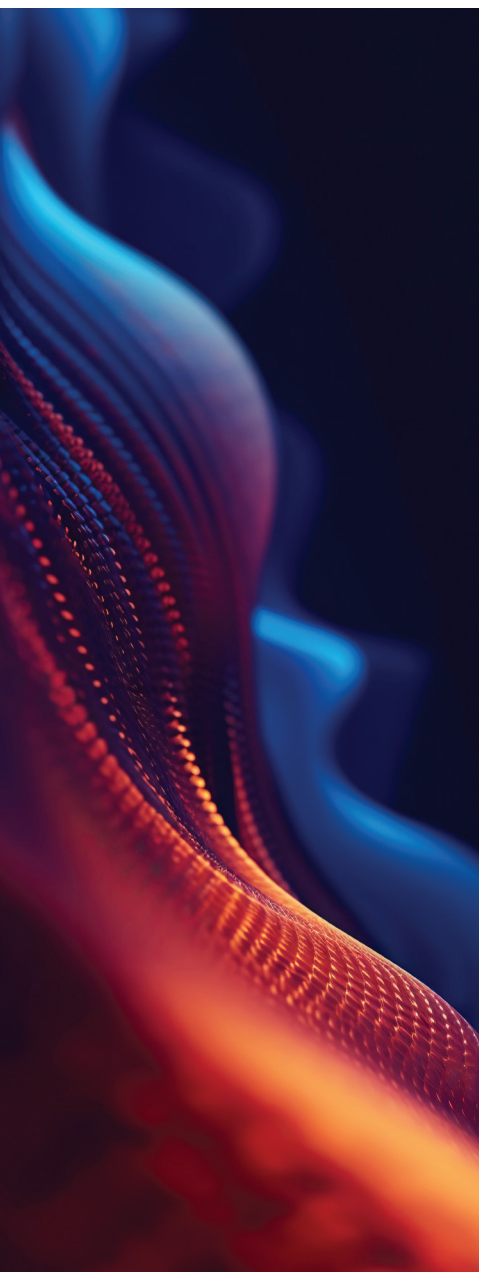




# SIDLEY



SIDLEY RESOURCE // MAY 2024

## AN ARTIFICIAL INTELLIGENCE, PRIVACY, AND CYBERSECURITY UPDATE FOR INDIAN COMPANIES DOING BUSINESS IN THE UNITED STATES AND EUROPE

