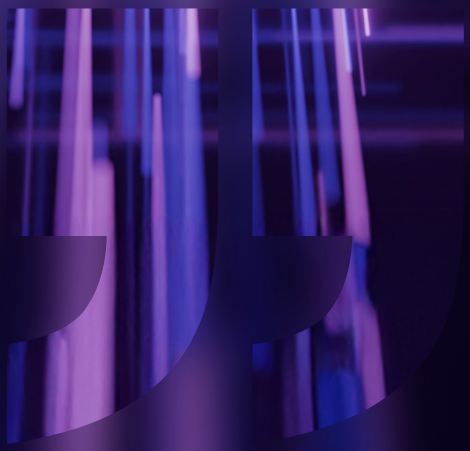
CLIFFORD
CHANCE

DATA PRIVACY LEGAL TRENDS 2025



— THOUGHT LEADERSHIP

JANUARY 2025

DATA PRIVACY LEGAL TRENDS 2025

Data protection and privacy laws continue to increase in number and scope globally, including a continued flow of comprehensive US. state privacy laws and quickly developing regimes in Asia Pacific and the Middle East. Legislators are also increasingly addressing data governance beyond privacy, including through laws aimed at facilitating data access, portability and re-use. European courts and regulators are focused on fundamental questions around application of privacy laws – including in relation to so-called 'Pay or Consent' models – and efforts around the world to clarify the application of privacy laws to artificial intelligence (AI) continue through enforcement, litigation and regulatory guidance.

We share five data privacy legal trends to watch in 2025.

1 Privacy laws are shaping AI governance

As AI becomes ubiquitous and regulators develop a more sophisticated understanding of these transformative models and systems, we can expect to see even more AI-related activity from data protection authorities (DPAs), and even more privacy litigation relating to AI.

Across the world, countries have implemented policies directing regulators to apply existing legal frameworks to the development and use of AI. Data protection and privacy laws (privacy laws) are being applied, alongside consumer protection, employment and equality, antitrust, product safety, cyber and IP laws.

In 2024, DPAs asserted their role as important regulators of AI by issuing guidance, opinions and frameworks on data protection-compliant AI and through high-profile enforcement. In the EU in particular, we saw significant DPA activity in applying the EU General Data Protection Regulation (GDPR) to AI – including the Dutch DPA's EUR 30.5 million fine of Clearview AI, the Irish Data Protection Commission's suspension proceedings against X in the Irish High Court, the Italian DPA's EUR 15 million fine of OpenAI and its investigation into DeepSeek in relation to GDPR compliance. In addition, a string of AI-related guidance was issued by the French, German, Spanish, Dutch and Belgian DPAs followed by the European Data Protection Board's (EDPB's) much anticipated Opinion on AI Models. Unsurprisingly, the EDPB and many EU DPAs have also issued statements recommending that the EU DPAs be designated as market surveillance authorities for the EU's landmark AI Act, which is now in force.

Other privacy regulators globally have also focused on AI. Examples include the US. Department of Justice's lawsuit against TikTok regarding the Children's Online Privacy Protection Act, the Hong Kong Privacy Commissioner's AI Model Personal Data Framework, Singapore's Personal Data Protection Commission Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems, the Australian Privacy Commissioner's enforcement against Bunnings in relation to facial recognition technology, the Office of the Australian Information Commissioner's guides on AI products and models, and the UK Information Commissioner's Office (ICO's) consultation series (and resulting guidance) on generative AI. While the ICO's investigation into errors made by Snap in their Data Protection Impact Assessment for 'My AI' did not ultimately result in enforcement action, the ICO's continued enforcement against Clearview AI will be one to watch – this was dismissed by a tribunal in 2023 on territorial scope grounds but the ICO has now been granted permission to appeal.

