SHIN&KIM
법무법인(유) 세종

국내 최초 인공지능 신뢰성 단체표준 제정

2023.12.15

과학기술정보통신부(이하 “과기정통부”)와 한국정보통신기술협회(이하 “TTA”)는 12월 6일 **정보통신단체표준**인 ‘**인공지능 시스템 신뢰성 제고를 위한 요구사항**(Requirements to enhancing trustworthiness for AI systems)’을 제정하였습니다.

이는 국내 최초로 마련된 인공지능(이하 “AI”) 신뢰성 단체표준*으로, **AI 시스템 생명주기 전체에서 관련 이해관계자가 신뢰성 제고를 위해 충족해야 할 요구사항**을 담아냈습니다.

* ‘단체표준’이란 국가표준·국제표준과 구분되는 것으로서, 산업표준화와 관련된 단체 중 산업통상자원부령으로 정하는 단체가 공공의 안전성 확보, 소비자 보호 및 구성원들의 편의를 도모하기 위하여 특정의 전문분야에 적용되는 기호·용어·성능·절차·방법·기술 등에 대해 제정한 표준을 말합니다(산업표준화법 제27조 참조).

구체적으로 위 표준에서는 과기정통부의 ‘**국가 AI윤리기준**’(’20.12.) 및 분야별 ‘**신뢰할 수 있는 AI 개발안내서**’(’22년 3종, ’23년 3종)를 기반으로, 신뢰성 적용범위, 특성, 시스템 생명주기 및 이해관계자 등 **AI 시스템 신뢰성 구성요소와 요구사항**을 제시하였습니다.

[‘인공지능 시스템 신뢰성 제고를 위한 요구사항’ 표준 세부 내용]

AI 시스템 신뢰성 구성요소	적용범위	AI 기술이 적용된 제품 및 서비스와 함께 AI 시스템 개발에 필요한 서비스 기획, 데이터 수집 및 가공, 시스템 통합, 배포 및 모니터링 과정의 전체 범위로, AI 시스템 사용 중 발생 가능한 위험 대상인 서비스 운영 및 사용자 관련 부분 포함(단, AI 시스템 개발, 성능평가와 같은 일반적 소프트웨어 요구사항과 네트워크 인프라 운영 요구사항은 제외)
	세부특성	견고성, 보안성, 설명가능성, 신뢰성, 안전성, 예측가능성, 제어가능성, 책임성, 투명성, 공정성, 프라이버시, 회복탄력성
	생명주기	초기, 설계 · 개발, 검증 · 확인, 배치, 운영 · 모니터링, 지속적 확인, 재평가, 폐기
	이해관계자	AI 제공자, AI 생산자, AI 고객, AI 파트너, AI 영향대상, 관계기관
요구사항		1. AI 시스템 위험관리 계획 및 수행 2. AI 거버넌스 체계 구성 3. AI 시스템의 신뢰성 테스트 계획 수립 4. AI 시스템의 추적가능성 및 변경이력 확보 5. 데이터의 활용을 위한 상세 정보 제공

	6. 데이터 견고성 확보를 위한 이상 데이터 점검 7. 수집 · 가공된 학습데이터의 편향 제거 8. AI 오픈소스 라이브러리의 보안성 및 호환성 점검 9. AI 모델의 편향 제거 10. AI 모델 공격에 대한 방어 대책 수립 11. AI 모델 명세 및 추론 결과에 대한 설명 제공 12. AI 시스템 구현 시 발생 가능한 편향 제거 13. AI 시스템의 안전모드 구현 및 문제발생 알림절차 수립 14. AI 시스템의 설명에 대한 사용자의 이해도 제고 15. 서비스 제공 범위 및 상호작용 대상에 대한 설명 제공

※ 위 요구사항은 **모두 '필수' 요구사항으로** 2023년도 기준 **「인공지능산업 육성 및 신뢰 확보에 관한 법률안」**에 명시된 **고위험영역 AI를 고려하여 그와 같이 결정되었음**

위 표준은 AI 신뢰성 관련 국제표준인 ISO/IEC TR 24028(신뢰성 개요), ISO/IEC 23894(위험관리), ISO/IEC 22989(용어)의 신뢰성 개념과 용어, 요구사항과의 내용 일관성을 유지함으로써 **국제 호환성을 확보**한 것으로 평가되며, 과기정통부와 TTA는 이번 단체표준 제정을 시작으로 향후 **(1) 단체표준의 요구사항에 대한 검증 프로세스 표준화, (2) 단체표준의 내용을 분야별로 확대하여 위험 기반의 검증 항목·절차에 대한 표준화**를 지속 추진하겠다고 밝혔습니다.

시사점

정부는 AI 윤리·신뢰성 확보를 AI 기술 혁신과 활용 확산을 위한 전제조건으로 두고, 국내 산업계 전반의 AI 윤리·신뢰성 제고를 위한 정책적 노력을 기울이고 있습니다. 그 일환으로 과기정통부와 TTA는 2021년부터 분야별 '신뢰할 수 있는 AI 개발안내서'를 개발·보급하고, 'AI 신뢰성 컨설팅 서비스'를 제공하고 있으며, 이번에 정보통신단체표준을 제정하여 발표하였습니다.

나아가 국회 과방위에서 중요하게 논의되고 있는 「인공지능산업 육성 및 신뢰 확보에 관한 법률안(윤두현의원 대표발의, 의안번호 18726)」 또한 '인공지능산업 발전과 신뢰성 확보의 균형을 달성하는 법제도 마련'을 입법 취지로 하여 기본원칙에 신뢰성 제고를 포함하고(안 제3조), 인공지능 신뢰성 전문위원회를 설치하며(안 제9조), 과기정통부가 신뢰성 확보를 위한 시책을 마련하고 신뢰성 검·인증 지원 사업을 추진하는 것(안 제24조 및 제25조) 등을 주요 내용으로 하고 있습니다.

이와 같이 인공지능산업의 신뢰성 확보에 대한 정부의 관심이 지대한만큼, 관련 사업자들은 정부 정책 및 입법 동향을 예의 주시하면서 AI 개발 등에서의 신뢰성 확보에 만전을 기할 필요가 있습니다.

About Shin & Kim's ICT Group

법무법인(유) 세종의 ICT그룹은 방송, 개인정보, 통신 분야에서 축적된 역량을 한 곳에 집중하는 동시에 과학기술정보통신부, 방송통신위원회, 정보통신정책연구원 등에서 근무한 우수한 전문가들을 중심으로 방송과 통신, 개인정보, 인터넷 IT 등 ICT 규제 전반에 관하여 통합적인 법률서비스를 제공하고 있을 뿐만 아니라 광범위한 네트워크를 바탕으로 업계를 선도할 수 있는 정책자문 및 전략자문까지 제공하고

있습니다. 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

강지현
변호사

02-316-1518
jhykang@shinkim.com

이원석
변호사

02-316-7933
wslee@shinkim.com

주해인
변호사

02-316-1825
hiju@shinkim.com

김지훈
수석전문위원

02-316-2883
jhookim@shinkim.com