*By: William RM Long, Ash Nagdev, and Colleen Theresa Brown*

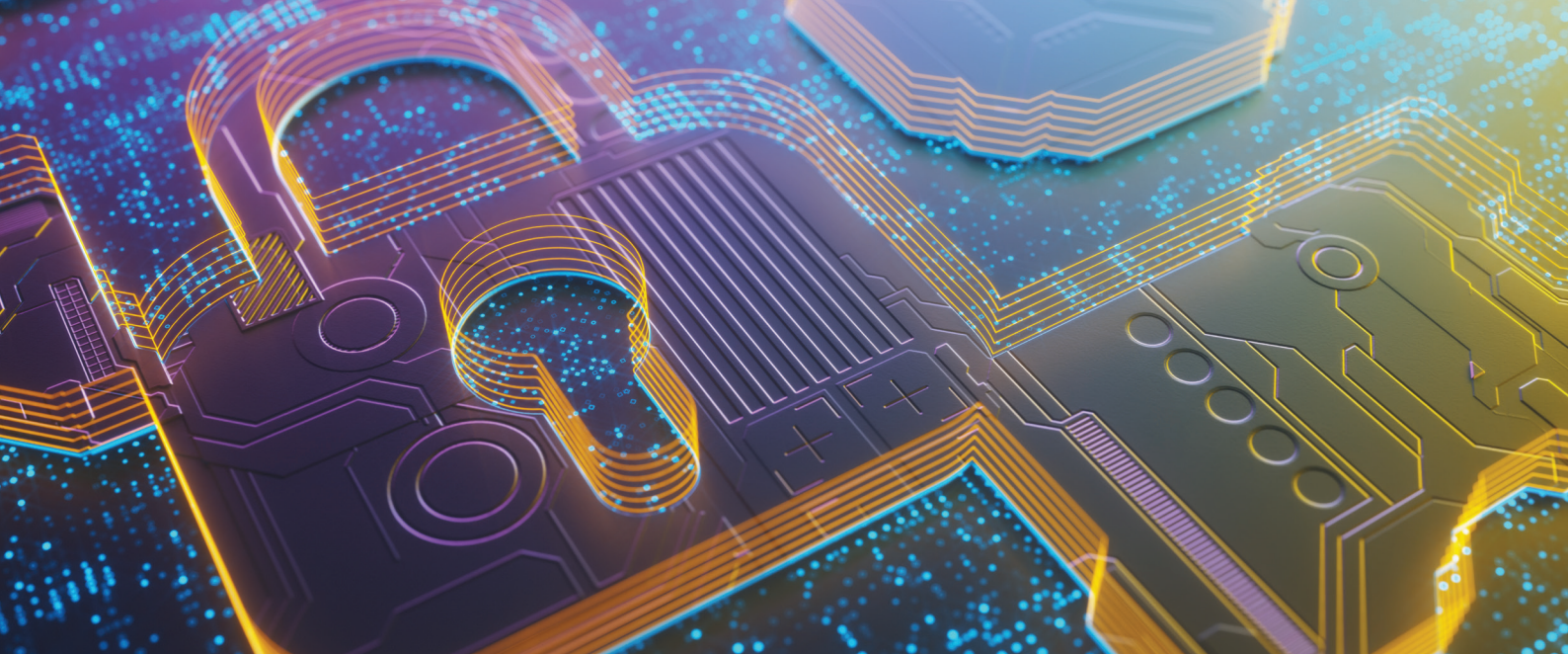
Pivotal shifts have occurred in global data privacy, artificial intelligence (AI), and cybersecurity from executives facing more pressure to monitor their organizations' cybersecurity operations, to an unprecedented wave of consumer data privacy laws and rapid advancements in AI technology use and deployment. Indian organizations should establish best practices to address these new (and emerging) laws, regulations, and frameworks.

Summarized below are key developments for Indian organizations with current operations in the United States and Europe and that want to grow their presence in those jurisdictions, together with recommendations for addressing these key developments.

### KEY TAKEAWAYS

In light of the fast-moving AI, privacy, and cyber laws; regulations; and litigation and enforcement risks in both the United States and Europe; organizations looking to adopt a comprehensive AI, data, and cyber strategy should consider:

- i. assessing the application of these laws and likelihood of the realization of these legal risks to the business;
- ii. where these laws apply or the legal risks may be likely, carrying out an assessment to determine the impact on the business;
- iii. implementing a governance program that involves senior management and governance structures to mitigate risk and establish a baseline to build flexible compliance;
- iv. regularly training and testing employees on the requirements under these laws and the governance program;
- v. building third-party risk management programs to mitigate risks from third-party software, data, tools, and services, and complying with oversight requirements (and where you offer third-party software, data, tools, and services, preparing to respond to such customer diligence and oversight); and
- vi. applying cyber resilience and response preparedness, conducting regular risk assessments, and carrying out cybersecurity policy reviews.



## DEVELOPING PRIVACY AND DATA LAWS

### U.S. State Data Privacy Laws



During 2023 and into 2024, the United States experienced a surge in consumer data privacy laws enacted and proposed on a state level, and this state legislative activity continues to pick up steam. As a result, in-scope Indian organizations are recommended to allocate significant and adequate resources to review and develop strategies and internal governance procedures to ensure that their businesses remain compliant.

During 2023 and continuing into 2024, the United States experienced a surge in consumer data privacy laws enacted and proposed on a state level, and this state legislative activity continues unabated. While there continues to be discussion of federal privacy legislation, the likelihood that federal legislation would fully preempt stronger state privacy laws is not probable. As a result, in-scope Indian organizations are recommended to allocate significant and adequate resources to review and develop strategies and internal governance procedures to ensure that their businesses are able to comply with the complexity of multistate privacy regimes that are not necessarily harmonious. Businesses are encouraged to review and revise external privacy notices, policies, and disclosures to address specific disclosure requirements, data use limitations, perform data mapping exercises, ensure that websites implement and recognize opt-out preference signals, and conduct data protection impact assessments and risk assessments, where necessary.

