



October 7, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

---

**Susanne Werry**

Counsel / Frankfurt  
49.69.74220.133  
susanne.werry@skadden.com

**William E. Ridgway**

Partner / Chicago  
312.407.0449  
william.ridgway@skadden.com

**David A. Simon**

Partner / Washington, D.C.  
202.371.7120  
david.simon@skadden.com

**Nicola Kerr-Shaw**

Counsel / London  
44.20.7519.7101  
nicola.kerr-shaw@skadden.com

**Joshua Silverstein**

Counsel / Washington, D.C.  
202.371.7148  
joshua.silverstein@skadden.com

---

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West  
New York, NY 10001  
212.735.3000

## EU Standardization Supporting the Artificial Intelligence Act

### Executive Summary

- With the EU's AI Act having entered into force on August 1, 2024, companies now need to focus on its implementation. Although the AI Act will not be fully enforceable until August 2, 2027, some obligations will become binding before then, and companies can do much to prepare in the course of the next three years.
- The AI Act sets out numerous vague requirements for AI systems, including risk assessments and cybersecurity specifications, that could pose compliance challenges for companies.
- "Harmonized Standards" developed by the European Standardization Organizations (ESOs) will play a pivotal role in clarifying these requirements, including, for example, the requirement to implement suitable risk management measures.
- Companies complying with Harmonized Standards can benefit from a "presumption of conformity," which means these companies will be presumed to comply with certain elements of the AI Act unless there is evidence of nonconformity. The ESOs are currently developing new standards which, according to the target set by the European Commission, are to be finalized by April 30, 2025, more than a year before the AI Act becomes fully enforceable. However, given the scope of the various required standards, their complexity, the limited resources of the ESOs and an already tight timeline, the deadline will likely shift to the end of 2025.
- The standardization bodies of the EU reviewed existing standards that could support compliance with the AI Act and, where possible, used them as a basis to develop the Harmonized Standards.<sup>1</sup> Companies may be able to leverage their work to adhere to these standards to facilitate AI Act compliance as well.
- Companies using AI tools that fall within the scope of the AI Act's coverage will want to check which of the existing standards they can leverage, and should track the working program and the development of new Harmonized Standards by the EU standardization bodies.

### The EU's AI Act – Background

The AI Act entered into force on August 1, 2024. It applies to providers, deployers, importers and distributors of AI systems, regardless of their location, if they market an AI system, serve AI system users or utilize the "output" of an AI system in the EU. It follows a risk-based approach and classifies AI systems into four different risk categories. While unacceptable risk is prohibited, AI systems falling into other risk categories (high-risk,

---

<sup>1</sup> Existing standards that are adapted by JTC 21 are available on the [CEN-CENELEC Status Dashboard](#) posted by the JTC 21 chair; and the JTC 21 work program is available in the CEN-CENELEC Focus Group Report "Road Map on Artificial Intelligence (AI)" (Sept. 2020).

# EU Standardization Supporting the Artificial Intelligence Act

limited-risk or low-risk) are subject to graded requirements. Certain provisions of the AI Act apply to general-purpose AI models regardless of the specific use case.<sup>2</sup>

The implementation of the AI Act follows a staggered approach, requiring companies to comply with provisions of the AI Act sequentially over the next three years.

<b>August 1, 2024</b>	Entry into force of the EU AI Act.
<b>February 2, 2025</b>	“Prohibited AI” considered to pose an unacceptable level of risk will be prohibited.
<b>May 2, 2025</b>	The Code of Practice for providers of general AI models becomes applicable. <sup>3</sup>
<b>August 2, 2025</b>	Provisions concerning (i) notification of authorities, (ii) obligations for providers of general-purpose AI models, (iii) governance, (iv) penalties and fines, and (v) confidentiality become applicable.
<b>August 2, 2026</b>	The EU AI Act starts applying to high-risk AI systems listed in Annex III (e.g., AI systems in the areas of biometrics, critical infrastructure, education, employment or law enforcement).
<b>August 2, 2027</b>	The entire EU AI Act starts to apply to all risk categories (including high-risk AI systems listed in Annex II).

