onetrust
DataGuidance

AI Report

Principles, laws, and frameworks

E-BOOK | 2025

Table of Contents

Table of Contents

Page 5: George Hammerstein/The Image Bank via Getty Images, Page 11: matdesign24/iStock via Getty Images, Page 28: Westend61/Westend61 via Getty Images, Page 31: Alexander Spatari/Moment via Getty Images, Page 40: moodboard/Connect Images via Getty Images, Page 45: MoMo Productions/DigitalVision via Getty Images, Page 57: Thomas Barwick/DigitalVision via Getty Images, Page 58:Thomas Barwick/DigitalVision via Getty Images

Introduction

Artificial intelligence (AI) has rapidly evolved from a niche technological innovation into a foundational element of modern digital infrastructure. Its integration across sectors, from healthcare, finance, education, law enforcement, and public administration, has reshaped how decisions are made, services are delivered, and data is processed. The proliferation of generative AI (Gen AI), large language models (LLMs), and automated decision systems (ADS) has further accelerated this transformation by offering unprecedented capabilities while simultaneously introducing complex ethical, legal, and societal challenges.

In this context, the AI Report provides a consolidated overview of the global AI regulatory landscape. It examines enacted legislation, draft proposals, and national and international frameworks, offering an understanding of how jurisdictions are responding to the risks and opportunities posed by AI technologies. The report highlights the growing consensus around key governance principles, such as transparency, accountability, conducting risk assessments, and human oversight, while also acknowledging the diversity of approaches taken by different legal systems.

In view of the volume and velocity of global AI-related legislative and policy developments, this report is intended as a non-exhaustive overview. The laws and frameworks included in this report were selected based on their regulatory relevance, scope, and maturity. Priority was given to instruments that:

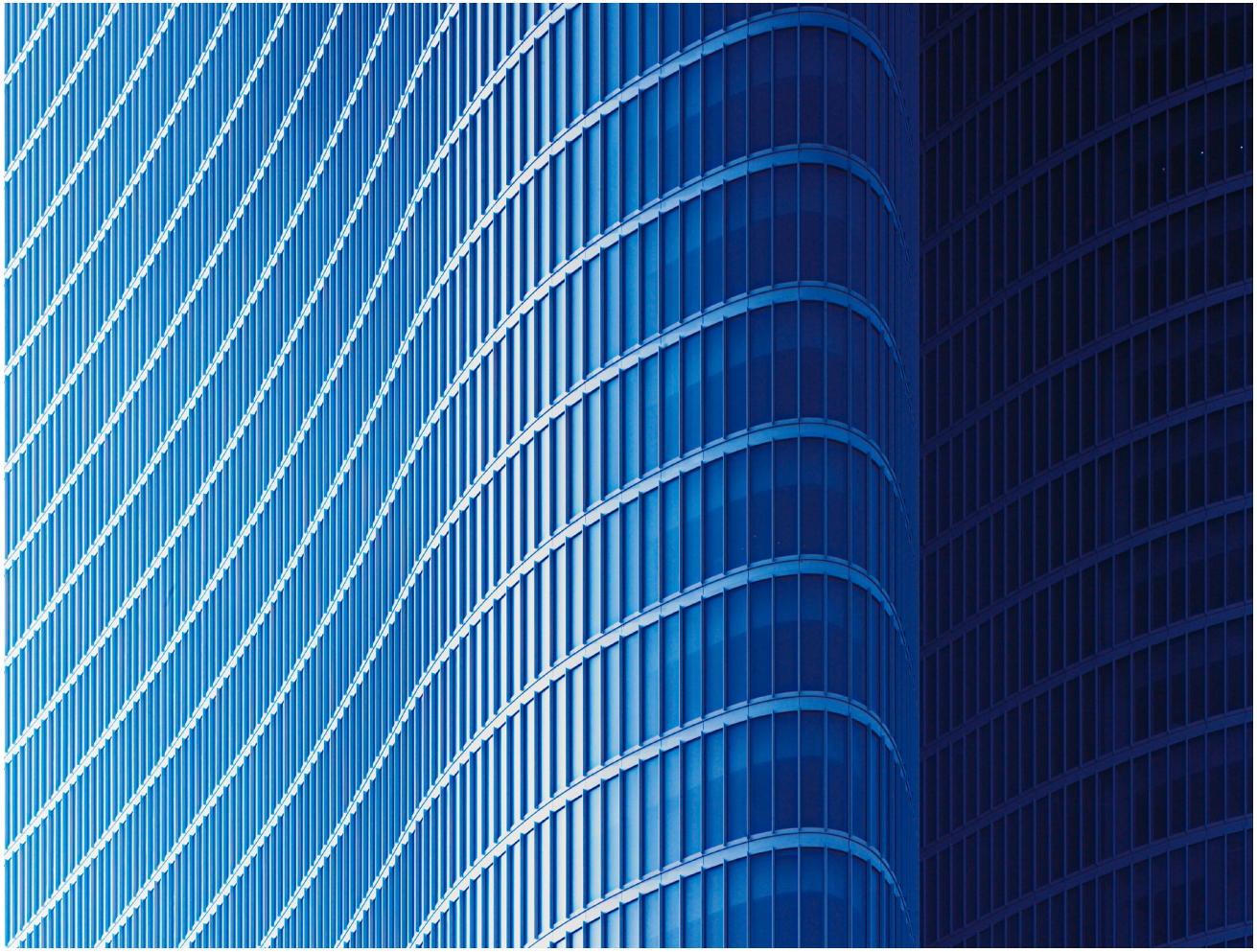
- have been formally enacted or adopted by national or international authorities;
- introduce binding obligations or enforceable standards for AI system governance;
- address core risks associated with AI, including algorithmic discrimination, synthetic content, biometric data processing, and automated decision-making;
- provide clear definitions of AI systems and stakeholder roles (e.g., developer, deployer, provider); and
- demonstrate international influence or interoperability with other legal regimes.

Furthermore, the report includes draft legislation and voluntary frameworks where they represent significant policy direction or are likely to shape future regulatory approaches.

By mapping these developments, the report aims to support legal, compliance, and policy professionals in understanding the evolving obligations and expectations surrounding AI. It also serves as a resource for organizations seeking to align their AI practices with emerging standards and prepare for future regulatory scrutiny.

Existing legislation

This section outlines several laws and regulations that have been enacted, some already in force across various jurisdictions. These instruments impose current or future binding obligations on AI developers, deployers, and other stakeholders, and often include enforcement mechanisms, penalties, and oversight structures. The selected legislation reflects a range of regulatory approaches, from comprehensive frameworks to targeted laws addressing synthetic content, biometric data, and algorithmic decision-making.



Existing legislation

EU

EU: AI Act

On March 13, 2024, the European Union Artificial Intelligence Act (the EU AI Act) was formally adopted by the European Parliament and subsequently approved by the Council of the European Union. On July 12, 2024, the EU AI Act was published in the Official Journal of the European Union and entered into force on August 1, 2024. The EU AI Act will be fully applicable 24 months after entry into force, i.e., August 2, 2026, except for:

- general provisions and prohibited practices, which came into force on February 2, 2025;
- general-purpose AI (GPAI) rules and provisions on penalties, which came into force on August 2, 2025; and
- obligations for high-risk systems, which will apply from August 2, 2027.

Scope

The EU AI Act establishes harmonized rules for the development, marketing, and use of AI systems across all industries, guided by a risk-based approach that tailors regulatory obligations to the level of risk posed by each system.

Specifically, it introduces transparency rules and requirements for 'high-risk AI systems,' and prohibits certain AI practices outright. At the same time, it introduces rules on market monitoring and surveillance. Similar to the General Data Protection Regulation (GDPR), the EU AI Act is designed to have an extraterritorial effect, where it captures operators of AI systems outside the EU. In particular, the EU AI Act would apply to:

- providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are established within the EU or in a third country;
- importers and distributors of AI systems;
- deployers of AI systems that have their place of establishment or are located within the EU;
- providers of AI systems that are located in a third country, where the output produced by the system is used in the EU;
- product manufacturers placing on the market or putting into service an AI system together with their product or under their own name or trademark;
- authorized representatives of providers, which are not established in the EU; and
- affected persons located in the EU.

Notably, the EU AI Act excludes from its scope AI systems used for:

- military, defense, or national security;
- non-professional activities; and
- the sole purpose of scientific research and development.

The EU AI Act also does not apply to AI systems released under free and open-source licenses unless they are placed on the market or put into service as high-risk AI systems.

Existing legislation

Definition of AI

The EU AI Act proposes a technology-neutral definition of 'AI system.' Namely, an AI system is 'a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.' Moreover, the European Commission published guidelines providing further clarification on the definition of an AI system under the EU AI Act.

Risk-based AI systems classification

Under the EU AI Act, systems are classified into three categories, which are based on the level of risk of the application.

Unacceptable risk: AI practices that are prohibited as they contravene EU values. The prohibitions cover AI practices that have a significant potential to manipulate behaviors by subliminal techniques, exploit vulnerable groups (such as children or disabled persons) to distort behaviors, social scoring, and real-time biometric identification. The European Commission published Guidelines on prohibited AI practices under the EU AI Act.

High-risk: AI systems are considered high risk if they pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by materially influencing the outcome of decision-making. These include AI systems used for credit scoring, profiling of natural persons, emotion recognition systems, and post-remote biometric identification systems.

Minimal or low risk: Minimal-risk AI systems would be subject to a limited set of obligations (e.g., transparency), and low-risk AI systems could be developed and used in the EU without additional legal obligations other than those existing in the legislation.

Obligations

The EU AI Act assigns specific obligations and responsibilities to different actors.

- **Provider:** A natural or legal person, public authority, agency, or other body that develops an AI system or a GPAI model or that has an AI system or a GPAI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.
- **Deployer:** Any natural or legal person, public authority, agency, or other body using an AI system under its authority, except where the AI system is used in the course of personal non-professional activity.

Other participants across the AI value chain such as importers, distributors, and authorized representatives are also subject to a narrow set of obligations.

High-risk AI systems

Specifically, providers of high-risk AI systems would be required to:

- have a quality management system in place to ensure compliance with the EU AI Act;

Existing legislation

- draw up technical documentation;
- ensure that the high-risk AI system undergoes relevant conformity assessment procedures, prior to its placing on the market or putting into service;
- when under their control, keep the logs automatically generated by their high-risk AI systems;
- immediately take necessary corrective measures upon determining that the high-risk system placed does not conform to the EU AI Act requirements;
- affix CE marking of conformity in a visible, legible, and indelible manner;
- establish and document a post-marketing monitoring system; and
- notify serious incidents and malfunctions, in certain circumstances, not later than 15 days after the providers become aware of the incident or malfunction.

On the other hand, deployers of high-risk AI systems would be required to:

- use the AI systems in accordance with the instructions of use accompanying them;
- monitor the operation of the AI system, and inform the provider or distributor when they have reason to consider that the use may result in the AI system presenting an unacceptable risk, and suspend use accordingly; and
- keep the logs automatically generated by the high-risk AI system, to the extent such logs are under their control.

Notably, prior to the deployment of a high-risk AI system, deployers providing public services and operators must perform an assessment on how the use of such high-risk AI systems may impact fundamental rights.

General-purpose AI models

The EU AI Act outlines provisions related to GPAIs, including criteria for determining whether an AI model qualifies as a GPAI. This qualification will depend on the AI model's capability, which can be based on the quantitative threshold of the cumulative amount of computing used for training measures in floating-point operations, or on an individual designation decision of the European Commission. GPAI obligations include:

- keeping up to date and making available, on request, technical documentation to the AI Office and national authorities;
- providing certain information and documentation to downstream providers for the purpose of compliance with the EU AI Act; and
- other requirements for models with systemic risks, such as risk assessments and ensuring an adequate level of cybersecurity protection.

Furthermore, the GPAI Code of Practice (the Code), finalized in July 2025 and deemed adequate by the AI Board, serves as a voluntary compliance tool to support providers in meeting their obligations. The Code includes transparency, copyright, and

Existing legislation

safety and security chapters, each outlining specific commitments for signatories.

The Commission has also issued interpretative guidelines for providers of GPAI models, clarifying the definition of GPAI models, the classification of GPAI models with systemic risk, and the exemptions from certain obligations for providers of GPAI models released under a free and open-source license.

Oversight and enforcement

National Competent Authority

Each EU Member State must designate at least one notifying authority and one market surveillance authority as national competent authorities for overseeing the EU AI Act. These entities must operate independently and impartially. National competent authorities may provide guidance on the implementation of the EU AI Act, with specific reference to Small- and Medium-Sized Enterprises (SMEs) and start-ups, but must be consulted before providing guidance on other areas covered by EU law. Member States are also required to nominate a single market surveillance authority to serve as a central point of contact.

The AI Office

The EU AI Act introduces a centralized system of oversight and enforcement for GPAI models, contrasting with the national-level market surveillance system applied to AI systems. This centralization is embodied in the creation of the AI Office, which is tasked with monitoring compliance and enforcing obligations related to GPAI models. The AI Office is responsible for supervising compliance with the requirement to conduct a fundamental rights impact assessment, and more generally, will investigate potential infringements of rules. The AI Office will also support the implementation of the EU AI Act by issuing guidelines, adopting, implementing, and delegating acts, as well as developing tools and methodologies to evaluate the capabilities and reach of GPAI models.

The EU AI Office announced the publication of a Living Repository of AI Literary Practices (the Practices).

The Practices aim to facilitate compliance with the provisions on AI literacy under Article 4 of the EU AI Act, which specifically entered into force on February 2, 2025.

The Practices are non-exhaustive and will be updated on a regular basis. They further clarify that the implementation of the AI training initiatives does not automatically grant a presumption of compliance with Article 4 of the AI Act.

