onetrust
DataGuidance

# Data privacy in 2024:

## 10 Moments that shaped the year

DECEMBER 2024

## External Contributors

Joelle Jleilaty, Associate at Axlaw

Gonazalo Muelas, Legal Management Group Manager at Banco Bilbao Vizcaya Argentaria S.A.

Alan Campos Elias Thomaz, Founding Partner at Campos Thomaz Advogados

Dr. Philipp Roos, Principal Associate at Freshfields

Jason Loring, Partner at Jones Walker LLP

Daniel Schlemann, Lawyer at ARQIS Rechtsanwälte

Desislava Krusteva-Doncheva, Partner at Dimitrov, Petrov & Co. Law Firm

Julia Jacobson, Partner at Squire Patton Boggs

Sam Castic, Partner at Hintze Law

Gil Zhang, Partner at Fangda Partners

Olivier Proust, Partner, and Thorsten Ihler, Partner, at Fieldfisher

## OneTrust DataGuidance Contributors

Keshawna Campbell, Harry Chambers, Maryam Abass, Anastasia Konova, and Mike Kuriuki

## Image production credits

Pavliha/E+ via Getty Images

zhen li/Moment via Getty Images

artpartner-images/The Image Bank via Getty Images

Praveen P.N/Moment via Getty Images

Photo by cuellar/Moment via Getty Images

DKosig/iStock via Getty Images

Garen Meguerian/Moment via Getty Images

Catherine McQueen/Moment via Getty Images

© Philippe LEJEANVRE/Moment via Getty Images

Ahmed Aldhaheri/500px via Getty Images

Oleg Breslavtsev/Moment via Getty Images

Delmaine Donson/E+ via Getty Images

Credit: ABBPhoto/iStock via Getty Images

**Website** www.dataguidance.com



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

# 10. Asia Pacific developments

The privacy landscape across APAC continues to develop with notable data protection developments unfolding in 2024.

In Australia, highly-anticipated reforms to the Privacy Act were adopted by Australian Parliament in late November and now await royal assent. The Privacy and Other Legislation Amendment Bill 2024, strengthens the enforcement powers of the Office of the Australian Information Commissioner (OAIC), and establishes provisions related to children's online privacy, automated decision-making, and data breaches.

Similarly, in Malaysia, the Personal Data Protection (Amendment) Act 2024, amending the Personal Data Protection Act, 2010, received royal assent, and will enter into effect on a date appointed by the Minister of Communications and Multimedia. In Vietnam, on the other hand, the Ministry of Public Security published the draft Law on Personal Data Protection, which would function as Vietnam's first comprehensive privacy law, supplementing the Personal Data Protection Decree which entered into force in 2023.

Focused on data transfers, the Cyberspace Administration of China (CAC) published the Regulations on Promoting and Regulating Cross-border Data Flows in May 2024. The Regulations simplify data transfer procedures, introducing exemptions for mandatory data export security measures such as security assessments and standard contracts in specified circumstances. Later, in September, the State Council published the Network Data Security Management Regulations which introduced security and transparency obligations for data processors.

# 9. Middle East developments

In the Middle East, the Israeli Parliament (Knesset) adopted the long-awaited Privacy Protection Bill (Amendment No. 13) (formerly known as Amendment 14) in August. The bill will enter into force in August 2025 and amends the Protection of Privacy Law with regard to enforcement, criminal records, and privacy protection officer appointments. In Jordan, inversely, the Personal Data Protection Law entered into effect in March after its publication in the Official Gazette in September 2023.

In Oman, the Ministry of Transport, Communications, and Information Technology kicked off the year with the issuance of executive regulations for the Personal Data Protection Law, detailing obligations for data controllers and processors, alongside penalties for violation of the Personal Data Protection Law. Likewise, in Saudi Arabia, a key focus for 2024 was the ongoing implementation of the Personal Data Protection Law (PDPL). To this end, the Saudi Data & Artificial Intelligence Authority (SDAIA) released rules on DPO Appointment, amendments to its Regulations on Data Transfers, and a plethora of other guidelines.

In line with international trends, the Middle East also had notable developments on artificial intelligence (AI). The UAE adopted its UAE Charter for the Development & Use of AI and established the Artificial Intelligence and Advanced Technology Council to develop and implement AI policies. Draft guidelines concerning deepfakes and Generative AI Guidelines were also published by the SDAIA in Saudi Arabia. In Qatar, AI guidelines were released by the Qatar Central Bank and National Cyber Security Agency (NCSA), aiming to mitigate potential risks associated with emerging technologies.

