Crowell

PRIVACY & CYBERSECURITY OUTLOOK

The 2025 Landscape

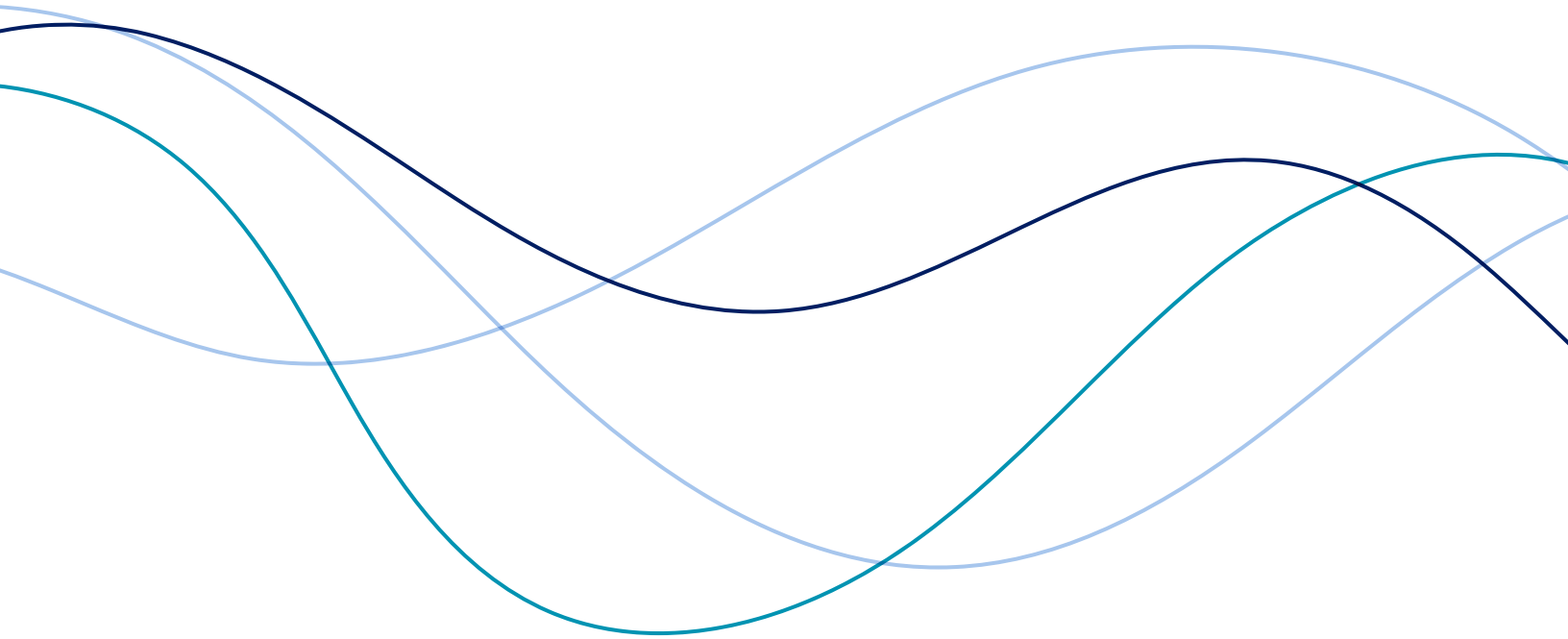
CONTENTS

INTRODUCTION

Crowell & Moring is proud to present our second edition of the year-end publication from our renowned Privacy and Cybersecurity Group. *The Privacy and Cybersecurity Outlook: The 2025 Landscape* offers clients forward-looking insights on the most significant trends impacting organizations worldwide, including developments in artificial intelligence (AI), critical infrastructure, the Asia-Pacific region, the Cybersecurity Maturity Model Certification process, and more.

For the first time this year, we are also pleased to offer a webinar to facilitate additional discussion around these critical topics, hosted by some of the attorney thought leaders at our firm who will share their perspectives on the real-world implications of these topics.

We hope you find the 2025 *Outlook* to be a valuable tool as you assess, plan, and respond to cybersecurity and privacy matters in the coming year. All of the articles from the Outlook are available here.



Changes to Critical Infrastructure Requirements

By Alexis Ward, Maida Oringher Lerner, Michael Gruden, and Evan Wolff

In 2025, owners and operators of critical infrastructure will have new security and information sharing obligations to consider under the National Security Memorandum 22 ("NSM-22" or the "Memorandum"). NSM-22 replaces the Obama-era Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21).

The Memorandum builds upon many of the foundations of PPD-21, while modernizing requirements and responsibilities to address technological advancements and increase collaboration. It also continues to focus on the 16 critical infrastructure sectors[1] originally defined in the PPD-21, managed under designated Sector Risk Management Agencies (SRMAs), but it also creates new obligations for critical infrastructure entities aimed at strengthening resiliency and enhancing cooperation within and among sectors. While it is unclear whether the requirements will continue to be in effect under the second Trump Administration, organizations may still want to consider preparations for actions under the Memorandum.

To create and enforce these new requirements, the NSM-22 establishes a new office to coordinate and increase cooperation between critical infrastructure sectors and SRMAs.

The new office, dubbed the Office of the National Coordinator, will be established by the Cybersecurity and Information Security Agency (CISA), underscoring the importance of cybersecurity to the new age of

critical infrastructure security. The Office of the National Coordinator will serve as a coordination point for all SRMAs and will be tasked with supporting the development of subject matter expertise, encouraging cooperation between critical infrastructure entities, consulting with the intelligence community, and assisting with the development and implementation of minimum security and resilience requirements.

Further, the Department of Homeland Security (DHS) will now be required to develop a National Information Risk Management Plan (National Plan) for critical infrastructure. The National Plan will be informed by sector-specific risk assessments conducted by the SRMAs and cross-sector risk assessments conducted by the Office of the National Coordinator. It will guide the federal actions to mitigate sector specific and cross-sector critical infrastructure risks. The plan will lay out the obligations and requirements for owners and operators of critical infrastructure, including long-term mitigation activities, minimum security and resilience requirements, and recommendations for pilot efforts.

[1] The 16 critical infrastructure sectors include: Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Services and Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and Water and Wastewater Sector.

NSM-22
now requires adoption of mandatory minimum security and resilience requirements developed by the federal government.

SIE
The National Coordinator is also tasked with identifying a list of **Systemically Important Entities.**

The responsibilities of owners and operators of critical infrastructure will become more demanding under the NSM-22. Noting that voluntary minimum security and resilience requirements have mitigated risk in the past, the NSM-22 now requires adoption of mandatory minimum security and resilience requirements developed by the federal government. The NSM-22 requires that DHS, SRMAs, and the National Coordinator use their authorities to develop and implement cross-sector and sector specific guidance and requirements. Notably, the NSM-22 requires that contracts now include appropriate audit rights in regards to these requirements and cybersecurity standards. The National Coordinator is also tasked with identifying a list of Systemically Important Entities (SIE). The SIE List will include organizations that own, operate, or control critical infrastructure whose disruption could cause significant national security impacts. Regulators are instructed to consider the list when developing and applying risk management requirements.

The Memorandum also creates new requirements to enhance the collection and sharing of threat information. The NSM-22 encourages information sharing between entities and creates requirements for the intelligence community. The Director of National Intelligence (DNI) is tasked with collecting information from intelligence reporting to identify threats to critical infrastructure. The director is also tasked with coordinating with DHS, SRMAs, federal and state entities, and the private sector to collect, analyze, and share information regarding the threats to critical infrastructure.

To prepare for the changes to come from the NSM-22, organizations should first understand whether they are considered owners and operators of critical infrastructure.

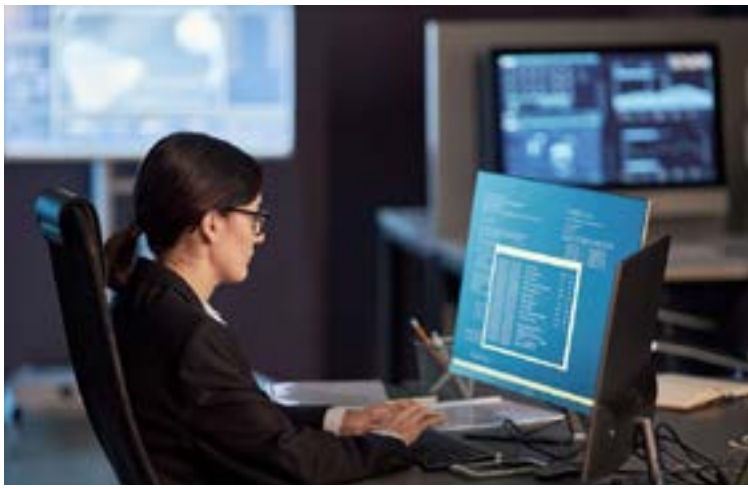
Owners and operators should be prepared to coordinate with their SRMA as it begins to draft a sector-specific risk management plan. Critical infrastructure organizations should also ensure that their systems are currently able to identify threats and that there are proper procedures in place for information sharing. The NSM-22 requires several reports to be developed and delivered in 2025, so organizations should continue to monitor these developments to understand what new requirements may be coming for their sector.

A Changing Tech and Legal Landscape in Corporate

By Bryan Brewer, Alexis Ward, and Candice Gwak

Whether it is personal, customer, training or other data, one thing is clear: data continues to be an important currency and revenue driver for companies. Rapidly changing technology, coupled with developing regulations, requires companies that use or disclose data to be extremely vigilant to stay current. Today, companies struggle to keep up with seemingly nonstop changes to state-level law. These struggles are exacerbated by quickly developing regulations and regimes overseas—creating challenges for international data transfers and international transactions. To optimize the value of their data into 2025 and beyond, companies should consider addressing these challenges with a new focus and additional precision in their commercial agreements.

