

Bridewell

Cyber Security.
Where it Matters.

Global Regulatory Landscape Guide: 2026



 Cyber Consulting  Managed Security  Penetration Testing  Data Privacy

What's on the Horizon?

“

We recognise that staying up to date with the regulatory landscape isn't easy, especially as new legislation and frameworks are introduced. This is why, since 2024, our Horizon Scanning packs have summarised the key changes; helping you anticipate the regulations that will impact you and guiding you towards compliance. As always, our team are available to support you on this journey, and if you'd like to discuss anything you read in this pack, please feel free to get in touch.

”



Chris Linnell

Associate Director – Data Privacy

[Get in Touch](#)

What's New: UK and Europe

UK: Key Movements to Track

- The European Commission has reaffirmed that the UK provides an adequate level of data protection. As a result, personal data can continue to flow from the EEA to the UK under safeguards considered broadly equivalent to those in the EU. This decision is valid until 27 December 2031.
- Following Royal Assent, the UK's Data Use and Access Act (DUAA) is being rolled out in phases across 2025–26 - with most provisions commencing two to six months post-Assent and certain elements extending up to twelve months into 2026.
- The Cyber Security and Resilience Bill will bring medium and large IT/cyber security providers into scope to strengthen resilience for essential services (e.g., health, water, transport, energy) (Implementation timing expected as 1–2 years).
- The Crime and Policing Bill includes an amendment aimed at stopping the use of AI image and video generators to create prohibited content. It signals that regulators may place clearer legal duties on organisations across the AI content “supply chain,” with implementation likely in the next 1–2 years.

EU: Implementation and National Transposition Focus

- Cyber Resilience Act – implementing rule for “important/critical” products (effective 1 Dec 2025): Defines which digital-element products must undergo stricter conformity assessment - relevant for device/software manufacturers. Planning launches in 2026.
- NIS2 national measures:
 - **Germany** enacted its NIS2 implementation law for federal administration (effective 6 Dec 2025), reinforcing essential information-security management.
 - **Portugal** transposed NIS2 via Decree-Law 125/2025, applying to essential/important entities across public and private sectors (with core national-security carve-outs).
- EU AI Act national enablement: **Hungary's** AI Act (2 Aug 2026) sets up an institutional and enforcement framework to operate the EU AI Act domestically.

Non-EU: New Data Privacy Regime

- **Bosnia and Herzegovina** adopted its local Data Protection law in October 2025 which closely aligns with General Data Protection Regulation (GDPR).

United Kingdom

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
UK Data Use and Access Act	The Data (Use and Access) Act received Royal Assent on June 19, 2025. Key changes include the transformation of the Information Commissioner's Office into an independent body (the Information Commission) and clarification on the "purpose limitation" principle. It also expands the scope of automated decision-making, restricts Article 22 of the UK GDPR to decisions involving special category data, and requires organisations to implement direct complaint processes for data subjects. The Act also introduces a more risk-based approach to international data transfers and simplifies Subject Access Request compliance. Fines under PECR and the data breach reporting regime align more closely with the UK GDPR. It also introduces the right for the research companies for the secondary use of data without getting a separate consent. It extends soft opt-in rules to charities. It allows to set functional and performance cookies without user consent.	Data Privacy	All	The Act applies to organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK. The Act amends and supplements the UK General Data Protection Regulation ("UK GDPR"), Data Protection Act 2018 ("DPA 2018") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") in the areas including but not limited to: - Complaints; - Information Commission (replacing ICO) enforcement capabilities; - Organisations' DSAR obligations; - New assessment for international transfers; - Recognised list of legitimate interests; - Obligations for providers of services likely to be accessed by children; - PECR obligations, infringements, enforcement and fines.	June 2025-June 2026

Europe

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
EU AI Act	The EU AI Act aims to strengthen Europe's position as a global hub of excellence in AI and will govern anyone who provides a product or a service that uses AI. The Act will cover systems that can generate output such as content, predictions, recommendations, or decisions influencing environments. As part of the act, organisations must: • Ensure that their AI systems comply with the regulatory requirements set out in the Act. • Ensure that their AI systems are transparent and that users are informed about the AI systems they interact with. • Ensure that their AI systems comply with the harmonised regulatory framework when operating across multiple EU Member States. • Prioritise ethical AI development to contribute to the broader societal goals of the EU.	Artificial Intelligence	All	The EU AI Act builds on Europe's existing product liability laws, but it is tailored specifically to AI systems. It will govern anyone who provides a product/service that uses AI. Any AI system that is developed by an EU provider, wherever in the world it is deployed, is covered. Systems that are developed outside of the EU and put onto the EU market are also covered. The AI Act would also cover systems that are developed and used outside of the EU, if the output of those systems is intended for use in the EU. The Act covers systems that can generate output such as content, predictions, recommendations, or decisions influencing environments. It does not cover personal use.	Entered into force on August 2, 2024. The full enforcement from August 2, 2026

Europe

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
German act implementing the EU NIS“ Directive: Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI Act, BSIG),	Act on the implementation of the NIS2 Directive and on the regulation of essential principles of information security management in the federal administration and critical sectors.	Cyber Security	Wide range of sectors including but not limited to: energy, transport, health, digital infrastructure, research, operators of critical installation and operators of public networks and services.	Cybersecurity obligations for operators of essential and important entities (classification follows a combined system based on sector and size and includes organisations that are not classified as essential but still play a critical role in the economy and society), Core principles for information security management within the federal administration and in-scope entities, including risk management, incident reporting and governance requirements. The sector-specific security obligations remain in force and are supplemented by NIS2 requirements.	Effective from December 6, 2025
Portugal Decree-Law 125/2025	This Law transposes the NIS2 Directive into national legislation	Cyber Security	Public and private entities	The Decree-Law applies to both public and private entities, including essential and important entities in critical and other key sectors, but excludes entities in national security, defense, intelligence and criminal investigation for systems directly related to their core functions (priority of the sector-specific security obligations).	Effective from April 3, 2026

