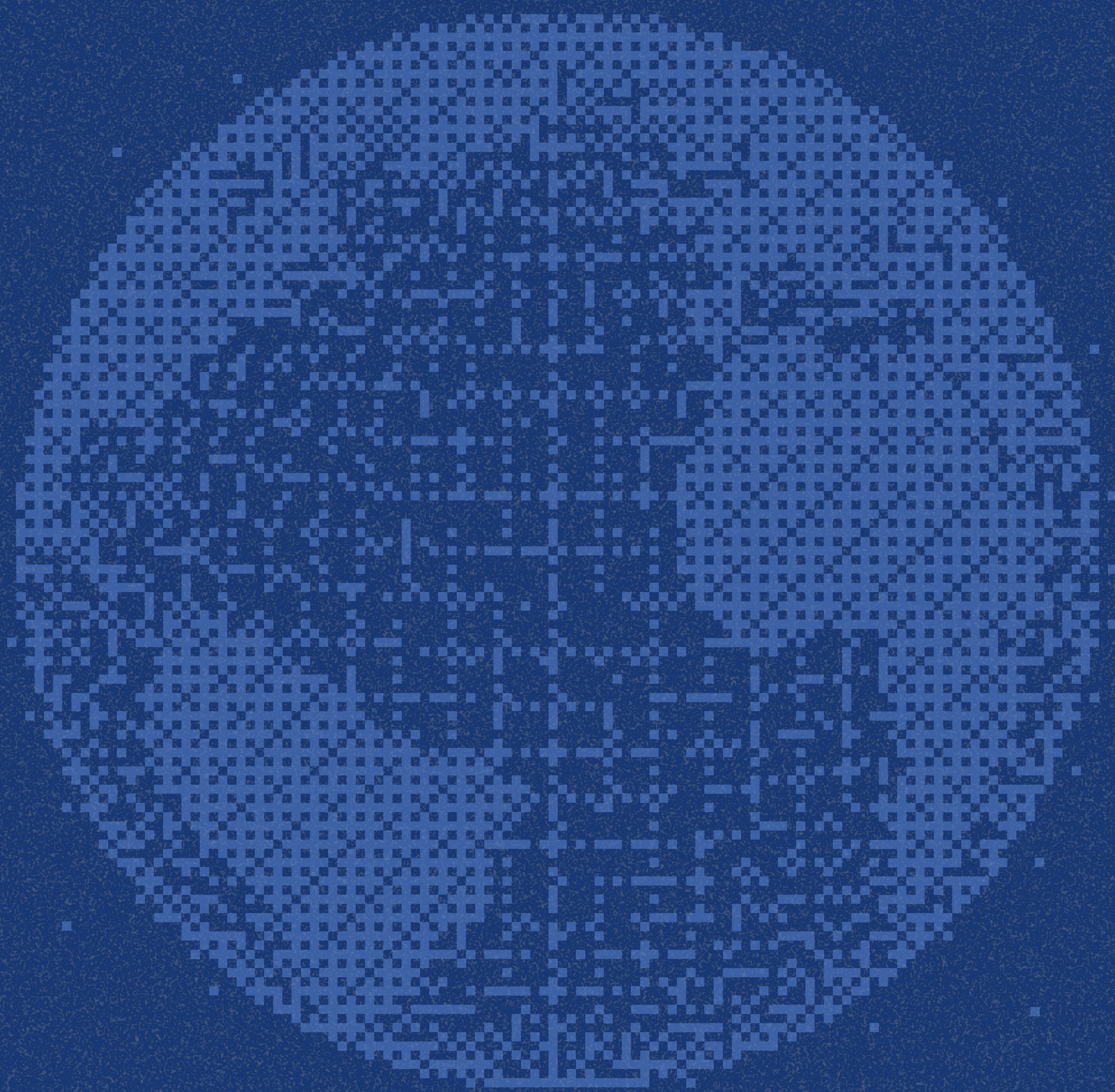


The State of Global AI Regulations



Content

01 Importance of AI Regulations

02 Purpose & Scope

03 Background Information on the Countries Covered

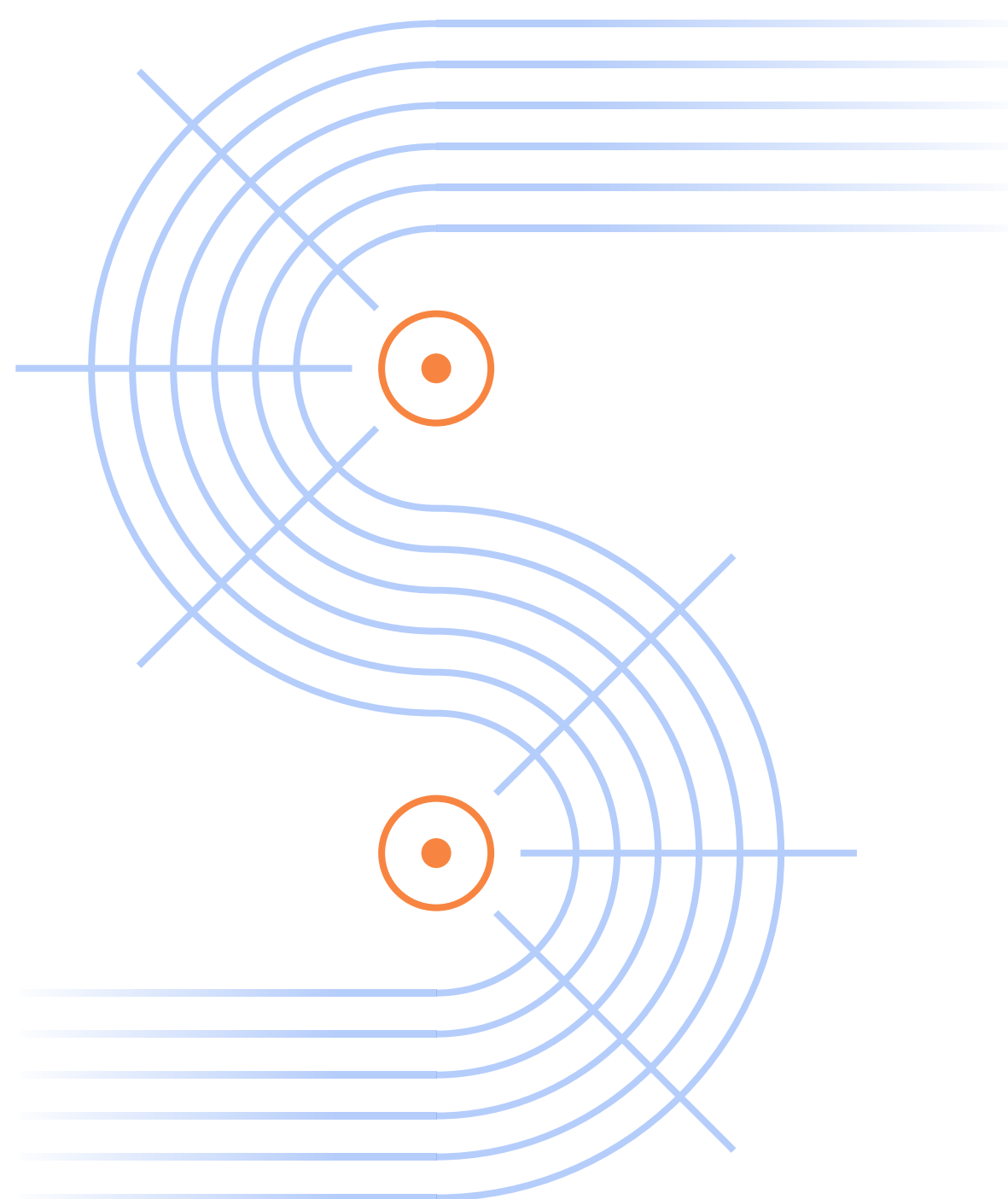
41 How Can Securiti Help


Importance of AI Regulations

The most surprising and vocal voice supporting AI regulations has been that of OpenAI's CEO, Sam Altman. At a Congressional hearing back in May 2023, Altman highlighted how little his organization understands its tech's true capabilities and potential.

He reiterated that rigorous regulatory intervention would be necessary to ensure all this potential is not negatively co-opted

