능 서비스나 제품을 출시하는 전세계 모든 기업에 적용된다. 유럽연합 시장에 진출하였거나 진출을 모색하는 우리나라 인공지능 스타트업이라면 EU 인공지능법의 내용을 사전에 숙지하고 대응 방안을 모색할 필요가 있는 것이다. 이러한 배경 하에 이 글에서는 EU 인공지능법의 주요 내용을 소개하고 우리나라 스타트업에 미치는 영향이 무엇인지 간략히 짚어보고자 한다.

---

## 목차 Table of Contents

---

1	서론	04
2	입법 배경 및 취지	07
	2-1 입법 배경	
	2-2 입법 취지	
3	주요 내용	11
	3-1 법률 체계	
	3-2 적용 범위	
	3-3 AI 규제 접근 방법: 위험 기반 규제(risk-based regulation)	
	3-4 AI 혁신 지원	
	3-5. 기타	
4	시사점	30

---

# 1

## 서론

---

# 1 서론

---

흔히 ‘세계 최초의 인공지능 규제법’으로 알려진 유럽연합(이하 ‘EU’라 한다)의 인공지능법(EU Artificial Intelligence Act,<sup>01</sup> 이하 ‘EU 인공지능법’이라 한다)이 2024. 3. 13. EU 의회(European Parliament)에서 찬성 523표, 반대 46표, 기권 49표로 가결되었다.<sup>02</sup> 특단의 사정이 없는 한 위 법은 향후 EU 이사회(European Council)<sup>03</sup>승인을 거쳐 올해부터 단계적으로 시행될 예정이다.<sup>04</sup>

우리나라를 비롯한 세계 주요국이 AI 법·제도를 고민하고 있는 상황에서 EU 인공지능법은 논의 단계가 아닌 제정 및 시행을 눈 앞에 둔 규범이라는 점에서 전세계적으로 상당한 영향력을 발휘할 것으로 보인다. 특히 우리의 경우 GDPR<sup>05</sup> 사례에서도 알 수 있듯이 정책 당국이나 입법자가 EU 인공지능법을 유력한 해외 입법례로 인식하고 유사한 내용의 법률을 제정하려 할 가능성이 크다고 본다. 그러나 EU는 우리와는 역사적, 문화적 전통 자체가 다를 뿐 아니라 현재 처한 정치, 경제, 사

---

<sup>01</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206>

<sup>02</sup> <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>

<sup>03</sup> EU 이사회(또는 ‘EU 각료 의사회’라고도 불림)는 EU 회원국별(현재 27개국) 1명의 장관급 각료로 구성되는 EU의 최고 입법기관이자 주요 정책 결정기구이다.

<sup>04</sup> 단계별 시행 일정 및 그 주요 내용은 뒤에서 설명한다.

<sup>05</sup> 우리나라 개인정보 보호법에 비견되는 EU의 일반개인정보보호규정(General Data Protection Regulation)을 말한다.

회 환경 또한 차이가 있다. 따라서 EU의 법제도를 참고하는 것은 별론으로 하더라도 이를 무분별하게 벤치마킹하는 것은 마땅히 지양되어야 한다. 이를 간과하면 굴이 탕자가 된다(橘化爲枳).

이러한 문제 인식을 바탕으로 이 글에서는 EU 인공지능법의 주요 내용을 개괄한 후 우리에게 주는 시사점, 특히 우리 스타트업에게 미치는 영향을 살펴보고자 한다. 참고로 이 글을 쓰는 2024. 4. 11. 기준으로 아직까지 2024. 3. 13.자 수정안이 공식적으로는 공개되지 않았으므로, 2024. 1. 26.자로 공개된 안을 기준으로 검토한다.<sup>06</sup>

---

06 <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>



# 2

## 입법 배경 및 취지

## 2 입법 배경 및 취지

---

### 2-1 입법 배경



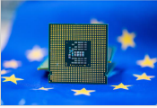





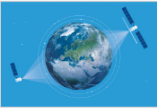

EU 인공지능법은 일회성, 단발성 법제도가 아니라, EU 차원의 ‘디지털 전략’이라는 큰 그림의 일환으로 추진된 법이다.<sup>07</sup>

EU는 2010년 이후 ‘Europe 2020’, ‘디지털 미래 형성(Shaping Europe’s digital future)’(2019-2024) 등의 전략을 개별 회원국이 아닌 EU 차원에서 수립, 추진하여 왔으며, 현재는 디지털 미래 형성 전략의 구체적인 정책으로 ‘디지털 10년(Europe’s digital decade)’ 프로그램을 실행하고 있다. 디지털 미래 형성 전략은 EU의 디지털 전환 촉진 및 지원, 디지털 시대에 부합하는 EU 시민의 권리 보장 등을 핵심 가치로 제시하고 있으나, 그 근저에는 미국 중심의 글로벌 디지털 기업으로부터 EU 내에 위치한 기업 및 시장을 보호하고 디지털 시대 글로벌 규범을 EU가 선도하는 등, EU의 이익을 보호하려는 목적이 내포되어 있다. EU의 디지털 미래 형성 전략은 시뿐 아니라 **그림 1.**과 같이 데이터, 플랫폼, 반도체, 사이버안보, 우주, 국제무역 등 다양한 분야를 포괄하고 있다. EU는 위 전략에 따라 2020년 이후 순차적으로 디지털서비스법(DSA), 디지털시장법(DMA), 데이터거버넌스법(DGA), 데이터법(Data Act), 사이버복원력법(Cyber Resilience Act), 반도체법(EU Chip Act) 등의 일련의 법률을 각 회원국 차원이 아닌 EU 차원에서 제정하고 있다.

---

<sup>07</sup> <https://www.europarl.europa.eu/topics/en/article/20201015STO89417/ai-rules-what-the-european-parliament-wants>

그림1. ‘디지털 미래 형성 전략’ 주요 실행 분야<sup>08</sup>

	<b>Digital Services Act</b> Ensuring a safe and accountable online environment		<b>Digital Markets Act</b> Ensuring fair and open digital markets
	<b>European Chips Act</b> Strengthening Europe's competitiveness and resilience in semiconductor technologies		<b>European Digital Identity</b> Giving you full control on how much information you share with third parties
	<b>Artificial Intelligence</b> Achieving better healthcare, safer and cleaner transport, more efficient manufacturing, and cheaper and more sustainable energy through AI		<b>European data strategy</b> Making the EU a role model for a society empowered by data
	<b>European industrial strategy</b> Ensuring European industry leads the transition towards climate neutrality and digital leadership		<b>Contributing to European Defence</b> Working together to tackle security threats and challenges more robustly
	<b>Space</b> EU initiatives for a satellite-based connectivity system and management of space traffic		<b>EU-US Trade and Technology Council</b> Coordinating approaches to key global trade, economic, and technology issues

이러한 ‘거시적인’ 디지털 전략을 근간으로 하여 EU는 AI 전략과 정책을 수립하고 이를 뒷받침할 수 있는 법·제도를 마련하여 왔다. 구체적으로 EU는 2018년 집행위원회가 ‘인공지능 전략’을 발표하면서 “인간중심적(human-centric)이고 신뢰할 수 있는(trustworthy) AI를 보장하고 EU를 세계 수준의 AI 허브(hub)로 육성”할 것을 목표로 제시하였으며, 이를 법·제도적으로 뒷받침하기 위하여 2021년에는 ① EU 인공지능법 뿐 아니라 ② 인공지능 사고에 적용할 수 있는 민사책임법제(AI Liability Directive<sup>09</sup>, Product Liability Directive<sup>10</sup>), 그리고 ③ 인공지능이 적용되는 특정 영역의 안전에 관한 법제(Machinery Regulation, General Product Safety Regulation)의 세 가지를 각 제안하였다. 즉, EU 인공지능법은

<sup>08</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en)

<sup>09</sup> European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM/2022/496 final (2022. 9. 28.). 현재 입법 절차가 진행 중이다.