Although AI competitiveness is a central feature of digital sovereignty and economic growth agendas around the world – with the US. and UK governments in particular sending strong 'pro-innovation' messaging to regulators in relation to AI at the start of 2025 – regulators will be balancing this against concerns around AI safety. Given that the application of privacy laws to AI remains both pivotal and far from clear, we can expect continued privacy investigations and enforcement and appeals focused on AI in 2025. Organisations will also need to continue to monitor AI-related privacy litigation, which is playing a crucial role in clarifying how privacy laws apply to various forms of AI and machine learning.

In the year ahead, organisations that have not already done so will need to ensure that their AI risk management and data governance frameworks are appropriately integrated to allow for effective oversight and informed risk calibration in the exploration of AI opportunities. This may include reviews of policies, notices, procedures and oversight bodies, due diligence processes, contracting terms and regulatory engagement strategies.

For more on data privacy and AI, see our Perspectives webinar recording: *Data and cyber considerations for AI*.

US state privacy laws are at the forefront of US privacy

2

US. data privacy continues to include a range of state and federal developments. Several states have enacted or are continuing to develop comprehensive data privacy laws with requirements that apply across almost all business sectors. In 2024 we saw a number of such comprehensive state privacy laws coming online, including the Texas Data Privacy and Security Act and the Oregon Consumer Privacy Act. In 2025, we're seeing a continuation, with privacy laws for Iowa, Delaware, New Hampshire, Nebraska and New Jersey coming into effect this month, with Tennessee, Minesota and Maryland due later this year.

Federal legislative efforts to create a comprehensive consumer data privacy law – similar to the California Consumer Privacy Act, Virginia Consumer Data Protection Act and Texas Data Privacy and Security Act – have yielded minimal results. Current efforts – for example, the American Privacy Rights Act of 2024 (ARPA) – have stalled. The fact that the executive, judiciary, and legislative branches are unified in creating such a law in theory, may mean that bipartisan legislation could pass. However, Cathy McMorris Rodgers, one of the ARPA authors, has retired, while the ranking member of the Senate Committee in charge of the APRA, Ted Cruz, won re-election. Cruz has been critical of APRA in the past (including wanting strong pre-emption), which may mean that any federal privacy law that does pass would differ from the APRA.

There is bipartisan support for certain data privacy initiatives, such as privacy protection for children's data, which may continue under the Trump administration. It is unclear whether (and potentially unlikely that) such support will carry into more comprehensive federal data privacy legislative proposals. As a result, legislative activity in the realm of consumer data privacy may continue at the US. state level, an apparent trend under the Biden administration.

Relatedly, while the Trans-Atlantic Data Privacy Framework (DPF), enabling businesses to comply with EU and US. data privacy laws when making data transfers from the EU to the United States, was signed into law under President Biden, it was created during President Trump's first presidency. It will be interesting to see whether it remains in place in the medium term. It is of course also potentially subject to challenge in the EU, although that is probably for the longer term (see section 3 below).

Underpinning much of US. data privacy and security federal regulation is the Federal Trade Commission (FTC) and its approach to enforcement under Section 5 of the Federal Trade Commission Act of 1914. The previous FTC Chair, Lina Khan, generally expressed a high-level of interest in enforcing data privacy and security regulations under the FTC's authority, with a particular focus on 'big tech'. Most recently, on 16 January 2025, the FTC finalized changes to the Children's Online Privacy Protection Rule to set new requirements around the collection, use and disclosure of children's personal information, while also giving parents new parental control tools.

On 20 January 2025, Andrew Ferguson, who has served as a Republican Commissioner on the FTC since last year, took over as the new FTC Chair. While the FTC's regulatory enforcement regime during President Trump's second term remains unclear, potential approaches may include fewer rule-makings, more traditional interpretations of the law, and a more restrained individual liability approach. The substantive priorities are likely to be consistent with those under President Biden, including AI, privacy and security, health data and consumer fraud.