Europe

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
The Implementing Regulation (EU) 2025/2392	Outlines important and critical products with digital elements under the Cyber Resilience Act (CRA).	Cyber Security	All	Defines which products with digital elements are considered “important” or “critical” under the CRA and therefore must undergo stricter conformity assessment procedures.	Effective from December 1, 2025
Digital Omnibus Regulation	The aim of the Omnibus is to simplify existing rules on artificial intelligence (AI), cyber security, and data. The Omnibus is complemented by a Data Union Strategy and European Business Wallets that will offer companies a single digital identity.	Data Privacy, Artificial Intelligence and Cyber Security	All	Consistent application of rules across areas such as online platforms, data governance, cyber security, and consumer protection, procedural and enforcement mechanisms to streamline compliance and cross-border oversight for the companies operating in the EU. The scope includes amendments to the Data Act, GDPR, ePrivacy Directive, NIS2 and AI act with a focus on efficiency and compliance for businesses.	1-2 years
Norway Act on Artificial intelligence	The Ministry of Digitisation and Administration published the draft AI Act for consultation. The deadline for submission of comments is September 30, 2025	Artificial Intelligence	All	Implementation of the EU AI act and supplementation with national rules on supervision and enforcement - including allocation of responsibilities with Norwegian Communications Authority (Nkom) as coordinating market-surveillance authority, sanctions tools, geographic applicability and supporting measures such as a regulatory AI sandbox - so the EU’s risk-based AI requirements can be applied and enforced in Norway.	<1 year

Europe

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
New EU Rules to improve cooperation between national data protection authorities (DPAs) for handling cross-border data protection complaints (adopted by European Council)	The new EU rules standardise complaint admissibility so the same basic information is required no matter which Member State receives the complaint. They also strengthen procedural rights (including the right to be heard and to comment on preliminary findings) and streamline case handling, with a simplified cooperation route for straightforward cases.	Data Privacy	All	Applies to all cross-border GDPR complaints and enforcement processes, establishing uniform rules for admissibility, enhanced procedural rights for complainants and investigated parties, binding investigation timelines (15 months for complex cases; 12 months for simpler cooperation proceedings), as well as streamlined cooperation and early-resolution mechanisms among national data protection authorities.	Effective from February 2027
Hungary AI Act	Establishes multi-tiered governance structure and designates the National Accreditation Authority (NAH) as the notifying authority. Defines procedural and enforcement framework for implementing the EU Artificial Intelligence Act (the EU AI Act).	Artificial Intelligence	AI industry	Applies to AI service providers, users, manufacturers, and importers in Hungary and foreign entities whose AI system outputs are used within Hungary. Covers key areas such as: •Prohibition of unacceptable AI practices •Obligations for high-risk systems •Transparency obligations on certain models •Exceptions for minimal-risk applications	Effective from August 2, 2026
Italy AI Law	Integrates and implements the broader European AI regulatory framework (EU AI Act) by establishing the responsibilities for AI governance and supervision in Italy. It designates National Cybersecurity Authority (ACN) as the supervising and enforcement authority.	Artificial Intelligence	All, has specific provisions for health, labor, intellectual professions, public administration, and judiciary.	The AI Law applies to all uses of artificial intelligence in across both public and private sectors. Key provisions cover among other aspects: •Human oversight and traceability •Access by children under 14 •Criminal penalties •Copyright	Effective from October 10, 2025

What's New: USA

USA: Key movements to Track

The US remains a state-by-state patchwork, with fast-moving developments in privacy, child/teen online protections, breach response, and AI accountability. There is a shift toward operational controls: risk assessments, privacy-by-default for minors, transparency obligations for AI/data practices, and stronger enforcement.

January 2026 marked the effective date for several privacy measures in different states:

- California introduces new risk assessment obligations, under-16 data treated as sensitive (right-to-limit), a 30-day breach notification deadline, and stronger penalties for unregistered data brokers.
- Indiana's Consumer Data Protection Act also takes effect, setting a baseline privacy regime for in-scope organisations, with consumer rights and transparency obligations broadly aligned to the Virginia-style model.

Later in the year, California's and Colorado's AI measures start to take effect. From 30 June 2026, Colorado's AI Act introduces a risk-based framework for high-risk AI systems to reduce algorithmic discrimination. From 2 August 2026, California's AI Transparency Act begins a phased rollout of provenance/disclosure expectations for

AI-generated content, with staged milestones continuing into 2027.

Across other states, three themes stand out:

- Child/teen safety drives Vermont's Age-Appropriate Design Code Act (effective 1 January 2027) and Michigan's HB 5357 (~18–24 months), both pushing high-privacy defaults and restrictions on profiling, sales, targeted ads and dark patterns for minors.
- Sensitive data regulation is tightening via Pennsylvania's HB 1530 (~1–2 years), targeting direct-to-consumer genetic testing with enhanced consent, security, and deletion/sample-destruction expectations.
- AI transparency and security are accelerating in New York (algorithmic pricing disclosure and AI "companion" rules already effective, plus the proposed RAISE Act), alongside phased cyber security regulation amendments; Florida's proposed AI Bill of Rights and data-centre measures point to growing links between AI governance and wider technology infrastructure controls.

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
The American Privacy Rights Act (APRA)	The proposed Act, introduced on 7 April 2024, seeks to 'patch together' the increasing number of state privacy laws and is intended to strengthen individuals' control over their personal data. However, it remains some way from being enacted and has already attracted criticism. For example, privacy stakeholders in California have expressed concern that the Bill could dilute existing safeguards by replacing legislation that provides stronger consumer protections.	Data Privacy	All	Covered entities include those that collect, process, retain, or transfer personal data (or have it done for them) and who are already subject to the Federal Trade Commission (FTC) Act. Small businesses, governments and the National Centre for Missing and Exploited Children are exempt. Small businesses have been defined as those: • With \$40M or less in annual revenue. • That collect, process, retain, or transfer the covered data of 200,000 or fewer individuals. • That do not earn revenue from transferring covered data to third parties (i.e., data brokers).	>3 years
US AI Bill	A US AI Bill is expected to follow the EU AI Act; however, the process is still in its early stages, and the path forward for US AI policy remains uncertain. A blueprint was unveiled in October 2022, but this is strictly a voluntary instrument and does not represent official US policy.	Artificial Intelligence	All	The scope will likely cover all AI systems in the US.	>3 years