In the absence of such legislation, AI's potential for causing incidents of catastrophic consequence, such as political manipulation, misinformation, and behaviorally targeted profiling, among others, can lead to chaos at an unprecedented scale and a systematic deterioration of individuals' rights online.

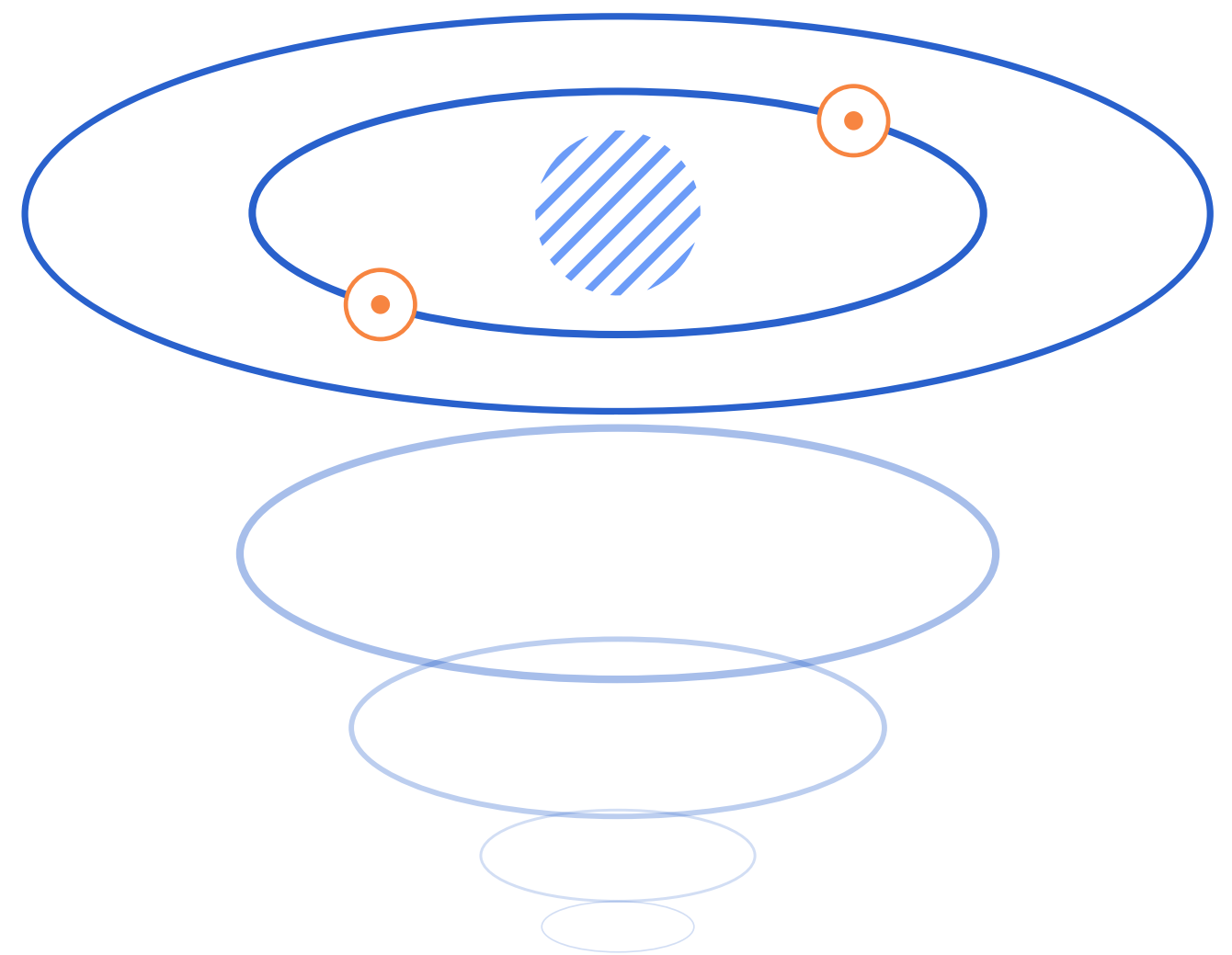


 Regulatory bodies ||  legislation

Purpose & Scope

This whitepaper aims to provide organizations and anyone interested in the subject with a dynamic and contextual overview of how AI-related regulations are shaping up in various countries. And, more importantly, how these regulations aim to protect the rights of individuals.