With no comprehensive federal data privacy law on the horizon, keeping up with State legislation and understanding the scope, applicability and requirements of these data privacy laws, and the approach taken by the FTC, is more crucial than ever for companies operating in the US. in 2025.

For more on the quickly developing US landscape under President Trump's administration, see our publications *Forecasting the Impact of Trump's Second Administration on the Tech Sector*, *President Trump's First Seven Days in Office: What's Out, What's In and What's Still In.*

3

Europe is tackling fundamental question on the application of its privacy laws

In Europe, we saw significant developments clarifying the application of privacy laws and can expect further decisions, enforcement and guidance in 2025 on key issues, including:

Approaches to GDPR enforcement and litigation:

- In recent years we have seen a string of cases before the European courts relating to calculations of fines under the GDPR, including whether fines for subsidiaries should reflect group turnover, the circumstances in which a fine can be imposed (including whether it is necessary to identify a breach which is attributable to, or known of by, a natural person), whether competitors are entitled to bring an injunction claim based on an infringement of the GDPR, and what constitutes sufficient compensation for non-material damages.
- The Supreme Court's 2021 judgment in *Lloyd v Google*, and the Court of Appeal's 2024 judgment in *Prismall v Google (Deep Mind)*, mean that it remains difficult to bring representative actions (an opt out process) in the English Court, where such claims are framed as 'loss of control' of personal data, or the tort of misuse of private information. An emerging trend is for claimants to seek to frame data issues in competition law, so that they can be determined by the UK Competition Appeals Tribunal (see, for example, *Dr Liza Lovdahl Gormsen v Meta Platforms, Inc. and Others).*
- The issue of personal liability for breach of the GDPR raised its head in 2024, with the Dutch DPA stating, in the context of its enforcement against Clearview AI (which was already subject to enforcement activity from other European DPAs) that it will investigate whether it can hold the management of the company personally liable and fine them for directing the violations. We await the outcome of this and any trend in this direction, noting that the EU's revised Network Information Security Directive (NISD 2) also looks to personal liability for management bodies.
- Also in 2024, the European Commission proposed new procedural rules to streamline cooperation between DPAs when enforcing the GDPR. These are expected to progress during 2025, potentially to completion.

"Consent or Pay" models:

- Last year, the EDPB adopted its Opinion of 'Consent or Pay' Models (applicable only to large internet services providers). While it did not go so far as to attempt ban these models, it did seek to set a very high bar for their lawful operation under the GPDR and stated that the EDPB's view is that they would not satisfy the requirements for valid consent 'in most cases'. In June 2024, Meta filed a lawsuit against the EDPB at the General Court of the European Union, challenging the EDPB Opinion, arguing (amongst other things) that it is an 'illegal and disproportionate

interference' with its right to freedom to conduct a business. It is worth noting that the UK's ICO has recently published its own guidance on 'Consent or Pay' models, signalling a different approach, subject to compliance with some rules.

- In 2025, the debate surrounding 'Consent or Pay' models is expected to intensify. Proponents argue that these models underpin the internet's 'grand bargain' – the exchange of free or subsidised tools, content and platforms for personalised advertising – and that they align with fundamental principles of data protection by empowering data subject choice and control. Critics argue that the right to data protection should not be transformed into a feature for which individuals have to pay, and express concerns over economic disparities potentially leading to a 'privacy divide'. Alongside online safety and content moderation regulation, the approach to 'Consent or Pay' models is one of the key areas to watch in relation to provision of online services in 2025 (and beyond). Debates on these issues may also crystalise around the possibility of an EU "Digital Fairness Act".

