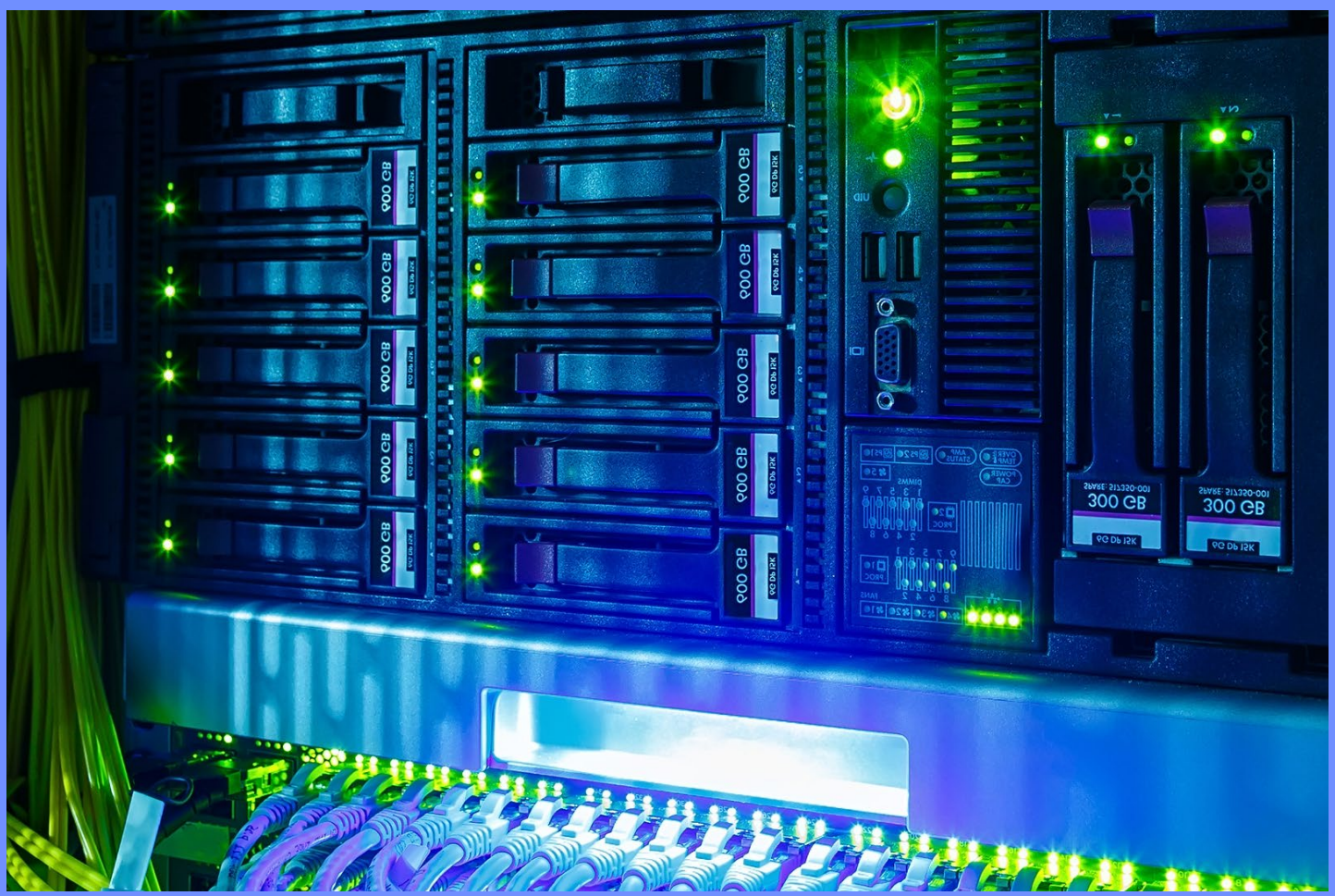
FRESHFIELDS

2025 DATA LAW TRENDS

Leading the change



Contents

Executive summary

The 2025 Data Law Trends report is here, and this year's findings reveal one thing loud and clear: the pace of change in data law is accelerating, profoundly impacting businesses.

We've identified eight key trends that will shape the future, and they're more than just legal shifts – they're strategic opportunities for those ready to act.

Last year, we reported on key disruptions as new technologies and regulations began to take hold. In 2025, the stakes are even higher. Data laws are shaping everything from risk management to growth opportunities, and staying ahead of these shifts is critical.

> Data law is no longer a peripheral concern – it's the heartbeat of modern business strategy. As we stand on the brink of transformative change, it's crucial to recognize that adapting to these emerging trends is not just about compliance; it's about seizing the competitive advantage in a data-driven landscape. This report equips you with the insights to not only navigate the complexities ahead but to thrive in them.
>
> **Christine Lyon, Giles Pratt and Christoph Werkmeister**
> Global Co-heads of the Freshfields data privacy and security practice.

From the rise of AI governance to the tightening of data transfers, these trends reflect the new realities of doing business in a data-driven world. Each one has been carefully pinpointed by our global team of experts, who are advising top tech companies on the frontlines of these changes.

This report breaks down the major trends, including:

1. **AI governance takes center stage –** As AI becomes increasingly central to business, the focus on governance and accountability intensifies.
2. **International data transfers are under the spotlight –** Navigating the evolving landscape of cross-border data flows will be essential.
3. **A new wave of cyber threats is here –** Cyber threats continue to evolve, and data laws are playing a key role in shaping how businesses respond.
4. **New global regulations are changing our digital operations –** Stricter regulations around online content and transparency are set to impact businesses worldwide.
5. **Tougher enforcement is reshaping data and privacy compliance –** Expect more robust enforcement actions, including as regulators intensify their focus on AI-related data practices.
6. **US state consumer privacy laws are expanding –** As privacy regulations spread across US states, businesses need to adapt quickly.
7. **Asia's privacy laws are maturing –** Asia's data privacy landscape is evolving fast, and businesses must stay agile to remain compliant.
8. **New EU data access regulations are shaping the future –** The EU's upcoming regulations on data access will have wide-reaching implications.