The AI Board

The AI Board, composed of representatives from EU Member States, will advise on the implementation and enforcement of AI regulations, as well as technical standards. It can also establish sub-groups to address specific issues and cooperate with relevant EU bodies. Furthermore, the AI Board is responsible for providing advice on the implementation of the EU AI Act and may issue recommendations and written opinions related to it.

Existing legislation

Penalties

In terms of enforcement, a lack of compliance with the EU AI Act would expose organizations to steep fines that surpass the penalties under the GDPR. Non-compliant companies may face fines ranging from:

- €35 million or 7% of global annual turnover for violations of banned AI applications;
- €15 million or 3% for violations of other obligations; and
- €7.5 million or 1% for supplying incorrect information.

Member State implementing laws

The EU AI Act requires EU Member States to comply with certain requirements, such as notifying national authorities of the implementation and enforcement of the provisions of the law.

To operationalize these requirements, several EU Member States have initiated national legislative processes to implement the EU AI Act. Notably, the following countries have published draft legislation:

- Finland;
- Germany;
- Luxembourg;
- Norway;
- Poland;
- Spain; and
- Slovenia.

While the above-referred draft laws remain in the early stages of the legislative process, they generally include provisions addressing key implementation areas. These typically focus on the designation and roles of national authorities, the enforcement and penalties for non-compliance, and the adoption of specific rules where the EU AI Act grants EU Member States the authority to establish national-level provisions.

Greece: Law on emerging information technology and communication technologies, strengthening digital governance, and other provisions

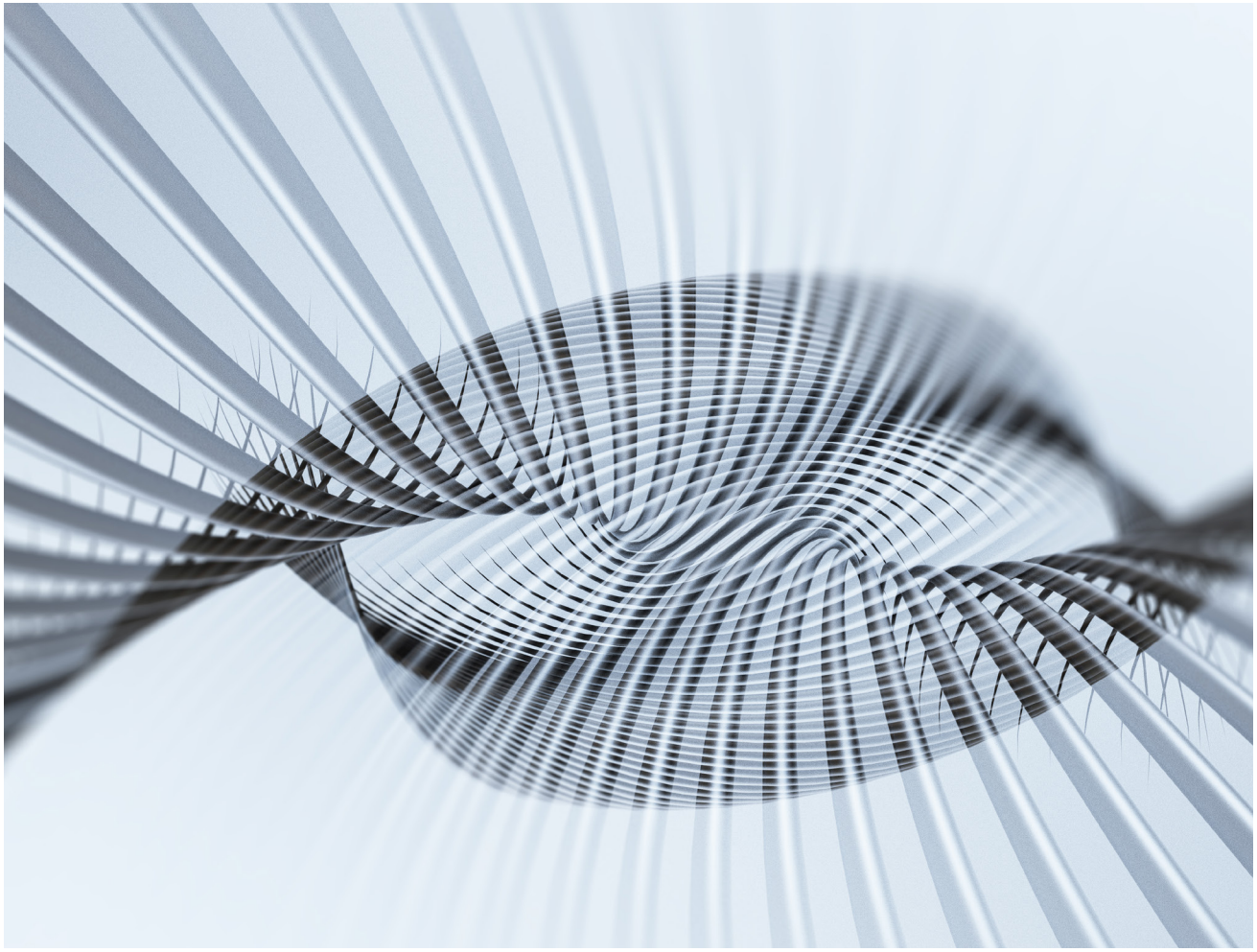
The Law on emerging information technology and communication technologies, strengthening digital governance and other provisions (the Law on emerging technologies) entered into effect on March 3, 2023. Applicable to both public and private sectors, the Law on emerging technologies aims to guarantee the rights of natural persons and legal entities and introduces accountability and transparency requirements for the use of AI systems. It also includes distinct requirements for Internet of Things (IoT) devices.

The Law on emerging technologies establishes requirements for private companies using AI systems in employment-related decision-making. In particular, employers must inform employees or job candidates when the use of such AI systems influences any decision-making process that impacts working conditions. They are also required to provide information on the parameters of the automated

Existing legislation

decision-making process and demonstrate compliance with the principle of equal treatment and non-discrimination in employment.

Additionally, medium and large private sector entities that use an AI system for consumer profiling or in employees' assessments must maintain a register of AI systems that are used. Regarding the oversight of AI, the Law on emerging technologies also establishes a Coordinating Committee for AI, responsible for the application of the National Strategy for the development of AI.



Existing legislation

USA

USA: TAKE IT DOWN Act

The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act) was signed by the U.S. President on May 19, 2025, entering into effect on its signature.

Scope and definitions

The TAKE IT DOWN Act generally prohibits the nonconsensual online publication of intimate visual depictions of individuals. A 'digital forgery' is defined as 'any intimate visual depiction of an identifiable individual created through the use of software, machine learning, AI, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.'

Requirements

Covered platforms must establish, within one year of their enactment, a process where identifiable individuals or an authorized person may:

- notify the covered platform of an intimate visual depiction published on the covered platform that:
  - includes a depiction of the identifiable individual; and
  - was published without consent; and
- submit a request for the covered platform to remove such intimate visual depiction.

In case of a request, covered platforms must remove intimate visual depictions of which they have been notified as soon as possible, but no later than 48 hours after receipt of a request.

In addition, covered platforms must provide a clear and conspicuous notice, provided through a clear and conspicuous link to another webpage or disclosure, of the notice and removal process. The notice must be easy to read and in plain language, and provide information on the responsibilities of the covered platform.

Enforcement

Under the TAKE IT DOWN Act, the failure to reasonably comply with notice and takedown obligations in relation to intimate visual depictions will be treated as a violation of a rule defining an unfair or deceptive act or practice under Section 18(a)(1)(B) of the Federal Trade Commission Act (the FTC Act).

California: AI Transparency Act (Senate Bill 942)

California has also taken legislative steps to address transparency in AI systems. On September 19, 2024, Senate Bill 942 for the AI Transparency Act (the AI Transparency Act) was signed by the Governor of California following its passage by the California legislature on August 29, 2024. The AI Transparency Act will enter into force on January 1, 2026.

Existing legislation

Scope

The AI Transparency Act places transparency requirements on entities that create, code, or otherwise produce a Gen AI system that has over 1,000,000 monthly visitors or users and is publicly accessible within the geographic boundaries of the State.

Any product, service, internet website, or app that provides exclusively non-user-generated video games, television, streaming, movies, or interactive experiences is excluded from the AI Transparency Act scope.

Requirements

The AI Transparency Act provides that a covered provider must offer a free, publicly accessible AI detection tool that enables users to determine whether content (image, video, audio, or combinations thereof) was generated or altered by the provider's Gen AI system. The tool must:

- detect and output system provenance data, excluding personal data that is detected in the content;
- impose reasonable limitations on access to the tool in case of security or integrity risks of its Gen AI system;
- allow content upload or URL submissions; and
- support application programming interface (API) access for integration.

Relating to the above AI detection tool, the AI Transparency Act provides that covered providers are prohibited from:

- collecting or retaining personal information from users, subject to exceptions for feedback and evaluation of the tool;
- retaining submitted content longer than necessary; and
- retaining any personal provenance data from content submitted to the AI detection tool.

In addition, covered providers must offer users the option to include a disclosure in AI-generated image, video, or audio content, or a combination thereof, that:

- identifies content as AI-generated;
- is clear, conspicuous, and appropriate for the medium of the content, and understandable to a reasonable person; and
- is permanent or extraordinarily difficult to remove, where technically feasible.

Furthermore, covered providers must include a latent disclosure that, where feasible and reasonable, conveys directly or through a link to a permanent website:

- the covered provider's name;
- the name and version number of the Gen AI system that created or altered the content;
- the time and date of the content's creation or alteration; and
- a unique identifier.

Third parties licensing the Gen AI system must be contractually obliged to maintain the system's

Existing legislation

capability to include the required disclosure in content that the system creates or alters. If a third party fails to comply, the provider must revoke the license within 96 hours of discovering the violation.

Enforcement

Any violation of the AI Transparency Act by a covered provider results in a civil penalty of $5,000 per violation. Each day that a provider remains non-compliant is considered a separate violation. Legal actions to enforce these penalties may be initiated by the California Attorney General (California AG), a city attorney, or a county counsel.

California: Gen AI: Training Data Transparency Act

While California's AI Transparency Act (Senate Bill 942) focuses on labeling and detection of AI-generated content for end users, the Generative Artificial Intelligence: Training Data Transparency Act (the Act) requires developers to publicly disclose high-level summaries of the datasets used to train Gen AI systems.

On September 28, 2024, the Act was signed into law by the Governor of California and will take effect on January 1, 2026.

Scope and definitions

The Act establishes mandatory transparency requirements for developers, meaning a person, partnership, state, or local government agency, or corporation that designs, codes, produces, or substantially modifies publicly available Gen AI systems or services.

Under the Act, Gen AI means AI that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the AI's training data.

However, the Act clarifies that it does not apply to data used to train a Gen AI system or service:

- whose sole purpose is to help ensure security and integrity;
- whose sole purpose is the operation of aircraft in the national airspace; or
- developed for national security, military, or defense purposes, that is only made available to a federal entity.

Requirements

By January 1, 2026, before each public release or substantial modification of a Gen AI system or service released on or after January 1, 2022, a developer of the system or service must post documentation regarding the data used to train the Gen AI system or service on their website, including a high-level summary covering:

- sources or owners of datasets;
- a description of how datasets further the purpose of the AI system or service;
- whether data is protected by copyright, trademark, or patent;
- whether the datasets were purchased or licensed by the developer;
- whether the datasets include personal

Existing legislation

information and aggregate consumer information;

- whether there was any cleaning, processing, or other modification to the datasets;
- the dates the datasets were first used during the development of the AI system or service; and
- whether the Gen AI system or service is used or continuously uses synthetic data generation.

Enforcement

The California AG is empowered to enforce the Act. Violations may be pursued under California's Unfair Competition Law (UCL), which allows for civil penalties of up to $2,500 per violation, and potentially higher amounts if the violation is deemed willful or affects vulnerable populations.

Colorado: Act Concerning Consumer Protections in Interactions with AI Systems

On May 17, 2024, the Colorado Governor signed Senate Bill 24-205 for an Act concerning consumer protections in interactions with artificial intelligence systems (the Colorado AI Act) into law. Set to take effect on February 1, 2026, the Colorado AI Act became the first comprehensive AI law to be enacted by a US state. The Colorado AI Act imposes obligations on developers and deployers of high-risk AI systems, specifically regarding the prevention of algorithmic discrimination and consumer transparency.

On April 28, 2025, Senate Bill 318 for an act concerning consumer protection in interaction with AI systems was introduced to amend the Colorado AI Act; however, in May 2025, a Senate committee voted to postpone the bill indefinitely. Among other things, the referred bill proposed amendments to the definitions of algorithmic discrimination and developer. Additionally, the bill removed certain obligations of developers and deployers, such as the duty of care and notification requirements to the Colorado Attorney General (Colorado AG) in relation to risks.

Scope

The Colorado AI Act applies to developers or deployers of high-risk AI systems who do business in Colorado. A 'developer' is a person doing business in Colorado who develops or intentionally substantially modifies an AI system.

Definition of AI

'AI system' is defined as a machine-based system that infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

A 'high-risk AI system' means an AI system that, when deployed, makes or is a substantial factor in making a consequential decision. However, this does not include AI systems intended to:

- perform a narrow procedural task;
- detect decision-making patterns without replacing or influencing human assessments without adequate review;

Existing legislation

- technologies that do not make consequential decisions, such as anti-fraud tools (without facial recognition), anti-virus, cybersecurity, calculators, databases, and similar systems; or
- natural language communication tools that provide information or recommendations, subject to policies preventing harmful or discriminatory content.

Obligations

The Colorado AI Act requires developers or deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination within the high-risk system. Further, companies and developers offering AI systems for consumer interaction must disclose to consumers when they are interacting with an AI system, unless it is clear to a reasonable person that AI is being used.