"Privacy developments across the Middle East are prompting organizations to reassess their data protection strategies and compliance frameworks, significantly impacting business operations and the region's digital economy. The enforcement of Saudi Arabia's PDPL after the allocated grace period has been particularly influential. By mandating that companies obtain explicit consent for data processing, ensure data localization, and adhere to stringent governance standards, the PDPL is setting a new benchmark for data privacy in the region.

These rigorous requirements are compelling businesses not only within Saudi Arabia but also across the Middle East to adapt their practices, which in turn is fostering a culture of data privacy throughout the region. As a result, there is increased investment in data infrastructure, a rise in cybersecurity initiatives, and a move toward regional harmonization of data protection laws. These developments enhance consumer trust and position the Middle East as an emerging hub for data privacy and security best practices."

- Joelle Jleilaty, Axlaw

# 8. The EU Data Act

2024 kicked off with the entry into force of the Data Act in January. The Data Act contains regulations on the access, sharing, and re-use of items that obtain, generate, or collect data from connected devices. The Data Act becomes applicable in September 2025 and will be enforced by the designated Member State authorities, with penalties for non-compliance and dispute resolution mechanisms in place.

The new rules aim to improve data interoperability by allowing users to switch between cloud data-processing service providers and grant users' rights. The Data Act also establishes obligations for data holders and third parties, as well as mechanisms for public sector bodies to access and use data held by private sector organizations for research purposes.

Notably, the Data Act covers personal and non-personal data, intersecting with intellectual property, consumer protection, and data protection laws.

"It is clear that the EU Data Act aims to ensure that Europe is at the forefront of the latest wave of data-driven advancements. From a practical standpoint, the EU Data Act will bring opportunities which I believe will be conditioned to the assumptions of important costs. By granting fairer access to data, this Regulation could reduce entry barriers and spark innovation across industries. Interoperability and accessibility sound great in theory, however, in practical terms, they require relevant training and investments from a technological perspective."

- Gonzalo Muelas, Banco Bilbao Vizcaya Argentaria S.A.

# 7. SCCs

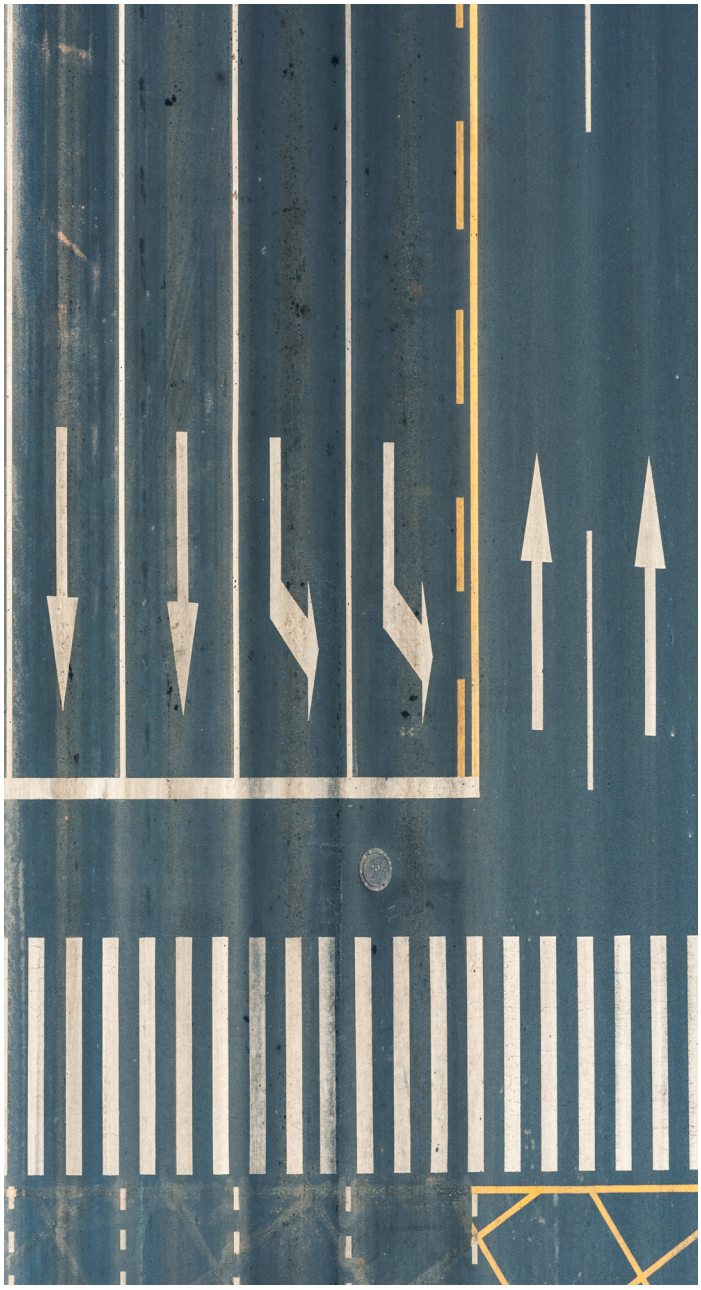
Data transfers continued to be a key focus area for regulators with several jurisdictions releasing draft and finalized Standard Contractual Clauses (SCCs).