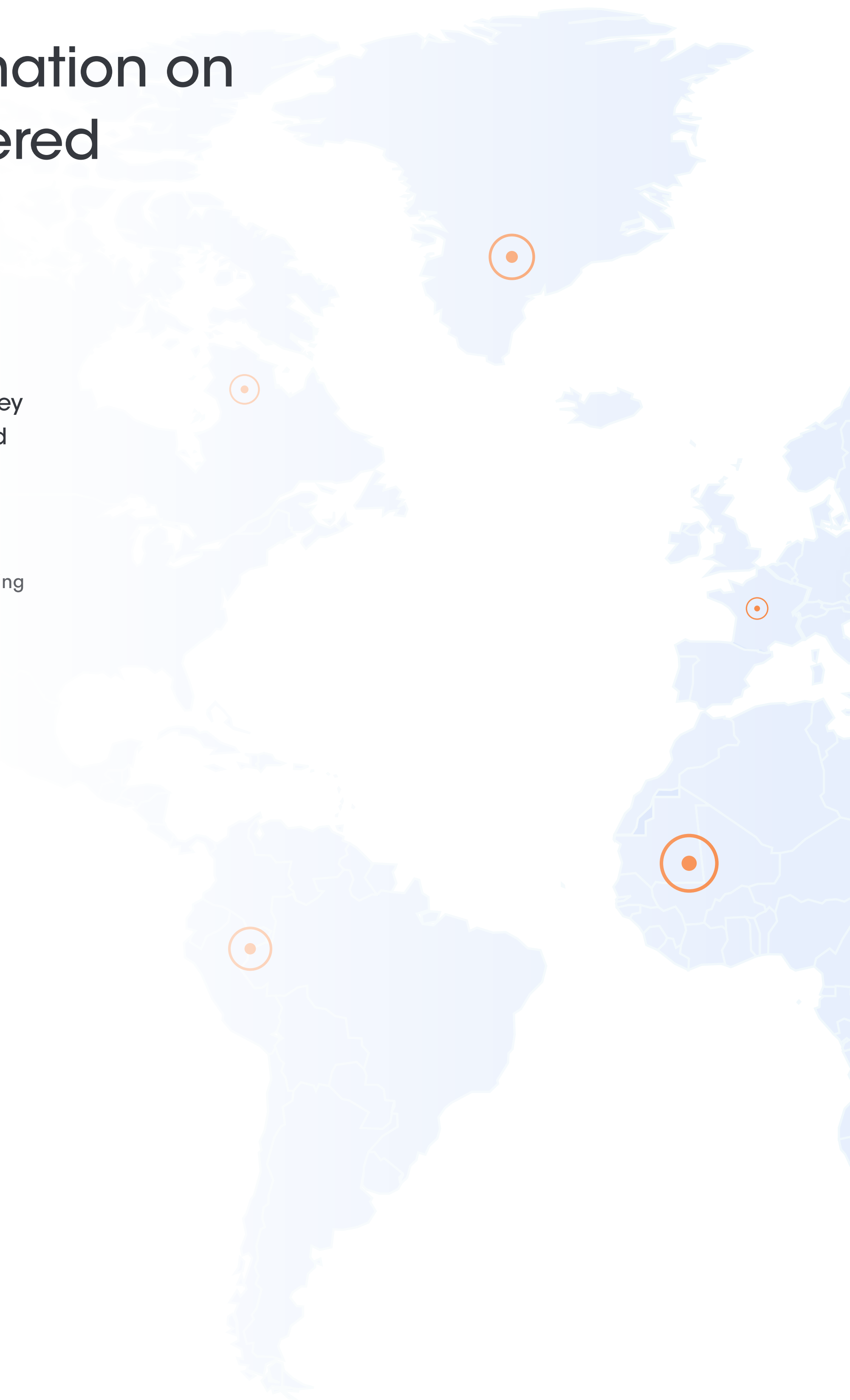
Each country and jurisdiction covered takes a unique and distinctive approach to legislation, with several federal, state, and municipal addendum guides.



Background Information on the Countries Covered

These countries and their AI regulatory efforts share several critical similarities but differ in key areas, depending on their specific needs and requirements.

As more and more countries begin their own legislative efforts related to regulating AI, this list will expand, giving the readers a holistic insight into the state of global AI regulations.



AI Regulations in the United States

Overview of Relevant Regulations

Currently, the United States (US) does not have dedicated AI legislation in force, nor have the legislators proposed one to date. Unlike the European Union (EU), so far, the US has taken a mixed approach towards AI governance characterized by general guidelines e.g., [Guidance for Regulation of Artificial Intelligence Applications](#), [Blueprint for an AI Bill of Rights](#), etc. as well as measures like [securing voluntary commitments from leading AI companies](#). At the same time, federal agencies have been active in regulating AI within their specific sectors.

Regulation by Federal Agencies

Among the federal agencies, the Federal Trade Commission (FTC) has been at the forefront of ensuring that AI use is not unfair and deceptive. Following are some guidelines issued by the FTC to make sure that AI is used responsibly:

- [Using Artificial Intelligence and Algorithms guidelines](#),
- [Aiming for truth, fairness, and equity in your company's use of AI](#)
- [Keep your AI claims in check](#),
- [Chatbots, deepfakes, and voiceclones: AI deception for sale](#),
- [The Luring Test: AI and the engineering of consumer trust](#)

In addition, the US Department of Defence's [AI Principles: Recommendations on the Ethical Use of Artificial Intelligence](#), the US Food and Drug Administration's [Artificial Intelligence/Machine Learning \(AI/ML\)-Based Software as a Medical Device \(SaMD\) Action Plan](#), the Department of Health & Human Services' [Trustworthy AI Playbook](#), and the Consumer Financial Protection Bureau's [Rules to Implement the Dodd-Frank Act](#) are among the AI regulatory guidances issued by the federal agencies in their respective domains.

State/City Regulations

Following are some of the laws enacted by the US states and cities to govern specific uses of AI within their jurisdictions:

- [Illinois' Artificial Intelligence Video Interview Act](#) requires all employers using AI technologies to analyze candidates interviewing for employment positions to appropriately inform all applicants and gain their consent before subjecting them to this automated processing.
- [New York City's Law on Automated Employment Decision Tools](#) expressly prohibits employers from using an automated employment decision tool (AEDT) to make an employment decision unless the tool is audited for bias annually, the employer publishes a public summary of the audit, and the employer provides certain notices to applicants and employees who are subject to screening by the tool.
- [San Jose's Generative AI Guidelines](#) provide for rules regarding the use of generative AI, including the governing principles, measures to assess and mitigate risks associated with using generative AI, etc.

Key Obligations

Based on the guidelines issued by the federal government and the federal agencies, the following are some of the key obligations which the organizations should comply with while developing or employing AI:

Data Privacy

Organizations should protect consumers from abusive data practices via built-in protections, and the consumer should have an agency over how data about the consumer is used.

Notice & Disclosure

Organizations should be transparent about the use of AI. Organizations should disclose to the consumers that an automated system is being used and should also enable them to understand how and why it contributes to the outcomes that impact the consumer.

Algorithmic Discrimination Protection

Organizations should take appropriate measures to ensure that consumers do not face discrimination by algorithms. AI systems should be used and designed in an equitable way.

Safe & Effective Systems

Organizations should develop and deploy AI systems that are safe for consumers. Consumers should be protected from ineffective and unsafe systems.

Opt-out Requirements

Organizations should provide consumers with an option to opt-out of data collection.

Deletion and Minimization Requirements

Organizations developing or deploying AI should collect the minimum data from the consumer necessary for their operations and should also provide mechanisms for the consumers to delete their data from existing datasets.

Other Applicable Guides, Considerations, and Policies

Here are some other critical guides, considerations, and frameworks:

→ [AI Risk Management Framework](#)

Issued by the National Institute of Standards & Technology, this framework aims to ensure organizations designing, developing, deploying, or using AI systems have adequate resources to promote the trustworthiness of their products via responsible development;

→ [Generative Artificial Intelligence and Data Privacy](#)

Published by the US Congressional Research Service, this report sheds light on privacy issues and policy considerations in the data collection context by AI developers.

Opinions of Industry Leaders in the US

Min Hwan Ahn, the owner of Ahn & Sinowitz, believes that in a country like the United States, it is improbable that a one-size-fits-all approach can be adopted when it comes to AI regulation. He highlights a cultural difference between the US and the EU, stating that the US regulations are more likely to focus on privacy concerns and fairness in decision-making, such as the FTC's Equity guidelines.