Developers of AI models are also required to maintain comprehensive documentation, including policies that comply with copyright laws and a detailed summary of the content used to train AI models. Developers must also provide documentation to deployers outlining the AI system's intended uses, limitations, and potential risks of harm or inappropriate uses. Additionally, developers are obligated to document how AI systems are evaluated for performance and risk mitigation before they are made available to deployers.

Deployers, in turn, must be informed about the data governance measures used for AI training datasets, AI systems' intended outputs, measures to mitigate algorithmic discrimination risks, and how AI systems should be used and monitored when making consequential decisions.

Oversight and enforcement

The Colorado AG has exclusive authority to enforce the Colorado AI Act and is empowered to issue additional rules as necessary. These rules may address developer documentation requirements, content for notices and disclosures, standards for risk management policies, and impact assessments. A violation of the requirements of the Colorado AI Act constitutes an unfair trade practice under the Colorado Revised Statutes.

New York: Local Law in relation to automated employment decisions

Enforcement of the Local Law in relation to automated employment decision tools (the Automated Employment Decision Law) took effect on January 1, 2023, and applies only to employers and employment agencies that use Automated Employment Decision Tools (AEDTs) in New York City (NYC). An AEDT is defined as a tool that uses machine learning (ML), statistical modeling, data analytics, or AI to help employers and employment agencies make employment decisions and substantially assists or replaces discretionary decision-making. AEDTs do not include junk email filters, firewalls, anti-virus software, calculators, spreadsheets, databases, data sets, or other compilations of data. Provisions of the Automated Employment Decision Law are clarified by the Finalized Rules implementing the NYC Department of Consumer and Worker Protection Local Law on automated employment decision tools (the Finalized Rules).

Existing legislation

Requirements

The Automated Employment Decision Law establishes that employers and employment agencies must notify candidates who are NYC residents at least 10 business days prior to using an AEDT for an assessment or evaluation for hire or promotion. Such an obligation to notify candidates represents one of the very few elements that overlap with other AI-focused initiatives, including the EU AI Act and other international frameworks that similarly provide for user transparency requirements. Employers are also required to inform employees and job candidates about the qualifications and characteristics that will be used by the AEDT and allow job candidates to request an alternative selection process or accommodation.

Further, like other AI initiatives, the Automated Employment Decision Law includes requirements for bias monitoring and detection, with the specifics including aims and methods for conducting bias audits outlined in the Finalized Rules. A summary of the results of the most recent bias audit, including the distribution date of the tool, must be published on the website of the employer or employment agency. Notably, candidates and employees have the right to request information about the type and source of data collected for the AEDT, and the employer or employment agency's data retention policy if such information is not disclosed on the employer or employment agency's website.

Enforcement

The Automated Employment Decision Law does not limit the right of any candidate or employee to bring a civil action in court. Civil penalties for violations of the Automated Employment Decision Law range from $500 for a first violation and for any additional violations occurring on the same day, and from $500 to $1,500 for each subsequent violation.

Texas: Responsible AI Governance Act

On June 22, 2025, the Texas State Governor signed House Bill 149, known as the Texas Responsible Artificial Intelligence Governance Act (the Texas AI Governance Act). The Texas AI Governance Act will take effect on January 1, 2026, and introduces obligations for developers and deployers of AI systems, particularly in relation to consumer transparency, biometric data protection, and the prevention of harmful or discriminatory uses of AI.

Scope

The Texas AI Governance Act applies to any person who promotes, advertises, or conducts business in Texas, produces products or services used by Texas residents, or develops or deploys AI systems within Texas. The Texas AI Governance Act extends protection to consumers, meaning residents acting in an individual or household context. Importantly, the majority of the obligations apply to 'governmental agencies.'

Definitions

Under the Texas AI Governance Act, an AI system is a machine-based system that infers from inputs on how to generate outputs, such as content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

Existing legislation

A 'developer' is a person who develops an AI system that is offered, sold, leased, given, or otherwise provided in Texas.

A 'deployer' is a person who deploys an AI system for use in Texas.

Obligations

Notably, the majority of the obligations under the Texas AI Governance Act are assigned to governmental agencies, including requirements to disclose to consumers when they are interacting with an AI system. Moreover, governmental agencies are specifically prohibited from using AI systems for social scoring, biometric identification, or gathering media from publicly available sources without the individual's consent.

Prohibited practices

The Texas Responsible AI Act prohibits the development and deployment of AI systems that, among other prohibited practices:

- manipulate human behavior by inciting self-harm, violence, or criminal activity;
- infringe, restrict, or otherwise impair an individual's constitutional rights;
- unlawfully discriminate against a protected class, including race, sex, religion, and disability; and
- produce or distribute child pornography or sexually explicit content involving minors.

Oversight and enforcement

The Texas Attorney General (Texas AG) has exclusive authority to enforce the Texas AI Governance Act. Consumers may submit complaints through an online portal. Upon receiving a complaint, the Texas AG may issue a civil investigative demand requesting documentation about the AI system's purpose, data, outputs, performance metrics, limitations, and safeguards.

If a violation is found, the Texas AG must allow the violator 60 days to cure the issue. No action can be brought against an AI system that has not been deployed. The Texas Responsible AI Act also reserves enforcement by state agencies.

Civil penalties range from $10,000 to $200,000 per violation, with additional daily penalties for continued violations. Entities may defend themselves by demonstrating reasonable care, third-party misuse, or compliance with recognized AI risk management frameworks.

Regulatory sandbox program and Texas AI Council

The Texas AI Governance Act establishes a regulatory sandbox program, allowing approved participants to test AI systems for up to 36 months without full regulatory compliance.

Moreover, the Texas Artificial Intelligence Council (Texas AI Council) is created and tasked with advising the legislature and state agencies, monitoring ethical and legal AI use, recommending reforms, and overseeing the sandbox program.

Existing legislation

Utah: AI Transparency Act

Senate Bill 226 on AI Consumer Protection Amendments (Utah AI Transparency Act) entered into force on May 7, 2025, and amends Utah's AI regulatory framework to strengthen consumer protections in interactions involving Gen AI. It introduces mandatory disclosures, liability rules, and enforcement mechanisms, particularly for high-risk AI interactions and regulated occupations.

Scope and definitions

The Utah AI Transparency Act applies to suppliers using Gen AI in consumer transactions with Utah residents and individuals in regulated occupations, meaning occupations requiring a license or state certification to practice, such as law, medicine, or finance, where Gen AI is used to deliver services.

Specifically, the Utah AI Transparency Act sets out disclosure obligations for high-risk AI interactions, which are considered an interaction with Gen AI that involves:

- the collection of sensitive personal information, such as health, financial, or biometric data;
- the provision of personalized recommendations, advice, or information that could reasonably be relied upon to make significant personal decisions;
- the provision of advice or services relating to the type of sensitive personal information, such as legal advice or services; or
- other applications as defined by the Utah Division of Consumer Protection.

Requirements

Suppliers that use Gen AI in consumer transactions must clearly and conspicuously disclose to the individual that they are interacting with Gen AI rather than a human, but only if the individual explicitly asks whether AI is being used. This disclosure requirement is triggered only when the consumer's prompt is clear and unambiguous.

In regulated occupations, Gen AI use must be disclosed proactively at the start of the interaction if it qualifies as high-risk. For verbal interactions, the disclosure must be spoken at the beginning; for written interactions, the disclosure must be provided in writing before the interaction begins.

Businesses are exempt from disclosure requirements if the Gen AI system clearly and conspicuously discloses its nature at the outset and throughout the interaction.

Enforcement

The Division of Consumer Protection oversees the enforcement of the Utah AI Transparency Act. The Division Director may impose fines up to $2,500 per violation and initiate court actions. Courts may issue injunctions, order restitution, and impose civil penalties of up to $2,500 per violation.

Existing legislation

Asia Pacific

China: Interim Measures for the Management of Generative AI Services

The Interim Measures for the Management of Generative AI Services (the Gen AI Services Management Measures) entered into force on August 15, 2023, outlining principles and obligations for Gen AI service providers and users.

Scope and definitions

The Gen AI Services Management Measures apply to Generative AI Service Providers (GAISPs) that use Gen AI technology to provide services for generating text, pictures, audio, video, and other content to the public within China.

Generative AI technology refers to models and related technology that have the ability to generate content such as text, pictures, audio, and video.

However, the Gen AI Services Management Measures do not apply to industry organizations, enterprises, educational and scientific research institutions, public cultural institutions, and relevant professional institutions that develop and apply Gen AI technology but do not provide Gen AI services to the domestic public.

Principles for the provision and use of Gen AI

Notably, the Gen AI Services Management Measures outline principles for the provision and use of Gen AI, including:

- taking measures to prevent discrimination based on ethnicity, belief, country, region, gender, age, occupation, and health in the process of algorithm design, training data selection, model generation and optimization, and service provision;
- respecting intellectual property rights, business ethics, keeping business secrets, and not using algorithms, data, platforms, and other advantages to implement a monopoly and unfair competition;
- respecting the legitimate rights and interests of others, not endangering the physical and mental health of others, and not infringing on the privacy rights and personal information of others; and
- based on the service type, take effective measures to improve the transparency of Gen AI services and improve the accuracy and reliability of generated content.

Obligations

Under the Gen AI Services Management Measures, GAISPs are required to:

- use data and basic models with legitimate sources;
- not infringe on the IP rights of others;
- obtain the consent of individuals when using personal information, or comply with other administrative regulations in accordance with the law;
- take effective measures to improve the quality of training data, and enhance the authenticity, accuracy, objectivity, and diversity of training data;

Existing legislation

- establish protection mechanisms for users' input information;
- only collect essential personal information; and
- not illegally retain input information and use records that can identify users.

Moreover, GAISPs must assume responsibility as network information content producers, and where personal information is involved, assume the responsibility of a personal information processor.

The Gen AI Services Management Measures also require GAISPs to establish vendor management requirements and protection for minors, including clarifying and disclosing specific information applicable to the population, circumstances, and use of their Gen AI technology more generally. Regarding users, the Gen AI Services Management Measures outline specific rights in connection to the exercising of user requests, including reviewing, copying, correcting, supplementing, and deleting their personal information. In addition, GAISPs must establish and maintain a complaint and report mechanism. Mainly, where a GAISP discovers that users engage in illegal activities through the service, they must warn, restrict, suspend, or terminate the provision of the service.

GAISPs are also required to mark pictures, videos, and other generated content in accordance with the Regulations on Administration of Deep Synthesis of Internet Information Services (the Deep Synthesis Regulations).

China: Regulations on the Administration of Deep Synthesis of Internet Information

The Deep Synthesis Regulations entered into effect on January 10, 2023. The Deep Synthesis Regulations define 'deep synthesis technology' as technology that uses deep learning, virtual reality, and other synthetic algorithms to produce text, images, audio, video, virtual scenes, and other network information. This includes technologies capable of generating or editing text content as well as generating or editing biometric features in images and video content, such as face generation, face replacement, or gesture manipulation.

The Deep Synthesis Regulations establish requirements for deep synthesis service providers, including the establishment of management systems for user registration, algorithm mechanism review, and data security and personal information protection review. Such providers must also implement and disclose management rules, including a real identity information authentication system.

In connection with personal information protection, the Deep Synthesis Regulations also stipulate that where personal information is used for algorithm training and the functions allow the editing of biometric information, data subjects must be notified, and their separate consent must be obtained. Additionally, before launching new products, applications, or functions with public opinion attributes or social mobilization capabilities, providers are required to conduct a security assessment.

Existing legislation

China: Measures for Identifying Synthetic Content Generated by AI

On March 14, 2025, the Cyberspace Administration of China (CAC) announced that it had released Measures for the Identification of Synthetic Content Generated by Artificial Intelligence (the Synthetic Content Identification Measures).

Moreover, the State Administration for Market Regulation and the National Standards Administration formally approved the national standard entitled 'Method for Identifying Synthetic Content Generated by Artificial Intelligence in Cybersecurity Technology' (the National Standard) that provides a standardized approach to the identification activities of AI-generated synthetic content by generation as well as synthesis service providers and content dissemination service providers.

On the same day, the National Information Security Standardization Technical Committee (TC260) also released a national security standard entitled 'Cybersecurity Standard Practice Guidelines - Coding Rules for Service Providers of Artificial Intelligence Generated Synthetic Content Identification' (the Cybersecurity Guidelines).

The Synthetic Content Identification Measures and the accompanying national standard will become effective on September 1, 2025.

Scope

The Synthetic Content Identification Measures and the national standard are mandatory and apply to service providers that generate content, disseminate content, and provide platforms or tools for users to create or share AI-generated content. The Synthetic Content Identification Measures also outline specific requirements for internet application distribution platforms.

Furthermore, the requirements apply to synthetic content generated by AI, including text, pictures, audio, video, virtual scenes, and other information generated and synthesized using AI technology.

The Synthetic Content Identification Measures provide for two forms of content labelling, explicit and implicit content labelling:

- explicit identification: Identification added in the generation of synthetic content or interactive scene interfaces, presented in the form of text, sound, or graphics, and which can be clearly perceived by users; and
- implicit identification: Identification added in the generation of the synthetic content file data by taking technical measures, not easily perceived by users.

Requirements

Service providers must use both explicit and implicit identification forms and ensure that such identifiers are retained at download. Metadata and user declarations must be verified before publishing, and generated/synthetic content must be labeled as such based on the metadata or user declaration. The service provider may provide content without explicit identifiers only if the user agrees to the responsibilities through a user agreement, and the logs are retained for at least six months.

Existing legislation

Internet application distribution platforms must require app providers to disclose whether their applications offer AI-generated synthesis services and verify that such applications comply with identification requirements.

Users must proactively declare and use identification tools when publishing synthetic content.

The Synthetic Content Identification Measures also prohibit organizations or individuals from maliciously deleting, tampering with, forging, or concealing the generated synthetic content identification.