In Saudia Arabia, the SDAIA published the SCCs for Personal Data Transfers. The SCCs aim to ensure compliance with the PDPL and its implementing regulations during international data transfers, defining the obligations of involved parties. The templates support various contract types and established SCC rules for their application. Similarly, in Turkey, the Personal Data Protection Authority (KVKK) published SCCs for use in particular types of data transfers. Moving to Latin America, the Brazilian Data Protection Authority (ANPD) issued Resolution No. 19/2024 regulating mechanisms for international data transfers under the General Data Protection Law (LGPD) which also includes SCCs in its Annex.

"In August, the ANPD published Resolution CD/ANPD No. 19, establishing rules for international data transfers. The regulation details how mechanisms such as SCCs and global corporate norms, as well as the possibility of adequacy decisions for countries with data protection levels equivalent to the LGPD. An SCC (as an annex) was introduced by ANPD, and such clauses shall be incorporated into existing contracts by August 2025. Specific data subject rights were introduced and regulated in the Brazilian SCCs."

- Alan Campos Elias Thomaz, Campos Thomaz Advogados

Still in the consultation phase, the European Commission (the Commission) announced in September its plan to open an additional set of SCCs for public consultation, to address transfers to third-country controllers and processors already subject to the General Data Protection Regulation (GDPR). At the international level, in June, the Council of Europe adopted its third Model Contractual Clause for the transfer of personal data from processor to processor.



# 6. Enforcement

Throughout 2024, European data protection authorities (DPAs) have been very active in enforcing the General Data Protection Regulation (GDPR). The DPAs in Spain, Belgium, and Italy imposed the greatest number of fines, with Spain totaling over 100. However, the highest fine, of €310 million, was issued by the Irish Data Protection Commissioner (DPC) for violation of the lawfulness principle.

The Court of Justice of the European Union (CJEU) also interpreted the GDPR in significant judgments on the performance of a contract as a legal basis (C-17/22 and C-18/2), joint-controllership of sectoral organizations in the context of consent management (C-604/22), as well as the concepts of non-material damages (C-741/21) and special category data (Lindenapotheke case, C-21/23).

"In its 'Lindenapotheke' decision the CJEU has confirmed its very broad interpretation of what constitutes health data as generally any information that can reveal a person's health status. The decision could have far-reaching consequences for various industries and companies whose products or services may be deemed harmful to a natural person's health, potentially being required to ask their customers for consent to the processing of their data in in relation to ordering their products and services. Therefore, it is on the data protection authorities and courts to interpret the decision in a practical manner and applying it to medicine and medical services rather than to a broad range of products and services."

- Dr. Philipp Roos, Freshfields

Outside of the EU, Kenya, Nigeria, South Korea, and Thailand also issued notable enforcement decisions, with Nigeria imposing a fine of $220 million for data transfer violations and South Korea issuing a fine of KRW 21.6 billion (approx. $15.6 million) for data collecting and processing without a legal basis.

In the US, the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) reached major settlements with companies over practices considered to risk the security and confidentiality of consumer personal information. At the state level, the Texas Attorney General (AG) secured a historic $1.4 billion settlement over the unauthorized capture and use of personal biometric data in July 2024, while the California AG reached a $6.75 million settlement over a data breach and security misrepresentations in June 2024.