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
California Consumer Privacy Act	The California Consumer Privacy Act (CCPA) is a state privacy law that gives consumers greater control over how businesses collect, use and share their personal information. It requires certain organisations to assess and manage privacy risks for higher-risk processing (including risk assessments from 1 January 2026, for specified activities) and strengthens consumer rights, such as opting out and accessing personal information (including, in some cases, data held from 1 January 2022). It also promotes data accuracy by requiring businesses to maintain corrected information and provides extra protections for under-16s by treating their personal information as sensitive and subject to the right to limit its use.	Data Privacy	All	Applies to for-profit entities doing business in California that collect and determine the purposes and means of processing personal information and meet certain revenue or data-processing thresholds. It governs how businesses collect, use, sell, and share consumers' personal information, while also outlining specific exemptions and circumstances under which businesses may handle data, such as complying with legal obligations or processing deidentified information.	Updates effective from January 1, 2026
California: Bill on customer notification of data breaches	The Bill requires individuals or businesses to disclose data breaches to affected consumers within 30 calendar days of discovery or notification of the data breach. Disclosure may be delayed to accommodate the legitimate needs of law enforcement, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Data Privacy	All	Any individuals or businesses that maintain computerised personal information of California residents. Mandates 30 days notification and allows delays in case of legitimate needs of law enforcement or to determine the scope of the breach. If more than 500 California resident are affected the attorney general must be notified within 15 calendar days after notifying affected individuals.	Effective from January 1, 2026
California Assembly Bill 566 California Consumer Privacy Act of 2018: opt-out preference signal	Prohibits businesses from developing or maintaining a mobile operating system that does not include a setting that enables a consumer to send opt-out preference signals. The bill defines 'opt-out preference signal' as a signal that communicates the consumer's choice to opt out of the sale and sharing of the consumer's personal information.	Data Privacy	Technology, software, and digital services	Covers businesses that develop or maintain mobile operating systems or web browsers. requiring to include functionality configurable by a consumer that enables the browser to send an opt-out preference signal to businesses with which the consumer interacts through the browser.	Effective from January 2027

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
California Senate Bill 243 Companion chatbots	The Act introduces obligations for operators of companion chatbots, aiming to make companion chatbot platforms safer for users.	Data Privacy	Technology, software, and digital services	Persons making a companion chatbot platform available to users in California. The law excludes chatbots used for customer service only, business operations, video game interaction and stand-alone consumer electronic devices that do not sustain ongoing relationships or elicit emotional responses.	Obligation to report to the Office of Suicide Prevention from July 1, 2027
California Bill on Age Verification Signals	Operating system providers must provide an interface for age verification at account setup, and developers must request age signals from operating system providers.	Data Privacy	Technology, software, and digital services	The Act applies to operating system providers and developers, excluding broadband internet access services and telecommunications services.	Effective from January 1, 2027
California AI transparency Act	Mandates provenance data disclosure for AI-generated content and latent disclosures for capture devices.	Artificial Intelligence	Technology, software	Act defines generative AI systems as those capable of producing synthetic content that emulates the characteristics of their training data; sets requirements for providers to provide AI detection tools and offer users the option to provide disclosures about AI-generated content and embed it within the content itself; provider licensees must enter into contract to ensure the AI system maintain the capability to include latent disclosures in the content it generates or alters.	Staged effective dates from August 2, 2026 to January 1, 2027
California Enforcement Advisory No. 2025-01	Under the DELETE Act, an unregistered data broker may face a \$200 per-day administrative fine, payment of overdue registration fees, and investigation/administration costs as determined by the court. Calprivacy is empowered to pursue administrative action against brokers that fail to register.	Data Privacy	Data brokers	Data brokers are required to independently register, even if they are subsidiaries of a parent company. All trade names and websites must be accurately listed during registration, Information about the trade names must be verified.	Effective from January 2026

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Indiana Consumer Data Protection Act (ICDPA)	The Indiana Consumer Data Protection Act (ICDPA) protects the consumer data privacy of Indiana residents. It closely follows the provisions present in other US state laws regulating the same matter and was signed into law on May 1, 2023.	Data Privacy	All (exemptions listed within the scope)	The ICDPA applies to organisations conducting business in Indiana, and any business that offers products or services targeted to Indiana residents. There are two threshold criteria for organisations under the law: • Control or process the personal information of at least 100,000 Indiana residents during a calendar year, or • Control or process the personal information of at least 25,000 Indiana consumers during a calendar year and derive more than 50% of their gross revenue from the sale of personal information. Exemptions include government entities, non-profits and higher education entities.	Effective from 1 January 2026
Florida AI Bill of Rights and Data Centers Bill	Florida is advancing paired proposals that set consumer-facing AI guardrails - including AI use disclosures, protections for minors/parental controls, and limits on certain high-impact uses (e.g., AI-provided “licensed” therapy and AI use in insurance claims) - and regulate hyperscale data centers by tightening siting/ approval processes, constraining utility cost pass-throughs to ratepayers and adding protections, including restrictions tied to foreign principals and sensitive land classifications.	Artificial Intelligence	All	Applies to AI providers and deployers interacting with Florida consumers (and state/local agency AI use/ procurement), plus developers/operators of hyperscale data centers seeking to build or operate in Florida, with compliance obligations spanning transparency, privacy/child safeguards, and infrastructure impacts (cost, land use, water).	1-2 years