According to the National Standard, explicit labels must be clearly visible or audible to users and include the terms 'AI' or 'Artificial Intelligence' and 'Generated' and/or 'Synthetic.' On the other hand, implicit identification is done by embedding in the file's metadata or by a digital watermark.

The Cybersecurity Guidelines provide the coding structure and coding rules for AI-generated synthetic content service providers and network information content dissemination service providers that carry out the implicit identification of file metadata for AI-generated synthetic content.

Enforcement

The violations of the provisions of the Synthetic Content Identification Measures will be handled by the relevant competent departments

China: Internet Information Service Algorithm Recommendation Management Regulations

The Internet Information Service Algorithm Recommendation Management Regulations (the Algorithm Regulations) entered into effect on March 1, 2022, and represent further legislation targeted at AI in China. The Algorithm Regulations apply to algorithm technologies, including those that generate personalized push notifications, sorting and selection, retrieval and filtering, and scheduling and decision-making to provide users with information. Generally, the Algorithm Regulations can be understood as a detailed implementation of the requirements of Article 24 of the PIPL regarding automated decision-making. In detail, the Algorithm Regulations require Algorithm Recommendation Service Providers to, among other obligations:

- strengthen information security and data protection;
- improve storage standards for personal information; and
- establish mechanisms to receive and process user complaints.

Similar to both the Synthetic Content Identification Measures and Deep Synthesis Regulations in China, the Algorithm Regulations provide for the protection of user rights. These include, among other obligations, offering users options that are not specific to their personal characteristics, allowing them to turn off algorithm recommendation services, and providing explanations on how such services may have a significant impact on their rights and interests.

.

Existing legislation

Japan: Act on Promotion of Research, Development, and Utilization of AI-Related Technology

The Act on Promotion of Research, Development, and Utilization of Artificial Intelligence-Related Technology (the Japan AI Act) was passed by the Japanese Parliament on May 28, 2025. The Japan AI Act came into force on June 4, 2025 (except for Chapters 3 and 4, and Articles 3 and 4 of Supplementary Provisions, which will become effective on a date as determined by a Cabinet Order). The timeline for determining such a date is within three months from the promulgation date of the Japan AI Act.

Notably, the Japan AI Act differs from the prescriptive approach adopted by the EU AI Act. Instead, it relies on basic principles, cooperation mechanisms, and the application of existing laws such as the Basic Act on Science, Technology and Innovation (the Basic Act on Science) and the Basic Act on the Formation of a Digital Society (the Basic Act on Digital Society) for the regulation of AI.

Scope

The Japan AI Act outlines responsibilities for:

- the State;
- local governments;
- research and development institutions;
- utilizing businesses; and
- general public.

Definitions

'Artificial intelligence related technology' is defined as 'technology necessary to realize functions that artificially substitute for human intellectual abilities related to cognition, reasoning, and judgment, as well as technology related to information processing systems that realize functions that use such technology to process input information and output the results.'

The Japan AI Act does not differentiate between developer and deployer and encapsulates both terms in its definition for 'utilizing business,' which is defined as 'any person who intends to develop or provide products or services that utilize AI-related technologies, or any other person who intends to utilize AI-related technologies in their business activities.'

Basic principles

The Japan AI Act states that the promotion of research, development, and utilization of AI-related technologies must be based on the basic principles as provided below, in addition to the requirements under the Basic Act on Science and the Basic Act on Digital Society.

The basic principles are categorized as follows.

- International competitiveness: conducting research and development in AI-related technologies to improve the international competitiveness of industries.
- Collaboration: ensuring close interrelationship between the efforts of stakeholders at each

Existing legislation

stage, from basic research into AI to their utilization in people's lives and economic activities.

- Transparency: taking measures to ensure that AI is not utilized for improper purposes or in an inappropriate manner, including criminal use, personal information breach, or copyright infringement
- International cooperation: promoting the development, research, and utilization of AI under international cooperation.

Obligations

The State is required to establish the Basic Plan for Artificial Intelligence (the Basic Plan) in accordance with the basic principles and taking into account the basic measures set out in the Japan AI Act. The Basic Plan will set out concrete measures to promote the research, development, and use of AI.

In accordance with the basic principles, utilizing businesses are required to endeavor the improvement, efficiency, and sophistication of their business activities and to create new industries through the active use of AI-related technologies. They must also cooperate with the measures implemented by the State and local government in accordance with the Japan AI Act.

Oversight and enforcement

Uniquely, the Japan AI Act does not contemplate monetary or other forms of penalties for non-compliance. Instead, it focuses on mutual cooperation between the State and other actors. The State is empowered to take necessary measures to strengthen cooperation among the State, local governments, research and development institutions, and utilizing businesses. Additionally, the State will establish guidelines for implementation in accordance with international norms.

Furthermore, the Cabinet will establish the Artificial Intelligence Strategy Headquarters, which will be responsible for drafting and implementing the Basic Plan and matters related to the planning, drafting, and overall coordination of important measures to promote research, development, and utilization of AI.

South Korea: Basic AI Act

The Basic Act on the Development of Artificial Intelligence and Establishment of Trust (the Basic AI Act) was signed into law on January 21, 2025, and will enter into force on January 22, 2026. As the second comprehensive regulatory framework for AI after the EU AI Act, this legislation represents a significant milestone in global AI governance.

On June 17, 2025, Bill 2210903 amending the Basic AI Act was introduced to the South Korean National Assembly Science, Technology, Information, Broadcasting, and Communications Committee. This bill includes provisions requiring Gen AI business operators to implement procedures that allow copyright holders to confirm whether their work has been used as training data.

Scope

The scope of the Basic AI Act is broad, as it applies to acts inside and outside South Korea if they impact the South Korean market and users.

Existing legislation

The Basic AI Act applies to a wide range of AI technologies, including AI systems, high-impact AI, Gen AI, and large-scale AI exceeding computational power thresholds as set by presidential decree. However, it does not apply to AI developed and used solely for national defense or national security purposes.

Definitions

The Basic AI Act defines AI as the electronic replication of human intellectual functions, including learning, reasoning, perception, judgment, and language comprehension. An AI system refers to any AI-based system with a varying degree of autonomy that produces outputs, such as predictions, recommendations, or decisions, that influence real or virtual environments.

Moreover, the Basic AI Act distinguishes between GPAI models and high-impact AI systems. GPAI refers to models producing outputs like text, sound, images, and video by mimicking the structure and characteristics of input data. On the other hand, high-impact AI systems are those that could significantly affect human life, safety, or fundamental rights, and are used in critical sectors. These classifications are important because they determine the level of regulatory obligations imposed on each type of AI.

Under the Basic AI Act, an AI Business Operator is defined as any corporation, organization, individual, or government agency engaged in AI-related commercial activities. This includes AI developers and AI-using business operators that offer AI products or services developed by others.

Requirements

AI Business Operators must ensure transparency by notifying users in advance when interacting with AI-based or Gen AI products, especially when the output may be mistaken for authentic media. Foreign AI business operators meeting certain thresholds must designate a domestic representative in South Korea to liaise with the government.

AI Business Operators of AI systems with computational resources exceeding thresholds defined by a future Presidential Decree must identify, assess, and mitigate risks throughout the AI lifecycle and build systems to monitor and respond to safety incidents.

AI Business Operators must carry out reviews to determine whether their AI qualifies as high-impact AI, in which case they must fulfil additional requirements. Where technically feasible, such business operators must explain the key criteria used to generate outputs and provide an overview of the learning data. Business operators must also establish and operate risk management plans and user protection measures, and before deploying high-impact AI, operators must assess its potential impact on basic human rights. Human supervision over high-impact AI systems must also be ensured.

Moreover, high-impact AI Business Operators must prepare and store documentation demonstrating safety and reliability measures.

Existing legislation

Enforcement

The Minister of Science and ICT is the central authority responsible for supervising compliance with the Basic AI Act. This includes conducting fact-finding investigations, on-site inspections, issuing corrective orders, and imposing penalties when violations occur. Both criminal and administrative penalties support enforcement:

- criminal penalties: up to three years of imprisonment or a fine of up to KRW 30 million (approx. $21,560) for unauthorized disclosure of confidential information by committee members; and
- administrative fines: up to KRW 30 million (approx. $21,560) for:
  - failure to notify users that a product or service is AI-based;
  - failure to designate a domestic representative for foreign AI operators; and
  - failure to comply with a cease or corrective order.

Vietnam: Law on Digital Technology Industry

The Law on Digital Technology Industry, 2025 (the Law on Digital Technology) was passed by the National Assembly of Vietnam on June 14, 2025. While the majority of the AI provisions are set to become operative on January 1, 2026, provisions in relation to financial and investment incentives, some of which include sections on AI, will take effect from July 1, 2025.

The Law on Digital Technology regulates the development of not only AI, but also digital technology industries, the semiconductor industry, and digital assets. While Chapter IV of the Law on Digital Technology specifically focuses on AI, references to AI are also contemplated in other chapters. Similar to the EU AI Act, the Law on Digital Technology takes a risk-based approach to AI classification.

Scope

The Law on Digital Technology applies to domestic and foreign agencies, organizations, and individuals participating in or related to the digital technology industry in Vietnam.

An exception to the scope is created for digital technology industry activities serving national defense and security purposes, or cryptographic activities to protect state secret information.

Definition of AI

The Law on Digital Technology defines an AI system as a machine-based system designed to operate with varying degrees of autonomy and adaptability after deployment to achieve explicit or implicit goals, reasoning from the input data it receives to generate predictions, content, recommendations, and decisions that can affect the physical or electronic environment. It is further clarified that an AI system is a digital technology product that integrates hardware, software, and data.

A high-risk AI system is classified as a system that, in certain use cases, is likely to cause risks and serious harm to human health, human rights, civil rights, legitimate rights and interests of organizations, individuals, public interests, and social order and safety, except in one of the following cases:

Existing legislation

- to perform one or several specific tasks, with impact within a narrow scope;
- to support people in optimizing work results; and
- to perform error checking of previously completed human work and not to replace human decisions.

Further, high-impact AI systems are multi-purpose AI systems with a large number of users, parameters, and data.

Principles

The principles guiding the development and deployment of AI systems adhere to international standards and include requirements for transparency, a human-centric approach, data protection, security, and risk management throughout the AI lifecycle.

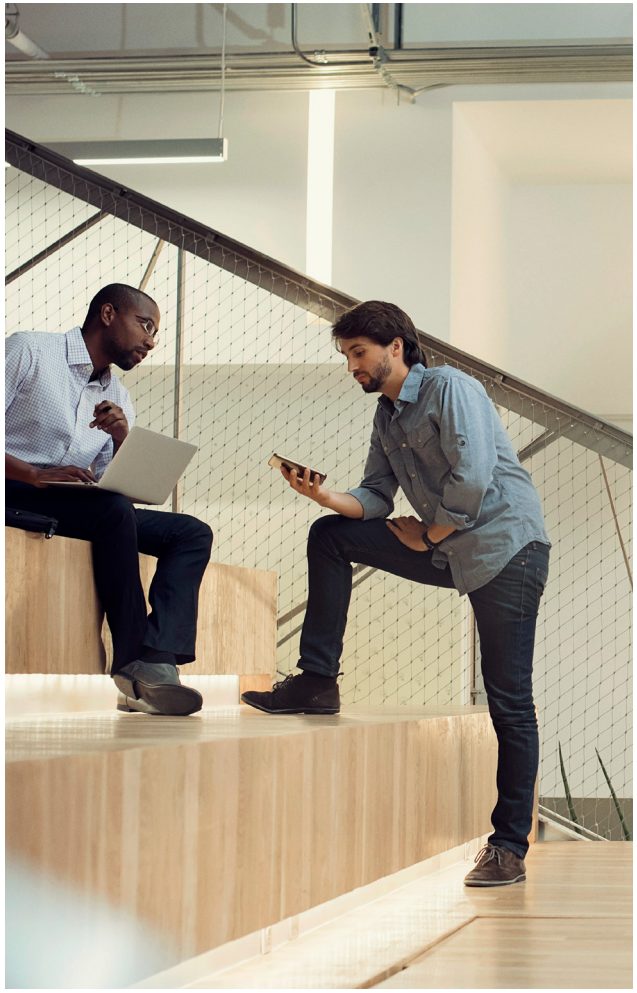
Obligations

The Law on Digital Technology outlines certain broad requirements for high-risk and high-impact AI systems; however, the Government will publish specific rules for their implementation.

Importantly, and similar to the EU AI Act, the Law on Digital Technology has labelling requirements for AI products. Additionally, transparency notices should be made available to users when interacting with AI.

Prohibitions

The Law on Digital Technology prohibits using, providing, and/or deploying AI systems to infringe national interests, ethnicity, national defense, national security, social order and safety, public interests, human rights, civil rights, legitimate rights and interests of organizations and individuals, as well as to destroy good customs and traditions.



Draft legislation

This section covers some of the legislative proposals that are currently under consideration, awaiting approval, or in the process of being finalized. While not yet enforceable, these drafts provide valuable insight into the direction of future regulatory efforts and the evolving priorities of lawmakers. The selected proposals span multiple jurisdictions and reflect a growing emphasis on transparency, accountability, and safeguards. Many of these drafts build upon existing privacy and consumer protection laws, while others introduce entirely new governance structures tailored to AI.

EU

EU: Directive on AI and algorithmic management in the workplace

The Directive on algorithmic management in the workplace (the Directive on algorithmic management) was proposed by the European Parliament Committee on Employment and Social Affairs to the European Commission in June 2025.

Scope

The Directive on algorithmic management was drafted explicitly in recognition of other EU legislation, such as the EU AI Act and the GDPR. The Directive on algorithmic management provides that the EU AI Act, though classifying AI tools based on their risk, does not apply to algorithmic management systems that are not AI-based, leaving a regulatory gap. Likewise, it notes that the GDPR leaves provisions related to employment open to interpretation and reasons that the GDPR only applies to fully automated decision-making processes.