One of the fastest developing verticals, in terms of both technology advancement and the law, is artificial intelligence. Because of these rapid changes, companies should carefully consider the potential impact of AI on their assets and agreements. AI has made and likely will continue to make data assets even more valuable, but it most certainly will introduce new challenges and risks, including in the privacy and cybersecurity and intellectual property areas, if it is not properly managed. Companies should first consider assessing what their existing agreements mandate regarding AI in these areas. They should also consider what type of data is being used and/or potentially developed under applicable contracts. Companies may want to carefully consider what information disclosure they require from counterparties about the counterparties' use of AI, including whether and in what context they are using AI. It, then, may also benefit companies to consider what data protection provisions may need to be added to existing contracts, as well as what should



be included in future agreements, such as provisions regarding the use of the company's data as training data for AI. Companies should also consider how the parties will address new and developing laws that are introduced during the term of such agreements. Additionally, with new AI regulations and regimes developing, companies will need to ensure that anyone processing their data does so in compliance with these new regimes.

Further, as management of data becomes more complex, companies should consider implementing additional fail-safes to protect their data and information.

Companies may want to assess what kind of information disclosures are appropriate to require of counterparties in transactions in order to be fully informed around the AI use cases. Companies should also consider what types of off-ramp termination provisions should be included in their transactions if a counterparty is not meeting stated data processing requirements, protection goals, or required informational covenants.

Transactions involving complex data and cybersecurity components may even usher a wider use of cutting edge, party-friendly contracts.

Organizations may turn to **visual contracts** in lieu of dense, technical language that may not define a system as clearly as a simple network diagram.

Visual contracts are legally binding agreements that are designed with an emphasis on visual components such as charts, diagrams, and illustrations. Visual contracts could be particularly useful in agreements involving the diagraming of networks or scoping of important system boundaries. Organizations may turn to visual contracts in lieu of dense, technical language that may not define a system as clearly as a simple network diagram. Even further, companies are beginning to explore how virtual contracts might be developed using AI itself, where the parties ask a question about an obligation to an interface and a response is provided detailing what each party must do to comply under the agreement.

Heading into 2025, companies have both enormous opportunities and challenges in the face of technological and legal advances surrounding data.

Only if companies keep on top of changing privacy and cybersecurity obligations will they be able to employ the appropriate strategies to fully contend with the evolving legal landscape to maximize the value of data.

NIS2 Directive is on the Edge of Enforcement: What Now for EU/U.S. Companies?

By Edward Taelman and Arthur Focquet

On October 18, 2024, the requirements of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) entered into force. The NIS2 Directive outlines the cybersecurity responsibilities of both "essential" and "important" entities, and sets out the duties of "management bodies," emphasizing their potential liability for failure to comply with the new mandates, along with significant penalties for entities that fail to meet their obligations.

What is NIS2?

The objective of the NIS2 Directive is to set out measures to achieve a high common level of cybersecurity across the EU. It expands the scope of cybersecurity requirements to include both "essential" and "important" entities in various sectors, including energy, transport, banking, health, digital infrastructure, and others. The NIS2 Directive introduces size-based thresholds for applicability and imposes substantial fines for non-compliance.

Which entities fall under the scope of NIS2?

To ascertain whether an organization needs to adhere to the NIS2 Directive, it is crucial to first identify if it is classified as either an "essential" or "important" entity, based on whether the company:

- provides services or carries out activities in the EU, without regard to an establishment in the EU;
- meets or exceeds the thresholds to qualify as an SME (small-medium enterprise); specifically, business employs more than 50 employees and has an annual turnover and/or annual balance sheet total of more than 10 million euros; and
- operates in the sectors listed in Annexes I and II of the NIS2 Directive (requires assessment by each entity).

Certain specific entities automatically fall under the purview of the NIS2 Directive, regardless of their number of employees or annual revenue, because of the potential for significant adverse impacts on European citizens resulting from disruptions to these businesses. These entities include:

a. Providers of public electronic communications networks or services that are available to the public;

b. Providers of trust services;

c. Registries for top-level domain names and providers of domain name system services; and

d. Public institutions.

As all EU Member States were required to transpose the NIS2 Directive into their national legislation by October 17, 2024, it is crucial for businesses to ensure that the Member State has not broadened the scope of the NIS2 Directive to apply to additional companies.

In addition, entities that are not established in the EU but provide their services within the EU must designate a representative (as per the GDPR, Digital Services Act, etc.). The Member State in which the

The NIS2 Directive outlines the cybersecurity responsibilities of both **"essential"** and **"important"** entities.

representative is established will be deemed to be the Member State in which the entity is subject to jurisdiction. In the absence of a representative, any Member State in which the entity provides its services may take direct action against the entity in the event of a breach of the NIS2 Directive.

Which obligations?

1. Risk management measures

Entities falling within the scope of the NIS2 Directive will be required to implement at least the following key measures:

- Risk analysis and information system security policies;
- Incident handling protocols;
- Business continuity plans, such as backup management and business resumption;
- Supply chain and network security measures, including the safety aspects between each entity and its direct suppliers or service providers. Companies must consider the specific vulnerabilities of each direct supplier and service provider, and evaluate the overall quality of their products and cybersecurity practices. This assessment shall include an examination of their secure development processes;
- Cybersecurity testing;
- Auditing procedures;
- Regular cybersecurity training, not only for management bodies but also for the employees;
- HR Security, access control policies and asset management; and
- The use of multi-factor authentication and encryption, and secure emergency communications systems within the entity (where appropriate).

Management bodies are tasked with approving the cybersecurity risk management measures adopted by their entities and overseeing their implementation, and are responsible for failures to comply with the above measures. In addition, management bodies are required to undergo cybersecurity training—or face significant liability, discussed below.

While the NIS2 Directive does not set forth specific standards for cybersecurity in the context of implementing risk management measures, it does encourage Member States to adopt European and international standards and technical specifications to ensure a harmonized implementation. For instance, Belgium, and very likely Luxembourg and Germany, have referenced ISO 27001 certification in their laws enacting NIS2, offering entities with this certification a presumption of compliance with the NIS2 Directive.

Beyond ISO standards, international frameworks like NIST or CMMC could also be instrumental for US-based entities aiming to ensure compliance with the NIS2 Directive.

2. Reporting obligations

Essential and important entities must promptly inform the national competent authority of any significant incident (i.e. a serious disruption to the service or financial loss, or significant material or non-material damage). Additionally, they are required to notify the users of their services about significant incidents that could impact service delivery. For example, in the event of a significant cyber incident, a chemical manufacturer is required to notify both the relevant authority and its suppliers and customers, offering them any possible measures or remedies they can take in response to the threat.

For important entities, fines can reach up to **7 million euros or 1.4 percent** of their total global annual turnover. Essential entities could be fined up to **10 million euros or 2 percent** of their total global annual turnover.

The initial reporting of the incident must occur within 24 hours of awareness, followed by an official incident notification within 72 hours. Interim and final reports should be submitted to the competent authority within one month of the formal notification.

Implementation

Essential and important entities, as well as entities providing domain name registration services, will have until January 17, 2025, to register with the competent authority. Essential entities are required to disclose their cybersecurity measures (ex ante) to the competent authorities, while important entities are only required to register, but the competent authorities may, at any time, require the important entity to provide evidence of compliance.

It is important to note that Member States may provide for a higher level of cybersecurity when implementing the NIS2 Directive into national law, so companies need to be careful and review the laws applicable in the countries where they provide services.

Enforcement

Each Member State will need to appoint a competent national authority whose role encompasses overseeing the directive's enforcement, ensuring that entities comply with their cybersecurity obligations, and facilitating a coordinated response to cybersecurity incidents. This oversight is crucial for maintaining a high level of cybersecurity across the nation and for protecting the integrity of essential and important services.

Sanctions and liability of management body?

The enforcement measures range from issuing simple warnings to mandating remediation actions or requiring the public disclosure of violations of law.

Entities that fail to meet their cybersecurity risk management or incident reporting requirements may face administrative fines. For important entities, fines can reach up to 7 million euros or 1.4 percent of their total global annual turnover. Essential entities could be fined up to 10 million euros or 2 percent of their total global annual turnover.

Concerning the accountability of management bodies, any individual responsible for an entity, or acting as its representative, bears personal liability for failing to comply with the NIS2 requirements—highlighting the significance of personal responsibility in cases of non-compliance.

Some Member States, in the process of integrating NIS2, have established provisions that allow for the temporary suspension of individuals in managerial roles, such as managing directors or representatives, from executing their managerial duties within the entity if they fail to comply with directives from the competent authority.

Conclusion

It is essential for entities to assess their relevance under the NIS2 Directive in order to clearly define their cybersecurity responsibilities and to perform a thorough gap analysis of their existing security measures. Although investing in cybersecurity may not be insignificant, it is important to note that the cost of these investments will likely be far less than the financial and reputational damage incurred from a cyber incident.

EU Cyber Resilience Act

By Edward Taelman and Arthur Focquet

The EU Cyber Resilience Act (CRA) was formally adopted by the European Council on October 10, 2024. Its main goal is to enhance cybersecurity and cyber resilience across the EU by establishing common cybersecurity standards for digitally enabled products, such as required incident reports and automatic security updates. This includes, for example, connected home products (cameras, fridges, toys), password managers, firewalls, and VPNs.

To whom does the CRA apply?