Ryan, the owner at OrganicallySEO, highlights the role individual departments will play in ensuring AI is appropriately leveraged. He points out the US Copyright Office's implication on how AI-generated art or content cannot be copyrighted. In such an environment, a sound combination of human ingenious and AI capabilities will likely be the order of the day for years to come.

Kyle Sobko, CEO of Sonder Care, corroborates the aforementioned thought by highlighting how the National Institute of Standards and Technology (NIST) has been actively working on defining AI standards and recommendations, focusing on topics like bias, transparency, and explainability.

AI Regulations in the European Union



Overview of Relevant Regulations

The European Union's proposed [Artificial Intelligence Act](#) (AI Act) looks perfectly poised to play the same role for AI-related regulations globally as the General Data Protection Regulation (GDPR) did for privacy regulations in 2018. The AI Act is one of the first comprehensive laws on AI globally.

The AI Act classifies AI systems into four distinct categories based on the risks they pose to the consumers and the obligations of the covered entities vary depending upon the category of AI system under consideration. Most of the compliance obligations provided under the AI Act apply to high-risk AI systems, whereas the use of AI systems that pose unacceptable risk i.e., endanger people's safety, livelihood, and fundamental rights, is completely prohibited.

Covered Entities

The AI Act will apply to the following entities:

- Providers placing on the market or putting into service AI systems in the European Union, irrespective of whether those providers are established within the Union or in a third country;
- Users of AI systems located within the European Union;
- Providers and users of AI systems that are located in a third country, where the output produced by the system is used in the European Union.

However, AI systems developed solely for military purposes will be exempt from the application of the AI Act. In addition, the law will also not apply to any public authorities in a third country or international organizations using these AI systems under international agreements or judicial cooperation.

Effective Date

The AI Act is expected to be adopted by late 2023 or early 2024 after due consideration, discussion, and necessary adjustments due to dynamic AI developments.

Key Obligations

Following are some of the key obligations under the AI Act for organizations dealing in high-risk AI systems:

Technical Documentation

Organizations are required to draw up the technical documentation of a high-risk AI system before the system is placed on the market.

Risk Management System

Organizations must establish, implement, document and maintain risk management systems in relation to the high-risk AI systems. The organizations must run the following steps throughout the lifecycle of the high-risk AI system:

- identification and analysis of the known and foreseeable risks associated with each high-risk AI system;
- estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;
- evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system;
- adoption of suitable risk management measures.

Accuracy, Robustness and Cybersecurity

Organizations must design and develop high-risk AI systems to ensure an appropriate level of accuracy, robustness, and cybersecurity throughout their lifecycle.

In addition to the above, organizations can be subject to various other obligations under the AI Act depending upon their role as a developer, providers, importers, distributors, or users of AI systems.

Data Governance

The organizations using high-risk AI systems that involve the training of the models with data must ensure that such models are developed based on training, validation, and testing data sets that are subject to appropriate data governance and management practices, particularly related to the following:

- the relevant design choices;
- data collection;

- c. relevant data preparation processing operations, such as annotation, labeling, cleaning, enrichment, and aggregation;
- d. the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;
- e. a prior assessment of the availability, quantity, and suitability of the data sets that are needed;
- f. examination in view of possible biases;
- g. the identification of any possible data gaps or shortcomings and how those gaps and shortcomings can be addressed.

The organizations must ensure that the training, validation, and testing data sets are relevant, representative, error-free, and complete.

Record Keeping

The organizations must design and develop high-risk AI systems with built-in capabilities of automatic recording of events ('log'). The logging capabilities must provide, at minimum, the following:

- a. recording of the period of each use of the system (start date and time and end date and time of each use);
- b. the reference database against which input data has been checked by the system;
- c. the input data for which the search has led to a match;
- d. the identification of the natural persons involved in the verification of the results.

Transparency and Disclosure

Organizations must make the operation of a high-risk AI system transparent for the consumers enabling them to interpret the system's output and use it appropriately. The organizations must also provide the users with instructions that are relevant, accessible, and comprehensible and specify the following:

- a. the identity and contact details of the provider and, where applicable, of its authorized representative;
- b. the characteristics, capabilities, and limitations of performance of the high-risk AI system, including:
 - i. its intended purpose;
 - ii. the level of accuracy, robustness, and cybersecurity against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness, and cybersecurity;
 - iii. any known or foreseeable circumstance related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights;
 - iv. its performance as regards the persons or groups of persons on which the system is intended to be used;
 - v. when appropriate, specifications for the input data or any other relevant information in terms of the training, validation, and testing data sets used, taking into account the intended purpose of the AI system.
- c. the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;
- d. the human oversight measures, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;
- e. the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.

Human Oversight

The organizations must design and develop high-risk AI systems in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during their use.

Organizations can ensure human oversight by either of the following two ways:

- a. identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service; or
- b. identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

Other Applicable Guides, Considerations, and Policies

Here are some other critical guides and considerations related to the use of AI within the European Union:

→ [AI and Personal Data Guidance](#)

A document published by the Confederation of European Data Protection Organisations (CEDPO) for Data Protection Officers (DPOs) on how their responsibilities will evolve in an era dominated by artificial intelligence and machine learning;

→ [The Ethical Use of Artificial Intelligence](#)

Guidelines issued by the European Commission on ensuring privacy and personal data are protected, both when building and running an AI system.

Opinions of Industry Leaders in the EU

Anthony Buzzetta, CEO & Founder of G Tier, believes that the EU has already taken a global leadership role in terms of AI regulation owing to just how comprehensive the AI Act is. Other countries have undertaken some sector-specific guidelines or executive orders in the US, but nothing compares to the sheer scale of the EU's AI Act.

Henri Hubert, founder of AI Engineering Hub, not only supports the aforementioned view of the EU as the global leader in AI regulations but states that it is also well-poised to be a highly pro-business legislation owing to how it avoids the pitfalls of overregulation and leaves enough room for EU-based organizations to continue leveraging AI for innovation.

AI Regulations in the United Kingdom



Overview of Relevant Regulations

The United Kingdom's [Data Protection and Digital Information \(No. 2\) Bill](#) ("Bill") is expected to cover the UK government's legislative stance on AI. The Bill will now undergo a report stage and a third reading, with dates yet to be announced; Amendments to the Bill's official text will be made at the report stage, with the Speaker selecting the appropriate amendments for debate in the House.

Covered Entities

The Bill's exact scope and applicability will be known once the legislative process moves forward. However, since the Bill provides extensive amendments to the already existing data protection framework of the UK, it seems that the covered entities would be organizations handling personal data and using AI-powered automated decision-making to process such data.

Effective Date

The Bill's effective date is unknown and will be announced once the legislative process moves forward.

Key Privacy Obligations

All covered entities engaging with AI will have the following critical obligations per Bill's current text:

Explicit Consent

Automated decision-making with special personal data requires explicit consent or legal obligation. The controller must provide information, allow the data subject to express opinions, request involvement, and enable contesting of decisions.

