GIBSON DUNN

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law

Client Alert | June 3, 2024

The Council of Europe Has Adopted the First International Treaty on Artificial Intelligence.

1. **Executive Summary**

On May 17, 2024, the Council of Europe adopted the first ever international legally binding treaty on artificial intelligence, human rights, democracy, and the rule of law (Convention)[1]. In contrast to the forthcoming EU AI Act[2], which will apply only in EU member states, the Convention is an international, potentially global treaty with contributions from various stakeholders, including the US. The ultimate goal of the Convention is to establish a global minimum standard for protecting human rights from risks posed by artificial intelligence (AI). The underlying core principles and key obligations are very similar to the EU AI Act, including a risk-based approach and obligations considering the entire life cycle of an AI system. However, while the EU AI Act encompasses comprehensive regulations on the development, deployment, and use of AI systems within the EU internal market, the AI Convention primarily focuses on the protection of universal human rights of people affected by AI systems. It is important to note that the Convention, as an international treaty, does not impose immediate compliance requirements; instead, it serves as a policy framework that signals the direction of future regulations and aims to align procedures at an international level.

2. **Background and Core Principles**

The Convention was drawn up by the Committee on Artificial Intelligence (CAI), an intergovernmental body bringing together the 46 member states of the Council of Europe, the European Union, and 11 non-member states (namely Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America, and Uruguay) as well as representatives of the private sector, civil society, and academia. Such multi-stakeholder participation has been shown to promote acceptance of similar regulatory efforts. The main focus lies on the protection of human rights, democracy, and the rule of law, the core guiding principles of the Council of Europe, by establishing common minimum standards for AI systems at the global level.

3. **Scope of Application**

The Convention is in line with the updated OECD definition of AI, which provides for a broad definition of an “artificial intelligence system” as “a machine-based system that for explicit or implicit objectives infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments.” The EU AI Act, OECD updated definition, and US Executive Order

Related People

Robert Spano

Joel Harrison

Yannick Oberacker

Christoph Jacob

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

(US EO) 14110 definitions of AI systems are generally aligned as they all emphasize machine-based systems capable of making predictions, recommendations, or decisions that impact physical or virtual environments, with varying levels of autonomy and adaptiveness. However, the EU and OECD definitions highlight post-deployment adaptiveness, while the US EO focuses more on the process of perceiving environments, abstracting perceptions into models, and using inference for decision-making.

Noteworthy is the emphasis on the entire life cycle of AI systems (similar to the EU AI Act). The Convention is primarily intended to regulate the activities of public authorities – including companies acting on their behalf. However, parties to the Convention must also address risks arising from the use of AI systems by private companies, either by applying the same principles or through "other appropriate measures," which are not specified. The Convention also contains exceptions, similar to those laid down by the EU AI Act. Its scope excludes:

- activities within the lifecycle of AI systems relating to the protection of national security interests, regardless of the type of entities carrying out the corresponding activities;
- all research and development activities regarding AI systems not yet made available for use; and
- matters relating to national defense.

4. **Obligations and Principles**

The Convention is principles-based and therefore by its nature formulated in high level commitments and open-ended terms. It contains several principles and obligations on the parties to take measures to ensure the protection of human rights, the integrity of democratic processes, and respect for the rule of law. These core obligations are familiar as they also form the basis of the EU AI Act. The core obligations include:

- measures to protect the individual's ability to freely form opinions;
- measures ensuring adequate transparency and oversight requirements, in particular regarding the identification of content generated by AI systems;
- measures ensuring accountability and responsibility for adverse impacts;
- measures to foster equality and non-discrimination in the use of AI systems, including gender equality;
- the protection of privacy rights of individuals and their personal data;
- to foster innovation, the parties are also obliged to enable the establishment of controlled environments for the development and testing of AI systems.

Two other key elements of the Convention are that each party must have the ability to prohibit certain AI systems that are incompatible with the Convention's core principles and to provide accessible and effective remedies for human rights violations. The examples given in the Convention underline that current issues have been included, *e.g.,* election interference seems to be one of the risks discussed.