Below are certain key sector-specific data privacy obligations:

- **Direct-to-consumer Indian businesses** collecting personal information may be subject to various comprehensive state consumer data privacy laws. As of May 2024, 18 states have passed comprehensive data privacy laws in the United States (California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Maryland, Montana, Oregon, Delaware, New Jersey, Kentucky, Nebraska, and New Hampshire). Of those 18, California, Colorado, Connecticut, Utah, and Virginia are in effect; those in Texas, Montana, and Oregon take effect later in 2024. Other states are advancing comprehensive data privacy bills that contain more expansive requirements, including for certain specific subject matters, such as for health information privacy and children's data. Although many of these state laws have overlapping requirements, Indian businesses must be aware of any nuances across the laws to ensure that compliance obligations are met and consumer rights upheld.
- **Indian businesses collecting consumer health data** outside of the traditional healthcare context (e.g., health and wellness companies, fertility tracking apps, wearable devices) are required to ensure compliance with in-scope federal and state laws regulating the collection, use, and disclosure of consumer health data. The Washington My Health My Data Act, for





example, offers a private right of action for consumers to file lawsuits, which significantly increases compliance risks for in-scope organizations. The U.S. Federal Trade Commission (FTC) expanded the scope of the Health Breach Notification Rule to cover digital health apps and websites, and pursued enforcement actions against businesses that disclosed sensitive health information to advertisers.

- **Indian businesses using advertising technology (or adtech)** to target customers should be aware of the surge in litigation and regulation over the use of tracking technologies, including tracking pixels (e.g., Meta Pixel) or session recording software, to collect and share personal information, such as sensitive information and children's data, with third parties. Businesses may need to update their internal privacy compliance programs or reconfigure technologies to minimize the collection and disclosure of certain personal information and recognize opt-out tools provided by the ad industry and ad blockers to limit the impact of targeted advertising.

## European Privacy and Data Laws

Data privacy laws in the EU and UK are governed by the General Data Protection Regulation (GDPR), which has applied since 2018, and, following Brexit, the UK has adopted a UK-version of the GDPR. The GDPR seeks to lay down uniform requirements in relation to the processing of personal data (i.e., data relating to an identified or identifiable individual), including requiring compliance with certain data protection principles when processing personal data (e.g., fairness, transparency, security) and providing for various data subject rights (e.g., access to personal data).

A key issue over the past few years has been the restrictions under the GDPR when transferring personal data to countries outside the EU/UK that are not considered by European authorities to have adequate data privacy laws, which currently include India. The various legal solutions to allow for these international data transfers, such as putting in place data transfer agreements, known as standard contractual clauses (SCCs), have been challenged through a number of high-profile cases. Another key issue under the GDPR is the strict requirements around the reporting of personal data breaches to data protection authorities (DPA) within 72 hours. Enforcement of the GDPR has also been very active, with total value of fines since adoption of the GDPR close to €5 billion.

More recently, the EU has been adopting a number of new data laws that will regulate the sharing and use of data, including information that does not involve any personal data, such as that collected from devices and machines. These new laws include:

- i. the Digital Services Act, which mainly regulates user-generated online data;
- ii. the Data Act, which mainly regulates the sharing of data from connected devices; and
- iii. the European Health Data Space, which will regulate the sharing of electronic health data, such as scientific research.

In addition, the EU has recently adopted the world's first artificial intelligence law, with the AI Act, and new cyber laws, as discussed further below. All of these existing and new European privacy and data laws require careful consideration to assess the application of these laws to the business and the development of a data governance program.

A key issue over the past few years has been the restrictions under the GDPR when transferring personal data to countries outside the EU/UK that are not considered by European authorities to have adequate data privacy laws, which currently include India. The various legal solutions to allow for these international data transfers, have been challenged through a number of high-profile cases.

# ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORKS

## U.S. AI Governance Framework

2023 marked an unprecedented wave of regulation and executive action driven by the rapid development and use of AI technologies globally. So far, 2024 has continued this trend. As the use of AI continues to accelerate, Indian organizations should consider developing an internal AI governance program to establish a foundation to comply with existing and future AI laws, mitigate AI legal and regulatory risks, and ensure the safe and responsible use of AI.



---

As the use of AI continues to accelerate, Indian organizations should consider developing an internal AI governance program to comply with existing and future AI frameworks, mitigate legal and regulatory risks, and ensure the safe and responsible use of AI.

The most significant recent development in the AI space in the United States was the comprehensive executive order issued in October 2023 by President Joe Biden. It required federal agencies, on an expedited timeline, to establish new standards for AI safety, privacy, and security across a range of industries. Federal agencies have completed all of the 90-day and 150-day actions tasked by the order, resulting in the promulgation of a wide range of new requirements and obligations that affect organizations in every industry. In turn, organizations deploying and/or using AI, particularly those that contract with the U.S. government, should keep abreast of guidance issued by federal agencies to ensure compliance and enhance business visibility into AI use. Similarly, the governors of multiple states have published executive orders with guidelines and principles for government agencies' use of AI.

Beyond federal regulations, state legislatures have also been active in regulating the use of AI in multiple contexts, including employment, insurance, and facial recognition. For example, New York City's Local Law 144, enacted in July 2023, was the first AI-related law prohibiting businesses operating in New York City from evaluating job applicants and/or promoting employees using AI-powered employment tools without conducting bias audits and providing notice to underlying individuals. And recently, Colorado became the first state to pass comprehensive AI legislation requiring certain compliance steps for high-risk AI deployments. It likely will not be the last state to pass specific requirements. In the meantime, administrative activity pursuant to the executive order is set to continue throughout 2024, with preliminary guidance recently issued by the Department of Commerce on April 29, 2024 — including a draft proposal to supplement Secure Software Development guidance for AI. It is an area of rapid policy activity and regulatory change.

The AI Act has a broad scope of application across all sectors and industries to companies both in and outside the EU. The AI Act imposes regulatory requirements on AI system providers, importers, distributors, and deployers in accordance with the level of risk involved with the respective AI system (being “unacceptable,” “high,” “limited,” and “minimal” risk).

Noncompliance with the AI Act may lead to regulatory fines of up to 7% of annual worldwide turnover.

Indian organizations developing, distributing, and using AI systems should consider developing an AI governance program and assess the impact and risk of AI and these new AI legal frameworks on their business to ensure compliance and the safe and responsible use and development of AI.

## EU and UK AI Governance Framework

The EU has recently implemented the AI Act, the first-ever stand-alone legal framework to govern the commercialization and use of AI systems throughout the EU. Many organizations deploy some form of AI that ultimately could be subject to the AI Act — whether internally or in customer-facing products and services. The AI Act has a broad scope of application across all sectors and industries of companies both in and outside the EU. The AI Act imposes regulatory requirements on AI system providers, importers, distributors, and deployers in accordance with the level of risk involved with the respective AI system (being “unacceptable,” “high,” “limited,” or “minimal” risk). Unacceptable-risk AI systems are banned from being offered and used in the EU, and high-risk AI systems are subject to stringent regulatory requirements that necessitate:

- i. the establishment of quality and post marketing monitoring and risk assessment systems;
- ii. the training of AI systems; and
- iii. the implementing of human oversight controls.

Limited-risk AI systems are subject mainly to transparency requirements only, and minimal-risk AI systems are not subject to obligations under the AI Act. General-purpose, foundation, and generative AI systems are subject to requirements similar to those for high-risk AI systems.

The AI Act is expected to become enforceable in a gradual manner, depending on the regulatory requirement in question, ranging from six to 36 months following adoption and entry into force of the AI Act, so some requirements will come into force during 2024. Noncompliance with the AI Act may lead to regulatory fines of up to 7% of annual worldwide turnover. In parallel, the EU has proposed revisions to the EU Product Liability Directive and has introduced a new EU AI Liability Directive to facilitate claims for damages brought by EU users of AI systems.