Designated Individual & Security Measures

The data controller and processor must designate one individual to be the person bearing individual responsibility for an organization's data practices. Additionally, organizations need to take organizational, technical, and physical measures to ensure that processing is taking place in a secure and lawful manner

Records of Processing Activities

The data controller must maintain a comprehensive record of all processing activities, whether performed directly or by a third party on its behalf. This record should include the following information:

- a. storage location of personal data, especially if stored outside the UK;
- b. purposes of data collection;
- c. categories of third parties with whom data has been shared;
- d. data retention duration;
- e. presence of special categories of data, if any; and
- f. whether the data includes details related to criminal convictions and offenses.

Cookie Consent

Under the Data Bill, prior consent is not needed in specific situations, including when providing an information society service, using tracking technologies for statistical and service enhancement purposes, updating software for system security, and identifying geolocation in emergency cases. However, organizations must offer clear and comprehensive information to users about their personal data collection at or before the point of collection for each of these exemptions.

Other Applicable Guides, Considerations, and Policies

Some other relevant guides, considerations, and policies related to AI within the United Kingdom include:

→ [Guidance on AI and Data Protection](#)

A detailed document released by the ICO on how to apply the principles of the UK GDPR to the use of information in AI systems;

→ [AI and Data Protection Risk Toolkit](#)

A toolkit released by the ICO to aid organizations in assessing the risks to individual rights and freedoms caused by their own AI systems;

→ [Data Ethics Framework](#)

A guidance issued by the UK government for public sector organizations on how to use data appropriately in planning, implementing, and evaluating a new policy or service;

→ [A Pro-Innovative Approach to AI Regulation Whitepaper](#)

A whitepaper released by the UK government on how existing legal frameworks can be leveraged to regulate the use of AI via technology-neutral legislation;

→ [Generative Artificial Intelligence in Education Whitepaper](#)

A whitepaper issued by the Department of Education on the potential impact of Generative AI on education.

Opinions of Industry Leaders in the UK

Allan McNabb, the VP of Image Building Media, believes organizations can ensure compliance with the UK's current and future AI regulations by staying informed, establishing internal governance, implementing clear policies, conducting audits, fostering a responsible AI culture, and collaborating with regulators and industry peers.

These may seem overly simplistic, but most organizations that run afoul of regulations are usually found negligent of the most fundamental requirements.

AI regulation in the UK is unlikely to place strenuous demands on enterprises other than asking them to exercise basic documentation and internal controls.

At the same time, David Cohen, the CEO of Badais International, believes that the recommendations and findings of the recently established AI Council will be of particular importance, specifically within the fields of data protection, algorithmic transparency, and bias mitigation.

AI Regulations in Australia



Overview of Relevant Regulations

Australia does not yet have a dedicated federal AI regulation. In lieu of AI regulation, the government has published regular policy papers to guide various regulatory bodies on approaching AI's ever-growing financial, political, and social influence.

Other Applicable Guides, Considerations, and Policies

Here are some other critical frameworks, guides, and documents necessary to understanding AI regulation in Australia:

→ [Artificial intelligence assurance framework](#)

The state of New South Wales (NSW) introduced the first AI strategy, prioritizing safe AI usage across the government with proper safeguards. It covers large language models and generative AI. The framework guides project teams, operational teams, Senior Officers, assessors, and the AI review body;

→ [The Artificial Intelligence Ethics Framework](#)

A guide published in 2019 for government and private bodies on how to responsibly design, develop, and implement AI in Australia;

→ [The Australian Human Rights Commission Human Rights and Technology Final Report](#)

A report calling for the establishment of an independent AI safety commissioner to oversee various aspects related to commercial AI use in Australia; and

→ [The Blueprint for Critical Technologies](#)

A government document published in 2021 to provide appropriate guiding resources to develop a "framework for capitalizing on critical technologies to drive a technologically-advanced, future-ready nation."

Opinions of Industry Leaders in Australia

Simon Brisk, CEO of Click Intelligence, believes Australia's preference for relying on minimal regulation will benefit small and medium businesses in leveraging AI capabilities.

Such an approach allows room for innovation and possible future regulation based on the unique market demands. Furthermore, that'll help cultivate an enterprise-driven culture of ethics and accountability.

AI Regulations in Canada

Overview of Relevant Regulations

To date, Canada does not have a dedicated AI regulation in force. However, in June 2022, the Government of Canada tabled the landmark Artificial Intelligence and Data Act (AIDA) as part of the Omnibus Bill C-27, the Digital Charter Implementation Act 2022.

AIDA aims to:

- a. regulate international and interprovincial trade and commerce in AI systems by establishing common requirements for the design, development, and use of those systems; and
- b. prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests.

Covered Entities

AIDA applies to any person who carries out the following activities in the course of international or interprovincial trade and commerce across Canada ('regulated activities'):

- processing or making available for use any data relating to human activities for the purpose of designing, developing, or using an artificial intelligence system; and
- designing, developing, or making an artificial intelligence system available or managing its operations.

However, the provisions of AIDA do not apply to government institutions or any product, service, or activity under the direction or control of a government institution or a person responsible for a federal or provincial department or agency.

Effective Date

AIDA does not provide an effective date. However, as per [the AIDA Companion document](#), the regulations will come into effect sometime in 2025.

Key Obligations

AIDA provides for a number of compliance obligations for the covered entities, focusing on identifying, mitigating, and notifying any potential risks of harm to the consumers. It is pertinent to note that the true scope of the obligations under AIDA will be determined by their respective applicable regulations, yet to be issued by the Governor in Council and the Minister.

Following is a brief overview of the obligations of the covered entities under AIDA:

Data Anonymization

The entities who carry out regulated activities and process or make available for use anonymized data in the course of a regulated activity must, in accordance with the applicable regulations, establish measures with respect to:

- a. the manner in which data is anonymized; and
- b. the use or management of anonymized data.

AI System Assessment

A person responsible for an AI system must make an assessment of whether the specific AI system is a high-impact system, as defined under the applicable regulations.

A person is responsible for an AI system if the person designs, develops, or makes available for use an AI system or manages its operation during the course of international or interprovincial trade and commerce.

Risk Assessment

A person responsible for a high-impact system must, in accordance with the applicable regulations, establish measures to identify, assess, and mitigate the potential risks of harm or biased output that could result from the use of the high-impact system.

Risk Monitoring

In addition to identifying potential risks of harm and taking measures to mitigate those risks, a person responsible for a high-impact system must also, in accordance with the applicable regulations, establish measures to monitor the compliance with the mitigations measures as well as the effectiveness of the said measures to deal with the identified risks.

Notification of Material Harm

The persons responsible for high-impact systems are also required, as per the applicable regulations and as soon as feasible, to notify the Minister if the use of the system results or is likely to result in material harm.

Record Keeping

The entities carrying out the regulated activities must keep the following records:

- a. the measures established for data anonymization, risk assessment, and risk monitoring; and
- b. the reasons supporting their assessment of an AI system i.e., whether an AI system is a high-impact system or not.

In addition, the entities must also keep general records of their obligations, as prescribed under the applicable regulations.