<sup>10</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, COM/2022/495 final (2022. 9. 28.). 2024. 3. 기준으로 현재 비공식적 합의가 이루어진 것으로 알려졌다.

EU에서 AI를 규율하기 위하여 추진 중인 유일한 법이 아니며, EU의 인공지능 법제는 규제뿐 아니라 공중의 안전, 나아가 민사책임에 관한 규범까지 포함하는 3대 축으로 마치 솔이 세 개의 발로 서있듯이 정립(鼎立)되어 있다는 점을 주지할 필요가 있다.

## 2-2 입법 취지

EU 인공지능법은 EU 시민들이 AI를 신뢰할 수 있도록 하며, AI 분야의 우수한 생태계를 조성하고, AI 분야의 글로벌 역량 및 경쟁력을 갖추기 위한 목적으로 추진된 법률이다<sup>11</sup>. EU 인공지능법 상설(recital) 제1항 및 제1조는 입법 취지를 보다 상세히 설명하고 있는데, 살펴보면 ① EU 역내 시장의 기능을 개선하고, ② 인간 중심적이고 신뢰할 수 있는 인공지능의 수용을 촉진하면서, ③ 인공지능의 해로운 영향으로부터 건강, 안전, EU 인권헌장상의 기본권, 민주주의, 법치주의 및 환경 보호를 두텁게 보호하고 혁신을 지원함에 있다.<sup>12</sup>

또한 EU 인공지능법은 인공지능에 기반한 상품과 서비스가 국경을 넘나들며 자유롭게 이동하는 것을 보장하며, 이 법에서 명시적으로 승인되지 않는 한 회원국이 개별적으로 인공지능 시스템의 개발, 마케팅 및 사용에 제한을 가하는 것을 금지한다.<sup>13</sup>

11 강진원·김혜나, EU 인공지능(AI) 규제 현황과 시사점, KISTEP 브리프 119, 한국과학기술기획평가원(2024. 2.), 1쪽.

12 EU 인공지능법 제1조 (1).

13 EU 인공지능법 상설 제1항.

# 3

## 주요 내용

## 3 주요 내용

---

### 3-1 법률 체계

EU 인공지능법은 **그림 2**.와 같이 12개의 장(title)으로 이루어진 본문, 171개의 상설(recital)<sup>14</sup> 및 13장의 부속서(annex)가 붙어 있는 방대한 규범이다.

---

<sup>14</sup> 제1조~제89조이며, 가지번호가 포함된 상설 규정이 있어 총 171개이다.

**그림2. EU 인공지능법 체계도<sup>15</sup>**

**Titles**

The EU AI Act consists of 12 main titles. Each title contains a set of Articles.

Title I: General Provisions	+
Title II: Prohibited Artificial Intelligence Practices	+
Title III: High-Risk AI System	+
Title IV: Transparency Obligations for Providers and Deployers of Certain AI Systems and GPAI Models	+
Title V: Measures in Support of Innovation	+
Title VI: Governance	+
Title VII: EU Database for High-Risk AI Systems Listed in Annex III	+
Title VIII: Post-Market Monitoring, Information Sharing, Market Surveillance	+
Title VIIIa: General Purpose AI Models	+
Title IX: Codes of Conduct	+
Title X: Confidentiality and Penalties	+
Title XI: Delegation of Power and Committee Procedure	+
Title XII: Final Provisions	+

**Annexes**

Annexes provide supplementary information alongside the Regulation.

Annex II: List of Union Harmonisation Legislation
Annex IIa: List of Criminal Offences Referred to in Article 5 (1)(iii)
Annex III: High-Risk AI Systems Referred to in Article 6(2)
Annex IV: Technical Documentation Referred to in Article 11(1)
Annex V: EU Declaration of Conformity
Annex VI: Conformity Assessment Procedure Based on Internal Control
Annex VII: Conformity Based on Assessment of Quality Management System and Assessment of Technical Documentation
Annex VIII: Information to be Submitted upon the Registration of High-Risk AI Systems in Accordance with Article 51
Annex VIIIa: Information to be Submitted upon the Registration of High-Risk AI Systems Listed in Annex III in Relation to Testing in Real World Conditions in Accordance with Article 54a
Annex IX: Union Legislation on Large-Scale IT Systems in the Area of Freedom, Security and Justice
Annex IXa: Technical Documentation Referred to in Article C(1a)
Annex IXb: Transparency Information Referred to in Article C(1b)
Annex IXc: Criteria for the designation of general purpose AI models with systemic risk referred to in Article 52a

**Recitals**

Recitals provide context about how an article should be interpreted or implemented.

1	1a	2	3	4
4a	5	5a	6	6a
7	7a	7b	8	8a
9	9b	10	11	12
12a	12c	14	14a	15
16	16a	17	18	19
20	21	21a	22	23
24	25	26	26a	26b
26c	26d	27	28	28a
29	30	31	32	32a
33a	34	35	36	37
38	39	40	40a	41
42	42a	43	44	45
45a	44c	46	47	48
49	50	51	51a	52
53	53a	54	56	56a
57	57a	57b	57c	57d
57e	57f	58	58b(1)	58d
58e	58g	60a	60b	60c
60d	60e	60i(1)	60f	60g
60j	60k	60ka	60m	60n
60o	60p	60q	60r	60s
60t	60u	60aa	60v	61
61a	62	63	64	65
65a	66	67	68	69
70	70a	70b	70c	70d
70e	71	72	72a	72b
72c	73	73a	74	74a
75	75a	76	76a	77
77a	78	79	79a	80
80-x	80x	80y	80z	80z2
81	82	83	84	84a
84aa	84b	84c	85	85a
86	87	87a	87b	88
89				

15 <https://artificialintelligenceact.eu/ai-act-explorer/>

## 3-2

## 적용 범위

### 가. 물적 범위

EU 인공지능법은 그 명칭대로 기본적으로 인공지능을 적용 대상으로 하는 법률이다. 그런데 인공지능이라는 개념은 그 자체로 모호하며 통일되지 않았으므로 법률의 수범 대상으로 삼으려면 인공지능이 무엇인지 규범적으로 정의할 필요가 있다.

EU 인공지능법은 인공지능을 ‘인공지능 시스템’, ‘범용 목적 인공지능 모델’, ‘범용 인공지능 시스템’의 세 가지로 세분화하여 정의하고 있는데, 살펴보면 다음과 같다.