Requirements and prohibited practices

Accordingly, the Directive on algorithmic management outlines its application to employers and the self-employed. For example, employers must provide information in writing to their employees about the use of algorithmic management in the workplace. The information must be provided on the first working day, prior to any significant changes to working conditions or performance monitoring, and upon request. Moreover, employees must have the right to request a human review of significant decisions made or supported by algorithmic systems.

Prohibited practices are also set out in the Directive on algorithmic management, including employers' processing of personal data concerning:

- the emotional or psychological state of workers or solo self-employed persons;
- neuro-surveillance;
- private conversations;
- the behavior of workers or solo self-employed persons while off-duty or in private rooms;
- the prediction of the exercise of fundamental rights; and
- inferences of the racial or ethnic origin, migration status, political opinions, religious or philosophical beliefs, disability, state of health, trade union membership, or sexual orientation.

Draft legislation

Enforcement

The Directive calls for proportionate and dissuasive penalties for non-compliance, though specific amounts are left to national implementation.

UK: AI (Regulation) Bill

On March 4, 2025, the Artificial Intelligence (Regulation) Bill (the UK Bill) was introduced to the UK Parliament and thereafter passed the first reading in the House of Lords on the same day. At the time of writing, the UK Bill is awaiting its second reading in the House of Lords.

Scope

The UK Bill aims to establish an AI Authority responsible for overseeing AI regulation and promoting consistency across relevant regulators. It also sets out requirements for businesses that develop or deploy AI systems.

Definition of AI

The UK Bill defines 'AI' as technology enabling the programming or training of a device or software to:

- perceive environments through the use of data;
- interpret data using automated processing designed to approximate cognitive abilities; and
- make recommendations, predictions, or decisions with a view to achieving a specific objective.

Under the UK Bill, AI also includes Gen AI, which is defined as deep or LLMs that are able to generate text and other content based on the data on which they were trained.

AI Authority

In particular, the UK Bill establishes an AI Authority tasked with ensuring that relevant regulators consider AI in their work, aligning regulatory approaches, identifying gaps in AI oversight, reviewing legislation related to product safety, privacy, and consumer protection, as well as promoting public education and awareness. The AI Authority must operate in line with principles of safety, transparency, fairness, accountability, and the ability to contest and seek redress.

Requirements

Under the UK Bill, businesses utilizing AI are required to be transparent about their use, test AI systems, and comply with applicable laws, including those on data protection, privacy, and intellectual property.

AI and its applications must also comply with equality laws. They should be inclusive by design, avoid discrimination, and meet the needs of those from lower socio-economic groups, older people, and disabled people. Furthermore, AI-generated data should be findable, accessible, interoperable, and reusable.

Additionally, the UK AI Bill requires that any restrictions or burdens imposed on a person or on activities carried out in respect of AI should be proportionate to the expected benefits. This includes considering the nature of the service or product

Draft legislation

being delivered, the risk to consumers and others, the cost of implementation in proportion to that level of risk, and whether the burden or restriction enhances UK international competitiveness.

Notably, the UK Bill provides that the Secretary of State must mandate that any business that develops, deploys, or uses AI should have a designated AI officer. The AI officer is responsible for ensuring that AI is used safely, ethically, and without bias or discrimination.

Further, the UK Bill mandates the Secretary of State to, by regulations:

- require any person involved in training AI to supply to the AI Authority a record of all third-party data and intellectual property (IP) used in that training and assure the AI Authority that they use all such data and IP by informed consent, and they comply with all applicable IP and copyright obligations;
- require any person supplying a product or service involving AI to give customers clear and unambiguous health warnings, labelling, and opportunities to give or withhold informed consent in advance; and
- require any business which develops, deploys, or uses AI to allow independent third parties accredited by the AI Authority to audit its processes and systems.

Enforcement

The UK Bill provides that regulations under the bill may create offenses and require payment of fees, penalties, and fines.

Draft legislation

USA

California: Automated Decisions Systems Safety Act

As California continues to expand its regulatory framework for AI, Senate Bill 1018, known as the Automated Decision Systems Safety Act, introduces new safety and accountability standards for developers and deployers of ADS, focusing on transparency, risk mitigation, and user rights.

On July 17, 2025, Senate Bill 1018 was read for the second time and amended in the California Senate Appropriations Committee. Senate Bill 1018 passed its third reading in the Assembly and was subsequently read for the first time in the California State Senate on June 3, 2025.

Scope and definitions

Senate Bill 1018 applies to an ADS defined as a computational process derived from machine learning, statistical modeling, data analytics, or AI, that issues simplified output, including a score, classification, or recommendation, that is designed or used to assist or replace human discretionary decision-making and materially impacts natural persons.

However, Senate Bill 1018 clarifies that ADS excludes spam email filters, firewalls, antivirus software, identity and access management tools, calculators, databases, datasets, or other data compilations. Additionally, Senate Bill 1018 excludes from its scope the ADS used:

- to detect, protect against, or respond to cybersecurity incidents or preserve the integrity or security of computer systems;
- to operate aircraft in the national airspace; or
- for a consumer credit score to inform a consequential decision that does not create an obligation under Senate Bill 1018.

Requirements

Developers

Developers of ADS must conduct annual performance evaluations to ensure system reliability and safety. For ADS deployed or made available before January 1, 2026, the first evaluation must be completed by January 1, 2027. For ADS deployed on or after January 1, 2026, an evaluation is required prior to initial deployment or availability, followed by annual reviews thereafter.

Each performance evaluation must include information on the purpose and approved uses of the ADS, as well as details on:

- its expected accuracy and reliability;
- the effects of fine-tuning it;
- analyses of disparate treatment and impact, including the necessity of the system and the availability of alternatives; and
- any mitigation measures for unanticipated

Draft legislation

impacts and reports from deployers on their response to such impacts.

Developers of ADS are further required to:

- designate at least one employee to oversee compliance; and
- maintain unredacted documentation of ADS performance evaluations, documentation provided to deployers and auditors, for the duration of the ADS deployment plus 10 years.

Deployers

Before finalizing a consequential decision made or assisted by a covered ADS, deployers must provide the affected individual with a clear, written disclosure that includes:

- a notice that an ADS is being used;
- the ADS's name, version, and developer;
- whether the use aligns with developer-approved purposes;
- a description of the personal data and characteristics assessed;
- the ADS's output format;
- how it influences the decision;
- whether a human will review the ADS's output or the final decision;
- information about their rights and how to exercise them; and
- the contact details for the deployer, the ADS manager, and the entity interpreting the results.

Notably, Senate Bill 1018 provides that deployers must give individuals an opportunity to opt out of the use of an ADS in consequential decisions. However, opt-out requests may be denied where the deployer is subject to the federal Gramm-Leach-Bliley Act (GLBA) and is using the ADS under specified financial services provisions, or where the individual is experiencing a medical emergency. In such cases, the deployer must provide an explanation for the denial.

Senate Bill 1018 also specifies that deployers must provide individuals subject to consequential decisions with a right to appeal and to request the correction of personal data, and the correction of the consequential decision if this is dependent on the correction of personal information. The individual must be notified of the denial of the correction request.

Enforcement

Several public entities, including the California AG, district attorney, and Civil Rights Department, may bring a civil action against a developer, deployer, or auditor who violates Senate Bill 1018, resulting in a civil penalty of up to $25,000 per violation.

Draft legislation

California: Bill on high-risk AI systems and duty to protect personal information

On April 22, 2025, Senate Bill 468 on high-risk artificial intelligence systems: duty to protect personal information, was referred to the California State Committee on Appropriations following its introduction on February 19, 2025, in the Senate.

Scope and definitions

Senate Bill 468 establishes mandatory data protection responsibilities for businesses that deploy a high-risk AI system that processes personal information in California.

Requirements

Senate Bill 468 imposes a duty on covered deployers to develop, implement, and maintain a comprehensive information security program that contains appropriate administrative, technical, and physical safeguards and that is tailored to their business size, resources, data volume, and the sensitivity of personal information they handle.

The information security programs must include, among other things:

- safeguards for the protection of personal information aligned with applicable state and federal data protection laws;
- designated employees responsible for maintaining the program;
- risk assessments of internal and external risks to the security, confidentiality, and integrity of personal information;
- processes for improving the effectiveness of safeguards, including employee training, and detection and prevention of system failures;
- security policies handling personal information outside of business premises;
- disciplinary measures for policy or procedure violations;
- access controls to prevent access by terminated employees;
- regular reviews of security measures, annually or after major business changes;
- data breach incident response documentation, including a mandatory post-incident review of each event and actions taken; and
- computer system security procedures and protocols, such as authentication protocols, access control measures, and encryption of data in transit.

Enforcement

A violation under the bill by a covered deployer constitutes a deceptive trade practice under California's Unfair Competition Law, with a possible civil penalty of up to $2,500 for each violation.

Draft legislation

California: AI Transparency Act (Senate Bill 420)

While California's AI Transparency Act (Senate Bill 942) focuses on consumer tools and content labeling for Gen AI, Senate Bill 420, also known as the California AI Transparency Act, takes a broader civil rights approach, aiming to regulate high-risk ADS and ensure transparency, fairness, and accountability in AI-driven decision-making. On June 9, 2025, Senate Bill 420 was referred to the California Assembly Privacy and Consumer Protection and Judiciary Committee after passing its first reading in the Assembly on June 3, 2025, and its third reading in the Senate on June 2, 2025.

Scope

Senate Bill 420 aims to protect individuals from potential harms caused by AI systems, such as discrimination, privacy violations, and a lack of transparency. It establishes rights, responsibilities, and oversight mechanisms for developers and deployers of high-risk ADS.

Definitions

Under Senate Bill 420, AI is defined as an engineered or machine-based system that varies in its autonomy level and can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

A developer means a natural person or entity that designs, codes, produces, or substantially modifies a high-risk automated decision system for use in California.

A deployer means a natural person or entity that uses a high-risk ADS in California.

A high-risk ADS is used to assist or replace human discretionary decisions that have a legal or similarly significant effect in areas such as education, employment, housing, healthcare, lending, legal rights, utilities, and government services.

Requirements

Developers

Under Senate Bill 420, developers must conduct an impact assessment:

- before public release if the high-risk ADS was made available on or after January 1, 2026; or
- by January 1, 2028, if the ADS was made available before January 1, 2026.

Assessments of high-risk ADS must include:

- the purpose, benefits, and intended use;
- the outputs and input data types;
- the potential for disproportionate impacts on protected classes;
- the safeguards against algorithmic discrimination;
- the monitoring mechanisms for deployers; and
- consistency with the intended use by deployers.

Draft legislation

In addition, developers must also share the impact assessment with deployers and potential deployers, including state agencies. The developers must also implement a regularly reviewed governance program that:

- addresses algorithmic discrimination risks; and
- aligns with standards like the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF 1.0) (AI RMF).

Deployers

Deployers must also conduct an impact assessment within two years of deploying a high-risk ADS if deployed after January 1, 2026.

Deployers must notify individuals when a high-risk ADS is used to make decisions about them, disclosing the purpose and decision made, ADS uses, data types used, and contact information.

Deployers must publish a statement on their website detailing:

- the types of high-risk ADS in use;
- risk management strategies; and
- the data sources used.

Individuals or groups adversely affected by AI-driven decisions must have access to a human review option, where technically feasible.

Enforcement

The California AG or the Civil Rights Department may bring a civil action against a deployer or developer for a violation of Senate Bill 420 and obtain any of the following civil penalties:

- if a developer or deployer fails to conduct an impact assessment, a civil penalty of $2,500 for a defendant with fewer than 100 employees, $5,000 if the defendant has fewer than 500 employees, and $10,000 if the defendant has at least 500 employees;
- if a violation is intentional, the civil penalty shall increase by $500 for each day that the defendant is non-compliant; or
- if the violation concerns algorithmic discrimination, a civil penalty of $25,000 per violation.

Connecticut: AI Act

Following the footsteps of the US states that have passed AI laws, Connecticut is currently in its second attempt to adopt a law on AI regulation. On February 19, 2025, Senate Bill 2 for an act concerning artificial intelligence was introduced in the Senate. As of May 14, 2025, the bill passed the Senate and is awaiting legislative process in the Connecticut House of Representatives.

Scope

The bill lays down comprehensive obligations for deployers and integrators of high-risk AI systems and developers of AI systems.

Specifically, the bill defines a deployer as any person doing business in the state that deploys a high-risk AI system within Connecticut. Further, the bill defines a 'developer' as any person doing business in Connecticut that develops, or intentionally and substantially modifies, an AI system. An 'integrator' is an entity doing business in Connecticut, with respect to a high-risk AI system that:

Draft legislation

- neither develops nor intentionally and substantially modifies the high-risk AI system; and
- integrates it into a product or service.

Notably, the bill carves out exceptions for certain free open-source general-purpose AI models.

Definitions

An AI system means any machine-based system that, for any explicit or implicit objective, infers from the inputs such a system receives how to generate outputs, including, but not limited to, content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

A high-risk AI system is classified as any AI system that is intended to make or be a substantial factor in making a consequential decision. The following AI systems are excluded unless they make a consequential decision:

- anti-fraud technology that does not make use of facial recognition;
- AI-enabled video game technology;
- digital utilities such as anti-malware, anti-virus, calculator, internet domain registration, robocall-filtering, spam-filtering, spellchecking, or web-hosting;
- technology exclusively used for the entity's internal management;
- document classification or duplicate detection tools with a limited task scope and limited discrimination risk;
- technology detecting decision-making patterns or deviations from prior decision-making patterns following a human assessment and requiring human review; or
- natural language technologies providing information, making referrals or recommendations, and answering questions, and subject to a use policy.