The CRA targets manufacturers, regardless of their location, who develop or produce products with digital elements for the EU market. Given the varying cybersecurity risks associated with different digital products, they are categorized into three main groups, with the level of obligations escalating based on the product's potential cybersecurity incident impact. These categories are:

a. Providers a) Products with digital elements: This default category encompasses products not specifically identified as "important" or "critical" with digital elements, covering both B2C and B2B products available in the EU market.

b. Important products with digital elements: Divided into two classes based on criticality level: Class I of Annex 3 of the CRA (e.g., password managers, VPN products, boot managers, routers, smart home assistants) and Class II of Annex 3 of the CRA (e.g., firewalls, hypervisors, tamper-resistant microcontrollers/ microprocessors).

c. Critical products with digital elements: Due to their critical importance in cybersecurity, these products are subject to the most rigorous cybersecurity requirements. Examples include hardware devices with security boxes, smart meter gateways, smartcards, and similar devices, including secure elements (Annex IV of the CRA).

Key obligations

Annexes I and II of the CRA outline the key requirements for manufacturers of digitally enabled products. Annex I includes:

- Designing products to ensure an appropriate level of cybersecurity (by design);
- Releasing products without known exploitable vulnerabilities and with secure default configurations;
- Addressing vulnerabilities through security updates;
- Protecting products from unauthorized access by appropriate control mechanisms and ensuring data confidentiality through encryption;
- Preventing unauthorized data manipulation or modification and reporting corruptions;
- Adhering to data minimization principles;
- Implementing resilience and mitigation measures against denial-of-service attacks;
- Identifying and documenting vulnerabilities with a software bill of materials;
- Promptly remediating vulnerabilities, including through security updates;
- Regularly testing and reviewing product security;

Manufacturers must perform a conformity assessment before market placement or significant product updates.

- Publicly disclosing information about fixed vulnerabilities;
- Establishing and enforcing a coordinated vulnerability disclosure policy;
- Facilitating information sharing about potential vulnerabilities;
- Distributing updates to fix or mitigate vulnerabilities promptly; and
- Ensuring the timely dissemination of security updates to address identified issues.

Additionally, Annex II mandates providing users with a minimum set of information and instructions for products containing digital elements.

Compliance with the CRA

Beyond risk assessment and security by design, manufacturers must perform a conformity assessment before market placement or significant product updates to ensure compliance with the Annex I requirements. These assessments can be self-conducted or performed by third-party entities. Products listed in Annex 3, Class II, and Annex 4, however, require third-party assessments due to their higher cybersecurity risk. Manufacturers must create an EU declaration of conformity confirming CRA compliance, as detailed in Annex V. Upon validation, manufacturers must affix the CE marking to their products, signifying CRA compliance.

Noncompliance with the CRA

The CRA imposes substantial administrative fines for noncompliance, including:

- Up to 2.5% of a company's global annual turnover or 15 million EUR for failing to meet cybersecurity requirements in Annex I;
- Up to 2% of global annual turnover or 10 million EUR for other obligations or requirements breaches;
- Up to 1% of global annual turnover or 5 million EUR for providing incorrect, incomplete, or misleading information to EU and national authorities upon request.

When does the CRA become applicable?

The CRA entered into force on Dec. 10, 2024. The regulation will be enforceable 36 months after coming into force, with certain provisions becoming applicable at 18 and 21 months after its entry into force.

EU Artificial Intelligence Act

By Sari Depreeuw and Arthur Focquet

On June 13, 2024, the European Union (EU) adopted the Artificial Intelligence Act (EU AI Act), making it the first-ever global law to regulate the use of artificial intelligence in a broad and horizontal manner. The historic measure applies to the development, deployment, and use of AI in the EU. Importantly, the EU AI Act has a certain "extra-territorial" effect to the extent that it is applicable to providers placing AI systems on the market in the EU, even if these providers are established outside the EU.

The EU AI Act entered into force on August 1, 2024, but its provisions will start applying gradually, starting from 2025. Below is a summary of the obligations set to become applicable in 2025, setting aside others that will go into effect on August 2, 2026. The provisions relating to high-risk AI systems within the product safety regulation regime outlined in Annex I will become applicable on August 2, 2027.

Obligations Effective in 2025

The year 2025 marks significant milestones for the EU AI Act, with critical dates in February and August that introduce new regulatory requirements.

Starting on February 2, 2025, the EU AI Act will apply to AI systems deemed prohibited due to their significant risk to the fundamental rights of EU citizens. Such AI systems include those designed for behavioral manipulation, social scoring by public authorities, and real-time remote biometric identification for law enforcement purposes. These systems will be banned outright to protect citizens' rights and freedoms.

By August 2, 2025, providers of General-Purpose AI Models (GPAI models), including Large Language Models (LLMs), will face new obligations. A general-purpose AI model is defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market" and it may serve as a basis for a "general-purpose AI system," which in turn has "the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems."

GPAI models with systemic risk have "high impact capabilities" or when the European Commission has designated it as such.

Obligations for Providers of GPAI Models

Providers of GPAI models must comply with several obligations, including:

- Drawing up technical documentation;
- Providing information to providers of AI systems in which the GPAI model is integrated;
- Putting in place a policy to comply with EU copyright laws (in particular the "opt-out" provisions of the general text and data mining-exception to ensure that they have lawful access

The EU AI Act entered into force in August 2024, but its provisions will start applying gradually.

to copyrighted content and comply with rights reservations);

- A sufficiently detailed summary about the content used for training the GPAI model;
- Cooperating with the EU Commission; and
- Relying on codes of practice to demonstrate compliance (until harmonized EU standards are published).

By the start of May 2025, the AI Office, a newly established entity within the European Commission, is expected to have released the code of practice for GPAI models. This document will clarify the practical application of the rules for providers.

Obligations for Providers of GPAI Models with Systemic Risk

In addition to the general obligations, providers of GPAI models identified as having systemic risks must:

- Perform model evaluation and identify, assess, and mitigate systemic risk;
- Track, document, remedy, and report serious incidents to the AI office/ national competent authorities, responsible for the enforcement of the EU AI Act in their Member State; and
- Ensure an adequate level of cybersecurity protection.

Non-Compliance Penalties

The EU AI Act outlines substantial administrative fines for non-compliance, which can reach up to 7 percent of a company's global annual turnover, or 35 million EUR (36 million).

As we move towards the implementation and enforcement of the EU AI Act in 2025, AI providers and deployers should consider familiarizing themselves with these obligations to ensure compliance and to avoid significant penalties.

European Union Health Data Space

By Edward Taelman and Jurgen Figys

In March 2024, after years of preparation, the Council of the European Union and the European Parliament reached a provisional agreement on a new regulation governing electronic health data. The regulation, known as the European Health Data Space, was first proposed in March 2022 and, when formally adopted, will apply to the primary use and secondary use of health data. This initiative is a key component of the broader EU data strategy and represents the first of nine sector– and domain–specific data spaces outlined in the European Commission's 2020 communication on "A European strategy for data."

The Council subsequently published the revised text for the EHDS, offering insights into the forthcoming regulation and its implications. Below is a review of the regulation, as it looks today.

EHDS: What's in a Name?

The EHDS aims to create a unified infrastructure and governance framework for the "primary use" and "secondary use" of health data. It uses the following definitions.

- Primary use: This involves utilizing health data to enhance health care delivery and improve patient outcomes. Examples include patient treatment, prescription and dispensation of medicinal products and medical devices, and data related to social security, administrative, or reimbursement.
- Secondary Use: This primarily supports research and innovation by providing researchers with access to larger volumes of high-quality data more efficiently and cost-effectively. Secondary use also encompasses data applications that benefit society, such as policy-making and personalized medicine.

Who Will be in Charge?

Each Member State will designate one or more digital health authorities to implement and enforce the primary use of health data under the EHDS at the national level. These authorities will handle various tasks, including serving as contact points for complaints from individuals regarding EHDS provisions. Additionally, data protection authorities will collaborate with digital health authorities to monitor and enforce data subject rights under the EHDS.

For the secondary use of health data, Member States will appoint a "health data access body" responsible for receiving, reviewing, and approving access requests. These bodies will also undertake monitoring and supervisory roles. Data protection authorities will oversee and enforce the right to object to the processing of personal electronic health data for secondary use.

A European Health Data Space Board will be established to facilitate cooperation and information exchange among Member States and the European Commission.

The European Health Data Space is a key component of the broader EU data strategy and represents the first of nine sector and domain–specific data spaces outlined in the European Commission's 2020 communication on "A European strategy for data."

When Will the EHDS Come into Effect?

The exact implementation date is yet to be determined. However, it is anticipated that the provisional agreement will soon receive endorsement from the European Council and the European Parliament, leading to formal adoption. The EHDS will come into effect twenty days after its publication in the Official Journal of the European Union. Generally, the EHDS will apply two years after its entry into force, with specific provisions, such as those governing the secondary use of health data, coming into effect four- or six-years post-entry into force.

Conclusion

The EHDS is an ambitious initiative aimed at establishing a unified health data governance framework across the EU, facilitating seamless data exchange across borders. This initiative can create tremendous opportunities for business ventures, but it also adds exposure to regulatory scrutiny. To effectively implement and benefit from the EHDS provisions once they are adopted, businesses should consider taking steps to prepare for compliance now.

Preparing for CMMC in 2025

By Jacob Harrison, Evan Wolff, and Michael Gruden

After years of anticipation and a series of delays, implementation of the U.S. Department of Defense's Cyber Maturity Model Certification Program (CMMC) is rapidly approaching. Though CMMC is not expected to enter into effect until early-to-mid 2025, DOD contactors can start taking steps now to ensure a smooth transition into this new regulatory era.