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Pennsylvania House Bill 1530	The Bill would require direct-to-consumer genetic testing companies to plainly explain how they collect, use and share genetic data, and to obtain express consent before collecting or disclosing it (with separate opt-ins for certain additional uses/transfers). It also requires a comprehensive security program and gives consumers the ability to access and delete their genetic data/account and request destruction of stored biological samples. The Pennsylvania Attorney General may enforce the law through civil actions, and courts may impose civil penalties (noted as \$2,500 per violation) plus actual damages and recovery of enforcement costs/fees.	Data Privacy	Genetic testing	Applies to entities that offer direct-to-consumer genetic testing or collect/use/analyze genetic data from those services for Pennsylvania consumers. Excludes entities that are only handling genetic data/samples solely in the context of regulated research (as defined and governed by referenced federal human-subjects frameworks including HIPAA and HITECH).	1-2 years
The Vermont Age-Appropriate Design Code Act	Prohibits collection, selling or sharing minors' data unless necessary and restrict content recommendation and push notifications to minors. It mandates transparency and duty of care with specific rules on monitoring minors and data usage.	Data Privacy	All	Applies to businesses processing children's data, children are defined as users under 18.	Effective January 1, 2027 with some sections effective from July 1, 2025

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Colorado Artificial Intelligence Act (CAIA)	Enacted on May 17, 2024, the CAIA addresses the development and deployment of "high-risk" AI systems and their potential to cause "algorithmic discrimination." It is the first comprehensive, risk-based approach to AI regulation to be signed into law in the United States.	Artificial Intelligence	All	The CAIA primarily regulates the development and deployment of AI systems in particular applications; namely, what the CAIA defines as "high-risk AI systems". Deployers that meet the following criteria are exempt from the CAIA: • The deployer employs less than 50 people. • The deployer does not use its own data to train the system. • The system deployed is used for its intended purpose (as specified by the developer and required under the CAIA). • The deployer makes available to consumers the impact assessment provided by the developer.	Implementation delayed from Feb 2026 to June 30, 2026
Virginia Senate Bill 854	Amends Virginia's Consumer Data Protection Act to require operators of a social media platform to use commercially reasonable age-assessment methods (e.g., a neutral age screen) to identify users under 16, and to impose a default one-hour-per-day limit per service/app (with the ability for a parent to adjust that limit via verifiable parental consent). Platforms may use information collected for age assessment only for age determination/age-appropriate experiences, and they may not withhold/degrade features or increase prices because a user is subject to the time limit. Note: although earlier versions discussed broader "addictive feed" restrictions, the enacted approach primarily centers on the time-limit + age-assessment model.	Data Privacy	Social Media	Applies to minors under 16 (the bill defines "minor" as a natural person younger than 16) using a social media platform in Virginia.	Effective from January 1, 2026

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Amendment to the Business & Commerce code, Texas	The amendment requires data brokers with a website or mobile app to post a conspicuous, plain, accessible notice stating they are a data broker and explaining how consumers can exercise applicable privacy rights (using required language set by the Secretary of State). It also expands what must be included in the data broker registration statement, adding (among other items) contact details, a prominent link with instructions for exercising privacy rights, categories of data processed/transferred, whether the broker uses purchaser credentialing, disclosures about known children’s data practices/compliance, and security-breach counts and affected consumers.	Data Privacy	All	Applies to entities that meet the Texas definition of a “data broker” under the Business & Commerce Code and that (a) maintain an internet website or mobile application (for the notice requirement) and/or (b) file a data broker registration statement with the Texas Secretary of State (for the expanded registration disclosures). The updated registration-statement content applies to registration statements submitted on or after the amendment’s effective date, and the consumer-rights references align with rights available under Chapter 541 (Texas privacy rights framework).	Effective from September 1, 2025
Texas Senate Bill 1188	Mandates that electronic health records (EHRs) containing patient information physically stored in the U.S./U.S. territories (including cloud/subcontractors), restrict access to those who need it for treatment, payment, or operations, and implement reasonable safeguards. It also bars EHRs from including credit scores or voter registration status and requires practitioners who use AI for diagnosis/treatment recommendations to review AI-created records and disclose AI use to patients.	Data Privacy	Health care providers	Applies to Texas “covered entities” (as defined in Health & Safety Code §181.001, including health care practitioners, with specified exclusions) and to EHR systems/records under their control, including vendor/cloud-hosted records. Most provisions apply to EHRs prepared on/after 1 Sept 2025, while the U.S. storage requirement applies to EHR storage on/after 1 Jan 2026 regardless of when the record was created.	Effective from September 1, 2025

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
The New York Artificial Intelligence Companion Models Act	The Act defines 'AI companion' as a system using artificial intelligence (AI), generative AI, and/or emotional recognition algorithms to simulate social human interaction, by retaining information on prior interactions and user preferences, asking questions, providing advice, and engaging in simulated conversation on matters of personal well-being.	Artificial Intelligence	Operators using AI systems simulating social human interactions	Applies to entities that operate or provide AI companions to users located in New York State. Generally excludes systems used only for customer service, internal/employee productivity, or primarily for efficiency improvements, research, or technical assistance.	Effective from November 14, 2025
New York Algorithmic Pricing Disclosure Act	The Act treats it as a deceptive act or practice under New York's General Business Law for a business to knowingly offer or promote a personalised algorithmic price - i.e., a price set by an algorithm using a particular consumer's personal data - without a clear, conspicuous disclosure shown with the price. The required disclosure is the statement: "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA."	Data Privacy	Businesses using algorithmic pricing	Applies to persons/entities doing business (or domiciled) in New York that use personalised algorithmic pricing (dynamic pricing set by an algorithm using personal data) and advertise, present, or otherwise communicate that price to consumers in New York without the mandated disclosure. Common carve-outs include certain insurance-regulated entities and specified financial institutions plus limited situations such as certain subscription-based pricing scenarios.	Effective from November 10, 2025
New York Cybersecurity Regulation Amendments	New obligations under the Cybersecurity Regulation as amended by the New York State Department of Financial Services (NYDFS) expands multi-factor authentication expectations to cover remote access and third-party access to information systems, requires more rigorous asset management—including a complete, accurate asset inventory and stronger data retention/secure disposal controls and elevates third-party cyber-risk governance through more prescriptive requirements for managing vendor and service-provider security risk.	Cyber Security	All	Applies to NYDFS-regulated entities and individuals (i.e., "Covered Entities" operating under, or required to operate under, a licence/charter/registration or similar authorisation under New York's Banking, Insurance, or Financial Services laws), with different requirements for entities that meet the Class A threshold and those that fall under limited/ small-entity exemptions.	Effective from November 1, 2027