The AI Act imposes requirements on various AI stakeholders, not only developers of AI. This includes providers (developers), deployers, importers and distributors.<sup>4</sup> For example, providers are obliged to take measures to minimize risks posed by the use of high-risk AI systems: Providers must first identify and analyze known and foreseeable risks posed by the intended use of the high-risk AI system.<sup>5</sup> Then they are required to implement a risk management system that includes the adoption of appropriate and targeted risk management measures.<sup>6</sup>

<sup>2</sup> See our article in the June 2024 edition of *Skadden Insights*, “[The EU AI Act: What Businesses Need To Know](#),” or this [summary of the AI Act](#).

<sup>3</sup> The Code of Practice will detail the AI Act rules for providers of general-purpose AI models and general-purpose AI models with systemic risks. Providers should be able to rely on the Code of Practice to demonstrate compliance.

<sup>4</sup> See our article in the June 2024 edition of *Skadden Insights*, “[The EU AI Act: What Businesses Need To Know](#).”

<sup>5</sup> Art. 9 (2) lit. a-AI Act.

<sup>6</sup> Art. 9 (2) lit. d-AI Act.

The specific requirements for “appropriate and targeted risk management measures” are, however, not further specified. Officials expect to provide needed clarity in the form of AI-specific Harmonized Standards.

## Defining Harmonized Standards

EU Standards are technical specifications that define requirements for products, production processes, services or test methods. These specifications are voluntary and are developed by industry and market actors. Standards ensure interoperability and safety, reduce costs and facilitate companies’ integration into the value chain and trade.<sup>7</sup> A “Harmonized Standard” is a European standard developed by a recognized ESO: the European Committee for Standardization (CEN), the European Electrotechnical Committee for Standardization (CENELEC) or the European Telecommunications Standards Institute (ETSI). Examples include Harmonized Standards for individual products to comply with general product safety requirements, e.g., standards regarding requirements and test methods for children’s high chairs<sup>8</sup> or standards to comply with the regulation for medical devices.<sup>9</sup>

The ESOs are currently developing standards related to various sectors and pieces of EU legislation. A notable example is the Digital Operational Resilience Act (DORA), which sets out sector-specific cybersecurity requirements for financial entities. DORA mandates that the European Supervisory Authorities (the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) — together the ESAs) jointly develop a total of 13 policy instruments, namely a set of standards, including e.g., “Regulatory Technical Standards” (RTS) for a risk management framework for information and communications technology (ICT) or RTS for companies subcontracting critical or important functions.

Harmonized Standards will offer crucial guidance to companies on how to assess and mitigate risks associated with AI products and will provide precise technical specifications to clarify the requirements of the basic legislation.

## Presumption of Conformity

Adherence to Harmonized Standards, which are specifically designed to underpin EU legislation, confers a “presumption of

<sup>7</sup> EC Directorate General for Internal Market, Industry, Entrepreneurship and SMEs, [European Standards](#).

<sup>8</sup> [Directive 2001/95/EC on General Product Safety – Summary List](#).

<sup>9</sup> [Commission Implementing Decision \(EU\) 2020/437](#) (March 24, 2020).

# EU Standardization Supporting the Artificial Intelligence Act

conformity” with the essential requirements of such legislation. In other words, if companies fulfill the Harmonized Standards, compliance with the requirement is presumed.<sup>10</sup>

## AI Act and EU Standards

### Need for Action

On May 22, 2023, the European Commission (EC) issued a standardization request for the upcoming AI Act.<sup>11</sup> The EC tasked CEN and the CENELEC with developing new European standards or standardization deliverables to support the AI Act by April 30, 2025.<sup>12</sup> The mandate requires these standards to ensure that AI systems introduced to the EU market are safe and uphold fundamental rights. Additionally, the standards should encourage investment and innovation in AI and enhance the competitiveness and growth of the EU market.<sup>13</sup>

In January 2023, the CEN-CENELEC Joint Technical Committee (JTC 21) proposed a road map to support the standardization of AI.<sup>14</sup> The committee conducted a landscape analysis to identify existing AI-related standards and ongoing standardization activities by other Standards Developing Organizations (SDOs), primarily ISO/IEC JTC 1/SC 42.<sup>15</sup>