5. **Criticism and Reactions**

The Convention has been criticized by civil society organizations[3] and the European Data Protection Supervisor[4]. The main points of criticism include:

- Broad Exceptions: The Convention includes exceptions for national security, research and development, and national defense. Critics argue that these loopholes could undermine essential safeguards and lead to unchecked AI experimentation and use in military applications without oversight. Similar criticism

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

has been levelled at the EU AI Act.

- Vague Provisions and Private Sector Regulation: The Convention's principles and obligations are seen as too general, lacking specific criteria for enforcement. Critics highlight the absence of explicit bans on high-risk AI applications, such as autonomous weapons and mass surveillance. Additionally, the Convention requires addressing risks from private companies but does not specify the measures, leading to concerns about inconsistent regulation.
- Enforcement and Accountability: The Convention mandates compliance reporting but lacks a robust enforcement mechanism. Critics argue that without stringent enforcement and accountability, the Convention's impact will be limited. There are also concerns about the adequacy of remedies for human rights violations by AI systems, due to vague implementation guidelines.

6. **Implementation and Entry into Force**

The parties to the Convention need to take measures for sufficient implementation. In order to take account of different legal systems, each party may opt to be directly bound by the relevant Convention provision or take measures to comply with the Convention's provisions. Overall, the Convention provides only for a common minimum standard of protection; parties are free to adopt more extensive regulations. To ensure compliance with the Convention, each party must report to the Conference of the Parties within two years of becoming a party and periodically thereafter on the activities it has undertaken.

7. **Next Steps and Takeaways**

The next step is for States to sign the declaration of accession. The Convention will be opened for signature on September 5, 2024. It is expected, although not certain, that the CoE Member States and the other 11 States (including the US) that contributed to the draft convention will become parties.

In the EU, the Convention will complement the EU AI Act sharing the risk based approach and similar core principles. Given the very general wording of the Convention's provisions and the broad exceptions to its scope, it seems that the EU AI Act, adopted on May 21, remains the most comprehensive and prescriptive set of standards in the field of AI at least in the EU. However, as the Convention will form the bedrock of AI regulation in the Council of Europe, it is to be expected that the European Court of Human Rights (**ECtHR**) will in the future draw inspiration from the Convention when interpreting the European Convention on Human Rights (**ECHR**).This may have significant cross-fertilisation effects for EU fundamental rights law, including in the implementation of the EU AI Act, as the ECHR forms the minimum standard of protection under Article 52(3) of the Charter of Fundamental Rights of the European Union (**Charter**). Both States and private companies will therefore have to be cognisant of the potential overlapping effects of the Convention and the EU AI Act.

---

[1] See Press release here. See the full text of the Convention here.

[2] On May 21, 2024, the Council of the European Union finally adopted the AI Regulation (AI Act). For details on the EU AI Act, please also see: https://www.gibsondunn.com/artificial-intelligence-review-and-outlook-2024/.

[3] See https://ecnl.org/sites/default/files/2024-03/CSOs_CoE_Calls_2501.docx.pdf.

[4] See https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial_en#_ftnref2.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

The following Gibson Dunn lawyers assisted in preparing this update: Robert Spano, Joel Harrison, Christoph Jacob, and Yannick Oberacker.

Gibson Dunn lawyers are available to assist in addressing any questions you may have regarding these issues. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Artificial Intelligence, Privacy, Cybersecurity & Data Innovation or Environmental, Social and Governance (ESG) practice groups:

Artificial Intelligence:
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Robert Spano – London/Paris (+44 20 7071 4902, rspano@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com)

Privacy, Cybersecurity and Data Innovation:
Ahmed Baladi – Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33 180, kgesing@gibsondunn.com)
Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com)

Environmental, Social and Governance (ESG):
Susy Bullock – London (+44 20 7071 4283, sbullock@gibsondunn.com)
Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
Perlette M. Jura – Los Angeles (+1 213.229.7121, pjura@gibsondunn.com)
Ronald Kirk – Dallas (+1 214.698.3295, rkirk@gibsondunn.com)
Michael K. Murphy – Washington, D.C. (+1 202.955.8238, mmurphy@gibsondunn.com)
Selina S. Sagayam – London (+44 20 7071 4263, ssagayam@gibsondunn.com)

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com.

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

Artificial Intelligence

Privacy, Cybersecurity, and Data Innovation

ESG: Risk, Litigation, and Reporting