#### ① 인공지능 시스템(이하 ‘AI 시스템’이라 한다)

AI 시스템은 “다양한 수준의 자율성을 가지고 작동하도록 설계된 기계 기반 시스템(machine-based system)으로, 배포(deploy) 후에도 적응력(adaptiveness)을 발휘할 수 있으며, 명시적 또는 암시적 목표를 위하여 수신한 입력으로부터 예측, 콘텐츠, 추천 또는 의사결정과 같이 물리적 환경 혹은 가상 환경에 영향을 줄 수 있는 출력을 생성하는 방법을 추론하는 시스템”으로 정의된다.<sup>16</sup> 통상적으로 우리가 사용하는 인공지능의 개념과 가장 유사한 용어로 이해된다.

#### ② 범용 목적 인공지능 모델

(general purpose AI Model, 이하 ‘GPAI-M’이라 한다)

GPAI-M은 AI 시스템과는 구별되는 개념으로, “대규모 자기 감독(self-supervision)을 사용하여 대량의 데이터로 훈련된 경우를 포함하여 상당한 일반성을 가지며 시장에 출시되는 방식에 관계없이 다양한 고유의 작업을 유능하게 수행할 수 있고 다양한 시스템이나 어플리케이션에 통합될 수 있는 인공지능 모델(단, 시장에 출시되기 전에 연구, 개발 및 프로토타이핑 활동에 사용되는 AI 모델은 제외)”로 정의된다.<sup>17</sup> 바꾸어 말하면, GPAI-M은 시장에서 소위 ‘파운데이션 모델’이라고 불리는 대상, 즉 특정 인공지능 ‘시스템’(즉 특정 인공지능 서비스나 상품 등)은 아니지만 다양한 인공지능 시스템 개발에 사용될 수 있는 모델, 즉

<sup>16</sup> EU 인공지능법 제3조 (1).

<sup>17</sup> EU 인공지능법 제3조 (44b).



범용적 결과를 생성할 수 있어 다양한 인공지능 서비스나 상품 개발의 기초가 될 수 있는 인공지능 모델을 일컫는 개념이다.

### ③ 범용 AI 시스템(general purpose AI system)

범용 AI 시스템은 AI 시스템과는 구별되는 개념으로, “GPAI-M을 기반으로 하여, 직접 사용은 물론 다른 AI 시스템과의 통합을 통하여 다양한 목적을 달성할 수 있는 기능을 갖춘 AI 시스템”을 말한다.<sup>18</sup> 즉, 범용 AI 시스템은 AI 시스템의 부분집합으로 GPAI-M에 기반한 AI 시스템을 특별히 칭하는 용어이다.

## 나. 인적(人的) 범위

EU 인공지능법의 인적 적용 범위는 크게 ‘공급’ 측면의 관련자와 ‘수요’ 측면의 관련자로 나눌 수 있다. 우선 AI 시스템(또는 GPAI-M)을 시장에 ‘공급’하는 측면의 관련자들은 EU 인공지능법에서 공급자(provider), 수입업자(importer), 유통업자(distributor) 등으로 세분화된다. AI 시스템을 시장에서 사용하는 ‘수요’ 측면에서는 비개인적이고 전문적인 활동 과정에서 AI 시스템을 사용하는 자가 주된 규율 대상이며 EU 인공지능법은 이를 운용자(deployer)<sup>19</sup>라고 부른다. 여기서 핵심 개념은 ‘공급자’와 ‘운용자’이며, 살펴보면 다음과 같다.

- **공급자:** AI 시스템(또는 GPAI-M)을 개발하거나, 개발된 AI 시스템(또는 GPAI-M)을 시장에 출시하거나 (placing on the market),<sup>20</sup> 자신의 이름이나 상표를 사용하여 유상 또는 무상으로 서비스를 제공하는 (putting into service)<sup>21</sup> 자연인, 법인, 공공기관, 기관 또는 기타 단체,<sup>22</sup> 즉 통상적으로 우리가 ‘인공지능 개발자’ 혹은 ‘인공지능 서비스 제공자’ 등으로 불리는 자를 의미한다.
- **운용자:** 자신의 권한 하에 AI 시스템을 사용하는 자연인, 법인, 공공기관, 기관 또는 기타 단체. 단 개인적이고 비전문적인 활동 과정에서 AI 시스템을 사용하는 경우는 제외한다.<sup>23</sup> 즉, 자기가 개발한 AI 시스템을 업무 목적으로 사용하는 자뿐 아니라 타인이 공급하는 AI 시스템을 업무 목적으로 사용하는 자(자연인, 법인 포함)를 칭하는 개념이다.

18 EU 인공지능법 제3조 (44e).

19 deployer를 ‘배포자’라고 번역한 문헌들도 있으나, 본문에서 설명하였듯이 EU 인공지능법은 deployer를 “자신의 권한 하에 AI 시스템을 사용하는 자”로 정의하고 있으므로, 배포자라고 번역하는 것은 적절치 않다.

20 ‘시장 출시’란 AI 시스템이나 GPAI-M을 EU 역내 시장에서 ‘최초로’ 이용가능하게 하는 행위(making available on the market)를 말한다. EU 인공지능법 제3조 (9).

21 AI 시스템을 그 목적에 맞게 EU 역내에서 운용자에게 직접 공급하거나 운용자가 자체적으로 사용토록(즉, 커스터마이징해서 사용할 수 있도록) 하는 행위를 말한다. EU 인공지능법 제3조 (11).

22 EU 인공지능법 제3조 (2).

23 EU 인공지능법 제3조 (4).

위 개념 정의를 기초로 EU 인공지능법은 인적 적용 범위를 다음과 같이 규정하고 있다.<sup>24</sup>

- ① **공급자**: EU 역내에 위치 또는 설립되었는지와 무관하게, EU 역내에서 AI 시스템을 시장에 출시하거나 서비스를 제공하는 모든 공급자 또는 GPAI-M을 시장에 출시한 모든 공급자에게 적용된다.<sup>25</sup> 또한 EU가 아닌 제3국에 위치하거나 설립된 공급자라 하더라도 AI 시스템이 생성한 결과물이 EU 내에서 사용될 경우에는 해당 AI 시스템의 공급자에게 적용된다.
- ② **운용자**: EU 내에 위치하거나 설립된 운용자에게 적용된다.<sup>26</sup> 또한 제3국에 위치하거나 설립된 운용자의 경우에도 해당 AI 시스템이 생성한 결과물이 EU 내에서 사용될 경우에는 그 운용자에게 적용된다.
- ③ **기타**: 제품 제조업자가 제품과 함께 자신의 이름 또는 상표를 붙여 AI 시스템을 시장에 출시하거나 서비스를 제공하는 경우 적용된다. 또한 EU 내에 위치하고 있으며 AI 시스템 또는 GPAI-M으로 인하여 영향을 받는 일반인에게도 적용된다.

EU 역내가 아닌 제3국에 설립된 공급자/운용자의 경우에도 해당 시스템에서 생성된 결과물이 EU에서 사용되도록 ‘의도된’(intended to be used in the Union) 범위 내에서는 그 공급자/운용자에게 EU 인공지능법이 적용된다.<sup>27</sup> 조문에는 결과물이 ‘사용된’ 경우라고 규정되어 있지만,<sup>28</sup> 상설과 결합하여 보면 단순한 ‘사용’이 아니라 사용되도록 ‘의도된’ 경우에 적용된다.

즉, EU 인공지능법은 GDPR과 유사하게 EU 역내에 위치하지 않은 공급자나 운용자에게도 일정한 경우(EU 역내에 인공지능을 출시하거나 인공지능 결과물이 EU 역내에서 사용되는 경우)에는 ‘적용’될 수 있다는 점에 유의하여야 한다.