# 6. Enforcement

"The FTC marked 2024 with an intensified focus on privacy enforcement, particularly targeting tracking technologies, health data and data related to children and teens. This enforcement strategy expanded beyond traditional privacy concerns to encompass emerging technologies, including generative AI, signalling a potentially transformative shift.

Among the most significant actions from the FTC in the privacy sphere is its ongoing case against [a] data broker [...]. The case, advancing under Section 5(a) of the FTC Act [...] represents a rare instance of the FTC taking privacy matters to court - a fact acknowledged by the FTC commissioner in a July 2024 letter of support [...]. The FTC prefers settlement - which is both pragmatic and strategic - but it also recognizes the need for judicial precedent. If the FTC can advance its theories in the case, additional scrutiny on data brokers is likely to result. And if the privacy harms alleged by the FTC become precedent, its authority to regulate privacy may expand.

The trajectory of FTC privacy enforcement, however, faces two significant challenges heading into 2025. First, the incoming Republican administration may shift enforcement priorities, potentially reducing federal privacy oversight. Additionally, the Supreme Court's decision to overturn the Chevron doctrine, which previously provided the basis for broad deference to administrative agencies in the face of statutory ambiguity, could constrain the FTC's interpretative authority regarding unfair or deceptive practices under Section 5 of the FTC Act."

- Jason Loring, Jones Walker LLP

# 5. Cookies

In September, the German Federal Government adopted the Consent Management Ordinance under the Telecommunications Digital Services Data Protection Act (TDDDG). The Ordinance establishes comprehensive requirements governing the use of cookie banners and the mechanisms for obtaining user consent. While the integration of these services by digital providers is voluntary, those who adopt them must inform users of their data protection practices and user rights.

"The Ordinance represents an effective initial measure to eliminate the inconvenience of consent banners on websites. It is not yet clear whether website owners will make use of the central consent service and to what extent consent banners will be removed. When making the decision to opt for such a service, businesses will need to consider a number of different factors. Firstly, businesses must trust the consent service to obtain valid consent, as they will remain liable for GDPR-compliant consent as the controller. Using a consent service will not absolve businesses of liability. Secondly, for individual services not covered by the consent service, separate consent must be obtained. In such cases, businesses will likely use their normal consent banner to obtain consent as usual. Lastly, website owners hope for visitors to just click 'accept all', but when using a central consent service, visitors might make their choices more carefully and decline to give their consent."

- Daniel Schlemann, ARQIS Rechtsanwälte

"Guidelines 2/2023 interpret the scope of Article 5(3) of the ePrivacy Directive very broadly, particularly with regard to the storage of information on a terminal device and the access granted to information that has already been stored. The technologies covered include for example tracking pixels, tracking links, device fingerprinting, IoT-systems, and SDKs. This broad definition brings technical processes into the scope of the directive that may have previously gone unnoticed but must now comply with the legal requirements. For any optional service like any form of tracking, businesses are obliged to obtain the explicit consent of from the users before storing or accessing any data on end devices. To ensure that the processing of data on end devices is in line with the requirements of the directive, it is recommended that existing processing and data protection processes be analysed and adapted."

- Daniel Schlemann, ARQIS Rechtsanwälte

At the EU level, the European Data Protection Board (EDPB) adopted its finalized Guidelines on the Technical Scope of Article 5(3) of the Directive on Privacy and Electronic Communications (as amended) (the ePrivacy Directive) in October. The Guidelines clarify its application to various technical solutions and confirm that Article 5(3) of the ePrivacy Directive applies broadly to the storage of and access to any type of information, not just personal data, on a user's device connected to a public communications network.