Indian organizations should assess whether they may be subject to the AI Act and consider its requirements on their products and services. Organizations developing, distributing, and using AI systems should consider developing an AI governance program and assess the impact and risk of AI and these new AI legal frameworks on their business to ensure compliance and the safe and responsible use and development of AI.

The UK is adopting a “soft law” approach to AI regulation, characterized by a cross-sector, principle-centered framework in which regulators will apply existing laws with supplementary guidance (in contrast to the EU’s approach). As highlighted above, organizations subject to the UK AI regime should consider the UK’s position on AI and implement an AI governance framework to address requirements.

# EVOLUTION OF CYBERSECURITY STRATEGIES AND LAWS

## U.S. Cybersecurity Strategy

... over the last few months the EU has adopted new cyber laws that impose detailed cybersecurity requirements and can impose personal liability on senior management and significant fines. It is important for Indian companies to be aware of the various requirements under these new cyber laws and implement a cybersecurity strategy to address their requirements.

In the United States, there continues to be refinement and strengthening of cybersecurity regulations and requirements across all sectorial regulatory regimes, driven in part by President Biden's National Cybersecurity Strategy. A key part of the National Cybersecurity Strategy is to focus on supply chain risk and software vulnerability management to strengthen private sector defenses. This policy leadership has in turn rippled across several updates to cybersecurity regulations, particularly in the financial services sector and others in critical infrastructure.

In November 2023, the New York Department of Financial Services adopted significant amendments to its cybersecurity regulations that will affect insurance, banking, and financial services organizations operating in New York City. These amendments include (but are not limited to) (i) executive oversight on cybersecurity programs, (ii) documenting and maintaining additional cybersecurity policies, (iii) implementing more enhanced technical controls, and (iv) conducting annual cybersecurity awareness training. In addition to these amendments, covered entities must oversee third-party service providers by addressing (i) the risk assessment of such service providers, (ii) minimum required cybersecurity practices, including multifactor authentication and encryption, (iii) due diligence processes to evaluate adequacy of such service providers, and (iv) periodic assessments of such service providers based on presented risks and continued adequacy of their cybersecurity practices.

Further, in October 2023, the FTC amended the Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA) to impose data breach reporting requirements on nonbanking financial entities, such as fintech companies, mortgage brokers, and retailers that extend credit (among others). According to these amendments, in-scope organizations are required to report to the FTC within 30 days after discovery of any incident affecting more than 500 consumers. In-scope organizations must also oversee third-party service providers by (i) taking reasonable steps to select and retain such service providers capable of maintaining appropriate safeguards, (ii) contractually requiring service providers to implement and maintain such safeguards, and (iii) periodically assessing service providers based on presented risks and continued adequacy of their safeguards.

For businesses operating in the critical infrastructure sectors, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency proposed significant cybersecurity reporting requirements that may require certain companies to report on certain cybersecurity incidents within tight timelines: 72 hours for "substantial cybersecurity incidents" and 24 hours for ransomware payments. Cyber risk management and governance has been another key trend in regulatory updates. For example, in July 2023, the Securities and Exchange Commission adopted new cybersecurity rules requiring publicly listed organizations to disclose cybersecurity incidents within four days of determining the incident is material, and also issues new requirements for disclosures around cyber risk management and strategy in annual risk disclosures to investors.





## EU and UK Cybersecurity Strategy

In addition to the information security requirements in relation to personal data that exist under the GDPR, over the last few months the EU has adopted new cyber laws that impose detailed cybersecurity requirements and can impose personal liability on senior management and significant fines. It is important for Indian companies to be aware of the various requirements under these new cyber laws and implement a cybersecurity strategy to address their requirements.

### THE NEW CYBER LAWS

#### The Network and Information Security 2 Directive (NISD2)

**To Whom It Applies:** This cyber law applies to “essential and important entities” and includes businesses in sectors such as transportation, energy, digital infrastructure, cloud computing service providers, managed service providers, and managed security service providers.