24 EU 인공지능법 제2조.

25 EU 인공지능법 제2조 1. (a).

26 EU 인공지능법 제2조 1. (b).

27 EU 인공지능법 상설 11. “this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union.”

28 EU 인공지능법 제1조 1. (c).

#### 다. 적용 제외 대상

EU 인공지능법은 다음과 같은 경우에는 적용되지 않는다.<sup>29</sup>

- ① AI 시스템이 전적으로 군사, 방위 또는 국가 안보 목적으로만 시장에 출시되거나 운용되거나 사용되는 경우
- ② 제3국의 공공당국 또는 국제기구, 나아가 제3국의 공공당국 또는 국제기구가 EU 또는 EU 회원국과 체결한 국제협약에 따라 법 집행 및 사법공조를 위하여 AI 시스템을 사용하는 경우. 이 경우 해당 공공당국 또는 국제기구는 기본권과 개인의 자유를 보장하기 위한 적절한 안전장치(adequate safeguard)를 제공하여야 한다.
- ③ 시장 출시 혹은 서비스 제공 전 단계의 AI 시스템 또는 모델에 관한 연구, 테스트 및 개발 활동
- ④ 과학적 연구개발 목적만을(sole purpose) 위하여 명확하게 개발되고 서비스가 제공되는 AI 시스템(모델 및 결과물 포함).
- ⑤ 순수하게 사적이고 비전문적인 활동을 위하여 AI 시스템을 사용하는 운전자(자연인에 한한다).
- ⑥ 무료 라이선스 혹은 오픈 소스 라이선스로 출시된 AI 시스템 중 후술하는 ‘금지된(prohibited) AI 시스템’, ‘고위험(high-risk) AI 시스템’, 또는 ‘범용 AI 시스템’에 해당하는 경우를 제외한 AI 시스템.<sup>30</sup> 무료 혹은 오픈 라이선스로 제공되는 AI 시스템은 해당 도구, 서비스, 프로세스 등이 이미 투명하게 일반 대중에게 공개되며 무료 혹은 오픈 라이선스 특성상 자유로운 접근, 수정, 재배포 등이 상대적으로 쉬우므로 EU 인공지능법에서 요구하는 각종 규제에서 일정 부분 자유를 필요가 있기 때문이다.<sup>31</sup>

<sup>29</sup> EU 인공지능법 제2조 3. ~ 5g.

<sup>30</sup> EU 인공지능법 제2조 5g.

<sup>31</sup> EU 인공지능법 상설 제57e조.

### 3-3 AI 규제 접근 방법: 위험 기반 규제(risk-based regulation)

#### 가. 기본 체계

EU 인공지능법은 인간의 건강과 안전, 그리고 기본권에 미치는 위험(risk)<sup>32</sup> 정도에 따라 고위험(high-risk) AI 시스템을 설정하고 이를 규제한다. 또한 EU 인공지능법은 AI 시스템의 특정 사용례(practice)는 인간의 건강, 안전, 기본권 등에 중대한 위험을 발생시킬 수 있어 특별한 예외가 없는 한 절대적으로 ‘금지’(prohibited)하는데 이를 이 글에서는 편의상 ‘금지된 AI 시스템’이라고 부른다. 즉 EU 인공지능법의 주된 규제 대상은 ‘금지된 AI 시스템’과 ‘고위험 AI 시스템’이다. 양자에 해당하지 않는 AI 시스템에 관하여는 일정한 경우 후술하는 ‘투명성 의무’를 부담하는 것 외에는 EU 인공지능법상 특별히 강제되는 규제는 없다.<sup>33</sup> 한마디로 EU 인공지능법은 위험 수준에 따라 AI 시스템에 대한 규제 수준을 차등화하는 ‘위험 기반 접근법’(risk-based approach)을 취하고 있다 할 수 있다.<sup>34</sup>

#### 나. 금지된 AI 시스템: 금지

##### (1) 개념

금지된 AI 시스템은 말 그대로 EU 인공지능법에 명문으로 규정된 특별한 예외가 없는 한 그 사용 자체가 ‘금지’(prohibited)된다.<sup>35</sup> 가장 강력한 규제라 할 수 있다. 따라서 법적 안정성과 수범자의 예측가능성을 위해서는 무엇이 ‘금지된’ 경우인지가 명확히 규정되어야 한다. 대원칙은 AI가 인간 의사 조작, 착취, 사회 통제 등에 악용되어 인간의 존엄성, 자유, 평등, 차별금지, 민주주의 및 법치 존중이라는 EU의 기본 가치에 위배되는 경우 공공, 민간을 불문하고 그 사용이 ‘금지’되어야 한다는 것이다.<sup>36</sup> 구체적으로 EU 인공지능법은 아래 경우를 ‘금지된 AI 시스템’(바꾸어 말하면, ‘금지된 AI 사용 관행’)으로 규정하고, 해당 AI 시스템이 시장에 출시되거나

32 EU 인공지능법상 ‘risk’는 ‘피해 발생 확률’과 ‘해당 피해로 인한 심각성’을 곱한 개념, 즉 피해의 ‘기대값’을 의미한다. EU 인공지능법 제3조 (1a).

33 EU 인공지능법 제69조.

34 EU 인공지능법 상설 제14조, 제14a조.

35 EU 인공지능법 Title II.

36 EU 인공지능법 상설 제16조.

서비스가 제공되는 것을 말 그대로 ‘금지’한다.<sup>37</sup>

- ① **잠재의식적 또는 조작적, 속임수적 기법으로 인간 의사 결정 왜곡, 조작:** (i) 인간의 의식을 넘어서는 잠재의식적 기법 또는 의도적으로 조작/속임수 기법을 사용하여 (ii) 인간이 사람이 정보에 기반한 의사 결정을 내릴 능력을 현저하게 저해하거나 그 사람이 그렇게 하지 않았을 결정을 내리도록 유도하고 (iii) 이로 인하여 그 해당인 혹은 그가 속한 집단에 심각한 피해를 초래하거나 초래할 가능성이 있는 방식으로 의사 결정을 내리게 하는 경우
- ② **취약성을 악용하여 인간 행동 왜곡:** (i) 사람 혹은 특정 집단의 취약성(연령, 장애, 장애, 특정 사회적 또는 경제적 상황 등)을 악용하여 (ii) 해당인 또는 관련 집단과 관련된 사람의 행동을 심각하게 왜곡하여 (iii) 해당인이나 그가 속한 집단에 심각한 피해를 초래하거나 초래할 가능성이 있는 방식으로 영향을 미치는 경우
- ③ **생체 데이터 기반 민감 정보 유추:** 얼굴, 지문 등 생체 인식 데이터를 기반으로 사람을 분류하여 인종, 정치적 의견, 노동 조합 가입 여부, 종교적 또는 철학적 신념, 성생활 또는 성적 성향을 추론하거나 유추하는 생체 분류 시스템을 사용하는 경우. 단 합법적으로 획득한 생체 인식 데이터 세트에 생체 인식 데이터를 기반으로 라벨링, 필터링하거나 법 집행 영역에서 생체 인식 데이터를 분류하는 경우에는 적용되지 않는다.
- ④ **개인의 사회 점수(social scoring) 시스템:** 일정 기간 동안 사회적 행동이나 알려진, 추론된 또는 예측된 개인 또는 성격적 특성을 기반으로 자연인 또는 그룹을 평가하거나 분류하는 경우
- ⑤ **법 집행 목적으로 공중에 개방된 장소(publicly accessible space)에서 실시간 원격 생체 인식:** (i) 납치, 인신 매매 및 인간의 성 착취의 특정 피해자를 대상으로 한 목표지향적 탐색 및 실종자 탐색, (ii) 자연인의 생명 또는 신체적 안전에 대한 구체적이고 상당하며 임박한 위협의 예방 또는 테러 공격의 실제