# 5. Cookies

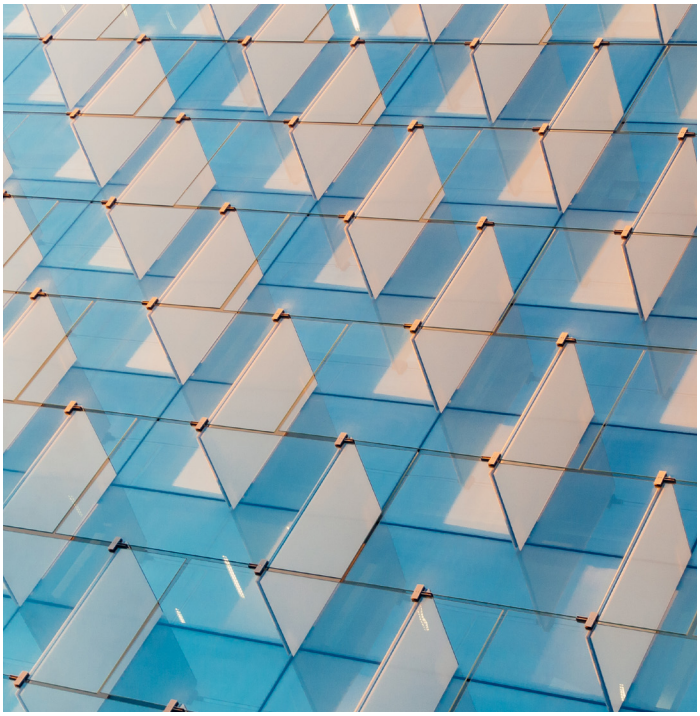
Notably, in Case C-604/22, the CJEU clarified the use of the IAB Europe's Transparency and Consent Framework (TCF) in online advertising. The CJEU held that the TCF's Transparency and Consent String could be considered personal data if, when combined with other information like an IP address, it can identify users. In May 2024, the Dutch DPA fined A.S. Watson Health and Beauty Continental Europe B.V. €600,000 for violations related to cookie consent requirements. Further, in October 2024, the Belgian DPA imposed a €40,000-a-day fine on RTL Belgium AS for having a non-compliant cookie banner.

Outside Europe, the California Privacy Protection Agency (CPPA) took steps to protect user choice, issuing an Enforcement Advisory on Dark Patterns, detailing requirements for valid user consent and the exercise of choice. Internationally, the Global Privacy Enforcement Network (GPEN) published its report on deceptive privacy practices, encouraging the design and use of default settings that protect privacy. Multiple DPAs, including Hong Kong's Personal Data Protection Commission, published guidelines aiming to facilitate such practices.

# 4. Cybersecurity

In 2024, the cybersecurity landscape transformed, with the introduction, passing, and entry into effect of cybersecurity regulation worldwide.

At the EU level, 2024 marked the entry into effect of the Network and Information Security Directive (the NIS 2 Directive) and the adoption of the Cyber Resilience Act (CRA), as well Cyber Solidarity Act (CSA). The NIS 2 Directive entered into effect on October 18, 2024, and required Member States to transpose the directive by October 17, 2024. Notwithstanding the deadline passing, there has been limited implementation by Member States, with the exception of jurisdictions such as Croatia, Hungary, and Italy. While several Member States have begun the process, with draft laws being proposed, many are still in the early stages. The EU Cyber Resilience Act, on the other hand, was adopted and entered into force on December 10, 2024. The CRA provides cybersecurity requirements for the design, development, and production of various hardware and software products. Similarly, in December, the EU adopted the Cyber Solidarity Act, establishing a pan-European infrastructure for responding to large-scale cybersecurity incidents.



"The key data related topics that have attracted the most attention during 2024 from EU perspective were without a doubt the new EU AI Act, DORA and the implementation of NIS 2. The requirements of DORA and NIS 2 are directly interrelated with the efforts of the business to ensure the protection of personal data and especially their security. On the other hand, we can expect from now on in the next couple of years the implications of the AI Act to gradually affect the area of data protection as well."

**- Desislava Krusteva-Doncheva, Dimitrov, Petrov & Co. Law Firm**

In the US, the National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework 2.0 in February, representing the first update since the original publication in 2014. President Biden also signed Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data, addressing cyber threats and to represented by countries of concern. In Canada, on the other hand, the Cybersecurity bill, designed to protect critical cyber systems, is set to receive royal assent following its passage in Parliament in December.

Looking at Asia Pacific, the Cybersecurity Act in Malayasia entered into effect in August. The act governs national critical information infrastructure (CII) and establishes the National Cyber Security Committee. Additionally, in May, Singapore passed a bill to amend the Cybersecurity Act, enhancing the powers of the Cyber Security Agency and broadening the Act's scope beyond the CII.

# 3. US state privacy developments

Privacy remained at the top of US legislative agendas, with 7 states (Kentucky, Minnesota, Maryland, Nebraska, New Hampshire, New Jersey, and Rhode Island) adopting comprehensive privacy laws, raising the total number of state laws to 20. The new state privacy laws generally mirror one another, establishing rules around impact assessments, privacy policies, vendor management, and enforcement.