Intentional and substantial modification refers to deliberate, material changes to an AI system that significantly increase the risk of algorithmic discrimination or to a GPAI model that alters its compliance or purpose. The definition excludes changes resulting from pre-defined learning processes documented in the system's technical documentation and assessed during initial impact evaluations.

Obligations

Deployers

Importantly, the bill requires people doing business in Connecticut, including deployers, to disclose to consumers when they are interacting with an AI system. Furthermore, deployers of high-risk AI systems are required to disclose known or reasonably foreseeable risks of algorithmic discrimination to the Connecticut AG.

The bill further elaborates on the distinct notice requirements for deployers of high-risk AI systems that result in a consequential decision concerning a consumer, and where the consequential decision has an adverse impact on the consumer. The bill stipulates format and accessibility requirements for the notice.

Draft legislation

Developers

A developer of high-risk AI systems must use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the system. The bill also requires developers and their third-party contractors to carry out impact assessments to identify and address potential risks associated with high-risk AI systems.

Moreover, the bill prescribes specific requirements for developers of GPAI models, including creating and maintaining technical documents.

*Integrator*s

Similar to a developer, an integrator is required to take reasonable care to protect consumers from risks related to algorithmic discrimination. Additionally, integrators must enter into a contract with the developer of a high-risk AI system prior to integrating the system into a product or service. An integrator must also publish a statement on their website summarizing the high-risk AI system integrations and associated risks.

Enforcement and oversight

The AG has the exclusive authority to enforce the provisions of the bill. If enacted, some of the bill's provisions would have been operational from July 1, 2025. The remaining provisions allow for staggered effective dates, with some entering into effect on October 1, 2025, others on January 1, 2026, or February 1, 2026, with some sections requiring compliance by October 1, 2026.

Notably, in any action commenced by the AG, as provided, a developer, integrator, deployer, or other person can take the defense of proving compliance with the latest version of frameworks such as NIST RMF, ISO, or IEC 42001 or any other standard with requirements as stringent as provided in the bill.

New York: AI Training Data Transparency Act

In an effort to improve oversight of the datasets used in AI systems, Assembly Bill 6578 for an act to amend the general business law, in relation to establishing the artificial intelligence training data transparency act, was passed by the New York State Assembly on June 10, 2025. Assembly Bill 6578 needs to be approved in the Senate before being sent to the Governor of New York State for signature.

Scope

Assembly Bill 6578 targets any 'developer,' which is defined as a person, partnership, state or local government agency, or corporation that designs, codes, produces, or substantially modifies, on or after January 1, 2022, an AI model or service for use by members of the public, or for internal use by processing employee or contractor data. Assembly Bill 6578 provides for exemptions regarding Gen AI models or services used solely in operating aircraft in the national airspace, and AI models or services developed for national security, military, or defense, made available exclusively to federal entities.

Requirements

Assembly Bill 6578 imposes extensive transparency obligations on developers regarding the training of AI models or services, providing that developers

Draft legislation

must publish on their websites documentation, including:

- the sources or owners of the datasets;
- a description of types of data points within the datasets and how the datasets further the intended purpose of the AI model or service;
- whether the datasets include any data protected by copyright, trademark, or patent;
- whether the datasets were purchased or licensed by the developer;
- whether the datasets include personal information;
- whether the datasets include aggregate consumer information;
- whether there was any cleaning, processing, or other modification to the datasets by the developer;
- the time period during which the data in the datasets were collected, including a notice if the data collection is ongoing; and
- whether the Gen AI model or service used or continuously uses synthetic data generation in its development.

Furthermore, Assembly Bill 6578 creates transparency obligations for developers that use employee or contractor data to design or substantially modify a Gen AI model or service, regardless of whether the model or service is made publicly available. Developers must disclose to each employee whose data is used to train the AI model:

- the model's or service's intended purpose;
- a description of how the collected datasets further the intended purpose of the AI model or service;
- whether the datasets include personal information or personal identifying information;
- the dates the datasets were first used during the development of the AI model or service; and
- the time period during which the data in the datasets were collected, including a notice if the data collection is ongoing.

New York: RAISE Act

While Assembly Bill 6578 focuses on transparency in the datasets, Senate Bill 6953B, known as the Responsible AI Safety and Education (RAISE) Act, takes a broader approach by regulating the training and deployment of frontier AI models, emphasizing safety planning, third-party audits, and incident disclosure. On June 12, 2025, Senate Bill 6953B passed both the New York State Senate and the Assembly; however, it has not yet been signed by the Governor of New York.

Scope and definitions

Senate Bill 6953B provides for obligations for a 'large developer,' which is defined as a person that has trained at least one frontier model, the compute cost of which exceeds $5 million, and has spent over $100 million in compute costs in aggregate in training frontier models. Senate Bill 6953B excludes accredited colleges and universities from its scope to the extent that such colleges and universities are engaging in academic research.

Draft legislation

Senate Bill 6953B defines 'frontier model' as an AI model:

- trained using greater than 1026 computational operations (e.g., integer or floating-point operations), the compute cost of which exceeds $100 million; or
- produced by applying knowledge distillation to a frontier model as defined above.

Requirements

Senate Bill 6953B focuses on safety and transparency obligations regarding frontier model training and use, including the requirement to implement a written safety protocol and submit it to the New York Attorney General (New York AG) before deploying a frontier model. Additionally, large developers must conduct an annual review of the safety and security protocol for any changes to the capabilities of their frontier models and industry best practices and, if necessary, make modifications to such safety and security protocol.

Frontier models that would create an unreasonable risk of critical harm are prohibited under Senate Bill 6953B. Security incidents affecting the frontier model must be disclosed to the New York AG within 72 hours of discovery or within 72 hours of the large developer learning facts sufficient to establish a reasonable belief that a safety incident has occurred. The incident notification must be made in the manner provided in Senate Bill 6953B.

Enforcement

Violations of Senate Bill 6953B are punishable in a civil action brought by the New York AG, and civil penalties are up to 5% of the total compute cost used to train the large developer's frontier models and 15% of that amount for any subsequent violation. Certain violations are punishable with penalties in an amount not exceeding $10,000 per employee for each violation.

Draft legislation

Latin America

Brazil: Bill No. 2338 of 2023

In May 2023, the Brazilian Senate presented Bill No. 2338 of 2023 (Bill 2338) to regulate AI systems in Brazil, which is expected to replace three previous attempts at the same. On December 19, 2024, Bill 2338 was approved in the Plenary of the Brazilian Senate and is now awaiting approval by the Chamber of Deputies. If approved, the bill will then be sent to the President for promulgation.

Bill 2338 shares significant commonalities with the EU AI Act, including the classification of AI systems according to a risk-based approach, the prohibition of certain practices, the imposition of different obligations on providers/users, transparency and governance requirements, and incident reporting obligations. Bill 2338 recognizes specific rights of individuals, including contesting decisions made by AI systems, requesting human participation in decision-making, and requesting correction of discriminatory bias.

Scope

Bill 2338 applies to both the public and private sectors and aims to establish general rules for the development, implementation, and responsible use of AI systems in Brazil, with the goal of protecting fundamental rights and guaranteeing the implementation of safe and reliable systems.

Bill 2338 defines specific roles and lays out their responsibilities. A differentiation is made between entities that develop AI systems under their own name or brand (developers) and entities that make AI systems available (distributors). Moreover, Bill 2338 also establishes a role for 'applicators,' defined as entities using AI systems in their name or benefit, similar to deployers under the EU AI Act.

Definition of AI

Bill 2338 captures AI systems that are computer-based, designed to use input data to infer, with different degrees of autonomy, how to achieve a given set of goals, producing predictions, recommendations, or decisions that can influence the virtual or real environment. In line with the EU AI Act, Bill 2338 also adopts a technology-neutral approach to defining AI.

Risk-based AI systems classification

Bill 2338 proposes a prescriptive model that is similar to the EU AI Act. It classifies AI systems based on their risk level and imposes restrictions and safeguards proportionate to such risk, including prohibiting certain practices whose level of risk is deemed excessive. The list of AI systems under both risk categories may be updated by a competent authority.

Prohibited practices

Bill 2338 prohibits certain AI systems that broadly match those banned under the EU AI Act:

- systems that have the purpose or effect of instigating or inducing a natural person to behave in a manner detrimental to themselves or others;
- systems that exploit any vulnerabilities of specific groups of natural persons, in order to

Draft legislation

induce them to behave in a detrimental manner; and

- social scoring systems used by the public authorities are illegitimate or disproportionate.

High-risk practices

Bill 2338 also outlines systems that will be considered high-risk, namely those that will be used for activities, such as:

- eligibility for access to essential private or public services, including social security;
- immigration and border control;
- administration of justice;
- implementation of autonomous vehicles in public spaces;
- medical diagnoses and procedures;
- decision-making about access to employment, education, or essential public and private services;
- selection of students and workers;
- management of critical infrastructure, such as traffic control and water, and electricity supply networks;
- health diagnosis and procedures; and
- analytical assessment of crimes related to individuals by law enforcement authorities, with the purpose of identifying patterns and behavioral profiles.

Obligations

Developers and applicators of AI systems, particularly those involving systems classified as high-risk, are required to abide by far-reaching obligations.

While general governance obligations are imposed on both developers and applicators in relation to each AI system, stricter governance measures are triggered when the mandatory preliminary assessment of the AI system classifies it as high-risk.

As mandatory measures in such instances, applicators must, among others:

- document the development process, the technology deployed, and how the systems work;
- use tools that automatically record the results of the system's operation, to evaluate its accuracy, robustness, and discriminatory character;
- test records to assess reliability and safety; and
- document human oversight processes that have contributed to the system's outcome.

Obligations for developers of high-risk AI systems include maintaining records for supporting applicators, conducting safety tests, implementing transparency measures, and mitigating and preventing bias.

Distributors must support and verify that the high-risk AI system complies with the governance measures prior to market release. Additionally, the developer or the applicator that makes the high-risk AI system available on the market shall conduct an algorithmic impact assessment.

Draft legislation

Similar to the EU AI Act, developers, distributors, and applicators are required to report to the occurrence of serious security incidents to the competent authority, including when there are risks posed to the life and integrity of individuals, interruption of the functioning of critical infrastructure operations, serious damage to property or the environment, as well as serious violations of fundamental rights. However, the timeframe for notification is only vaguely defined and will be further determined by the competent authority.

Rights

Individuals affected by high-risk AI systems must be provided with the right to:

- contest and request explanations on decisions made by these systems;
- request human participation in the decisions of these systems in certain situations; and
- obtain information about its functioning.

Furthermore, independently of the level of risk of the AI system, individuals have the right to information, to privacy and personal data protection, and to not be discriminated against and request correction of discriminatory bias.

Oversight and enforcement

The responsibility to monitor compliance with Bill 2338 is attributed to a 'competent authority,' to be appointed by the Executive Branch. The competent authority would also be empowered to impose administrative penalties of both a monetary and non-monetary nature. Regarding the former, amounts are limited to BRL 50 million (approx. $8.9 million) per infringement, up to 2% of a legal entity's revenue for the preceding financial year.

Moreover, the developer, distributor, or applicator of an AI system that causes damage would also be exposed to civil liability according to general civil liability rules, taking into account the level of autonomy of the AI system and the nature of the agent involved.

Brazil: Bill No. 526 of 2025

On February 18, 2025, Bill No. 526/2025 regulating the use of artificial intelligence in Brazil (Bill 526) was introduced to the Chamber of Deputies, and, at the time of writing, has not yet been approved.

Compared to Bill 2338, Bill 526 is more concise, as it provides high-level principles, key obligations, and prohibitions, and does not specifically outline any scope of application.

Definition of AI

AI is defined as technological systems capable of performing tasks that would normally require human intelligence.

Principles

The principles outlined in Bill 526 follow international standards and norms such as respect for human rights; transparency and explainability; security and robustness; responsibility and accountability; and innovations and sustainable development.

Draft legislation

Obligations

While Bill 526 does not define high-risk AI systems, it mandates users and developers of such systems to conduct an impact assessment, ensure human supervision, adopt technical and organizational measures to ensure the safety, privacy, and data protection, as well as provide clear and accessible information to users on the functioning and limitations of the system.

Prohibitions

Notably, Bill 526 prohibits the use of AI in specific circumstances that are not included in Bill 2338:

- massive surveillance without judicial authorization;
- manipulation of information for the spread of misinformation;
- promotion of racial, gender, sexual, religious, or other forms of discrimination; and
- completely automated decisions in judicial and administrative proceedings, where there is no possibility of human oversight.

Asia Pacific

Taiwan: Draft AI law

On July 15, 2024, the National Science and Technology Council (NSTC) of Taiwan introduced the Draft Basic Law on Artificial Intelligence (the Draft Law). The Draft Law is still in the pre-legislative phase. It has undergone public consultation and is being revised based on feedback from civil society, legal experts, and political parties. However, there are alternative proposals for an AI law, which have been submitted by members of different political parties.

Scope

The Draft Law applies to the development, deployment, and governance of AI technologies across both public and private sectors. The Draft Law encompasses AI applications in various sectors, including healthcare, finance, transportation, education, and public services.

Definition of AI

'AI' is defined as a machine-based system with autonomous operational capabilities that, through input or sensing, and using machine learning and algorithms, can produce outputs such as predictions, content, recommendations, or decisions that affect physical or virtual environments. The definition of AI in the Draft Law draws from international standards, including the NIST AI RMF and the EU AI Act.

Principles and obligations

The Draft Law is built around the following seven core principles that align with internationally accepted standards:

- sustainable development;
- human autonomy;
- privacy and data governance;
- safety and security;
- transparency and explainability;

Draft legislation

- fairness and non-discrimination; and
- accountability.

The Draft Law requires AI developers and deployers to ensure data minimization, label AI-generated content, and adhere to a risk classification framework. The government is also expected to support AI innovation through regulatory sandboxes and promote AI literacy and workforce transformation.