37 EU 인공지능법 제5조. 유의할 점은 앞서 언급하였듯이 시장 출시 혹은 서비스 제공 ‘전’ 단계의 AI 시스템은 ‘금지된 AI 시스템’에 해당하지 않는다는 것이다.

및 현재 또는 예견 가능한 위협, (iii) 범행을 저지른 것으로 의심되는 사람의 확인 또는 식별을 위해 범죄 수사, 기소 또는 회원국에서 최소한 4년 이상의 징역형 또는 구금 명령에 의해 처벌되는 범죄에 대한 범죄 수사, 기소 또는 범죄 처벌의 목적을 제외하고 법 집행 목적으로 공개된 장소에서 실시간으로 원격 생체 인식을 하는 경우<sup>38</sup>

- ⑥ **범죄 위험 평가, 예측:** 사람의 프로파일링 또는 성격 특성 및 그 평가만을 기반으로 사람이 범죄를 저지를 위험을 평가하거나 예측하는 경우. 단 범죄 행위와 직접적으로 연결된 객관적이고 검증 가능한 사실에 기초하여 ‘인간’이 범죄 위험을 평가하거나 예측하는 것을 지원하는 경우는 제외한다.
- ⑦ **표적화되지 않은 불특정 다수의 얼굴 이미지 처리:** 인터넷 또는 CCTV에서 표적화되지 않은 얼굴 이미지를 스크랩하여 안면 인식 데이터베이스를 생성 또는 확장하는 경우
- ⑧ **근로자 또는 학생의 감정 자동 인식:** 직장 및 교육 기관 분야에서 자연인의 감정을 추론하기 위해 시장에 내놓거나 이를 위한 서비스를 제공하거나 사용하는 경우. 단 의료 또는 안전 목적을 위한 경우는 제외한다.

## (2) 위반시 효과

금지된 AI 시스템을 시장에 출시하거나 서비스를 제공한 자에 대하여 EU 인공지능법은 3,500만 유로 또는 연간 전세계 매출액의 7% 중 큰 금액에 상당하는 과징금을 부과할 것을 가이드라인으로 제시하고 있다.<sup>39</sup> EU 회원국은 위 가이드라인에 근거하여 구체적인 처벌 및 기타 제재 조치를 규정하여야 한다.<sup>40</sup>

<sup>38</sup> 이 경우에도 사전에 당국의 명시적이고 구체적인 허가(즉 사전 승인)를 받는 것이 원칙이며, 예외적으로만 사후 승인이 허용된다.

<sup>39</sup> EU 인공지능법 제71조 1, 3.

<sup>40</sup> EU 인공지능법 제71조 1.

## 다. 고위험 AI 시스템: 공급자/운용자에게 다양한 의무 부과

### (1) 개념

고위험 AI 시스템은 개념적으로는 “사람의 건강, 안전이나 기본권의 보장에 악영향을 미칠 위험이 있는 AI 시스템”을 말한다. 이는 다소 추상적이고 모호하므로, EU 인공지능법은 고위험 AI로 간주해야 하는 경우를 다음 두 가지로 나누어 규정하고 있다.

① AI 시스템이 제품의 안전 구성 요소로 사용되거나 AI 시스템 자체가 부속서 II(Annex II)에 규정된 EU 법규의 적용을 받는 제품(기계류, 장난감, 엘리베이터, 케이블카, 의료기기, 수상기기, 항공기기, 철도시스템, 자동차 등)인 경우. 이 경우에는 EU 기존 규범상 시장에 출시하거나 서비스에 제공되기 위하여 해당 제품에 관한 EU의 기존 규범에 따라 ‘제3자 적합성 평가’를 받아야 한다.

② ①에 해당하지 않으나 부속서 III(Annex III)에 규정된 AI 시스템.<sup>41</sup> 부속서 III에 규정된 AI 시스템은 다음과 같다. (i) EU 또는 국내법에 따라 허용되는 생체인식 시스템(원격 생체 인식 시스템, 생체 분류 시스템, 감정 인식 시스템), (ii) 기반 시설(critical infrastructure) 시스템, (iii) 교육 및 직업 훈련 시스템(교육/훈련 기회 결정, 학습 결과 평가, 응시자 시험감독) (iv) 고용, 근로자 관리 시스템(채용 또는 선발 관련 입사 지원서 분석, 필터링, 후보자 평가, 사람의 성과 및 행동의 모니터링 및 평가) (v) 필수 공공/민간 서비스의 접근과 향유 관련 시스템(의료/복지 관련 자격 평가, 혜택 지급/감액/취소/환수, 사람의 신용도를 평가하거나 신용 점수 산정, 생명보험/건강보험의 위험 평가 및 가격 책정), (vi) 법 집행 및 치안 시스템, (vii) 이민, 망명, 출입국관리 시스템 (viii) 사법 및 민주적 절차 관리 시스템. 유의할 점은, 부속서 III에서 열거된 경우에 해당하지 않더라도 자연인의 프로파일링을 수행하는 경우에는 항상 고위험 AI 시스템으로 간주된다는 것이다.<sup>42</sup>

41 Annex II와 별도로 Annex III에서 고위험 AI를 다시 열거하여 규정한 이유는, EU의 기존 법령상 위험하다고 관리되어 온 제품(혹은 그 제품의 안전성 구성 요소)가 아닌 새롭게 출현하는 AI 제품/서비스 중 사람의 건강, 안전 또는 기본권 보장에 높은 위험을 초래할 가능성이 높고, 위험이 실현되었을 경우 피해의 심각성과 발생 확률을 모두 고려하여 고위험으로 분류하여 관리할 필요성이 있는 경우에 탄력적으로 대응하기 위함이다. EU 인공지능법 Recital 32.

42 EU 인공지능법 제6조 2.

## (2) 고위험 AI 시스템 AI ‘공급자’의 의무

고위험 AI 시스템 공급자는 해당 AI 시스템을 시장에 출시하기 전, 그리고 출시한 후 각각 다음과 같은 의무를 부담한다.