**When It Takes Effect:** NISD2 will take full effect and be enforceable following implementation into national EU member state law in October 2024.

**What You Need to Know:** NISD2 imposes stringent cybersecurity and incident reporting requirements, including reporting certain cyber incidents within 24 hours. Importantly, among the sanctions for noncompliance under NISD2 is the ability for senior management to be held personally liable, face administrative fines, or be temporarily suspended from managerial functions at the legal representative or chief executive officer level.

#### THE DIGITAL OPERATIONS RESILIENCE ACT (DORA)

**To Whom It Applies:** This new cyber law applies to entities in the financial services industry and the information and communication technology (ICT) third-party service providers with which they contract.

**When It Takes Effect:** DORA becomes enforceable as of January 2025.

**What You Need to Know:** DORA imposes regulatory obligations to reinforce the digital operational resilience of entities operating in the financial services industry and to adequately manage and remediate risks related to the engagement of ICT third-party service providers. Sanctions may be administrative or criminal in nature, while members of management bodies can also be held personally liable. Obligations include:

- i. implementing an internal governance framework to manage ICT risk with strategies, policies, and procedures to ensure digital operational resilience;
- ii. conducting annual assessments of internal governance;
- iii. reporting certain data incidents within 24 hours; and
- iv. maintaining a register of contracts with ICT third-party service providers and ensuring that such contracts have mandatory provisions prescribed under DORA. maintaining a register of contracts with ICT third-party service providers and ensuring that such contracts have mandatory provisions prescribed under DORA.

## THE CYBER RESILIENCE ACT (CRA)

**To Whom It Applies:** This cyber law applies to manufacturers, distributors, and importers of “products with digital elements” connected to a network or the internet (i.e., connected products) and related services which are commercialized and provided in the EU.

**When It Takes Effect:** The CRA enters into force in Q2 2024 and will enter into application with a phased transition of between 18 and 36 months, depending on the regulatory obligation in question.

**What You Need to Know:** The CRA requires manufacturers of products within scope of the CRA to ensure that their products meet certain “essential” cybersecurity requirements, for example:

- i. designing, developing, and producing products to ensure an appropriate level of cybersecurity based on the risks;
- ii. promoting data minimization;
- iii. including a “secure by default” configuration, with the option to reset digital products to their original state; and
- iv. ensuring that vulnerabilities are easily addressed via security updates.

Importantly, the CRA also imposes both vulnerability and incident handling requirements on manufacturers of such connected products — with manufacturers required to notify of any actively exploited vulnerability in such products, and any severe incident, within 24 hours to the competent authority.

## ABOUT THE FIRM

Sidley is an elite global law firm. With 2,300 lawyers, annual revenue of US\$3.1 billion, and experience that spans 158 years, we have established a reputation using Built to Win<sup>SM</sup> legal strategies in successfully representing clients in more than 70 countries on complex transactional, investigation, regulatory, and litigation matters.

With 21 offices strategically situated in key commercial and financial hubs throughout the United States, Europe, and Asia Pacific, our perspective and our reach are truly global. Our lawyers and business professionals, fluent in more than 80 languages, possess the cultural awareness and cross-border legal acumen needed to bring clarity to a dynamic business landscape.

### Contacts



**William RM Long**  
Partner  
London  
+44 20 7360 2061  
wlong@sidley.com



**Ash Nagdev**  
Counsel  
Palo Alto  
+1 650 565 7057  
anagdev@sidley.com



**Colleen Theresa Brown**  
Partner  
Washington, D.C.  
+1 202 736 8465  
ctbrown@sidley.com

# SIDLEY

AMERICA • ASIA PACIFIC • EUROPE

[sidley.com](https://www.sidley.com)

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at [www.sidley.com/en/locations/offices](https://www.sidley.com/en/locations/offices). Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at [www.sidley.com/disclaimer](https://www.sidley.com/disclaimer).

All service marks herein are registered or used by Sidley Austin Holding LLP worldwide. © 2023 Sidley Austin Holding LLP. All rights reserved.

MN-23346-05/24