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Guidance on Managing Risks Related to Third-Party Service Providers (New York)	The guidance provides that covered entities must develop a tailored, risk-based plan to mitigate risks posed by each Third-party service provider (TPSP) and perform due diligence on TPSPs through a proactive, risk-based and continuously adaptive third-party governance programme.	Cyber Security	Financial services	Applies to all NYDFS “Covered Entities” subject to 23 NYCRR Part 500 that use TPSPs for services involving access to information systems and/or nonpublic information (e.g., cloud, file-transfer, AI, fintech and similar managed technologies). The guidance is intended to clarify and operationalise Covered Entities’ existing third-party obligations under Part 500 (including expectations around due diligence, contracting, and oversight of TPSP cyber risk), and it is relevant regardless of whether the TPSP is critical, offshore, or uses downstream subcontractors—because NYDFS highlights the need for tailored risk treatment by provider and service.	October 21, 2025
The RAISE Act (New York)	The RAISE Act amends New York’s General Business Law to impose safety, transparency, and incident-reporting duties on developers of frontier AI models, including requirements to maintain/publish safety protocols and to avoid deploying models that pose an unreasonable risk of “critical harm” (e.g., mass-casualty outcomes or ~\$1B in damages). It also requires 72-hour reporting of qualifying safety incidents and provides for state enforcement (with an NYDFS oversight function and Attorney General authority), with civil penalty levels reflecting the signed framework/expected chapter amendments.	Artificial Intelligence	AI	Applies to “large developers” of “frontier models” that are developed, deployed, or operating (in whole or in part) in New York, with exclusions for certain academic research contexts (and other carve-outs described in commentary). The definitions and thresholds for “large developer” are the key trigger (initially framed around compute-cost/FLOPs thresholds, with a publicly reported plan to shift to a revenue-based threshold (e.g., >\$500M annual revenue) via chapter amendments).	1-2 years

USA

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Michigan House Bill 5357	The Bill would require online services used by known minors to default to high-privacy and safety settings (e.g., tighter limits on account visibility, sharing, messaging, and precise geolocation) and to bar common high-risk practices such as selling minors' data, dark patterns, targeted ads, and unnecessary profiling. It also requires age-appropriate privacy notices, alerts when a minor is tracked/monitored, data minimisation, and easy tools for minors/parents to report harms.	Data Privacy	Online services	Applies to for-profit businesses doing business in Michigan that provide online services/products/features accessed by known minors, generally triggered where the business meets size thresholds (e.g., >\$25M annual revenue or processes personal information of 50,000+ consumers/households). The bill is framed to govern how these covered services collect/use/share minors' personal information and how they configure default settings and product design for minors	1.5-2 years

What's New: Global



Global: New Comprehensive Privacy Regimes, AI regulation and Cross-border Transfer Compliance

Outside the EU/UK and USA, regulation is accelerating, with many jurisdictions moving toward enforceable privacy, tighter cross-border transfer controls, stronger cyber security oversight, and early but fast-maturing AI governance.

January 2026 marks the effective date for several major Asia-Pacific measures: Vietnam's Personal Data Protection Law takes effect on 1 January 2026, introducing a comprehensive framework with cross-border transfer conditions and significant penalties; China's Cybersecurity Law amendments also take effect on 1 January 2026, reinforcing cybersecurity governance and linking it to AI security/development; and China's Measures for Authentication of Personal Information Exported Abroad begin the same day, adding a certification-based pathway for certain international transfers.

March 2026 brings a further AI milestone, with Vietnam's AI Law effective 1 March 2026, embedding fairness, transparency and accountability principles and higher expectations for riskier applications.

Other themes stand out across different jurisdictions:

- Cross-border transfer compliance is becoming more structured, with Chile's Model Contractual Clauses (valid until December 2026) and India's DPDPA Rules phasing in through May 2027 (alongside proposed amendments affecting children's protections).
- Comprehensive privacy regimes and enforcement readiness are expanding (e.g., Gambia's DP law and proposed reforms in Bangladesh and Colombia). A longer-horizon datapoint is Paraguay's DP act listed for November 2027, reinforcing continued global convergence.
- Cybersecurity and "trustworthy AI" controls are tightening, including Singapore's expanded cybersecurity oversight, Canada's proposed critical cyber systems framework, and practical AI security/assessment guidance from South Korea and Australia.

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Australian Privacy and Other Legislation Amendment Bill 2024	On 10 December 2024, the Privacy and Other Legislation Amendment Bill 2024 received Royal Assent, amending the Privacy Act to strengthen enforcement and introduce new privacy measures. Key changes include allowing courts to award compensation for privacy breaches and requiring organisations using automated decision-making to disclose relevant data use in their privacy policies. The automated decision provisions subject to a two-year grace period ending 10 December 2026.	Data Privacy	All	The Bill applies to any person who processes or has control over the processing of personal data. It applies to all foreign entities offering products or services to individuals or organisations in Australia, even if personal information is not initially collected.	Effective from 10 December 2024 and fully effective prior to 10 December 2026.
The Children’s Online Privacy Code (Australia)	Public consultation launched seeking feedback for drafting the Children's Online Privacy Code. Feedback can be submitted until July 31, 2025	Data Privacy	All	Entities (Privacy Act-regulated organisations) that operate online services likely to be accessed by children, i.e., entities handling children’s personal information in an online context covered by the forthcoming Code.	Expected by December 2026
The AI Impact Assessment Tool Australia	The Guidance provides step-by-step advice on AI procurement in line with the Digital Sourcing Lifecycle to help Australian Government teams identify, assess and manage risks and impacts of AI use cases against Australia’s AI Ethics Principles and to support compliance with the Government’s responsible AI policy.	Artificial Intelligence	Government bodies	Applies to Australian Government agencies/teams planning, procuring, or deploying AI use cases (including where AI materially affects decision-making, service delivery, or public interaction), and is designed to be embedded into existing governance, risk and procurement workflows.	Advisory