### ① 시장 출시 전

공급자는 (i) 위험관리 시스템, (ii) 데이터 거버넌스(데이터의 완전성 및 충분성, 관련성 등), (iii) 기술 명세서 제작/보관, (iv) 결과 추적 로그의 기록/관리, (v) 운 용자에 대한 정보 공개의 투명성, (vi) 사람에 의한 감독 (vii) 그 외 AI 시스템의 정확성, 신뢰성, 보안 등에 관한 사항을 갖추어야 하며,<sup>43</sup> 이에 관하여 ‘적합성 평가’를 받아야 한다.<sup>44</sup> 또한 적합성 평가를 통과한 고위험 AI 시스템을 시장에 출시하기 전 EU 데이터베이스에 등록하여야 한다.<sup>45</sup>

### ② 시장 출시 후

공급자는 고위험 AI 시스템 출시 후에 다음과 같은 의무를 준수하여야 한다. (i) 최소 6개월간의 로그 기록 보관 (ii) 품질 관리 시스템 운영 (iii) 관련 문서의 보 관 (iv) 시장 출시 후 해당 AI 시스템이 EU 인공지능법에 위배되거나 그렇다고 볼 이유가 있는 경우 필요한 조치(위험 원인 조사, 수정, 비활성화, 시장 철수 등)를 취하고 관련 정보를 운 용자 등에게 통지하며 관련 당국에 원인을 통보

## (3) 고위험 AI 시스템 ‘운용자’의 의무

고위험 AI 시스템 운용자는 (i) 필요한 능력, 권한, 자원을 갖춘 자연인을 감독자로 지정할 의무, (ii) 운용자가 입력 데이터를 통제하는 경우, 해당 데이터가 고위험 AI 시스템의 목적을 고려할 때 관련성과 대표성이 있음을 보장할 의무, (iii) 사용 설명 서에 따라 고위험 AI 시스템의 동작을 모니터링하고 필요한 경우 공급자나 관련 당 국에 통보할 의무, (iv) 최소 6개월 간의 로그 기록 보관 의무, (v) 고위험 AI 시스템 을 운용자의 사업장에서 사용할 경우 근로자 대표 및 근로자에게 해당 AI 시스템 의 사용을 알릴 의무를 각 부담한다.<sup>46</sup>

43 각각의 사항은 EU 인공지능법 제8조~제15조에서 상세히 규정하고 있다.

44 EU 인공지능법 제43조~제49조. 부속서 II 및 부속서 III.1.(생체인식)의 적용 대상인 경우에는 제3자 적합성 평가를, 그 외의 경우에는 내부통제에 기반한 자체 적합성 평가를 받아야 한다.

45 EU 인공지능법 제51조.

46 EU 인공지능법 제29조.



또한 운영자가 이미 시장에 출시되었거나 서비스가 개시된 고위험 AI 시스템(A)을 ‘실질적으로 변경’(substantial modification)하고 변경된 AI 시스템(B)이 여전히 고위험 AI 시스템에 해당하거나, 고위험 AI 시스템으로 분류되지 않았던 AI 시스템(A)을 변경(modification)하여 고위험 AI 시스템(B)으로 만든 경우, 운영자가 아닌 공급자로서의 의무를 부담한다. 이 경우 원래의 AI 시스템(A)의 공급자는 더 이상 변경된 AI 시스템(B)의 공급자로 간주되지 않는다.<sup>47</sup>

#### (4) 기본권 영향 평가

고위험 AI 시스템(‘중요 인프라’는 제외) 중에서 (i) 공공 서비스를 제공하는 자(공급자 및 운영자를 모두 포함하는 개념으로, 공인/사인 불문함), (ii) 자연인 신용도 평가 또는 생명보험 및 건강보험 위험 평가 및 가격 책정 용도로 운영하는 자(공급자 및 운영자를 모두 포함하는 개념임)는 사전에 ‘기본권 영향 평가(fundamental rights impact assessment)’를 수행하여야 한다.<sup>48</sup>

#### (5) 위반 시 효과

고위험 AI 시스템에 관한 규제를 위반한 자에게는 최대 1,500만 유로 또는 전세계 연간 매출액의 3% 중 큰 금액에 해당하는 과징금이 부과된다.<sup>49</sup>

<sup>47</sup> EU 인공지능법 제28조.

<sup>48</sup> EU 인공지능법 제29a조.

<sup>49</sup> EU 인공지능법 제71조 4.

## 마. GPAI-M: 일반 규제 + 시스템적 위험(systemic risk) 존재시 추가 규제

EU 인공지능법의 초안과 현행안을 비교할 때 가장 큰 차이는 초안에는 없었던 GPAI-M 규제가 신설되었다는 점에 있다. 현행안은 GPAI-M에 관하여 별도의 장(title)을 신설하고 해당 장에 총 6개의 조문을 규정하고 있다.

GPAI-M 규제의 핵심은 (i) 모든 GPAI-M에 적용되는 일반적 규제와 (ii) GPAI-M 중에서도 ‘시스템적 위험’(systemic risk)이 존재하는 경우에 추가로 적용되는 규제의 두 가지로 구성되어 있다는 점이다. ‘시스템적 위험’이란 GPAI-M로 인하여 EU 시장에 중대한 영향을 미치며 공공 보건, 안전, 안보, 기본권 또는 EU 사회 전체에 실질적으로 또는 합리적으로 예측가능한 부정적인 영향을 미칠 위험을 말한다.<sup>50</sup> 적절한 기술적 도구와 방법론을 기반으로 평가된 ‘높은 영향력’이 인정되면 시스템적 위험이 있는 GPAI-M으로 분류될 수 있으며, 이 법에 따라 설치되는 EU 인공지능 위원회(이하 ‘EU AI 위원회’라 한다)가 직권으로 해당 여부를 결정할 수도 있다. 또한  $10^{25}$  FLOPS<sup>51</sup> 컴퓨팅 파워 이상을 가진 컴퓨터로 훈련된 GPAI-M은 시스템적 위험이 있는 것으로 간주된다.<sup>52</sup>

GPAI-M 공급자는 일반적으로 (i) 학습 및 테스트 절차, 학습 콘텐츠 및 성능 평가 결과 등을 포함하는 기술 문서의 작성, 유지 및 이를 감독 당국 및 해당 모델을 사용하는 공급자에게 제공할 의무(투명성 의무) (ii) EU 디지털 시장 저작권 지침(DSM)을<sup>53</sup> 존중(respect)하는 정책을 수립, 시행할 의무를 진다.<sup>54</sup>

시스템적 위험이 있는 GPAI-M 공급자는 위 일반적 의무에 더하여 (i) 최신 기술이 반영된 표준화된 프로토콜 및 수단을 사용한 모델 평가[특히, 적대적 테스트(adversarial test)<sup>55</sup>]를 수행하고 그 결과를 문서화할 의무, (ii) 시스템적 위험을 평가하고 이를 완화할 의무, (iii) 중대 사고 발생시 이를 감독 당국에 보고할 의무,

<sup>50</sup> EU 인공지능법 제2조 44d.

<sup>51</sup> 초당 부동 소수점 연산 능력(floating point operations per seconds). H/W의 성능 측정 단위이다.

<sup>52</sup> EU 인공지능법 제52a조 1. (c). 이는 GPT-4 모델을 학습할 때 사용된 컴퓨팅 파워 수준이다.

<sup>53</sup> Directive (EU) 2019/790.

<sup>54</sup> EU 인공지능법 제52c.

<sup>55</sup> 적대적 테스트는 악의적이거나 실수로 입력값이 주어졌을때 생성형 AI가 어떻게 동작하는지를 평가하는 방법이다.

(iv) 적절한 수준의 사이버 보안을 보장할 의무 등을 부담한다.<sup>56</sup>

GPAI-M 규제를 위반한 자에게는 최대 1,500만 유로 또는 전세계 연간 매출액의 3% 중 큰 금액에 해당하는 과징금이 부과된다.<sup>57</sup>

## 바. 특정(specific) AI 시스템(GPAI-M 포함): 투명성 의무

아래에 해당하는 특정(specific) AI 시스템(GPAI-M 포함)의 공급자 및 운영자는 위에서 언급한 의무에 더하여 일정한 투명성 의무를 부담한다.