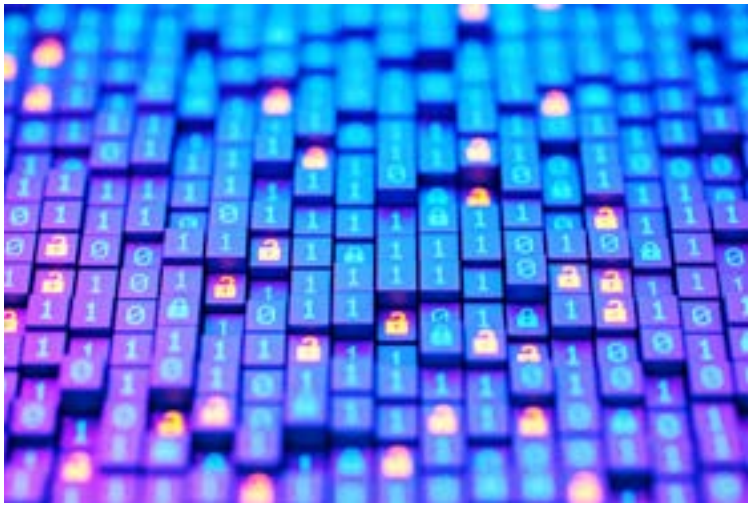
On October 15, 2024, DOD published a final rule, which builds on prior CMMC rulemaking and crystalizes its requirements ahead of CMMC's phased rollout to DOD contractors and subcontractors. Importantly, publication of the Final Program Rule does *not* immediately implement the DOD's CMMC contract requirements. Instead, the trigger for CMMC's implementation for contractors is tied to a separate CMMC rule, known as the "CMMC Clause Rule," which is currently at the proposed rule stage and will likely not be finalized until sometime in 2025. However, the release of the Final Program Rule allows CMMC Certified Third-Party Assessment Organizations (C3PAOs) to begin assessing contractor compliance against the CMMC framework, enabling contractors to get a head start on developing compliance programs prior to enforcement.

Below is a brief overview of the CMMC program, followed by a summary of four impactful CMMC changes introduced by DOD in the Final Program Rule.

What is CMMC?

CMMC is a forthcoming DOD regulatory framework designed to ensure that DOD contractors and subcontractors adequately safeguard sensitive government information, specifically Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

DOD contractors that handle CUI are currently subject to the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS)



clauses 252.204-7012. 252.204-7019, and 252.204-7020. CMMC builds on these DFARS requirements by requiring all contractors and subcontractors who handle CUI and FCI during contract performance to confirm their compliance with CMMC security controls via mandatory assessments and affirmations of compliance. The type of assessment and security controls that apply to a contractor will be informed by the type of data (i.e. CUI or FCI) and the sensitivity of the contract work being performed.

Prime contractors will be required to flow down CMMC requirements to their subcontractors who handle CUI and/or FCI in the course of performance.

CMMC Model Overview

The CMMC framework consists of three tiers, CMMC Levels 1, 2, and 3. DOD will determine the applicable Level for each contract. To be eligible for a contract or subcontract award, contractors will need to obtain assessments and provide affirmations showing that they meet the requirements of the Level specified in their contract or subcontract.

- CMMC Level 1 will apply to contractors and subcontractors who store, process, or transmit FCI. Level 1 includes 15 requirements from Federal Acquisition Regulation (FAR) clause 52.204-21(b)(1). Contractors at Level 1 will need to provide an annual self-assessment

The trigger for CMMC's implementation for contractors is tied to a separate CMMC rule, known as the "CMMC Clause Rule," which is currently at the proposed rule stage.

demonstrating their compliance with all 15 requirements.

- CMMC Level 2 will apply to contractors and subcontractors who store, process, or transmit CUI. Level 2 includes 110 requirements from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Rev. 2, and will require either a self-assessment or a C3PAO certification every three years. A C3PAO certification is a third-party certification from a private entity that is accredited or authorized by the CMMC Accreditation Body to conduct Level 2 assessments.
- CMMC Level 3 will apply to contractors that DOD determines store, process, or transmit high-value CUI. Level 3 includes 24 select requirements from NIST SP 800-172, as well as all Level 2 requirements. For Level 3 certification, contractors must submit to DOD-conducted assessments every three years.

In addition to assessments, contractors at all Levels will be required to provide annual affirmations from a senior official within the contractor's organization confirming their compliance with all applicable CMMC requirements.

Four Significant Changes in the Final Program Rule

While the Final Program Rule is mostly aligned with the CMMC requirements from the Proposed Program Rule that DOD released in December 2023, the DOD has made several notable revisions, including the following.

- A 6-month extension for CMMC implementation Phase 2. The Final Program Rule maintains the same structure as the Proposed Program Rule for the phased 7-year rollout of CMMC to contractors, but the start of Phase 2—the Phase at which Level 2 requirements will begin to be included in contracts—was pushed back six months. In practice, this change will likely mean that contractors and subcontractors subject to Level 2 will have one year from the finalization of the CMMC Clause Rule to obtain assessments and implement CMMC requirements, instead of the 6-month period included in the Proposed Program Rule.
- Reduced requirements for External Service Providers. Under the Final Program Rule, External Service Providers (ESPs) for contractors involved in handling or securing CUI are no longer required to obtain their own CMMC certification as the December 2023 Proposed Rule prescribed. However, ESPs will likely need to work closely with contractors as they navigate the CMMC assessment process, as ESPs' services may be assessed as a part of a contractor's overall compliance with the CMMC requirements, depending on the data the ESP handle and whether it handles such data in the cloud or not.
- Six-year artifact retention period extended to cover all assessments. Contractors are now required to retain artifacts from all CMMC assessments, whether self-assessed or conducted by a third party, for six years following the date of certification. In response to public comments on the Final Proposed Rule, DOD noted that DOJ suggested the six-year retention period. Significantly, the statute of limitations for the False Claims Act is six years, suggesting that the artifact retention period was deliberately chosen to aid future DOJ investigations into CMMC compliance.
- DIBCAC Authority to Audit Assessment Result. The Final Program Rule expands on the Defense Industrial Base Cybersecurity Assessment

Center's (DIBCAC) ability to audit contractors despite their CMMC status. If a DIBCAC audit is conducted and its results are different from the contractor's previously reported CMMC status, DOD will rely on the DIBCAC audit over the contractor's self- or C3PAO-reported CMMC compliance status and can independently update DOD's Supplier Performance Risk System (SPRS) to indicate that the contractor does not meet CMMC requirements. The rule notes that contractors could face contractual penalties if DIBCAC finds them noncompliant.

Next Steps for DOD Contractors and Subcontractors

Contractors and subcontractors who expect to be subject to CMMC requirements should act now to ensure that they have a compliance plan in place and are prepared for their assessments, including by:

- Reviewing active DOD contracts to determine their likely CMMC Level.
- Developing and refining a System Security Plan (SSP) documenting their CMMC assessment scope and compliance with CMMC controls.
- Defining roles and responsibilities and engaging key internal stakeholders across relevant business units.
- Conducting a CMMC readiness assessment under attorney-client privilege.
- Developing and tailoring corporate policies to align with CMMC control requirements.
- Engaging with C3PAOs to discuss assessment approach and scheduling.

Will Higher Education Institutions Face Enhanced Cybersecurity Requirements?

By Jacob Harrison and Michael Gruden

U.S. colleges and universities watched closely this summer when the DOJ, in a novel move, scrutinized the cybersecurity compliance of a research lab at an academic institution.

The lab at the Georgia Institute of Technology held contracts with the DOD, and the DOJ alleged in a lawsuit that the lab failed to apply required information security controls to DOD data in its possession. As a result, institutions of higher education should consider paying close attention to a proposed Department of Education rule that, if finalized, may soon require universities and colleges to protect personal data and other categories of Controlled Unclassified Information (CUI) according to the same standards required by the DOD.

What Information Will the Education CUI Rule Apply To?

The Rule's Abstract focuses on **Controlled Unclassified Information**, a broadly defined class of federal government-regulated data that includes many categories of information. The Rule specifically identifies personally identifiable information (PII) as a category of CUI the Department of Education wants to protect, but in practice, CUI can include information such as financial or tax records, health information, law enforcement information, and other unclassified, sensitive data. For colleges and universities, this could include students' or parents' personal information, financial aid data, and student health information, among other data categories commonly handled by schools.

What Entities Will the Education CUI Rule Apply To?

The first sentence of the Rule's Abstract suggests that "schools participating in the federal student financial assistance programs and other grant

programs under the Higher Education Act (HEA)" will be the Department of Education's primary concern in implementing the Rule. If the Rule is structured similarly to other executive agencies' CUI programs, schools may also be required to ensure that their vendors and contractors apply appropriate cybersecurity safeguards if they handle CUI on the school's behalf.

What Will Covered Entities Have to Do to Protect CUI?

The Abstract explains that the Department of Education intends to require covered entities to implement the requirements from National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) to protect CUI on school information systems. NIST SP 800-171 contains over 100 discrete technical and physical security requirements and is the same standard the DOD requires of its contractors to safeguard CUI. NIST SP 800-171's requirements are generally far more stringent than those imposed by the Family Educational Rights and Privacy Act of 1974 and other privacy obligations currently applicable to universities and colleges.

A proposed Department of Education rule would, if finalized, require universities and colleges to protect personal data and other categories of Controlled Unclassified Information (CUI) according to the same standards required by the DOD.

Some key requirements of NIST SP 800-171 include:

- Multi-factor authentication for network and remote access by all users.
- Encryption of data in transit and at rest per Federal Information Processing Standard 140-2.
- Sophisticated physical and technical access controls.
- Periodic vulnerability scans and compliance assessments.
- Comprehensive incident response procedures.
- Robust documentation of technical control implementation and related policies.