Disclosure Requirements

AIDA provides several disclosure requirements for persons making high-impact systems available for use and those managing high-operating systems. The entities must publish on a publicly available website, in accordance with the applicable regulations, a plain-language description of the high-impact system, including the following details:

- a. how the system is used or intended to be used;
- b. the types of content that the system generates or intends to generate and the decisions, recommendations, and predictions the system makes or intends to make;
- c. the risk mitigation measures established with respect to the system; and
- d. any other information prescribed under the applicable regulations.

Other Applicable Guides, Considerations, and Policies

Some of the other relevant AI-related guides, considerations, and policies include the following:

→ [Regulatory Framework for AI](#)

A list of recommendations released by the Office of the Privacy Commissioner of Canada (OPC) related to several amendments and additions to the regulation of AI within the Personal Information Protection and Electronic Documents Act (PIPEDA);

→ [Ontario's Trustworthy Artificial Intelligence \(AI\) Framework](#)

A report published by the provincial government of Ontario on the role the provincial government could play in ensuring the safe and reliable use of AI;

→ [Responsible Use of Artificial Intelligence \(AI\)](#)

A report issued by the federal government of Canada on the internal measures its various departments and agencies can adopt for the responsible and accountable use of AI;

→ [Directive on Automated Decision Making](#)

A policy directive released by the federal government of Canada related to responsible corporate use of AI in matters related to decision-making within the public sphere.

→ [Canadian Center for Cyber Security's Guidance on Generative AI:](#)

A guidance on potential risks associated with the use of generative AI and mitigation measures that can be adopted by organizations as well as individuals

Opinions of Industry Leaders in Canada

Dave Conway, a co-founder at EcoMotionCentral, points out that Canada has adopted a mixed approach to AI regulation. It has allowed its provinces to legislate per their requirements while releasing policy directives to officially state how organizations offering AI services should operate within the public sphere.

At the same time, AIDA aims to ensure that a clear set of rules are in place to guarantee the use of AI responsibly and ethically.

AI Regulations in Brazil

Overview of Relevant Regulations

Over the past few years, there have been regular discussions within legislative bodies in Brazil related to establishing legal frameworks governing artificial intelligence. These discussions finally bore fruit when in December 2022, the Commission of Legal Experts delivered its first report on what became the first draft of Bill of Law 2338/2023.

The Brazilian Senate announced in May 2023 that it was analyzing the text of the Bill. If approved, the Bill would establish user rights in light of artificial intelligence systems, transparency requirements, penalties for violations, and a supervising body overseeing law enforcement.

Covered Entities

In its current form, the Bill applies to all AI agents, including the providers and operators of the AI systems.

Effective Date

More information will be on this once the Senate passes the Bill and it becomes an official law within Brazil.

Key Obligations

Following a risk-based approach, the proposed law classifies the AI systems into Excessive-risk AI systems and High-risk AI systems. While the use of the former is completely prohibited, the latter is subject to a number of mandatory requirements, including the following:

Preliminary Assessments

The providers of the AI systems must conduct a preliminary risk assessment before placing on the market or putting into service an AI system. Based on the preliminary assessment, the providers must categorize the AI systems into excessive-risk or high-risk AI systems.

Notification of Serious Incidents

The AI agents must notify the regulatory authority about the occurrence of serious security incidents, 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.

Governance Frameworks

The providers and the operators of the AI systems must establish internal processes, including the following, to ensure the security of the AI systems as well as to fulfill the rights of the affected persons:

- a. transparency measures regarding the use of AI systems in their interactions with natural persons;
- b. transparency regarding governance measures adopted within the development and employment of the AI system;
- c. appropriate data management measures for mitigating and preventing potential discriminatory biases;
- d. data processing compliance with the data protection laws and regulations and the adoption of techniques that minimize the use of personal data;
- e. adoption of adequate parameters of dataset separation and organization for training, testing and validation of the system outcomes; and
- f. adoption of adequate security information measures from system design to operation.

In the case of high-risk AI systems, the following additional governance measures must also be adopted:

- a. documentation about how the system works and the decisions involved in its building-up, implementation, and use;
- b. use of tools for the automatic recording of the system's operation;
- c. conducting tests to assess appropriate levels of reliability, depending on the industry and type of application of the AI system;
- d. data management measures to mitigate and prevent discriminatory biases; and
- e. adoption of technical measures enabling the explainability of the AI system's outcomes and interpretation of the outcomes.

Algorithmic Impact Assessment

For the AI systems deemed high-risk as a result of the preliminary assessment, the AI agents must conduct an algorithmic impact assessment, which must consider and record at least the following:

- a. known and foreseeable risks associated with the AI system;
- b. the benefits associated with the AI system;
- c. the likelihood of adverse consequences, including the number of people potentially impacted;
- d. the severity of the adverse consequences, including the effort required to mitigate them;
- e. the operating logic of the AI system;
- f. the process and the result of testing and evaluation and mitigation measures;
- g. training and actions to raise awareness of the risks associated with the AI system;
- h. mitigation measures and indication and justification of the residual risk of the AI system, accompanied by quality control testing on a regular basis; and
- i. transparency measures to the public, especially to potential users of the system, regarding residual risks whenever such risks involve a high level of harmfulness or danger to the users' health or safety.

More importantly, AI regulations have proliferated with the rise in AI capabilities over the past few years. Hence, they're unlikely to be set in stone, with regular amendments to follow reflecting the evolving nature.

A proactive approach towards compliance in such a scenario would help organizations adjust their compliance efforts accordingly.

At the same time, Matthew Anderson, the Founder of Random Timer, believes that the key to compliance with the Bill of Law 2338/2023 will require adapting the same sound data governance policies that have proven fruitful for organizations over the past couple of years.

Of course, the exact tactics and measures necessary will not become apparent until the final draft of the proposed regulation is approved and passed, but staple mechanisms such as risk assessments for high-risk systems, human-in-the-loop framework, privacy and security by design, and a proactive approach to internal accountability should form the basis for any organization's compliance policy with respect to the Bill of Law 2338/2023.

Opinions of Industry Leaders

Brazil represents a fairly unique case as far as AI regulations are concerned.

William Davis, the Chief Technology Officer at EcoMotionCentral, states that once the proposed Bill of Law 2338/2023 comes into effect, organizations must adopt a highly proactive mindset toward compliance akin to LGPD compliance efforts. These will include AI ethics and compliance training for the regular workforce with similar AI governance workshops for the higher-ups.

AI Regulations in China

Overview of Relevant Regulations

AI-related regulations in China are a much more localized affair with various decrees and laws being passed for application within specific provinces and sectors. For a country as expansive as China, this allows for better application of laws with relevant requirements based on each region or sector's needs. More importantly, such laws can then be amended and adjusted accordingly with greater efficiency.

Management of Generative Artificial Intelligence Services (AI Measures)

Covered Entities

The AI Measures are applicable to the use of Generative AI (GenAI) technology when offering GenAI services to the public within China's territory (People's Republic of China, PRC).

Effective Date

The Cyberspace Administration of China (CAC) published the AI measures on July 13, 2023. The AI Measures will come into effect on August 15, 2023.