- ① **상호작용을 알릴 의무:** 자연인과 직접적으로 상호작용할 목적으로 설계되고 개발된 AI 시스템의 공급자는 상대방에게 사람이 아닌 AI 시스템과 상호작용하고 있다는 사실을 알려야 한다.<sup>58</sup>
- ② **AI 생성물 표시 의무:** (i) 합성 콘텐츠(오디오, 이미지, 동영상, 텍스트 등)를 생성하는 AI 시스템(범용 AI 시스템 포함)의 공급자는 결과물을 기계판독이 가능한 형태(machine-readable format)로 표시하여야 하며 인공적으로 생성되거나 조작되었음을 판별할 수 있도록 해야 한다.<sup>59</sup> (ii) 딥페이크에 해당하는 콘텐츠를 생성하거나 조작하는 AI 시스템의 운영자는 그러한 사실을 공개(disclose)하여야 한다.<sup>60</sup> (iii) 공공에게 공익에 관한 사실을 알릴 목적으로 배포되는 텍스트를 생성하거나 조작하는 AI 시스템의 운영자는 해당 텍스트가 인위적으로 생성 또는 조작되었다는 사실을 공개(disclose)하여야 한다.

투명성 의무를 위반한 자에게는 최대 1,500만 유로 또는 전세계 연간 매출액의 3% 중 큰 금액에 해당하는 과징금이 부과된다.<sup>61</sup>

<sup>56</sup> EU 인공지능법 제52d.

<sup>57</sup> EU 인공지능법 제71조 4.

<sup>58</sup> EU 인공지능법 제52조 1. 다만 공급자가 그러한 사실을 알리지 않더라도 합리적이고 사려깊은 평균적인 일반인을 기준으로 할 때 AI와 상호작용하고 있다는 점을 알거나 알 수 있다는 점이 명백한 경우는 이러한 의무를 부담하지 않는다.

<sup>59</sup> EU 인공지능법 제52조 1a.

<sup>60</sup> EU 인공지능법 제52조 3.

<sup>61</sup> EU 인공지능법 제71조 4.

### 3-4 AI 혁신 지원

EU 인공지능법은 인공지능 ‘규제’만을 규정한 법률은 아니며, 인공지능 혁신과 발전에 관하여도 규정하고 있다(Title V). 관련 주요 내용은 (i) 규제 샌드박스(regulatory sandbox), (ii) 실 세계에서에서의 실험(real world test), (iii) 중소기업/스타트업 지원의 세 가지이다.

#### 가. AI 규제 샌드박스

EU 회원국은 국가적 차원에서 혁신적 AI 시스템의 개발과 테스트를 용이하게 하는 AI 규제 샌드박스 제도를 적어도 하나 이상 설치하고 시행 후 24개월 동안 운영하여야 한다.<sup>62</sup> AI 규제 샌드박스는 AI 시스템이 시장에 출시되거나 서비스를 제공하기 전에 제한된 기간 동안 개발, 교육, 테스트 및 검증을 용이하게 하는 통제된 환경을 제공해야 한다. 샌드박스에서 진행된 실험의 결과로 제3자에게 손해가 발생한 경우에도 해당 시스템 공급자는 모든 책임을 져야 하지만, 규제당국이 제시한 계획 및 약관을 준수하고 관련 지침을 성실히 준수한 경우라면 금전적 행정제재로부터는 면책된다.<sup>63</sup>

규제 샌드박스에서 공익을 위하여 특정 AI 시스템을 개발할 경우, 다음 조건이 모두 충족될 경우 합법적으로 수집된 개인정보를 샌드박스 내에서 특정 AI 시스템의 개발, 교육, 테스트를 위하여 애초 수집 외 목적으로 처리할 수 있다. (i) 중요한 공익 보호(공공 안전, 공중 보건, 질병 감지·진단, 에너지 등)을 위하여 공적 주체 혹은 공무수탁사인에 의하여 개발되는 경우 (ii) 익명화나 합성 처리 등으로는 처리에 적합하지 않은 경우 (iii) 정보주체의 권리와 자유에 높은 위험을 초래하는지를 식별할 수 있는 효과적인 모니터링/대응 매커니즘이 있는 경우 (iv) 데이터 분리, 격리 및 접근 인가 통제가 되는 경우 (v) 샌드박스 외부에서 공유되지 않는 경우 등.<sup>64</sup>

62 EU 인공지능법 제53조

63 EU 인공지능법 제53조 4.

64 EU 인공지능법 제54조.

## 나. 실세계에서의 테스트

고위험 AI 시스템 공급자(잠재적 공급자 포함)는 EU 인공지능법에 규정된 모든 조건을 충족한 경우에는 규제 샌드박스가 아닌 실제 환경에서도 테스트를 할 수 있다.<sup>65</sup> (i) 테스트 계획이 작성되고 해당 계획이 테스트가 진행될 회원국의 감독 당국에 제출되고 (ii) 감독 당국이 해당 계획을 승인하고 (iii) 해당 테스트를 EU 데이터 베이스에 등록하고 (iv) 해당 공급자가 EU 내에 설립되었거나 EU 내에 법적 대리인을 지정하고 (v) 테스트 목적으로 수집 및 처리된 데이터를 EU와 제3국으로 이전할 경우 EU 규범(예컨대, GDPR)에 따라 적절하고 적용가능한 보호조치가 시행되어야 하며 (vi) 테스트 기간은 그 목표 달성에 필요한 시간을 초과하지 않아야 하고, 어떠한 경우에도 6개월을 초과하지 않으며(단 추가로 6개월까지 연장될 수 있음) (vii) 나이나 신체적, 정신적 장애로 인하여 취약한 집단에 속하는 사람들이 적절히 보호되어야 하고 (viii) 테스트 대상으로부터 사전에 동의를 받았거나 동의를 받을 수 없는 경우에는(법집행에 관한 AI 시스템 등 사전 동의를 받는 것이 테스트를 불가능하게 하는 경우) 테스트 결과가 테스트 대상에게 어떠한 부정적 영향도 미치지 않아야 하며, 테스트가 실행된 이후 테스트 대상의 데이터가 삭제되는 경우 등.

결국, 테스트 계획 작성 및 당국 승인, 테스트 내용 등록(즉 공시), 테스트 대상 보호 조치(특히, 개인정보), 테스트 대상에 대한 사전 고지 및 동의(informed consent) 등이 갖추어지면, 고위험 AI 시스템의 경우에도 규제 샌드박스가 아닌 실세계에서의 test가 최대 12개월(6개월+6개월) 허용되는 것이다. 다만 위 규정에 따라 실세계에서 테스트를 실시한 경우에도 그로 인하여 발생한 손해에 관하여 공급자(또는 잠재적 공급자)는 면책되지 않으며 회원국 및 EU 법에 따른 법적 책임을 진다.<sup>66</sup>

## 다. 중소기업/스타트업 지원

EU 내에 설립된 중소기업/스타트업에 관하여 EU 회원국은 다음과 같은 조치를 취하여야 한다.<sup>67</sup> (i) AI 규제 샌드박스 우선 접근 기회 제공 (ii) EU 인공지능법 적용에 관한 인식 제고 및 교육 제공 (iii) EU 인공지능법 이행에 관한 상담 창구 제공 (iv)

<sup>65</sup> EU 인공지능법 제54조a.