Enforcement

The Ministry of Digital Affairs (MODA) will be responsible for developing the AI risk classification framework and coordinating enforcement across sectors. However, sector-specific agencies are responsible for implementing and managing AI-related regulations within their domains.

Frameworks

This section presents non-binding instruments that guide the responsible development and use of AI systems. These include international standards and governance models developed by multilateral organizations, national authorities, and industry bodies. While not legally enforceable, these frameworks play a critical role in shaping best practices, informing regulatory design, and supporting cross-border interoperability.

International

ASEAN Guide on AI Governance and Ethics

In February 2024, a Guide on AI Governance and Ethics (the Guide) was released by the Association of South East Asian Nations (ASEAN). The Guide is meant to serve as a practical tool for organizations that want to design, develop, and deploy AI technologies in commercial and non-military or dual-use applications, and increase users' trust in AI. The Guide encourages alignment within ASEAN and fosters the interoperability of AI frameworks across jurisdictions, providing recommendations for individuals and organizations along the entire value chain, including for both AI developers and deployers.

The Guide also establishes general principles for an AI governance framework, including:

- transparency and explainability;
- fairness and equity;
- security and safety;
- robustness and reliability;
- human-centricity; privacy and data governance; and
- accountability and integrity.

With regard to AI governance frameworks, the Guide examines four key components, namely:

- adapting existing or setting up internal governance structures and measures to incorporate values, risks, and responsibilities relating to algorithmic decision-making;
- determining the appropriate level of human involvement in AI-augmented decision-making based on the risks assessed, i.e., human-in-the-loop, human-over-the-loop, and human-out-of-the-loop;
- conducting risk assessments before starting any data collection and processing, mitigating risk bias with tests on training data; and
- developing communication and trust with stakeholders, providing disclosure on when AI is used in products, and putting in place measures to help employees adapt to AI.

The Guide was supplemented by the ASEAN Guide on AI Governance and Ethics - Generative AI, published in January 2025, which provides guidance on the six Gen AI risks identified in the Guide, namely:

- mistakes and anthropomorphism;
- factually inaccurate responses and disinformation;
- deepfakes, impersonation, fraudulent, and malicious activities;
- infringement of intellectual property rights;
- privacy and confidentiality; and
- propagation of embedded biases.

Frameworks

ISO/IEC standards

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IE) have issued standards pertaining to AI. In 2020, ISO/IEC issued ISO/IEC TR 24028:2020 Information technology - AI - Overview of trustworthiness in AI that analyzes the factors that can impact the trustworthiness of AI systems, covering the existing approaches that can support or improve trustworthiness and other possible approaches to mitigating AI system vulnerabilities that relate to trustworthiness. The bodies also published ISO/IEC 23894:2023 to assist organizations that develop, deploy, or use AI systems to manage their risks. In addition, it aims to support organizations in integrating risk management into their AI-related activities and functions, where it describes processes for the effective implementation and integration of AI risk management.

ISO/IEC 42001:2023 provides requirements and guidance for establishing, implementing, maintaining, and improving AI management systems within an organization. This includes advising organizations to develop and maintain AI management systems tailored to their specific needs, objectives, processes, size, structure, and stakeholder expectations. Organizations are recommended to apply the requirements of the AI management system using a risk-based approach to ensure the appropriate level of control is applied to different AI use cases, services, or products, considering their specific risks and implications.

ISO/IEC 42005:2025 is an AI system impact assessment standard that complements ISO/IEC 42001, ISO/IEC 38507, and ISO/IEC 23894. Specifically, the standards recommend performing assessments throughout the AI system lifecycle, from design and development to deployment and post-market monitoring, and updating them as needed.

More recently, ISO/IEC 42006:2025, published in July 2025, outlines requirements for bodies providing audit and certification of AI management systems. The standard builds on ISO/IEC 17021-1, adding AI-specific requirements for auditing and certification processes.

OECD Recommendation of the Council on AI

The Organization for Economic Co-operation and Development (OECD) issued the Recommendation of the Council on AI (the Recommendation), which is a standard for AI policies. The Recommendation provides a foundation to conduct further analysis and develop tools to support governments in their implementation efforts, but also includes principles relevant for AI stakeholders. The Recommendation was amended in 2024 after its initial adoption in 2019 and is open to non-OECD Members. The Recommendation aims to foster innovation and trust in AI while complementing existing OECD standards in areas such as privacy, digital security risk management, and responsible business conduct.

The Recommendation differs from the other frameworks, such as NIST and ISO, as it seeks to provide guidance to governments creating legislation and/or national policies for trustworthy AI, while also providing guidance to AI stakeholders. The Recommendation is quite high-level when compared to other frameworks and is divided into two

Frameworks

substantive sections. The first outlines five principles for responsible implementation of trustworthy AI by relevant actors, including transparency and explainability, accountability, human-centered values and fairness, robustness, security, and safety, and accountability. The second provides five recommendations to implement in national policies and international cooperation, such as investing in AI research and development, fostering a digital ecosystem for AI, shaping an enabling policy environment for AI, and international cooperation for trustworthy AI.

OECD Framework for the Classification of AI Systems

The OECD's Framework for the Classification of AI Systems (the OECD Framework) was developed by the OECD to help policymakers, regulators, legislators, and others characterize AI systems for specific projects and contexts. The OECD Framework is designed as a user-friendly tool for evaluating and classifying AI-specific risks, such as bias, explainability, and robustness.

The OECD Framework classifies AI systems and applications along the following dimensions: People & Planet, Economic Context, Data & Input, AI Model, and Task & Output. Notably, the OECD Framework does not currently address governance at the corporate, institutional, or AI systems level, nor does it cover the use of mitigation measures or compliance and enforcement measures in the AI system lifecycle. Instead, it is meant to facilitate the development of policies and regulations, and provide a baseline to:

- promote a common understanding of AI;
- inform registries or inventories;
- support sector-specific frameworks;
- support risk assessment; and
- support risk management.

CoE Framework Convention on AI

The Council of Europe (CoE) Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (the Convention) is the first international legally binding treaty on AI. The Convention was adopted on May 17, 2024, and was opened for signatures in September 2024. Currently, 16 countries/bodies, including the US, UK, EU, Japan, and Canada, are signatories to the Convention; however, none have ratified it yet.

The Convention became effective on the first day of the month after three months had passed since five countries (including at least three Council of Europe member states) officially consented. Similarly, effective dates for subsequent signatories are noted in the Convention.

Importantly, the Convention adopts a risk-based approach to the design, development, use, and

Frameworks

decommissioning of AI systems, and sets out a legal framework that covers the entire lifecycle of AI systems, addressing the risks they may pose while promoting responsible innovation.

Scope

The Convention applies to both the public and private actors. The Convention has a broad scope, encompassing activities within the lifecycle of AI systems that have the potential to interfere with human rights, democracy, and the rule of law.

Importantly, parties to the Convention may either opt to be directly obliged by the Convention's provisions or take other measures to comply with the provisions while respecting their international obligations. This approach is necessary to account for the differences in legal systems around the world.

The Convention does not apply to national defense matters nor to research and development activities, except when the testing of AI systems may have the potential to interfere with human rights, democracy, or the rule of law.

Definition of AI

The Convention defines an AI 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Principles

The Convention outlines the principles related to activities within the lifecycle of an AI system that each party must implement in accordance with their national legal system:

- human dignity and individual autonomy;
- equality and non-discrimination;
- respect for privacy and personal data protection;
- transparency and oversight;
- accountability and responsibility;
- reliability; and
- safe innovation.

Requirements

The Convention includes requirements for adopting or maintaining measures for the identification, assessment, prevention, and mitigation of risks posed by AI systems. There is a requirement specifically for carrying out impact assessment with respect to actual and potential impacts on human rights, democracy, and the rule of law.

Additionally, there is a need to establish transparency and oversight mechanisms tailored to specific contexts and risks, including identifying content generated by AI systems. Specifically, a notice should be provided when one is interacting with AI systems.

Importantly, parties are required to provide effective procedural guarantees, safeguards, and rights to affected people in connection with the application of an AI system.

The Convention also grants each party the ability to assess the need for a moratorium/ban/other measures in respect of certain uses of AI systems

Frameworks

where it considers the uses incompatible with the respect for human rights, the functioning of democracy, or the rule of law.

Enforcement and oversight

For effective implementation of the Convention, a follow-up mechanism is established in addition to provisions on international co-operation. Additionally, parties must establish an independent oversight mechanism to oversee compliance.

EU

EU: ENISA Multilayer Framework for Good Cybersecurity Practices for AI

In June 2023, the European Union Agency for Cybersecurity (ENISA) published a Multilayer Framework for Good Cybersecurity Practices for AI, to guide national competent authorities and AI stakeholders on the steps aiming to secure their AI systems and processes. The framework was published as part of four broader reports on AI and cybersecurity, and aims to provide a step-by-step approach to following good cybersecurity practices in order to build trustworthiness in AI operations.

The framework provides more high-level guidance in comparison to guidance documents such as the NIST AI RMF. The methodology utilized in the framework involves review and analysis of other guidance, such as from OECD and NIST, where it identifies different types of AI, tips for AI threat assessment, and AI security management. The overarching recommendation is to complement existing cybersecurity practices with AI-specific practices, including dynamic and measurable risk assessments of AI technical (e.g., poisoning data) and social threats (e.g., bias, lack of fairness), and continuous risk management during the AI system lifecycle. The framework explains that AI should be treated as an additional effort to existing practices for the security of organizations' information and communications technology (ICT).

UK: AI and Data Protection Risk Toolkit

In May 2022, the Information Commissioner's Office (ICO) launched its updated AI and data protection risk toolkit (the Toolkit). The Toolkit is aimed at helping organizations assess the privacy risks associated with their use of AI. The Toolkit highlights risk areas during different stages of an AI lifecycle, from design and development to testing and deployment. The Toolkit suggests four classifications when scoring privacy risks associated with the use of AI, i.e., 'high,' 'medium,' 'low,' and 'non-applicable.'

Notably, the Toolkit discusses practical steps organizations can take to mitigate said risks, including conducting a Data Protection Impact Assessment (DPIA) and testing the security of software. Additionally, the Toolkit provides relevant guidance to help with each control objective. According to the ICO, the Toolkit is not intended to replace a DPIA, and using the Toolkit is optional.

Frameworks

USA

USA: NIST AI Risk Management Framework

On January 26, 2023, the AI Risk Management Framework (the AI RMF) was released by the U.S. Department of Commerce's NIST. The AI RMF is a voluntary guidance document designed to help manage risks stemming from AI technologies and equips AI actors with approaches that increase the trustworthiness of AI systems.

The AI RMF is accompanied by an AI RMF Playbook, which provides input on how to navigate and use the AI RMF, as well as a Generative AI Profile (NIST-AI-600-1), which addresses 12 unique risks posed by Gen AI systems and provides 200 for Gen AI risk management.

Scope and definitions

The AI RMF is designed for use by organizations of all sizes and sectors that are involved in the AI lifecycle, including developers, deployers, evaluators, and users. It applies across a wide range of AI technologies and use cases and is intended to be adaptable to different organizational contexts, risk tolerances, and resources.

AI risk management refers to the coordinated activities to direct and control risks associated with AI systems. These risks may affect individuals, organizations, and society, and include concerns related to safety, fairness, privacy, security, and reliability.

Framework structure

Part one of the AI RMF identifies and analyzes the AI actors intended to use this framework, discusses how organizations can frame AI risks, and outlines the characteristics of trustworthy AI systems. Specific characteristics that form the basis of a trustworthy AI system are outlined in the AI RMF, including secure and resilient, accountable and transparent, explainable and interpretable, and privacy-enhanced. Generally, the AI RMF maintains that creating trustworthy AI requires the balancing of each of these characteristics based on the AI system's context of use.

Part two of the AI RMF outlines four high-level functions to provide organizations with assistance in addressing the risks of AI systems. These functions can be applied in context-specific use cases and at any stage of the AI lifecycle.

- Govern: Establishing and overseeing the policies, practices, and organizational structures necessary for effective AI risk management in a product's lifecycle.
- Map: Understanding the context in which an AI system is developed and deployed, including its intended purpose, capabilities, limitations, and potential impacts.
- Measure: Assessing and tracking AI system performance, risks, and trustworthiness characteristics using qualitative and quantitative methods.
- Manage: Implementing risk controls and mitigation strategies throughout the AI lifecycle and continuously improving risk management practices.

Frameworks

Obligations

Similar to the EU AI Act, the AI RMF adopts a prescriptive approach to documentation obligations, and it outlines requirements to maintain records covering various procedural aspects of the AI system. Moreover, akin to Singapore's Model AI Framework, the AI RMF places an emphasis on adequate training to allow individuals to perform their roles and use the system in a way that is consistent with the related policies and procedures.

Furthermore, where the EU AI Act specifically requires operators to design systems so they can automatically record event logs to monitor the AI system during its lifecycle, the AI RMF takes a lighter approach and only recommends that organizations monitor the functionality and behavior of the system and its components. Organizations must also assess and monitor AI systems for harmful bias, privacy risks, and security vulnerabilities, and take corrective actions when needed.

Asia Pacific

Australia: Voluntary AI Safety Standard

At the time of writing, Australia has not yet enacted any specific statutes or regulations that directly regulate AI; however, on September 5, 2024, the Department of Industry, Science, and Resources (DISR) published the Voluntary AI Safety Standard published the Voluntary AI Safety Standard (VAISS). The VAISS establishes a unified set of practices for organizations to ensure safe and responsible development and deployment of AI.

Whereas the VAISS applies to both AI deployers and developers, its initial version primarily focuses on providing guidance for AI deployers. In December 2024, the DISR launched a consultation on the second version of the VAISS, which is expected to include additional practices for AI system developers.