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Brazil AI Bill	Brazil is advancing a comprehensive AI governance bill that would consolidate and replace earlier draft proposals and set national rules for the ethical and responsible development and use of AI. The proposal follows a risk-based model inspired by the EU approach, pairing baseline duties with stricter controls for high-risk systems and prohibitions for “excessive-risk” uses.	Artificial Intelligence	All	Applies broadly to activities involving the development, provision, distribution, or operation of AI systems in Brazil (including general-purpose and generative AI), across sectors. Commonly cited exclusions include AI used for private, non-economic purposes, national defence, certain research activities, and some open/free formats—unless the system is classified as high risk.	1 - 3 years
Brazil Bill No.36/2025	Bill No. 36/2025 would amend Brazil’s LGPD to add a definition of “sensitive biometric data” (biometric personal data derived from technical processing of physical, physiological, or behavioural traits — e.g., fingerprints and DNA) and to ban its commercialisation (any transfer/availability in exchange for payment). Violations would be subject to LGPD sanctions, including fines of up to 2% of the entity’s revenue in Brazil, capped at BRL 50 million per violation (with stricter consequences for repeat/non-compliance referenced in the legislative materials).	Data Privacy	All	Applies broadly to any person or entity (public or private, domestic or foreign) that processes sensitive biometric data in Brazil or targets the Brazilian market, and specifically to any arrangement involving paid disclosure/transfer of such biometric data to or from the data subject.	<1 year

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
General Regulations for the Application of Legitimate Interest as a Basis for the Legalization of the Processing of Personal Data within the Territory of the Republic of Ecuador	The regulation (issued by Ecuador’s data protection authority, SPDP) clarifies when “legitimate interest” can be relied on as a lawful basis for processing personal data, requiring controllers to demonstrate that their interest is lawful and that it does not override the data subject’s rights. It operationalises this through a prior, documented balancing assessment (evaluación de ponderación) and reinforces transparency and accountability expectations when processing without consent.	Data Privacy	Private entities	Applies only to private-sector data controllers in Ecuador that intend to use legitimate interest as the legal basis for a processing activity; the regulation is described as mandatory for the private sector, and public-sector entities are excluded from using this basis.	Effective from November 7, 2025
Colombia Bills No. 214/2025 and No. 274/2025	Amendments to the Data Protection Law, expanding extraterritorial reach; adding definitions for biometric/genetic data, profiling and automated decisions; allowing consent by adolescents 14+ (with parental authorisation under that age); broadening lawful bases beyond consent (e.g., contract/legal duty/vital interests); tightening international transfer rules (adequate destinations or approved safeguards such as BCRs and model contractual clauses); and increasing/strengthening sanctions and accountability obligations).	Data Privacy	All	The reform would apply to controllers and processors inside or outside Colombia when processing is carried out in Colombia or is linked to offering goods/services to people located in Colombia or monitoring their behaviour in Colombia.	1-2 years

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Law 21.719 is Chile’s major privacy reform	It overhauls and modernises the existing regime by modifying Law No. 19.628 (previously framed around “vida privada”) into a data-protection framework focused on “datos personales”, with stronger requirements for processing and enforcement.	Data Privacy	All	Applies broadly to the processing of personal data of natural persons by public and private entities, and it includes territorial and extraterritorial reach in specified scenarios (e.g., when processing is linked to Chile). It excludes processing carried out purely for freedom of expression/information purposes and certain personal/household activities by individuals.	Promulgation: 25 Nov 2024 Publication in the Official Gazette: 13 Dec 2024 General entry into force (deferred): 1 Dec 2026
Chile Model Contractual Clauses	Chile’s Ministry of Economy (Subsecretaría de Economía y Empresas de Menor Tamaño) approved Model Contractual Clauses (MCCs) as an “appropriate safeguards” mechanism to enable international transfers of personal data under Chile’s new data-transfer rules). The approval was issued via Exempt Resolution RAEX202503748 (dated 11 Dec 2025) and later published in the Official Gazette on 19 Dec 2025, making the MCCs formally available for use.	Data Privacy	All	The MCCs are intended for transfers to destinations that are not covered by an adequacy finding, allowing exporters to rely on standard contractual safeguards instead. They include two templates aligned to common transfer relationships: • Controller-to-Controller and • Controller-to-Processor.	Effective until December 1, 2026 (may be reviewed in line with the date the new Data Protection Law becomes enforceable).

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Paraguay Personal Data Protection Act	Establishes the country's first comprehensive, GDPR-style framework for personal data processing, setting out core principles, lawful bases, enhanced consent requirements, data subject rights, rules for international transfers, and governance measures and an independent data protection authority. It also introduces organisational obligations such as security measures and incident-notification expectations and oversight by the new National Personal Data Protection Agency, with a transition period before full enforceability.	Data Privacy	All	The Act applies to personal data processing in Paraguay and has extraterritorial reach, capturing organisations that (among other triggers) are present in Paraguay, process data of individuals located in Paraguay, offer goods/services in Paraguay, or monitor behaviour of individuals located in Paraguay.	November 27, 2027
Argentina Data Protection Law Draft	The Chamber of Deputies in Argentina has launched a public consultation on a draft law to establish a new framework for personal data protection, replacing the 2000 Act. It outlines principles such as lawfulness, purpose limitation, and transparency, and provides lawful bases for data processing, data subject rights, and organisational obligations. The text is framed as a modern, flexible regime for privacy in digital environments and explicitly addresses emerging technologies, including AI and inferred data, with staggered/transition-style implementation concepts discussed in accompanying commentary. Public comments on the proposal were open until 25 July 2025.	Data Privacy	All	The proposal applies broadly to domestic and foreign public or private actors where: • processing occurs in Argentina or the entity offers goods/services to people in Argentina; • it involves data of individuals resident in Argentina, even if processing happens abroad; • it covers automated or non-automated processing, including inferred data, and explicitly brings in AI systems that process personal data in ways relevant to decisions about individuals.	1-2 years