International data transfers

In the wake of the European Commission's adequacy decision for the EU-US. DPF (see also section 2 above) and the UK's approval of its extension to the framework, last year was relatively quiet in relation to European activity on international data transfers. We did see the Dutch DPA fine Uber for not having appropriate safeguards in place for personal data transfers to the US., and the European Commission announced a consultation on a new module to its standard contractual clauses for use where the data importer is subject to the extraterritorial effect of the GDPR, as well as the first review of the EU-US. DPF. Notably, the Irish High Court gave Max Schrems approval to be joined as a notice party in Meta's legal challenge against the Irish Data Protection Commission's 2023 decision (which fined the company EUR 1.2 billion and required the suspension of user data transfers from Europe to the US.). In 2025, we could see a third round of challenges to transatlantic data transfers from Max Schrems or other privacy activists, although it will likely take some time for these to be decided in the courts. We may also see the EU and UK diverging in their granting of adequacy decisions for countries to which personal data can be transferred without additional safeguards under data privacy laws, although the UK will likely proceed carefully in this area.

Cookies and targeted online advertising

- Discussions stalled last year on the European Commission's voluntary 'Cookie Pledge' principles, which aimed to better empower consumers to make effective advertising choices. Developments in this space include the EDPB's updated guidelines on Article 5(3) of the e-Privacy Directive, which take a broad interpretation of the application of this "cookie rule", and the Irish DPC's EUR 310 million fine of LinkedIn in connection with behavioural analysis and targeted advertising. The Court of Justice of the European Union handed down a preliminary judgment in the long running case on IAB Europe's Transparency and Consent Framework – with this ruling taking an expansive view of joint controllership under the GDPR – allowing the proceedings to resume the Belgian Market Court for final determination.
- In the UK, consultations were held on possible approaches to cookie management in the context of the Data Protection and Digital Information Bill, which has since been replaced by the Data (Use and Access) Bill (DUA Bill), which also proposes some relatively modest amendments to the UK's version of the GDPR. The DUA Bill proposes, amongst other things, to clarify and expand the circumstances in which cookie consent is not needed, but timelines are unclear for any further exploration of cookie management reform in the UK through opt-out models. Case law on targeted advertising is also developing in the UK, most recently through the High Court's judgment in *RTM v Bonne Terre Ltd & Hestview Ltd* (the "Sky Betting case"), which was handed down at the start of the year. The judgment's three-stranded analysis for assessing the validity of consent to cookies and direct email marketing in the context of online gambling is an example of the complexities of demonstrating valid consent.

- In 2025, we can expect to see further debate on how to alleviate cookie fatigue, even as the e-Privacy Regulation continues to stall.

4

Strengthened privacy laws in Asia Pacific and the Middle East

The legal landscape for privacy is continuing to see significant transformations more broadly across the world. In 2024, several jurisdictions saw new comprehensive data protection laws become enforceable, and others will follow in the year ahead. For example, the Saudi Personal Data Protection Law's one year grace period ended in September 2024 and Indonesia's Personal Data Protection Law came into force in October 2024. India's Digital Personal Data Protection Act is expected to be fully operational in 2025, while Vietnam's new Personal Data Protection Law is set to come into effect on 1 January 2026.

Other countries with existing privacy laws will also see important updates in 2025. Australia has begun the first phase of reforms to its Privacy Act – introduced in December 2024 under the Privacy and Other Legislation Amendment Act 2024 (see our overview *here*) – and consultation on a second tranche of reforms is expected in 2025. Substantial updates to Malaysia's Personal Data Protection Act have been approved and new rules relating to breach notification, DPO appointment and data portability are being worked on. Israel will transition to a new data protection regime when Amendment No. 13 to its Protection of Privacy Protection Law takes effect in August 2025.

Although many of these laws take inspiration from aspects of the GDPR in some of their provisions, they also vary in a myriad of significant ways – including, in some cases, in relation to legal bases for data processing, cross-border data transfer and data breach notification requirements – and this variation, and a trend towards stronger enforcement regimes, make tracking and mapping the evolving tapestry of privacy requirements more important than ever for businesses operating in multiple jurisdictions.