The Department of Education has not provided an implementation timeline for its CUI Rule. Schools should actively monitor department communications for rulemaking updates, as it may not provide an extended ramp up period to implement NIST SP 800-171 controls once the rule is published. Once the rule has been published and its requirements are clear, schools should consider conducting readiness assessments to confirm their compliance, ideally under attorney-client privilege to protect assessment findings in the event of litigation or a government investigation.

AI Regulation: New York and California Take the Lead

By Paul B. Keller

The rapid advancement of artificial intelligence (AI) has spurred a wave of legislative action across the United States—with New York and California arguably emerging as frontrunners. Both states enacted laws in 2024 aimed at regulating AI, but their approaches differ significantly, reflecting distinct priorities and concerns.

Although California's broader regulatory efforts have focused on transparency and political content, New York has taken a narrower aim, zeroing in on public agency use of AI. Despite their differences, both New York and California's legislation share a common goal: to harness the benefits of AI while mitigating its potential harms. These initiatives from California and New York set the stage for other states to follow suit.

California, a long-time hub for technological innovation, has adopted a comprehensive approach, passing a series of bills addressing various aspects of AI. One key focus is transparency. The California AI Transparency Act that became law in September 2024 mandates that businesses with large-scale generative AI systems disclose their use to the public and provide tools for users to identify AI-generated content. This act aims to combat the spread of misinformation and deep fakes, particularly concerning elections and political discourse. Further emphasizing ethical considerations, California also passed AB 2839, requiring political advertisements to clearly label any AI-generated content. This measure seeks to preserve the integrity of elections and ensure voters are not misled by synthetic media, though a federal judge has temporarily blocked the legislation due to a First Amendment challenge.

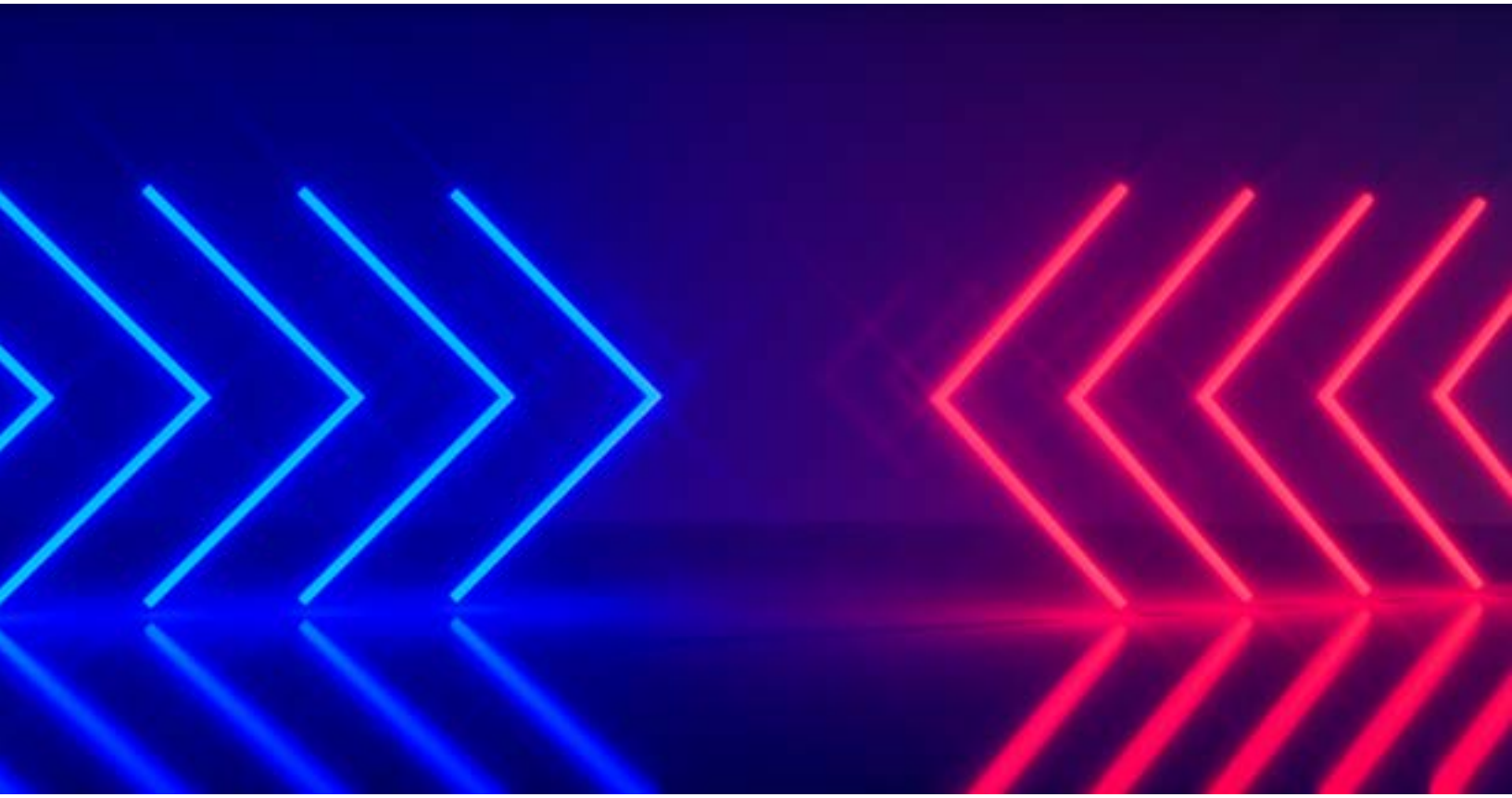
New York, on the other hand, has taken a more targeted approach, prioritizing the impact of AI on employment and government services. The "LOADinG Act" (Lawful Obligations and Due Diligence in Government Act) imposes strict requirements on state agencies using automated decision systems (ADS). These agencies must conduct impact assessments, ensure due process for individuals affected by ADS decisions, and provide transparency about how these systems function. This legislation reflects a growing concern about the potential for AI bias and discrimination, particularly in areas like criminal justice and social services.

These laws represent important steps toward a regulatory framework for AI in the United States, setting a precedent for other states and potential federal policy. It is important to note, however, that these laws also pose challenges. Critics argue that California's transparency requirements may be difficult to enforce and could stifle innovation. Concerns also abound about the potential for over-regulation and the need to balance consumer protection with the First Amendment rights of businesses, a tension that will play out in the courts as the fate of AB 2839 is decided. In New York, the

Despite their differences, both New York and California's legislation share a common goal: to harness the benefits of AI while mitigating its potential harms.

LOADinG Act's focus on government agencies leaves a gap in regulating private sector use of AI, raising questions about potential biases in areas like hiring and lending.

New York and California's AI legislation seek to address the ethical and societal implications of this transformative technology. Although their approaches differ, both states are paving the way for a future where AI is used responsibly and transparently, and their action may prompt other legislatures to adopt their own regulations. As AI technology continues to evolve, ongoing dialogue and collaboration between lawmakers, technologists, and the public will be essential to ensure that AI serves humanity in a responsible and ethical manner.



Guidance on Managing the Risks of AI Discrimination

By Shauneida Navarrete

When President Joe Biden issued the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence in 2023, his administration recognized not only the extraordinary promise of artificial intelligence (AI) but also the risks that irresponsible use of the technology posed. The risks identified by the President include algorithmic discrimination in activities that impact consumers, job candidates, and employees.

Since the executive order, numerous states have proposed bills focused on managing the risk of AI discrimination. The federal government has also released several memos intended to guide its agencies on navigating the new technology without discriminating against those the agencies serve. The regulations and guidance span a variety of settings, from the consumer protection realm to the employment sphere, with particular attention on both AI developers and deployers. Below is a snapshot of the notable federal guidance and summaries of proposed and enacted state regulations in 2024 that focus on managing the risk of AI discrimination.

Anti-Discrimination Consumer Protection Legislation

- **Enacted State Law**
  - **Colorado:** In May 2024, Colorado's S.B. 24-205, Consumer Protections for Artificial Intelligence, was signed into law. Several provisions within this law were designed to ensure that developers and deployers of AI programs use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the use of an AI program.[2] Crowell provided a summary of this legislation here: https://www.crowell.com/en/insights/client-alerts/colorado-ai-bias
  - **New Jersey:** In January 2024, New Jersey's Senate Bill No. 332, a consumer data privacy bill, was signed into law. SB 332 requires controllers—entities or individuals that determine the purpose and means of processing personal data—to notify consumers (New Jersey residents) when the controller collects and discloses personal data to third parties. The law also requires that the controllers provide consumers with the ability to opt-out of that collection or disclosure of their data. SB 332 bans controllers from processing consumer's personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.[3]

[2] S.B. 24-205, Consumer Protections for Artificial Intelligence, *available at* https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf

[3] New Jersey Senate Bill 332, *available at* https://legiscan.com/NJ/text/S332/id/2865878

- **Proposed State Law**
  - **Oklahoma:** In February 2024, lawmakers proposed the Ethical Artificial Intelligence Act. The act requires developers and deployers of automated decision tools to conduct an annual impact assessment, which includes a risk assessment of algorithmic discrimination. Furthermore, developers must provide operators with information regarding the risks of algorithmic discrimination and make publicly available a policy summarizing: 1) the types of automated decision-making tools the developers offer and 2) how the developers manage the risks of algorithmic discrimination in the tools it offers.[4]