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Canada Bill C-26	On 14 th June 2022, the House of Commons of Canada introduced Bill C-26, the Act Respecting Cyber Security (ARCS), proposing new cybersecurity requirements to protect Canada's vital systems and services. The Act ensures that cybersecurity risks, including those from supply chains and third-party services, are identified and managed; critical cyber systems are protected, and incidents detected; and the impacts of incidents are minimised.	Cyber Security	All	The bill will impose duties on "designated operators," which the government will classify. These operators include individuals, partnerships, or organisations operating businesses under Parliament's legislative authority concerning vital services or systems.	1 - 3 years
Canada Bill C-8 on Cybersecurity	Creates a federal cybersecurity regime by (1) amending the Telecommunications Act to make the security of Canada's telecom system a core policy objective and to enable binding security directions/orders for telecom service providers, and (2) enacting the Critical Cyber Systems Protection Act (CCSPA) to protect "vital services and vital systems" that are critical to national security or public safety. Under the CCSPA, designated operators must implement and maintain a cybersecurity program, manage supply-chain/third-party risks, and report cybersecurity incidents (and comply with government cyber directions), backed by enforcement powers and consequences for non-compliance.	Cyber Security	Critical cyber systems	Applies to federally regulated critical infrastructure: telecommunications service providers (Part 1) and operators of "vital services or vital systems" whose critical cyber systems support services/systems that are within federal legislative authority (Part 2 / CCSPA). The Governor in Council may designate what counts as a vital service/system and establish classes of operators and CCSPA obligations attach to entities designated as operators that own, control, or operate the relevant critical cyber system.	1-2 years

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Ethiopia Personal Data Protection Bill (PDPP)	On 4 April, 2024, the Ethiopian House of Peoples' Representatives announced that Parliament had approved the Personal Data Protection Bill. The Bill defines data subject rights, sets principles for personal data processing, and outlines conditions necessary to protect individual rights during data processing. It also establishes an independent supervisory authority.	Data Privacy	All	The scope of the Bill applies to any personal data applicable to a data controller or data processor: - established in Ethiopia and the data is compiled by the organisation in terms of context; or - not established in Ethiopia, the data is processed using a device located in Ethiopia and is not intended to leave Ethiopia, but only if there is an agent based in Ethiopia.	1 - 3 years
Gambia The Personal Data Protection and Privacy Act	A comprehensive data protection law, giving rights to the data subjects, prescribing controller and processor obligations and introducing enforcement for non-compliance.	Data Privacy	All	Processing carried out by controllers and processors established in Gambia or outside Gambia where the processing relates to individuals within the jurisdiction of Gambia.	Effective from November 13, 2025
Bangladesh Bill for the Personal Data Protection Ordinance	The bill sets out rules for the lawful processing of personal data, to safeguard privacy, confidentiality and security, aligns with best practice principles and recognises personal data as a right of the data subject.	Data Privacy	All	This bill will apply to any data fiduciary or processor that: - is domiciled, ordinarily resident, or ordinarily operating in Bangladesh; - processes personal data in Bangladesh (excluding mere transit); - or processes personal data outside Bangladesh where it relates to offering goods or services to, or monitoring/profiling, individuals located in Bangladesh.	Less than 1 year, awaiting President's assent

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
South Korea Publication and Distribution of Artificial Intelligence (AI) Security Guide	The Guide aims to help stakeholders prevent security threats related to AI technologies and services, ensure the safety of data and systems, and foster a trustworthy AI environment for developers, service providers and users.	Artificial Intelligence	All	The Guide applies to AI model developers, AI service providers, and users, and sets out CIA-based (confidentiality, integrity, availability) cybersecurity requirements to protect AI models/services from external attacks, presented as a structured checklist across the AI lifecycle plus user security rules.	Published on December 10, 2025
Bill 2210903 (South Korea)	Amends the Act on the Development of AI and Creation of a Trust Base. It outlines a mechanism for generative artificial intelligence to verify with copyright holders that the content they created is being used as training data. It also requires the AI business operators to put in place procedures for copyright holders to confirm whether their work has been used as training data.	Artificial Intelligence	All	The Bill focuses narrowly on training-data transparency for generative AI: when a copyright holder requests confirmation, AI businesses would be required to provide a process to verify whether the work was used as training data. Its practical impact falls on developers/operators of generative AI (and related AI businesses) that maintain or control training datasets and must be able to respond to rightsholder verification requests.	Effective from January 22, 2026
Singapore The Cybersecurity (Amendment) Act	The Act updates the Cybersecurity Act 2018 by strengthening and extending CII (Critical Information Infrastructure) regulation (including virtual systems used to deliver essential services) and introducing a framework for regulating Temporary Cybersecurity Concern (STCCs) during high-risk periods.	Cyber Security	All	Covers CII owners/essential service operators and STCC owners who must implement specified safeguards and report qualifying incidents within mandated timelines during the designation period; additional categories created by the amendments may commence separately.	Effective from October 31, 2025

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
India Bills 182 amendment to the DPDPA	Reframes children’s personal-data processing around a “best interests of the child” standard, including rulemaking that can account for children’s cognitive development levels. It would also refine the children’s section to allow the Government to calibrate restrictions on tracking, behavioural monitoring, and targeted advertising based on “best interests” and context and introduce a self-assessment pathway (including potential submission to the Data Protection Board and recognition of sector/industry practices). Additionally, it expands the “certain legitimate uses” provision to include processing for advancing and protecting the rights and best interests of children, gender minorities and persons with disabilities.	Data Privacy	All	Focused on children’s-data governance under DPDPA, mainly by amending Section 9 (children) and related rulemaking powers. It would apply to Data Fiduciaries whenever they process a child’s personal data, imposing a “best interests” test, enabling risk-based restrictions for tracking/monitoring/targeted ads, and allowing documented self-assessment mechanisms that may be reviewed/ recognised by the Board or approved by Government. It does not itself lay out detailed operational controls (e.g., age-verification methods, retention schedules); those are typically set via prescribed rules under the Act.	Introduced to Parliament on December 5, 2025. 1-2 years
India Bills 277 amendment to the DPDPA	Proposes amendments to the DPDPA’s definitions to strengthen compliance clarity by defining: “harm” with a broad, illustrative list, including identity theft, discrimination, surveillance not reasonably expected, psychological manipulation, and unauthorised profiling), profiling” (processing that analyses/predicts behaviour, attributes, or interests), and “reasonable security safeguards”, explicitly linking them to a comprehensive, documented information-security programme (managerial/technical/operational/physical controls) and recognised standards such as ISO/IEC 27001, with an expectation that entities can demonstrate implemented controls when a breach occurs.	Data Privacy	All	It applies to Data Fiduciaries and (where relevant) Data Processors, effectively raising the compliance bar by steering organisations toward documented security programmes and recognised security standards as evidence of “reasonable safeguards.”	Introduced to Parliament on December 5, 2025. 1-2 years