Voluntary guardrails

The VAISS consists of the following 10 voluntary guardrails that apply to all organizations throughout the AI supply chain.

1. Establish, implement, and publish an accountability process including governance, internal capability, and a strategy for regulatory compliance.
2. Establish and implement a risk management process to identify and mitigate risks.
3. Protect AI systems and implement data governance measures to manage data quality and provenance.
4. Test AI models and systems to evaluate model performance and monitor the system once deployed.
5. Enable human control or intervention in an AI system to achieve meaningful human oversight.
6. Inform end users of AI-enabled decisions, interactions with AI, and AI-generated content.
7. Establish processes for people impacted by AI systems to challenge use or outcomes.

Frameworks

8. Be transparent with other organizations across the AI supply chain about data, models, and systems to help them effectively address risks.
9. Keep and maintain records to allow third parties to assess compliance with guardrails.
10. Engage their stakeholders and evaluate their needs and circumstances, with a focus on safety, diversity, inclusion, and fairness.

Notably, the VAISS states that the first nine guardrails are aligned with proposed mandatory requirements for AI deployment in high-risk settings. The VAISS further notes that the voluntary guardrails serve as preparatory measures for organizations to improve their AI practices and ensure compliance with potential future regulations.

To aid deployers of AI systems, the VAISS includes procurement guidance to enable AI suppliers and developers to incorporate the guardrails through contractual agreements.

The VAISS also explains what developers and deployers of AI systems must do to comply with the guardrails and provides practical examples to demonstrate how organizations can apply the guardrails in different AI use cases. The examples cover scenarios such as general-purpose AI chatbots, facial recognition technology, recommender engines, and warehouse accident detection systems. Each example shows how specific guardrails can help manage the risks and benefits of deploying AI systems in real-world contexts.

China: AI Safety Governance Framework

On September 9, 2024, the TC260 released the first version of the 'Artificial Intelligence Security Governance Framework' (the Framework), which focuses on safety risk assessment and governance of AI. The Framework is not a mandatory law, regulation, or standard.

Principles

The Framework highlights key principles, which include development, innovation, and an inclusive approach to AI research and application, the identification of AI safety risks from the technology and its application, and the implementation of tailored preventive measures.

Framework for AI safety governance

The Framework states that control measures, such as targeting technical countermeasures in software development, data quality improvement, and evaluation activities, must be continuously updated. It also establishes measures that all stakeholders, including providers, users, and government agencies, should take regarding AI safety risks. Moreover, safety guidelines for AI development must be issued.

Classification of AI safety risks

The Framework identifies inherent safety risks of AI in:

- models and algorithms: explainability challenges, bias and discrimination, lack of robustness, tampering, unreliable output, and adversarial attacks;

Frameworks

- data: inaccuracy, illegal collection and use of data, improper content and poisoning in training data, and data leakage; and
- AI systems: exploitation through defects and backdoors, computing infrastructure security, and supply chain security.

On the other hand, the Framework classifies safety risks in AI applications into the following:

- cyberspace: information and content safety, confusing facts, authentication bypass, information leakage, and cyberattacks;
- real-world: illegal and criminal use of AI;
- cognitive: amplification of the effect of 'information cocoons;' and
- ethical: increased social discrimination and prejudice.

The Framework also outlines several risk mitigation approaches, which include:

- clear explanations for the internal structure, reasoning logic, technical interfaces, and output results of AI systems;
- secure development standards across the supply chain;
- security rules on data collection, usage, and personal information processing, and users' rights;
- strict selectivity in training data, including using precise and diverse data;
- compliance with regulations on cross-border data flow;
- strengthened risk identification, detection, and mitigation;
- data safeguards to ensure compliance with the law when outputting sensitive personal information and important data; and
- identification of unexpected, untruthful, and inaccurate outputs via technological means.

Comprehensive governance measures

The Framework proposes comprehensive governance measures, which include:

- tiered and category-based (e.g., based on features, functions, and application scenarios) management for AI applications;
- traceability management system for AI services, including digital certificates, standards, and regulations;
- inclusion of requirements for data security and personal information protection in various stages of the AI cycle;
- creation of responsible AI research and development, and application systems;
- strengthening the AI supply chain security; and
- sharing information and enhancing training.

Frameworks

Safety guidelines for AI development and application

The Framework outlines four types of safety guidelines:

- for model algorithm developers: people-centered approach and strengthening of data security, personal information protection, intellectual property, and copyright;
- for AI service providers: disclosure of information to the users, increasing awareness, and reporting safety and security incidents;
- for users in key areas: assessment of impact and carrying out audits; and
- for general users: careful review of documentation and raising awareness.

China - Draft AI Security Standard

On January 26, 2025, the TC260 solicited public comments on the draft Artificial Intelligence Security Standard System (the AI Security Standard) until February 21, 2025.

Scope

The AI Security Standard sets out a framework for managing AI security risks and outlines guidance for AI security implementation, standard development, and international cooperation.

The AI security risk is classified into three categories: model and algorithm safety, data safety, and system safety. In addition, it identifies four types of application security risks: network domain, reality domain, cognitive domain, and ethical domain.

Requirements

The AI Security Standard is organized into five components:

- Foundational Common Standards, which establish core definitions, classification and grading schemes, general requirements, and security assessment frameworks for AI applications;
- Security Management Standards, which outline requirements to manage AI security risks across the AI system lifecycle, including development, application, operation, and maintenance;
- Key Technology Standards, which define security protocols for advanced and emerging AI technologies, including Gen AI, multimodal AI, and generative synthesis;
- Testing and Evaluation Standards that provide a framework for evaluating the security effectiveness of AI models, products, and services; and
- Product and Application Standards, which address security requirements for personal AI applications, such as facial recognition, and key industry-specific uses, including AI-assisted code generation.

Frameworks

Middle East

Saudi Arabia: AI Ethics Framework version 2.0

In September 2023, the Saudi Data & Artificial Intelligence Authority (SDAIA) published version 2.0 of its Artificial Intelligence Ethics Framework (the AI Ethics Framework), which focuses on helping entities develop responsible AI-based solutions that limit the negative implications of AI systems while encouraging innovation. The AI Ethics Framework applies to natural or legal persons, across public, private, and non-profit sectors, that design, develop, deploy, implement, use, or are affected by AI systems in Saudi Arabia, as well as researchers, workers, and consumers. Notably, the AI Ethics Framework includes a list of AI ethics tools and checklists.

Similar to the EU AI Act, the AI Ethics Framework also establishes the categories and levels of risk associated with the development and use of AI, dividing them into four categories ranging from 'little or no risk,' to 'unacceptable risk.'

'High risk' AI systems must undergo pre- and post-conformity assessments, while AI systems that pose an 'unacceptable risk' to basic rights are prohibited. Moreover, the AI Ethics Framework outlines seven principles for governing AI use and development in Saudi Arabia, similar to principles provided in other frameworks such as the OECD Framework, namely: fairness, privacy and security, humanity, social and environmental benefits, reliability and safety, transparency and explainability, and accountability, as well as responsibility. The AI Ethics Framework also outlines the AI system lifecycle and notes that risk management should be directly connected to AI initiatives, provides steps to guide entities when applying the principles in each stage of the AI System Lifecycle, and identifies the roles and responsibilities of the SDAIA and adopting entities.

Singapore: Model AI Governance Framework for Gen AI

On May 30, 2024, the Infocomm Media Development Authority (IMDA) and AI Verify Foundation announced the publication of the Model AI Governance Framework for Generative AI (the Framework).

The Framework was first published in 2019 and updated in 2020, with the current publication, which was released for public consultation in January 2024, seeking to address specific AI risks stemming from Gen AI. The updated Framework includes additional considerations (such as robustness and reproducibility) and refines the original Model Framework for greater relevance and usability. The Framework sets forth a systematic and balanced approach to address Gen AI concerns while facilitating innovation.

Requirements

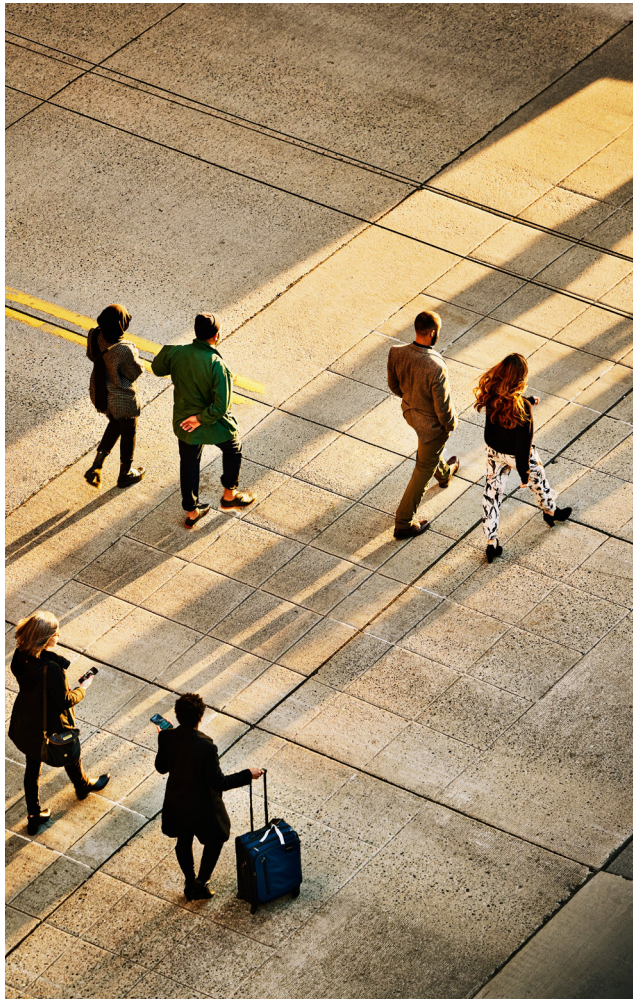
The Framework outlines the following nine dimensions.

- Accountability - the Framework considers how responsibility can be allocated during the development process, with allocation based on the level of control each stakeholder has in Gen AI development.
- Data - the Framework recommends referring to existing personal data protection legislation as

Frameworks

a starting point, the use of Privacy Enhancing Technologies (PETs), and measures to ensure data quality.

- Trusted development and deployment - the Framework recommends evaluation during the training of AI models, including techniques such as Reinforcement Learning from Human Feedback, and Retrieval Augmented Generation, alongside benchmarking test models and red teaming.
- Incident reporting - the Framework suggests the establishment of structures and processes to enable incident reporting for timely notification and remediation.
- Testing and assurance - notably, the Framework outlines the role of external audits as a mechanism to provide greater transparency, detailing the need for such audits to be done according to a standardized method.
- Security - the Framework, in recognizing novel security threats from Gen AI, recommends a 'security-by-design' approach, noting new security safeguards such as input filters and digital forensic tools for Gen AI.
- Content provenance - owing to the creation of realistic synthetic content at scale, the Framework stipulates the need for digital solutions, including digital watermarking and cryptographic provenance.
- Safety and alignment R&D - the Framework provides that safety techniques and evaluation tools at present do not fully address all potential risks, and the need to ensure human capacity to align and control Gen AI. At the design stage, the Framework recommends Reinforcement Learning from AI Feedback and the evaluation of a model after it is trained to validate its alignment.
- AI for public good - the Framework also recognizes the need for Gen AI to empower the public, outlining the need to democratize access to technology, public service delivery, workforce, and sustainability.



Conclusion

As AI continues to evolve and permeate critical domains of public and private life, regulatory responses have intensified across jurisdictions. This report addresses the evolving responsibilities of AI stakeholders and the mechanisms being introduced to ensure compliance, such as AI impact assessments, disclosures, and post-market monitoring. It also considers enforcement models, ranging from centralized oversight bodies like the EU AI Office to decentralized approaches involving US State Attorney Generals.

The report highlighted the emergence of binding laws such as the EU AI Act, South Korea's Basic AI Act, China's Measures for the Identification of Synthetic Content Generated by AI, and California's AI Transparency Act, alongside influential frameworks like the OECD Recommendation on AI, the NIST AI RMF, and ISO/IEC standards providing guidance on best practices for AI lifecycle management. Despite differences in legal systems and regulatory maturity, there is a clear alignment on foundational principles such as transparency, accountability, risk management, and human oversight.

Another notable trend is that several laws now distinguish between developers, deployers, distributors, and service providers, assigning tailored obligations to each, leading toward more operationalized governance.

Many instruments also adopt a risk-based approach, classifying AI systems according to their potential impact on individuals and society. High-risk systems are subject to stricter requirements, including impact assessments, documentation, and monitoring. Additionally, there is growing attention to the entire lifecycle of AI systems, from design and training to deployment and post-market surveillance, underscoring the need for continuous accountability.

While the report provides a consolidated view of key developments, it does not aim to be exhaustive. The pace and volume of legislative activity in the AI domain continue to accelerate, and new proposals and standards are emerging regularly. Nonetheless, the instruments included represent a meaningful cross-section of current regulatory thinking and offer valuable guidance for organizations seeking to navigate the evolving landscape of AI governance.

onetrust
DataGuidance

About OneTrust DataGuidance™

OneTrust DataGuidance provides a comprehensive platform for regulatory research, offering over two decades of expertise to privacy professionals worldwide. With contributions from more than 1,700 experts and daily updates from 300+ jurisdictions, the platform includes access to over 27,000 articles, insights, and guidance notes. DataGuidance simplifies the complexity of global regulations, covering emerging areas like artificial intelligence and US privacy laws, while tracking enforcement trends. Integrated with the AI-powered OneTrust Copilot, it enhances research speed and efficiency, empowering organizations to collaborate across the enterprise and take the first step in establishing and evolving privacy, data, and AI strategies to stay ahead of regulatory change.

To learn more, visit DataGuidance.com or connect on LinkedIn.