In addition to new state laws being passed, a few existing privacy laws entered into force in 2024. In July, Texas's Data Privacy and Security Act (TDPSA), Oregon's Consumer Privacy Act (OCPA), and Florida's Digital Bill of Rights (FDBR) entered into effect; while Montana's Consumer Data Privacy Act (MCDPA) took effect in October. Furthermore, several states amended their existing privacy laws, including Colorado, California, and Virginia in relation to biometric data and opt-out rights among other things.

At the federal level, the American Privacy Rights Act (APRA) was introduced in April 2024 and establishes national data privacy standards, impacting a broad spectrum of businesses currently outside the scope of state data protection laws. However, there has been no movement on the bill since June, making it seem unlikely to be adopted. Again at the federal level, the US Supreme Court shocked many by overturning the 1984 Chevron v. Natural Resources Defense Council decision. The reversal of this decision removes judicial deference for regulatory agencies in interpreting statutes and shifting that responsibility to the courts.

"Although the American Privacy Rights Act (APRA) stalled in 2024, the 'Trump 2.0' administration and a Republican controlled Congress could pass a general federal privacy law - just without the private right of action. Strong pre-emption is, however, a likely component of federal privacy law a Republican controlled congress since the web of 20 state privacy laws is not considered business friendly. Children's privacy will, however, remain front and center - whether through a federal law - like the Kids Online Safety and Privacy Act (KOSPA), which passed the Senate on August 1, 2024, by an overwhelming majority - or through continued activity at the state level - like 2025's expanded privacy protections for minors in Colorado and Virginia or the Maryland privacy law's prohibitions on personal data sales and targeted advertising for Maryland's minors."

- Julia Jacobson, Squire Patton Boggs

# 2. AI developments

AI remains at the forefront of legislative agendas, with various legal and policy initiatives being introduced and progressing in jurisdictions such as the EU, the US, and China. Arguably, the most significant development in 2024 was the enactment of the EU Artificial Intelligence Act (the EU AI Act). Companies and regulators are actively preparing for the act's entry into effect, with some provisions entering to effect in early 2025.

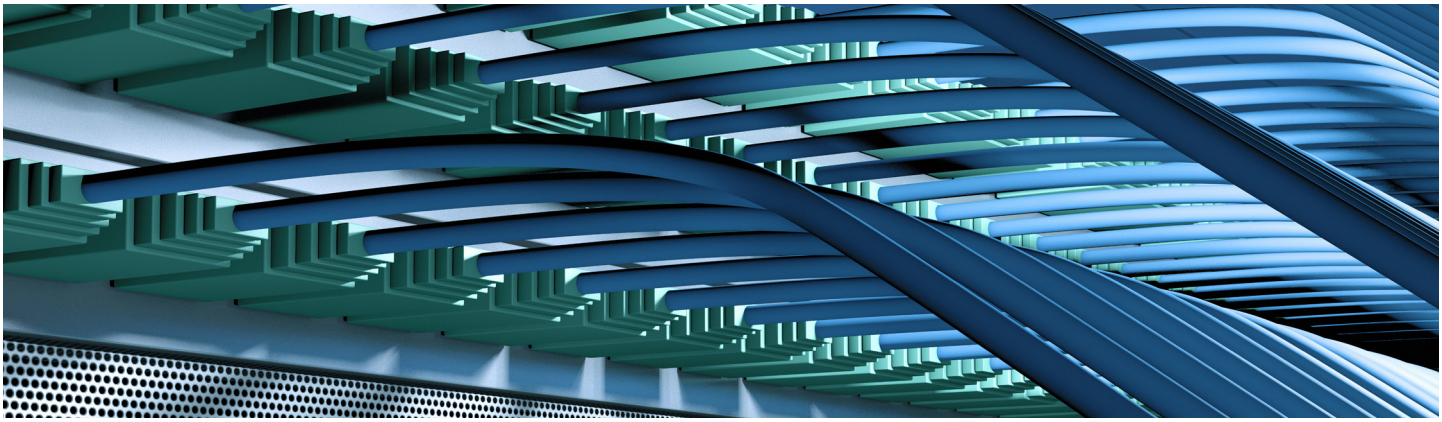
In May 2024, the Council of Europe (CoE) adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (the Convention) which establishes transparency and oversight requirements to ensure compatibility of AI systems with human rights standards. Norway signed the Convention in September 2024 when it was open for signature.