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
China Amendments to Cybersecurity Law	The amendments strengthen the law's guiding framework for cybersecurity work (including an explicit "development + security" orientation) and add a dedicated provision to support the safe and healthy development of AI - covering foundational research, key technologies (e.g., algorithms), AI infrastructure (training data resources and computing power), ethics, and risk monitoring/supervision. They also tighten legal liabilities and enforcement, including stronger penalties for certain violations and improved alignment with related laws (e.g., personal information protection).	Cyber Security	All	The amendments apply within the Cybersecurity Law's general coverage - i.e., entities building/operating/maintaining/using networks in China and those subject to cybersecurity supervision, while sharpening obligations and sanctions for network operators and critical information infrastructure (CII) operators in relation to security duties and incident consequences.	Effective from January 1, 2026
Thailand Draft Guidelines on AI use in Financial Services	These guidelines emphasise accountability, lifecycle risk management and customer protection. They propose AI usage policies aligned with legal standards, risk assessment strategies, human oversight, data and model controls and security measures. Consultations closed on June 30, 2025	Artificial Intelligence	Financial Services	The draft applies to financial service providers under Bank Of Thailand (BOT) supervision, including financial institutions and specialised financial institutions (under the Financial Institutions Business Act) and payment service/providers (under the Payment Systems Act). It covers AI systems used across the AI lifecycle (design/development, deployment, operation/monitoring), including machine learning, deep learning, generative AI (e.g., LLMs) and agentic AI, while explicitly excluding simple rule-based automation such as RPA/condition-matching. The guidelines are intended to supplement existing BOT expectations on IT risk, third-party risk, data governance, and market conduct, and apply to both in-house and third-party AI used by regulated providers.	1 year

Global

Title	Brief Overview	Discipline	Sector Focus	Scope	Time Frame
Personal Data Protection Law (PDPL) (Vietnam)	Upgrades the country's privacy regime into a comprehensive statutory framework and strengthens alignment with international data-governance expectations. It tightens rules on misuse of personal data (including restrictions on buying/selling personal data, subject to limited legal exceptions) and introduces a stronger enforcement model to deter non-compliance.	Data Protection	All	The PDPL applies broadly to organisations processing personal data in/related to Vietnam and introduces obligations for processing and cross-border transfers, while providing five-year transitional relief for certain requirements (e.g., impact assessment dossiers and appointing/designating data-protection personnel) for small enterprises and startups, with micro/household businesses generally exempt (subject to specified higher-risk exceptions). Penalties are significant, including fines up to 10× illegal gains for unlawful personal data trading and up to 5% of prior-year revenue for cross-border transfer violations.	Effective from January 1, 2026
Vietnam Law on Artificial Intelligence	The Law establishes fundamental principles, including human-centered AI, fairness, transparency, accountability, and sustainability. It sets state policies to promote AI as a driver of growth, innovation, and social welfare, while encouraging public-private partnerships and international cooperation. Applications in healthcare, education, and scientific research are subject to stricter risk management. Prohibited acts include exploiting AI for illegal purposes, manipulating vulnerable groups, violating data protection laws, and obstructing human oversight.	Artificial Intelligence	All	The law applies to Vietnamese and foreign organisations and individuals participating in AI-related activities in Vietnam, covering the research, development, provision, deployment, and use of AI systems, as well as related rights/obligations and state governance. It expressly excludes AI activities conducted exclusively for national defence, security, and cipher/cryptography purposes. Regulatory duties are structured by stakeholder role (e.g., developer, provider, deployer, user) and scale with system risk; for example, medium/high-risk systems require documentation and notification of classification results to the competent authority via a national portal prior to deployment.	Effective from March 1, 2026

Relevant Blogs, Webinars & Whitepapers

Cyber Threat Intelligence Report 2025

Enhance your defensive security strategy using the latest research into the cyber threat landscape

Cyber Security in Transport: 2025

Learn about the top cyber threats, trends and challenges facing transport organisations in 2025 and beyond.

Cyber Security in Energy: 2025

Learn about the top cyber threats, trends and challenges facing energy organisations in 2025 and beyond.

Cyber Security in Central Government: 2025

Learn about the top cyber threats, trends and challenges facing Central Government in 2025 and beyond.

Data Privacy in Financial Services: 2025

This guide looks at the most pertinent regulations and legislation impacting financial services organisations. It also offers guidance on how to address the main data privacy and cyber security requirements established within them .

Data Privacy and AI

This [blog](#) touches on the potential threat of AI to your organisation, the accountability and governance of AI, and underlying bias. You can also view our recent webinar [here](#).

Guide to Digital Operational Resilience Act (DORA)

This e-guide covers in greater detail the purpose, scope and key requirements of DORA, how it will impact your organisation, and what you can do to prepare.

Enhanced Data Security for Microsoft Copilot Toolkit

This guide explains why Purview is a necessity for organisations using Copilot, while also providing step-by-step guidance on how you deploy key capabilities across data security, governance, and compliance.

Bridewell

Cyber Security. Where it Matters.

Find out how Bridewell can transform and protect your organisation's critical business functions through our modern cyber security services.

☎ +44 (0)3303 110 940

✉ hello@bridewell.com

🌐 www.bridewell.com