Key Obligations

The AI Measures outline a number of obligations for the GenAI providers. These include:

Data Processing Activities Training

Providers must carry out training data processing activities, encompassing pre-training and optimization training, strictly adhering to the law. They must ensure the use of legitimate data sources and models, respect intellectual property rights, obtain consent for using personal information, improve data quality, and comply with relevant laws and regulations.

Security Assessments

Providers with public opinion or social mobilization attributes must conduct security assessments as per state regulations and complete algorithm filing procedures according to the Internet Information Service Algorithm Recommendation Management Regulations.

Vendor and User Agreements

The AI Measures stipulate that providers have responsibilities for the actions of network content producers and network information security obligations according to relevant laws. To safeguard personal information and comply with the law, providers must establish binding agreements with vendors, outlining their obligations and regularly monitoring their compliance. Additionally, providers are required to enter into service agreements with users, clearly defining the rights and obligations of both parties.

Data Labeling

During the research and development of GenAI technology, providers must adhere to certain guidelines for data labeling. This includes establishing clear and specific labeling rules, conducting quality assessments, verifying labeling accuracy through sampling, providing necessary training for labeling personnel to ensure legal compliance, and supervising and guiding labeling personnel to maintain standardized labeling practices.

Monitoring and Complaint Mechanism

The Providers must regularly monitor their GenAI services and promptly take action against illegal content. They should also address users engaging in illegal activities and maintain records, reporting to the relevant authority. Additionally, the Providers must establish a complaint mechanism, handle complaints promptly, and provide feedback on resolutions.

Rights of Users

The AI Measures grant users certain rights, and providers must promptly handle requests from individuals to exercise these rights. Users have the right to review, obtain a copy, correct, supplement, and delete their personal information. Additionally, users can file complaints and report GenAI services that do not comply with the relevant laws, regulations, and AI Measures.

China - Shenzhen Regulations

Covered Entities

These regulations apply to all activities directly and indirectly related to the development of AI Science & Technology (S&T), in-depth integration, and application of AI in economic and social fields within the Shenzhen Special Economic Zone.

Effective Date

This regulation was adopted at the 11th session of the Standing Committee of the Seventh People's Congress of Shenzhen Municipality on August 30, 2022.

Key Obligations

Here are some of the critical obligations of covered entities as well as the administrative authorities:

Adherence to Guiding Principles

All AI developers must ensure that the development of the municipality's AI industry follows the principles of being technology-led, application-driven, people-centered, secure, and controllable.

Risk and Security Assessments

Organizations and individuals engaged in AI research and application shall abide by AI ethical and security norms and carry out relevant activities within a reasonable scope. Such entities must review ethical and security norms and conduct risk assessments on the possible adverse effects of AI products and services on national interests, public security, commercial order, and individual rights and interests.

TM Intellectual Property Rights Protection

Organizations must also develop mechanisms to ensure intellectual property protection for new technologies, new business formats, and new models and promote the establishment of an intellectual property protection system in the AI industry field.

Use of Data from Public Platforms

Individuals and organizations engaged in AI research and applications are encouraged to rely on public data open platforms, develop AI products and services, and promote innovative applications of public data in AI scenarios.

Anonymization of Data

Organizations and individuals engaged in AI research and applications that provide legally obtained personal data to external parties must anonymize that data.

China - Shanghai Regulations

Covered Entities

These regulations apply to all activities directly and indirectly related to the development of AI Science & Technology (S&T), industrial development, application empowerment, and industrial governance within the administrative region of Shanghai.

Effective Date

These regulations came into effect on October 1, 2022.

Key Obligations

Here are some of the critical obligations of covered entities as well as the administrative authorities:

Safeguarding Rights and Interests

Industry organizations in the AI sector must safeguard their members' legal rights and interests. They should encourage AI technology research and promotion, foster collaboration within the industry, enhance self-regulation, conduct industry monitoring, establish standards, and ensure orderly industry growth.

Establish Standards for Data Protection & other Technology

Industry organizations in the AI sector must take a leading role in formulating national standards, industry standards, and local standards for AI and participate in formulating technical standards for algorithm performance, data security, privacy protection, product compatibility, and performance testing. They should also formulate standards for robot intelligence level categorization and application safety testing and guide the iteration of intelligent robot technology.

Risk Determination

AI developers must implement a checklist management style for all identified high, medium, and low-risk AI products, with pilot trials for products deemed safe by various departments.

Prohibited Activities in the AI Field R&D

All organizations involved in AI field R&D must not engage in the following activities under any circumstances:

- a. Provide products and services that endanger national, social, and public safety;
- b. Provide products and services that endanger the safety of people or the property of people or infringe on their privacy and information rights;
- c. Provide products and services that discriminate against users based on ethnicity, race, gender, age, occupation, or religious belief;
- d. Develop and use algorithmic technology for the specific purpose of price discrimination, consumer fraud, or other behaviors that harm the rights and interests of consumers;
- e. Use deep synthesis technology to engage in activities prohibited by the state;
- f. Provide products and services that violate other relevant local, national, and international regulations.

Other Applicable Guides, Considerations, and Policies

Here are some other sources and guides organizations should keep in mind when dealing with AI regulations in China:

→ [A Next Generation Artificial Intelligence Development Plan](#)

A roadmap issued by the State Council of the People's Republic of China on how various state and private institutions can help in the development, deployment, and oversight of AI technologies in a responsible manner;

→ [Code of Ethics for New-Generation Artificial Intelligence](#)

A guide issued by the National Special Committee of New-Generation Artificial Intelligence to ensure all future AI technology is in line with six critical ethical standards;

→ [Measures for the Management of Generating Artificial Intelligence Services](#)

A set of draft measures issued by the Central Cyberspace Affairs Commission to ensure the development and application of Gen AI tech aligns with China's other privacy regulations via independent security assessments before deployment.

Opinions of Industry Leaders in China

Oliver Goodwin, the founder and CEO at Synthesys, points out a distinct area where China stands out from the rest of the world. Facial recognition and its usage are heavily regulated within China's several regulations on data privacy, cybersecurity, and AI.

Thoriq Noor further adds that compared to the rest of the countries on this list, China has a noticeably more "state-centric" model where the government has taken a fairly proactive role in AI development.

AI Regulations in Singapore

Overview of Relevant Regulations

Singapore has leaned towards economic initiatives incentivizing the responsible use and development of AI systems rather than strict regulation.

Other Existing Regulations

Several existing regulations were amended to either bolster the development of such capabilities or to mandate the adaptation of new mechanisms and processes reflecting the potential of AI within those specific domains. These include the following:

→ [The Cybersecurity Act of 2018](#)

The only major amendment to the 2018 Act was the requirement for all enterprises developing AI products and services to ensure all relevant security methodologies and mechanisms adopted are appropriately communicated to all users.

The privacy policy page on their website would be the most effective way for an organization to comply with this requirement.

→ [The Protection From Online Falsehoods and Manipulation Act 2019](#)

Also known as Singapore's anti-fake news law, it mandates technology companies to proactively counter fake news elements online.