Within this landscape of increasingly complex privacy requirements for multinational organisations, China's Provisions on Regulating and Promoting Cross-border Data Flows, issued by the Cyberspace Administration of China (CAC) in March 2024, stood out as an example of an easing of cross-border transfer requirements. The CAC also published guidelines on security assessments and standard contractual clauses (see our briefing on the provisions and guidance *here*). Together, these developments brought welcome exemptions to, and clarifications of, China's data export regime as China continues to seek to balance data sovereignty considerations with attracting foreign investment, and we can expect to see ripple effects in 2025 and beyond.

Watch our webinar on key themes in data regulation and enforcement in APAC: *APAC Data Regulatory Themes and Strategies*.

5

Holistic approaches to data governance

Increasingly, privacy laws are just one amongst many of the digital regulations governing data. In 2025, successful data strategies will need to go beyond anticipating appropriate application of privacy law – organisations will need to break any silos between teams applying digital regulations in order to leverage a holistic approach. Examples include:

Cyber

While cyber and privacy laws have long needed to be understood 'hand-in-hand', a global trend towards increased (and broadened) cybersecurity and resilience regulation means there are more of these laws to navigate than ever before. There are complicated incident classification and reporting requirements (in some cases outstripping the notification timelines in privacy laws), as well as specific requirements around internal policies and supplier contracting. In the face of increasingly

sophisticated cyber-attacks and hyper-connected businesses, getting right the fundamentals of readiness and response will be crucial for both privacy and cyber compliance for years to come. See our *Cybersecurity Handbook*.

Consumer protection and antitrust laws

Increasingly, government agencies and private plaintiffs are arguing that increased competition leads to improved privacy practices and better protections for consumers. Although tensions can exist between privacy and competition goals – for example between making data available to promote competition and restricting access to data to protect privacy and security – we are seeing privacy, consumer protection and competition regulators working more closely together than ever before. We may see more inclusion of privacy law breaches in competition proceedings, in particular as regulators continue to enforce competition laws against online platforms. At the same time, regulators may investigate allegations that privacy concerns mask anticompetitive conduct.

Data access, portability and re-use laws

Governments around the world are refining their data strategies to stimulate innovation and boost their digital economies.

- The EU is leading the charge on legislation aimed at 'unlocking' access to data within the EU market (perhaps, in part, because the GDPR has been very effective in inspiring caution). The EU's Data Governance Act, which became applicable in 2023 laid foundations for the re-use of protected data (beyond personal data) held by public sector bodies, as well as requirements for trustworthy data sharing and measures to encourage 'data altruism'. This was followed by the entry into force of the EU Data Act in January 2024, which includes rules for access to, and re-use of, certain data relating to connected products and related services which are placed on the market in the EU – these are set to apply from September 2025. Facilitating access to data remains a key theme for the new European Commission as part of its drive to enhance European competitiveness, including through its announced Data Union strategy to improve and secure private and public data sharing. Look out for more guidance in this space, which may help to navigate the increasingly multi-layered data law architecture.
- The EU's Common European Data Spaces initiatives also seek to empower data sharing for re-use in the EU digital market with the goals of fostering innovation and research and encouraging new data business models. These include the European Health Data Space (EHDS), which was adopted by the Council of the European Union on 21 January 2025 and should be published in the Official Journal in the coming weeks, and the Financial Data Access (FIDA) framework, which is still under negotiation.
- Other countries are exploring their own approaches to stimulating data markets, and the UK's DUA Bill, Vietnam's Data Law and New Zealand's Customer and Product Data Bill will be among those to watch in 2025.
- Organisations will need to both prepare to be able to comply with data sharing requirements and to assess the opportunities that these initiatives may create. Many laws of this type also include restrictions around storing or processing data outside of the relevant market, which should be factored into governance of cross-border data sharing.

To get in touch with us about any of the topics in this paper, see our contacts list at **www.cliffordchance.com/insights/thought_leadership/trends/2025/data-privacy-legal-trends.html**

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 UppAer Bank Street, London, E14 5JJ

JOB0000042090