Employment and Labor Legislation

- **Federal Guidance**
  - In April 2024, the Department of Labor's (DOL) Office of Federal Contract Compliance Programs issued guidance for federal contractors regarding the use of artificial intelligence in hiring and employment practices. The guidance reminded federal contractors and subcontractors that the use of artificial intelligence does not exempt them from Equal Employment Opportunity (EEO) compliance. The guidance also reminded federal contractors that they must take affirmative action to ensure that employees and applicants are not treated differently based on their race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or status as a protected veteran. Federal contractors must also conduct routine independent assessments of the AI programs for bias.[5]
  - In October 2024, the Department of Labor released a list of AI best practices for developers and employers aimed at assisting employers with using AI programs while protecting employees from unlawful discrimination. The guidance is clear that prior to deployment, employers should audit the AI systems for impacts of discrimination on the basis of "race, color, national origin, religion, sex, disability, age, genetic information and other protected bases," and recommends making the audit results public. The Department of Labor also recommends limiting the role of AI in making significant employment decisions and urges companies to ensure "meaningful human oversight of any decision supported by AI systems." For instance, those who oversee employment decisions informed by AI outputs must be trained in the programs so they can properly interpret the AI outputs.[6]

---

[4] Oklahoma House Bill 3835, Ethical Artificial Intelligence Act, *available at* http://webserver1.lsb.state.ok.us/cf_pdf/2023-24%20INT/hB/HB3835%20INT.PDF

[5] Office of Federal Contract Compliance Programs, Artificial Intelligence and Equal Employment Opportunity for Federal Contractors, *available at* https://www.dol.gov/agencies/ofccp/ai/ai-eeo-guide

[6] U.S. Department of Labor, Artificial Intelligence And Worker Well-being: Principles And Best Practices For Developers And Employers, *available at* https://www.dol.gov/general/AI-Principles

President Joe Biden's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence identifies the risks of AI as algorithmic discrimination in activities that impact consumers, job candidates, and employees.

- **Enacted State Law**
  - **Illinois:** In August 2024, Illinois amended their Human Rights Act to state that employers using predictive data analysis in hiring decisions may not consider the applicant's protected class status. Pursuant to the amendment, an employer is prohibited from using AI that has the effect of subjecting employees to discrimination with respect to recruitment, hiring, promotion, discharge, discipline, or the terms, privileges, or conditions of employment. Additionally, the amendment prohibits employers from using zip codes as a proxy for protected classes.[7] Crowell provided a summary of the amendment here: https://www.crowell.com/en/insights/client-alerts/artificial-intelligence-in-employment-update-illinois-requires-notice-and-prohibits-discriminatory-impact-in-use-of-ai
- **Proposed State Law**
  - **Maryland:** Introduced in February 2024, HB1255 restricts employers from using automated employment decision tools in making hiring decisions. The bill permits the use of the tool if an impact assessment determines that the tool would not result in unlawful discrimination or have an unlawful disparate impact on an individual based on their actual or perceived characteristics.[8]
  - **New Jersey:** Introduced in February 2024, A3854 seeks to regulate automated employment decision tools to ultimately minimize any employment discrimination that may result from the use of such tools.[9] A3854 generally mirrors New York City's Local Law 144, which Crowell summarized here: https://www.crowell.com/en/insights/client-alerts/july-5-is-almost-here-are-you-using-automated-employment-decision-tools-in-nyc.

In April 2024, the New Jersey Senate proposed S3015, which regulates the use of AI in video interviews during the hiring process. The bill would require employers to annually report to the New Jersey Department of Labor and Workforce Development the race and ethnicity of applicants who are extended an opportunity to apply and who are offered a position.[10]

General Federal Guidance and State Legislation

- **Federal Guidance**
  - In March 2024, the Office of Management and Budget released Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence. The

[7] Illinois General Assembly HB 3773, *available at* https://www.ilga.gov/legislation/fulltext.asp?SessionId=112&GA=103&DocTypeId=HB&DocNum=3773&GAID=17

[8] Maryland House Bill 1255, *available at* https://mgaleg.maryland.gov/2024RS/bills/hb/hb1255f.pdf

[9] New Jersey Assembly Bill 3854, *available at* https://legiscan.com/NJ/text/A3854/2024; see also New Jersey Assembly Bill 4030, *available at* https://legiscan.com/NJ/text/A4030/2024 (similar proposed New Jersey 2024 legislation); New Jersey Senate Bill 1588, *available at*https://legiscan.com/NJ/bill/S1588/2024 (similar proposed New Jersey 2024 legislation).

[10] New Jersey Senate Bill 3015, *available at* https://legiscan.com/NJ/text/S3015/id/2976788.

memo provides guidance for federal agencies, and vendors selling AI programs to agencies, using "rights-impacting" artificial intelligence.[11] Per the memo, agencies must identify and assess an AI program's impact on equity and fairness and mitigate any algorithmic discrimination when it is present. Crowell provided a summary of that guidance here: https://www.crowell.com/en/insights/client-alerts/omb-releases-final-guidance-memo-on-the-governments-use-of-ai

- **Proposed State Law**
  - **Illinois:** HB 5116 was introduced in February 2024 and requires deployers of automated decision-making tools to safeguard against reasonably foreseeable risks of algorithmic discrimination and to conduct impact assessments on the technology. The assessments are to be submitted to the state attorney general, who would have the authority to enforce violations of discrimination laws. The bill applies to employment as well as education and housing-based decisions.[12]
  - **New York:** In February 2024, the New York Assembly introduced A9149, which requires insurers authorized to write accident and health insurance in New York, among other insurers, to notify insureds and enrollees about the use of artificial intelligence in the utilization review process. The proposed legislation requires these entities submit their AI-based algorithms to the state Department of Financial Services, which must certify that the algorithms minimize the risk of bias based on a person's race, color, religious creed, ancestry, age, sex, gender, national origin, or disability. Proposed penalties for violations of the law include license suspension or revocation, fines, and refusal to issue new licenses.[13]
  - **Oklahoma:** In February 2024, lawmakers proposed the Oklahoma Artificial Intelligence Bill of Rights. The bill specifies that Oklahoma residents are not to be subjected to algorithmic or model bias that discriminates based on age, race, national origin, sex, disability, pregnancy, religious beliefs, veteran status, or other legally protected classes.[14]

---

[11] Rights-impacting AI is defined as AI "whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect" on (1) civil rights, (2) equal opportunity, or (3) access to critical government resources or services.

[12] Illinois 103rd General Assembly HB5116, *available at* https://ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=HB&DocNum=5116&GAID=17&LegID=&SpecSess=&Session=

[13] New York Assembly Bill A9149, *available at* https://www.nysenate.gov/legislation/bills/2023/A9149.

[14] Oklahoma Artificial Intelligence Bill of Rights, *available at* http://webserver1.lsb.state.ok.us/cf_pdf/2023-24%20ENGR/hB/HB3453%20ENGR.PDF

- **Vermont:** In January 2024, H.710 was introduced, requiring, among other things, for developers and deployers of high-risk artificial intelligence systems (AI systems that make or are a controlling factor in making a consequential decision) to use reasonable care to avoid the risk of algorithmic discrimination, and specifically, to impose numerous disclosure requirements upon developers.[15]
- **Virginia:** In February 2024, Virginia lawmakers introduced the Artificial Intelligence Developer Act. The bill makes it unlawful for a developer or vendor to sell an artificial intelligence system without providing sufficient information on risk assessment. Deployers of the AI programs must take reasonable care to avoid the risk of algorithmic discrimination and implement a risk management policy.[16]

[15] Vermont H.710, *available at* https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf

[16] Virginia Artificial Intelligence Developer Act, House Bill 747, *available at* https://legacylis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1

Asia-Pacific Strives to Keep Pace with Cyber Threats

By Clark Jennings, Kate Growley, Nigel Cory, Akanksha Sinha, and Caitlyn Weeks

The Asia-Pacific (APAC) region witnessed a rapid digital transformation in 2024, powered by its connectivity and technological innovations. However, these advancements have introduced new vulnerabilities into the region's digital ecosystem, which more sophisticated and nuanced cyber threats are already exploiting. In Q2 2024 alone, the APAC region experienced an average of 2,510 weekly cyberattacks per organization, marking a 23 percent increase compared to the same period in 2023.

To keep pace with this evolving threat landscape, several APAC countries, including Australia, Hong Kong, Japan, and Singapore implemented new or updated cyber policies. The most popular areas of regulatory action this year included: **critical infrastructure (CI); artificial intelligence (AI); operational technology (OT);** and **Internet of Things (IoT).**

Moving into 2025, these legislative developments will serve as models for other APAC countries as they consider their own measures to reduce cyber risk. Companies operating in or servicing the APAC region should actively monitor these developments and engage early and often. Doing so will help ensure that policymakers have the benefit of the private sector's experience—and that companies thoroughly understand the nuances of their regulatory obligations.

Critical Infrastructure

Securing CI emerged as a top priority for APAC countries in 2024, particularly in response to headline-making incidents such as cyber espionage attacks against India's government and energy sectors and a cyber-attack on Indonesia's National Data Centre that disrupted hundreds of public services.

In May 2024, Singapore made landmark amendments to its Cybersecurity Act to identify and include essential infrastructure beyond CI.

The Singapore Parliament enacted the Cybersecurity (Amendment) Bill No. 15/2024, introducing key changes to its Cyber Security Act 2018. The amendments extend the Act's coverage to both physical and virtual critical information infrastructure (CII) systems, such as those hosted on cloud platforms and located overseas. The bill also expands the scope of reportable cybersecurity incidents to encompass systems controlled by Critical Information Infrastructure (CII) owners and their external suppliers. Additionally, it regulates newly defined Systems of Temporary Cybersecurity Concern (STCC), Entities of Special Cybersecurity Interest (ESCI), and providers of Foundational Digital Infrastructure Services (FDIS).