Companies are incentivized to develop robust algorithms that identify, flag, and block all fake news content independently verified by fact-checkers. Offenders can be fined as much as \$200 for every single offense.

Google, Facebook, Twitter, SPH Magazines, WeChat, Baidu, and other similar platforms are designated as digital advertising and internet intermediaries subject to specific codes of practice.

→ [The Road Traffic \(Autonomous Vehicles\) Rules 2017](#)

Per the latest amendments to these rules, autonomous motor vehicles (AV) have been allowed to operate on public and private roads only if they have gained special authorization from the Land Transport Authority of Singapore (LTA).

The authorization will be for a specific geographical region, and the AV must undergo a trial before it can be given formal permission.

In case of any damages caused by the AV, the liability shall be completely over the individual who applied for the authorization for the AV and not the manufacturer themselves.

Other Applicable Guides, Considerations, and Policies

Here are some other important guides, roadmaps, and programs to know about AI regulation in Singapore:

→ [AI Singapore](#)

A government initiative launched in 2017 to increase collaboration between research institutions and the vibrant ecosystem of AI start-ups and companies developing AI products to perform use-inspired research, grow knowledge, create tools, and develop the talent to power Singapore's AI efforts

→ [Model AI Governance Framework](#)

Launched at the World Economic Forum in 2019, the Model Framework represents Singapore's pioneering role in making a unique contribution to the global discourse on AI ethics via practical recommendations that organizations could readily adopt to deploy AI responsibly;

→ [National Artificial Intelligence \(AI\) Strategy](#)

published in 2019, this policy approaches harnessing AI's potential for economic transformation. It involves identifying priority areas for national attention and resource allocation. Additionally, it emphasizes collaboration among the Government, companies, and researchers to maximize the positive impact of AI. Moreover, it addresses the need to manage change and address potential risks as AI becomes more prevalent in various sectors.

→ [AI Verify](#)

A special initiative by the Ministry of Communications & Information, AI Verify is a roadmap that helps boost AI testing capabilities and assurance to meet the needs of companies and regulators globally.

Opinions of Industry Leaders in Singapore

David Ly, CEO at Iveda, believes Singapore has adopted a careful approach of giving AI time and space to mature before it begins regulating it.

This approach has served it well in the past as it resisted regulating NFTs and cryptocurrencies before it had a better understanding of their long-term impact. Regulation done in such a manner proves more prudent while allowing innovation to flourish.

Similarly, Thoriq Noor, founder at Thoriq Noor and, more importantly, a resident of Singapore, shares his first-hand experience of how the Model AI Governance Framework has affected him professionally.

The guide has proven immensely valuable as an asset for organizations in addressing key ethical and governance issues when deploying AI solutions.

AI Regulations in Japan





Overview of Relevant Regulations

As of now, Japan does not have a dedicated federal AI regulation. In July 2021, the Ministry of Economy, Trade, and Industry (METI) published the [AI Governance in Japan Ver. 1.1 report](#), stating that legally binding horizontal requirements for AI systems are currently considered unnecessary.

However, since then, the government has chosen to amend several existing regulations to address AI's broader societal, financial, and political implications. These amendments aim to prevent the widespread negligent use of AI while encouraging organizations to voluntarily develop AI systems and mechanisms that adhere to Japan's guiding principles for AI technology development.

Some of the major regulations in Japan that have been amended as a result include the following:

→ [Road Traffic Act](#)

In April 2023, Japan officially began enforcing the revised Road Traffic Act of 1960.

Under the new amendments, self-driving cars that the Japanese authorities had cleared were safe enough for Japanese roads to operate.

Self-driving car manufacturers must submit detailed operation plans to the public safety commissions of every city they wish to operate in. Additionally, as part of the pilot program, each autonomous vehicle is to be monitored remotely by a person.

→ [Financial Instruments & Exchange Act](#)

The amendments to this regulation have been fairly minimal. Organizations involved in algorithmic high-speed trading must now register with the government.

Simultaneously, all organizations must develop and maintain a risk management system and detailed records of their transactions to ensure greater transparency.

→ [Digital Platform Transparency Act](#)

Specifically designed to curate how online search results are displayed to users.

Under the new amendments, all malls, app stores, and digital advertising businesses that advertise their products and services online must be transparent about any tactics and strategies that may affect their search rankings.

→ [Social Principles of Human-Centric AI](#)

A government guide issued in 2019 to lay down fundamental principles for individuals and enterprises developing AI systems;

→ [The Governance Guidelines for Implementation of AI Principles](#)

A government guide issued in 2022 with input from several industrial experts on how organizations may instill AI governance internally;

→ [The Guidebook on Corporate Governance for Privacy in Digital Transformation](#)

A joint document released by the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications with case study examples of responsible utilization of personal data and the construction of privacy governance within an AI context.

Opinions of Industry Leaders in Japan

Guillaume van de Laar believes Japan has focused on a human-centric society harmonized with AI. Rather than treat AI as a unique challenge or problem, as some other countries have, it chooses to see it as the usual indicator of the evergreen march of time.

This is reflected in its insistence on abstaining from regulating AI directly, instead letting organizations devise strategies that comply with the AI governance standards being adopted globally.

Additionally, wherever necessary, Japan has amended existing regulations to facilitate the use of AI.

Other Applicable Guides, Considerations, and Policies

Here are some other important guides and documents released that may help organizations in complying with current and future AI regulations in Japan:

How Can Securiti Help

AI regulations remain a highly dynamic domain. Nearly every country globally has been evaluating AI's financial, political, and social impact. At the same time, AI represents the dawn of the next industrial age, heralding a new chapter in productivity and capabilities.

With that in mind, it is critical that any legislation aiming to regulate AI and its usage does not stifle innovation. Hence, responsible regulation will be incalculably important.

The responsibility is even greater for organizations and enterprises that either use or proffer such AI services. Not only will they be subject to intense scrutiny in their overall usage of AI, but they will also likely find themselves having to adhere to extraordinarily diverse obligations owing to just how unique each country's regulatory attitude towards AI can be.

Attempting to honor these obligations manually can be an unnecessary strain on human and technical resources.

Securiti, a global leader in providing enterprise data privacy, security, compliance, and governance solutions, can greatly help.

Thanks to its DataControls Cloud™, an enterprise solution based on a Unified Data Controls framework, it can empower organizations to optimize their oversight and compliance with various data regulatory obligations.

Easy-to-use, deploy, and monitor, DataControls Cloud™ comes equipped with all the necessary modules and solutions necessary to ensure you can automate your various consent, privacy policy, and individual data requests-related obligations.

Similarly, numerous other modules, such as data mapping and lineage, allow for real-time tracking of all data in motion across different AI models or systems. Doing so helps in understanding data transformation over time with absolute transparency.

Request a [demo](#) today and learn more about how Securiti can help your organization comply with any AI-specific regulation you may be subject to.

Stay On Top Of All The Critical Information You Need To Know About AI-Related Relations Globally.

Achieve AI Compliance Today

[Sign up for a Demo](#)

[Learn More](#)