AI regulation in the US has also started to take shape, with Colorado becoming the first US state to enact a comprehensive AI law in May. Set to take effect in February 2026, the Act concerning consumer protections in interactions with artificial intelligence systems (the Colorado AI Act) imposes obligations regarding the prevention of algorithmic discrimination and consumer transparency. California also took steps to enact legislation relating to AI, with the passage of the AI Accountability Act and the AI Transparency Act among others. Notable draft legislation in California that failed to pass included Senate Bill 1047 on Frontier AI Models.

"Colorado was the first state to enact a comprehensive private sector AI law. It contains different obligations for AI developers and deployers, with developers having robust information disclosure and regulator reporting obligations for discrimination risks, and deployers having detailed AI risk assessment and governance obligations. The law focuses on high-risk AI systems used to make certain types of decisions about people may serve as a model for other states looking take a harm-based approach to regulating AI."

- Sam Castic, Hintze Law

In China, the National Information Security Standardization Technical Committee (TC260) built on existing AI legislation with the publication of the Artificial Intelligence Security Governance Framework in September 2024. Also in the APAC region, the Singapore Infocom and Media Development Authority (IMDA) published the Model AI Governance Framework for Generative AI in May 2024, supplementing the Model AI Governance Framework published in 2020.



# 2. AI developments

"The TC260's AI Security Governance Framework proposes comprehensive mapping of risks related to AI development, use and deployment in the entire life cycle, and principles and mitigation proposal to address such risks. Such [a] AI Security Governance Framework signals China's regulatory roadmap for the next five years where detailed national standards on the AI risk identification and classification and the detailed national standards on case-specific AI risk mitigation may follow in light of such roadmap. Pilot programs based on such framework[s] and national standards may evolve into China's AI laws and regulations covering different aspects of AI which is a different approach from EU AI Act."

- Gil Zhang, Fangda Partners

# 1. The EU AI Act

In August 2024, the highly anticipated EU AI Act entered into force. The EU AI Act establishes harmonized AI governance rules and places new obligations on various entities involved with AI systems and General-purpose AI (GPAI) models. Under the EU AI Act, AI systems are classified according to a risk-based approach namely: prohibited, high-risk, and limited-risk, which are subject to different obligations. The EU AI Act imposes stringent penalties for violations, with fines of up to €35 million and 7% of global annual turnover. In preparation for the EU AI Act's applicability, the Commission created the AI Office as its enforcement body, alongside the AI Board which serves as its advisory body.

Key dates to keep in mind for 2025 include: February 2025 for the ban on prohibited AI practices; May 2025 for the general-purpose AI (GPAI) Code of Practice; and GPAI obligations in August 2025.

"The EU AI Act is at the forefront of global policymaking on AI. Inspired by the OECD's principles for trustworthy AI and the preparatory work carried out by the EU Commission, the AI Act is a comprehensive legal text that aims to regulate the development, use, distribution, and import of AI within the EU [...]. Companies have less than two years to comply with a complex set of rules imposed mainly on developers and deployers of high-risk AI systems and models. These rules will require them to carry out detailed risk assessments to determine their role under the AI Act and to comply with the subsequent obligations that are imposed. AI literacy is also very much at the heart of AI governance. Beyond the compliance aspect, the AI Act will also have a deep impact on contract negotiation, risk mitigation and litigation (especially in the field of product liability) and cybersecurity. Companies must view their responsibility holistically and also assess their obligations within the broader EU digital framework."

- Olivier Proust, Fieldfisher

# 1. The EU AI Act

"The EU AI Act has significant impact on the global legal and ethical discussion [...]. Similar to the GDPR, one commercial reason is that Europe is a large market, therefore companies addressing the continent need to define their compliance strategy in light of potential queries from customers or regulators. Additional instruments like the voluntary AI Pact and the anticipated guidelines for implementation and codes of practice may further influence AI products worldwide, possibly again as a repercussion of complaints or queries. A main challenge for providers and deployers of AI systems is the implementation complexity caused by the overlap with various other regulations in areas such as privacy and consumer protection. By contrast and based on experience with other technology regulations, consequences of non-compliance – regulatory measures, individuals' complaints, product liability claims, etc. – will be handled differently and in accordance with local law and enforcement practices."

- Thorsten Ihler, Fieldfisher

onetrust
DataGuidance