The European Commission’s Joint Research Center (JRC) evaluated this standardization road map and concluded that existing international standards partially meet the AI Act’s requirements for trustworthy AI, with many gaps addressed by planned European standards. The report highlights areas needing further attention and suggests additional standards to support the AI Act.<sup>16</sup> For example, the JRC evaluated the suitability of ISO/IEC 42001 for adoption as a Harmonized Standard under the AI Act: ISO/IEC 42001 provides limited coverage of logging and recordkeeping, treating both as optional risk controls. Further requirements are expected from new standards, such as the CEN-CENELEC JTC 21’s “AI Trustworthiness Characterization,” which includes in its outline provisions on recordkeeping and traceability.<sup>17</sup>

<sup>10</sup>This presumption of conformity is specifically outlined in Art. 40 (1) AI Act. The Act stipulates that high-risk systems or GPAI models that comply with the relevant harmonized standards — yet to be developed — are presumed to comply with the relevant requirements for these systems (e.g., Chapter III, Section 2, Requirements for High-Risk AI).

<sup>11</sup>C(2023)3215.

<sup>12</sup>Art. 1 C(2023)3215.

<sup>13</sup>Recital C(2023)3215.

<sup>14</sup>CEN-CENELEC on Artificial Intelligence.

<sup>15</sup>E.g., ISO/IEC JTC 1 and its subcommittees.

<sup>16</sup>“Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act” (May 2023).

<sup>17</sup>Ibid, p. 2.

## Available Standards

### Standards Already Adopted by JTC 21

JTC 21 published a list of AI Harmonized Standards that the committee has officially adopted.<sup>18</sup> The adopted standards include:

- **CEN/CLC ISO/IEC TR 24027:2023**, published in December 2023, addresses bias related to AI systems and **describes measurement techniques and methods for assessing bias**.
- **ISO/IEC 23894:2023**, published in February 2024, provides guidance **on how organizations that develop, produce or deploy AI or that use products, systems and services that utilize AI can manage risk** specifically related to AI.

### Standards Not Specific to AI

In addition, Harmonized Standards not specific to AI are relevant to the development and use of AI. **ISO/IEC 27001**, for example, **can guide the development of policies for AI ethics and data protection impact assessments** by providing a structured approach to managing risks associated with AI technologies, even though it is not a Harmonized Standard under the AI Act.<sup>19</sup> Notably however, these standards, though useful, do not convey the presumption of conformity with the AI Act.

## Work Program and Standard-Setting Timeline

With the AI Act officially passed, the ESOs have begun developing additional Harmonized Standards. CEN and CENELEC published a work program delineating which standards have already been drafted or modified and which ones will be developed, including an expected time frame.<sup>20</sup> CEN and CENELEC also published a dashboard of work items on September 1, 2024. **The dashboard details the current progress of the standards and shows which standards will fulfill the requirements in the EC’s standardization request.**

However, according to Sebastian Hallensleben, the chair of JTC 21, the Harmonized Standards will likely be completed at the end of 2025, eight months later than the original deadline of April 30, 2025.<sup>21</sup> This would leave companies with less time to assess and implement the standards before the general enforcement of the EU AI Act in August 2026.

<sup>18</sup>CEN/CLC/JTC 21 Published Standards.

<sup>19</sup>CEN-CENELEC Focus Group Report “Road Map on Artificial Intelligence (AI)” (Sept. 2020), p. 8.

<sup>20</sup>CEN/CLC/JTC 21 Work Programme.

<sup>21</sup>MLex, “Deadline for AI Standards To Be Postponed, EU Standards Chief Says” (Aug. 1, 2024).

# EU Standardization Supporting the Artificial Intelligence Act

---

## Adaptive Standards

**CEN and CENELEC broadly agree that international standards, e.g., ISO standards, should be used but adapted to meet the requirements of the AI Act.** This means that companies that must comply with the AI Act and already comply with international standards, such as, e.g., ISO/IEC 42001, will be able to leverage their original compliance to meet the relevant provisions of the AI Act.

## Recommendation

Companies are further advised to maintain currency with the standards developed by the ESOs in order to make sure their business models and products meet any applicable legal requirements.