In June 2024, the Hong Kong Special Administrative Region proposed the Protection of Critical Infrastructure (Computer System) Bill to enhance the protection of computer systems of critical infrastructures.

In Q2 2024 alone, the APAC region experienced an average of 2,510 weekly cyberattacks per organization.

Partly formulated in response to a series of high-profile data breaches, the bill imposes statutory obligations on CI operators (CIOs) to strengthen their critical computer systems (CCSs). It expands the scope of cybersecurity regulation to include both physical and virtual CIs, establishes a new commissioner's office for implementation, and introduces mandatory measures for CIOs to prevent, respond to, and recover from cyberattacks. The SAR Government plans to introduce the proposed Bill into the Legislative Council by the end of 2024, with the aim of setting up the Commissioner's Office within one year following the passage of the bill and bringing the legislation into force within six months thereafter.

Artificial Intelligence

The growing use of AI technologies in the APAC region is a double-edged sword. While AI enhances threat detection, automates responses, and predicts potential vulnerabilities, the technology comes with its own unique security risks. Consequently, there is a heightened focus on developing robust AI security through stringent regulations, mandatory security assessments, and secure AI development practices. Key trends in AI security regulation include adopting sector-specific approaches, focusing on continuous system testing and monitoring, and implementing risk-based regulatory frameworks, inspired by the U.S. National Institute of Science and Technology's (NIST) AI Risk Management Framework and the European Union's AI Act.

The Cyber Security Agency of Singapore (CSA) introduced the region's first comprehensive Guidelines on Securing Artificial Intelligence (AI) Systems and a Companion Guide on Securing AI Systems in October 2024.

The documents aim to ensure that AI systems are secure-by-design and secure-by-default, thereby helping system owners manage security risks from the outset and building user confidence in AI systems. The guidelines outline a lifecycle approach to AI security, covering five stages: planning and design, development, deployment, operations and maintenance, and end-of-life. Key recommendations include conducting security risk assessments, securing the AI supply chain, implementing secure development environments, and establishing incident management procedures tailored to AI systems. Additionally, the guidelines also advocate for continuous monitoring of AI system inputs and outputs, secure-by-design updates, and a vulnerability disclosure process.

Operational Technology

Securing OT has become a focal point for industries across the APAC region, particularly those reliant on industrial sectors like transportation and manufacturing. Unlike traditional IT systems, OT environments often involve legacy systems that were not originally designed with cybersecurity in mind, making them particularly vulnerable to cyberattacks.

Singapore's CSA published the Operational Technology (OT) Cybersecurity Masterplan 2024 to enhance the security and resilience of industrial control systems and OT technologies.

The Masterplan addresses nuanced cyber threats, aiming to enhance the security and resilience of both critical and non-critical OT systems. It outlines four key objectives:

1. improving OT cybersecurity professional competency,

2. enhancing information sharing and reporting,
3. uplifting OT cybersecurity resilience beyond CII, and
4. establishing an OT Cybersecurity Centre of Excellence while promoting secure-by-deployment principles throughout the OT system lifecycle.

Internet of Things

IoT cybersecurity has become crucial as the proliferation of IoT devices revolutionizes various sectors from smart homes and healthcare to industrial automation and urban infrastructure. However, the rapid expansion of IoT devices also introduce myriad cybersecurity challenges, as IoT devices often lack robust security measures, making them prime targets for cyberattacks.

Australia's proposed Cyber Security Bill 2024 aims to enhance cybersecurity across public and private sectors through a bevy of initiatives, including compliance standards for IoT devices.

The bill mandates that manufacturers and suppliers of IoT devices comply with security standards specified by the Australian Government, which will be detailed in upcoming rules and updated as new standards emerge. Manufacturers and suppliers must also provide and retain a statement of compliance. Non-compliance can result in enforcement actions such as compliance notices, stop notices, and recall notices.

Japan has drafted an IoT Product Security Conformity Assessment Scheme.

Additionally, Japan's Ministry of Economy, Trade and Industry (METI) developed a voluntary scheme that establishes baseline and category-specific security requirements for IoT products. Labels will be granted based on self-declarations or third-party evaluations, with the aim of aligning with international standards to reduce conformity assessment costs for vendors. The scheme is set to begin accepting self-declarations and granting labels by March 2025.

Singapore is pioneering interoperability of IoT labelling schemes through mutual recognition agreements (MRAs) with Germany and, more recently, South Korea.

Meanwhile, Singapore's CSA has signed MRAs with three international cybersecurity agencies in Finland, Germany and South Korea to mutually recognize cybersecurity labels for smart consumer products. The agreements, with Germany and South Korea came into effect on January 1, 2025. The MRAs will streamline the certification process, reduce costs, and enhance market access for manufacturers by acknowledging each other's cybersecurity labels for devices such as smart home assistants and health trackers. The MRAs also aim to facilitate the global trade of secure smart devices. Whether similar MRAs will be established with other IoT labelling regimes, such as those in Australia, Japan, and the United States, remains to be seen. The United States and EU are also working to align their respective IoT cybersecurity labeling systems.

Latin American Data Privacy

By Anna Z. Saber

In 2024, Latin American countries ramped up their data protection laws, following the general trend seen in international privacy law outside of the European Union. While many countries in Latin America enacted measures in 2024, others scheduled their regulations to go into effect in early 2025, and still others continue to wrestle with the legislative process.

As a result, a patchwork of privacy laws blankets the region, and companies must ensure they understand key regulatory differences depending on where they operate. With so many countries adopting legal frameworks that align closely with the GDPR, companies that do business in Latin America should refresh their privacy practices to ensure compliance with these new laws. Below is a review of key developments in Latin American countries in 2024 and a preview of what the landscape will look like in 2025.

Enacted Laws

Argentina, which was the first Latin American country to adopt an "adequacy determination" from the European Commission, continues to develop its privacy laws. On June 1, 2024, Resolution No. 126/2024 of the Access to Public Information Agency (Argentina's data protection authority) went into effect. The Resolution establishes a new classification of sanctions for violations of the existing Data Protection Law No. 25,326 (Argentina's overarching law governing privacy of personal data, which generally aligns with the GDPR) and Telephony Services Law No. 26,951 (which establishes the National Do Not Call Registry). Additionally, the Resolution unifies in one source the records of violation for each law.

Bermuda's Personal Information Protection Act (PIPA) is slated to take effect on January 1, 2025 after years of waiting—the statute was passed in 2016. Key provisions of PIPA include requirements for organizations to implement standardized safeguards, breach notifications, updated and accurate privacy notices, and a review of contracts with service providers to ensure protection of personal data. One significant aspect of PIPA is that, with the exception of Bermuda's Human Rights Act, PIPA will prevail in the event of any conflict with any other laws enacted.

Brazil enacted the General Data Protection Law (LGPD), which generally aligns with EU's GDPR, in 2020. During 2024, the LGPD saw significant upgrades, including approving standard contractual clauses (SCCs) for international data transfers, granting data subjects more control over their own data, enhanced and stricter penalties for non-compliance, more stringent data reporting requirements, an expansion of scope of what LGPD applies to, and an election campaign-specific resolution.

In **Paraguay**, a law called the Regulation of Credit Information Bureaus and Protection of Credit Personal Information went into effect on January 1, 2024. It limits which Credit Information Bureaus are permitted to operate. More controversially, Law 7269/2024 also went into effect in 2024 Law 7269/2024 authorizes and requires the collection of biometric data (including facial recognition) from all attendees of sporting events. Proponents of the law state it is

A patchwork of privacy laws blankets Latin America, and companies must ensure they understand key regulatory differences depending on where they operate.

designed to prevent and control violence in sports. Opponents of this law state that there is no distinction between people who are participating in violent acts at sporting events and those who are mere attendees. Lastly, the Personal Data Protection Bill remains in the legislative chambers. First proposed in 2021, the Personal Data Protection Bill includes data subject rights, security standards, data protection officer responsibilities, and processes for creating an enforcement authority.

Pending Legislation

Bolivia does not yet have a comprehensive data protection law in place. However, there are several privacy-related bills pending in Bolivia's Congress, including both a Personal Data Protection Bill, which establishes processing and consent requirements for personal data, and a Comprehensive Data Protection Law. If passed, this would augment the right to privacy, which is recognized in the Bolivian Constitution. As 2025 approaches, the Bolivian legislature may make moves to advance these bills.

Chile's Congress passed the Personal Data Protection Bill on August 26, 2024. The bill is now under review by the Constitutional Court, which must approve it before it is enacted by the President. This bill modernizes Chile's existing data protection regulations and aligns Chile's framework with the GDPR's. It also explicitly includes anonymization and pseudonymization as recommended practices to comply with the law.

Colombia seeks to reform its existing General Data Protection Regulation. Like many other Latin American countries, the reforms seek to align Colombia's privacy regime with international standards, including the GDPR. Key areas of reform relate to establishing new legal bases for legitimate data processing, consent for minors over 16, limiting data processing, new timelines for reporting incidents, and the right of data subjects to not be subjected to fully automated decisions. Colombia's focus on addressing AI and automated processes is consistent with its recent focus on reconciling data privacy rights with the increasing use of AI.

How Businesses Can Navigate China's Data Regulations in 2025

By Kate Growley and Zhiwei Chen

The People's Republic of China's data protection laws have evolved rapidly in recent years, reflecting the global trend towards greater data privacy and security. The cornerstone of this legal framework has been a trio of measures: the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL). These three laws collectively govern the whole lifecycle of data processing.