<sup>66</sup> EU 인공지능법 제54a조 8.

<sup>67</sup> EU 인공지능법 제55조.

표준화 절차 참여 촉진. 또한 EU 회원국은 중소기업/스타트업이 EU 인공지능법에 따라 제3자 적합성 평가를 해야 할 경우 그 수수료를 기업 규모, 시장 규모, 기타 관련 지표에 비례하여 감면하여야 한다.

### 3-5. 기타

#### 가. 경과 조치

EU 인공지능법은 관보에 실린 날로부터 20일째 되는 날에 발효되며, 발효일 기준 24개월 후에 시행되는 것을 원칙으로 하되 특정 규정들은 순차적으로 시행될 예정이다.<sup>68</sup> 그렇다면 법 시행일(즉, 발효일 기준 24개월째 되는 날) 이전에 EU 역내에 출시되었거나 서비스를 제공 중인 AI 시스템은 어떻게 되는가? EU 인공지능법은 이에 관한 경과 규정을 두고 있다.<sup>69</sup>

우선 (i) 시행일 12개월 이전에 EU 시장에 출시되거나 서비스를 제공 중이며 부속서 IX에 열거된 AI 시스템은<sup>70</sup> 2030년 말까지 동 법을 준수하여야 한다. (ii) (i)에 언급된 시스템 외의 고위험 AI 시스템 중 이미 EU 시장에 출시되거나 서비스를 제공 중인 고위험 AI 시스템은 시행일 이후 설계에 상당한 변화를 겪은 경우에 한하여 적용된다. (iii) 공공에서 사용하려는 고위험 AI 시스템의 공급자 및 운영자는 시행일로부터 4년 이내에 이 법을 준수하기 위하여 필요한 조치를 취해야 한다. (iv) GPAI-M 공급자는 시행일로부터 2년 이내에 이 법을 준수하기 위하여 필요한 조치를 취하여야 한다.<sup>71</sup>

68 EU 인공지능법 제85조.

69 EU 인공지능법 제83조.

70 생겐 조약에 따른 출입국/통관/비자 등 관련 시스템, 범죄정보 연계 시스템 등 기존 EU 규범/조약에 따른 EU 차원의 공적 사무 수행에 관련된 대규모 전산 시스템이다.

71 EU 인공지능법 제83조.

## 나. 향후 일정

앞서 언급하였듯이 EU 인공지능법은 발효일 기준으로 24개월째 되는 날부터 시행될 것을 원칙으로 하되, 다음과 같이 특정 규정들은 순차적으로 위 날보다 빨리 혹은 늦게 시행될 예정이다. (i) 금지된 AI 시스템 관련 규정: 발효 후 6개월 (ii) GPAI-M 관련 규정: 발효 후 12개월 (iii) 고위험 AI 시스템 중 부속서 II 관련 규정: 발효 후 36개월.

# 4

## 시사점



---

## 4 시사점

---

EU 인공지능법은 2021년에 발의되어 2024년에 이르기까지 3년이라는 시간 동안 수많은 논의를 거쳐 마련된 법률이며, 논의 과정에서 GPT로 대표되는 생성형 인공지능의 출현과 그로 인한 기술적, 경제적 패러다임의 변화와 같은 급격한 변화까지 담아낸 법률이다.

앞서 살펴보았듯이 EU 인공지능법은 그 내용이 양적, 질적으로 방대할 뿐 아니라 법문상 여전히 모호한 부분이 많고 아직 시행되지 않은 법률(정확하게는 ‘법안’)이어서 향후 어떻게 적용되고 해석될 지 현 시점에서 예측하기는 매우 어렵다. 그러나 2016년 제정, 2018년 시행된 GDPR이 그러하였듯이 EU 인공지능법 또한 EU 역내에 위치한 기업은 물론 역외에 위치한 기업, 즉 우리나라 스타트업에게도 직접 적용될 수 있다. 따라서 위 법이 본격적으로 시행되기 전에 선제적으로 주요 내용을 살펴보고 대응 방안을 마련할 필요가 있다.

앞서 언급하였듯이 EU 인공지능법은 우리나라 스타트업이 EU 역내를 대상으로 자사의 인공지능 제품이나 서비스 혹은 GPAI-M을 출시하는 경우에 적용되며(이 경우 우리나라 스타트업은 ‘공급자’라 볼 수 있다), 또한 우리나라 스타트업이 타사의 AI 제품이나 서비스를 가지고 인공지능 비즈니스가 아닌 다른 비즈니스(예컨대, 게임이나 광고 등)를 EU 역내에서 영위하는 경우에도 적용되는 것으로 보인다(이 경우에는 ‘운용자’라 볼 수 있다). 즉, 위 법이 시행되면 향후 EU 역내 시장을 타겟으로 한 인공지능에 직, 간접적으로 기반을 둔 우리나라 스타트업의 비즈니스는 모두

EU 인공지능법의 적용 대상이 될 가능성이 높다. 앞서 살펴보았듯이 EU 인공지능법은 공급자뿐 아니라 운용자에게도 다양한 법정 의무를 부과하고 있으며 이를 위반할 경우 상당히 높은 수준의 행정제재(시정명령, 과징금 등)를 가하도록 규정하고 있다. 이러한 규제를 준수하기 위하여는 시간과 비용이 소요될 수 밖에 없고, 이는 EU 시장 진출을 도모하는 우리나라 스타트업에게 상당한 부담으로 작용할 것이다. EU 인공지능법상 ‘금지된 AI 시스템’으로 규정된 경우에는 특별한 사정이 없는 한 아예 EU 역내 시장에 출시 자체가 금지된다는 점 또한 스타트업이 기술 개발과 비즈니스 모델 수립에 있어 참고할 필요가 있다.

물론 EU 인공지능법이 인공지능법을 무조건 ‘규제’만 하는 규범은 아니며 AI 규제 샌드박스나 실세계 테스트와 같은 혁신적인 사항도 규정하고 있지만, EU 역내에 설립되지 않은 우리나라 스타트업도 위 제도들을 활용할 수 있는지는 아직까지는 다소 불명확하다는 점도 유념하여야 한다.<sup>72</sup>

결국, GDPR의 사례에서도 그러하였듯이 개별 기업들이 EU 인공지능법을 각자 알아서 대응하기에는 한계가 있으며, 정부 및 유관기관들의 협조와 지원이 절실히 필요할 것으로 보인다.

---

<sup>72</sup> 일례로 AI 규제 샌드박스 참여 자격 및 선정 절차 등은 EU 인공지능법에는 구체적 사항이 없으며, 향후 EU 집행위원회가 세부 규정을 정할 예정이다. EU 인공지능법 제53a조 1.





## STARTUP ALLIANCE

**발행인** 스타트업얼라이언스  
**기획/제작** 스타트업얼라이언스  
**발행처** 스타트업얼라이언스  
서울특별시 강남구 봉은사로 215,  
11층(논현동, KTS 빌딩)  
<https://startupall.kr>  
**발행일** 2024.4.30

ISSN 2982-4834

이 책의 저작권은  
스타트업얼라이언스에 있으며  
무단복제와 전재를 금합니다.