As we approach 2025, data protection remains a focus for the Chinese government and multinational companies alike, with significant developments that reshape and streamline cross-border data transfers and other compliance requirements. Here, we review key updates from 2024, offering practical insights into China's evolving regulatory landscape and its impact on business

Provisions on Promoting and Regulating Cross-Border Data Flows

On March 22, 2024, the Cyberspace Administration of China (CAC) issued the long-awaited *Provisions on Promoting and Regulating Cross-Border Data Transfer* (CBDT Provisions). The Provisions were welcomed by the business community, as they significantly lessen the cases in which companies need to complete the formal mechanisms established in the PIPL to transfer data outside of Mainland China, which had been: an official security assessment by the CAC, a security certification by a third party, or execution of the standard contractual clauses (SCCs) with the receiving party (collectively, CBDT Mechanisms).

New Exemptions from the CBDT Mechanisms

Under the CBDT Provisions, a company need not meet any of the three CBDT Mechanisms in the following circumstances:

1. Transfer of personal information (PI)[1] that is collected or generated outside of China, provided that no Chinese PI or Important Data[2] is introduced during the processing in China.
2. Transfer of PI that is necessary for entering into and performing a contract to which the individual transferor is a party, such as cross-border shopping, delivery, remittances and payment, bank account opening, air ticket or hotel reservations, visa processing, or exam services.
3. Transfer of employee PI that is necessary for implementing cross-border human resources management in accordance with lawfully formulated labor or employment policies or signed collective contracts.
4. Transfer of PI that is necessary for protecting the life, health, or safety of persons in emergencies.
5. Transfer of PI of less than 100,000 individuals by non-CIIO[3] (critical infrastructure information operator) processors in the current year.
6. Transfer of data that does not contain PI or Important Data.

Relaxed Thresholds for CBDT Mechanisms

Prior to the CBDT Provisions, the volume threshold for an onerous CAC security review was relatively

low—transferring only 100,000 individuals' PI since January 1 of the preceding year. Transfer of PI below this threshold triggered SCCs or security certification. Now, the CBDT Provisions significantly relax these thresholds as follows:

No CBDT Mechanism at all required for:

- Transfers of PI of less than 100,000 individuals in the current year.

Certifications or SCCs are required for:

- Transfers of PI ranging from 100,000 to one million individuals in the current year; or
- Transfers of *sensitive* PI[4] of less than 10,000 individuals in the current year.

A CAC security assessment is required for:

- Transfers of PI exceeding one million individuals in the current year;
- Transfers of *sensitive* PI of 10,000 individuals or more in the current year;
- Transfers of any amount of Important Data; or
- Transfers made by CIIOs.

Network Data Security Regulations

Published on September 30, 2024, and effective January 1, 2025, the Network Data Security Regulations were first introduced by the CAC in 2021. They are the first administrative regulations-level legal instrument on data protection since the three fundamental laws noted above. As such, they supersede any rules previously issued by the CAC. That said, the Regulations reflect insights and experience that the CAC has obtained over the past three years, particularly where prior practices sometime created challenges for businesses.

Clarifying Compliance and Important Data

The Regulations provide more detail on how processors of Important Data can meet their obligations, including regarding the appointment of a network data security officer, establishment of a data security management organization, and conducting risk assessments when providing and sharing Important Data with other parties.

Under the Regulations, a National Data Security Coordination Mechanism will be established to develop catalogues of Important Data. Local and industrial regulators are tasked to identify and safeguard Important Data within their jurisdictions or industries. Network data processors must use these catalogues to identify and report Important Data to the corresponding regulators.

In addition, the Regulations clarify that processing PI of more than *10 million* individuals triggers the same requirements as processing Important Data. By contrast, the draft Regulations had set the threshold at only PI of one million individuals.

Additional Exemption from the CBDT Mechanisms

The Regulations introduced a new exemption beyond those under the new CBDT Provisions. The new exemption allows companies to transfer PI necessary to perform statutory duties or obligations without going through any of the CBDT Mechanisms.

Additional Obligations for Large-Scale Network Platform Service Providers:

The Regulations impose additional compliance obligations on network platform service providers, defined as having over 50 million registered users or more than 10 million monthly active users, with complex business types whose network data processing activity significantly impacts national security, economic operations, or public welfare. Large-scale network platform service providers are now required to conduct annual network risk assessments and publish an annual personal protection social responsibility report.

As we approach 2025, data protection remains a focus for the Chinese government and multinational companies alike.

Regional and Policy Developments to Support Cross-Border Data Transfers

In 2024, China introduced a range of regional and policy-based initiatives in strategic markets to further ease cross-border data transfers and support foreign investment.

For instance, on August 30, 2024, Beijing issued a "negative list," where only transfers of data on the negative list must comply with corresponding CBDT Mechanisms. Currently, the negative list covers transfers of Important Data and PI by companies in five industries: automobiles, medicine, retail, civil aviation, and artificial intelligence. Data not included in the negative list can be freely transferred out of China by companies registered in the Beijing Free Trade Zone (FTZ).

On September 10, 2024, the CAC and the Macau Special Administrative Region (SAR) jointly issued guidelines on SCC filing procedures for data flows within the Greater Bay Area (GBA). Prior to this, the CAC had issued similar guidelines to facilitate and streamline cross-border data flows between the Hong Kong SAR and nine Mainland cities in the GBA, including the tech hub Shenzhen.

Actionable Takeaways for Businesses

In 2024, China witnessed a series of regulatory shifts that balance stringent compliance with practical flexibility, providing opportunities for companies to reduce administrative burdens. Here's how businesses can adapt:

Evaluate Exemptions for Cross-Border Transfers: Review data activities to determine eligibility for the new cross-border PI transfer exemptions. Utilizing these exemptions can help reduce the need for time-consuming security assessments and streamline data flows across borders.

Enhance Compliance Procedures: Companies handling Important Data should update their compliance protocols, including their risk assessments and data security reporting. Ensuring that key personnel understand China's new compliance standards will be critical for seamless operations.

Leverage Regional Policies: For businesses in the FTZs or GBA, taking advantage of industry-specific guidelines and exemptions can further ease cross-border data handling. Business should regularly monitor updates to FTZ policies to remain aligned with any regional changes.

Monitor Emerging Regulations: Anticipate further sector-specific data security requirements. Staying informed on new data catalogues or proposed guidelines can help align long-term compliance strategies with China's evolving regulatory priorities.

The Future of AI Regulation in South Africa, India, and Brazil

By Neda M. Shaheen

Artificial intelligence (AI) is rapidly reshaping global economies. South Africa, Brazil, and India are each leveraging AI to boost innovation in important areas, but they face different challenges. As a result, each country has developed its own rules on using AI, as well as on privacy, cybersecurity, and other efforts for digital transformation.

Compliance with existing laws and alignment with emerging frameworks will be crucial in navigating the regulatory landscape and mitigating risks associated with global AI deployment. Businesses in these countries must stay informed about changing AI regulations. Following current guidance, frameworks, and laws, as well as adapting to new rules, will help companies avoid problems and use AI effectively.

South Africa

Clients operating in South Africa should be aware that while there are no specific AI regulations yet, the country has launched the Draft National Artificial Intelligence Plan. The plan was introduced by the Department of Communications and Digital Technologies (DCDT) during the National AI Summit, and it outlines the government's vision for integrating AI into various sectors to boost innovation. The draft plan will also guide the development of legal and regulatory frameworks for AI and aims to provide a clear roadmap for developing and implementing AI solutions, encouraging individuals and organizations to adopt the technology.

At the same time, existing laws, such as the Protection of Personal Information Act (POPIA), the Copyright Act, the Patents Act, and the Competition Act impact AI development and deployment, and should be reviewed before developing or using AI technology in South Africa.

India

India is in the process of formulating and implementing policy frameworks to govern various aspects of AI regulation. While comprehensive AI-specific regulations are still evolving, several initiatives and guidelines are in place to guide the responsible development and deployment of AI technologies.

In 2018, India introduced its National Strategy for AI, known as #AIFORALL. In February 2021, India introduced Part 1 of Principles for Responsible AI as a follow-up to the national strategy. It serves as India's roadmap for the creation of an ethical, responsible AI ecosystem across sectors. In August 2021, India released Part 2, which concentrates on operationalizing the principles derived from the ethical considerations in Part 1.

India has also created special rules for areas like finance and health. Businesses in India should be cautious to follow these guidelines and any rules for their specific industry. In addition, the proposed Digital India Act (DIA) of 2023, if enacted, would replace the Information and Technology Act of 2000.

These developments indicate a robust regulatory environment across various countries.

Brazil

Brazil is considering Bill No. 2,338/2023, a comprehensive effort to regulate AI, but the measure has not been approved. Most notably, this proposed law would classify AI systems by how risky they are and set rules for those who create and use them. The proposed AI regulation defines high or excessive risk systems as those that can harm health or safety, can exploit specific vulnerabilities, like age or disability status, or can be used by public authorities to unfairly evaluate, classify, or rank people, affecting their access to goods, services, and public policies. Businesses should assess the risks of their AI systems and set up proper management to follow the upcoming rules.

In July 2024, Brazil's government unveiled a $4.07 billion proposal to invest in AI to achievement technological autonomy and competitiveness. The proposal is set to advance public and private investments for AI as part of the country's 2024 to 2028 AI plan.

Conclusion

Overall, these developments indicate a robust regulatory environment for AI in South Africa, India, and Brazil, emphasizing global considerations which will impact various sectors and stakeholders. As such, it is critical that clients prepare for the potential enactment of AI regulations, which will impose new compliance obligations, especially for high-risk AI systems.

Staying updated on global AI developments is crucial to anticipate and adapt to new requirements. As new rules and regulations move forward, Crowell & Moring, LLP will continue to follow AI, advising clients on all global compliance needs.

crowell.com