Our goal with this report is simple: to give you the insights you need to stay ahead of these changes. It's a guide to help you prepare your business, navigate the challenges, and seize the opportunities.

Dive in – the future of data law is here, and it's moving fast.

1.

AI governance takes center stage

AI governance takes center stage

Rachael Annear
London

Zofia Aszendorf
London

Georgina Bayly
London

Richard Bird
Hong Kong

Theresa Ehlen
Düsseldorf/ Frankfurt

Beth George
Silicon Valley

Adam Gillert
London

Cat Greenwood-Smith
London

Giles Pratt
London

Lutz Riede
Vienna/Düsseldorf

In brief

With regulatory pressures, changing expectations from shareholders and customers, and the increasing risk of litigation, it's clear that addressing AI governance is more important than ever.

As a result, many organizations today are feeling the heat to show they have the right governance structures and decision-making processes in place for their use of AI – or for deciding not to use it at all.

In this chapter, we'll dive into why a proactive AI governance framework is essential. It's not just about ticking boxes; it's about taking control of AI's potential while managing its risks. We'll explore the key pressures you're facing and highlight the foundational elements that can lead to successful AI governance.

Increasing pressures to develop AI governance frameworks

Pressures to develop AI governance frameworks include:

AI-specific regulatory regimes

These regimes are taking more discernible shape across the globe, with AI-specific regulation now in force across the EU and China, and planned at national level (with published draft texts) in Brazil, Canada, South Korea, Thailand and Vietnam. New (albeit narrow) AI-specific regulation was introduced to protect the integrity of India's recent elections and is also anticipated in the UK.

AI governance takes center stage

A proliferation of guidance as to the application of existing regulatory regimes to the use of AI

The UK, US and other jurisdictions (including Australia, Hong Kong, India, Japan, Russia, Saudia Arabia, Singapore, South Korea and Turkey) have implemented policies aimed at streamlining AI regulation at the national level. These fall short of AI-specific laws and instead direct established regulators to apply existing regimes to the use of AI. Non-regulatory government bodies are also being vocal in this space – for example, the US Department of Justice, primarily a law enforcement agency, has spoken about its expectations that corporate compliance programs are effective at mitigating AI-related risks.

The emergence of global standards for AI governance, such as ISO/IEC JTC 1/SC 42

Customers, distributors and other contractual counterparties may start expecting compliance with these types of standards as a 'badging' of an organization's AI maturity.

Increased scrutiny of company reporting with respect to use of AI from shareholders

Companies in the US are already facing scrutiny from shareholders who view them as being insufficiently transparent about their use of AI. We have seen a trend of shareholder petitions being filed at the US Securities and Exchange Commission aimed at eliciting further detail relating to a company's AI strategy. AI risks and opportunities are becoming a common theme of listed company reports; see infographic on the next page.

Increasing focus from NGOs on AI and the potential risks it poses

For example, Amnesty International published a report titled The State of the World's Human Rights in April 2024, which looked at human rights concerns from 2023. This report highlighted AI as a potential threat to human rights citing use cases such as state deployment of facial recognition software to aid policing of mass events, including protests, as well as use of biometrics and algorithmic decision-making in migration and border enforcement. The Austrian privacy advocacy group 'noyb' has been vocal in relation to the privacy implications of AI technologies.

Increasing risk of AI litigation and regulatory enforcement

> Companies are feeling the pressure to get AI governance right not only from regulators, but also from the markets, the emergence of global standards for AI governance and third-party actors such as NGOs.
>
> **Giles Pratt**
> Partner

Companies need a framework to ensure compliance and respond to regulatory scrutiny and allow them to make the most of AI while navigating the risks associated with its use.

Data-related matters will be a core component of this framework. The EU AI Act, which is the world's first comprehensive AI-specific legislation, imposes numerous governance and documentation-related obligations, including specific data governance obligations on providers of high-risk AI systems. Similarly, data protection regulators globally have not shied away from enforcement activity relating to the use of personal data in connection with AI systems (we have seen activity in this space from data protection regulators in the UK, Ireland, Italy, the Netherlands, Hong Kong and elsewhere. The US Federal Trade Commission is also active in this space as part of its consumer protection remit) and are also proactively consulting on the application of data protection laws to AI.

AI governance takes center stage

Trends in board oversight of AI:

Director expertise in AI in the US* and the UK**

S&P 500

13%

30%

60%

13% of S&P 500 have at least one director with AI expertise. This increases to 30% of S&P companies in the IT sector (and up to 60% in the automotive space).

FTSE 100

18%

18% of the FTSE 100 have at least one director with AI expertise.

AI

The FTSE 100 companies whose annual reports mention AI expertise of directors span a number of sectors, including financial services, pharma and retail.

Sources:
* Deloitte and Society for Corporate Governance: Board Practices Quarterly: Future of Tech: Artificial Intelligence (2023): ISS-Corporate AI and Board of Directors Oversight: AI Governance Appears on Corporate Radar (2024)
** Data sourced by Freshfields

Emerging AI litigation and regulatory enforcement themes

As AI becomes increasingly advanced, companies face a growing risk of litigation or regulatory investigations concerning AI use or development. Governments and regulators are heightening their focus on both the opportunities and risks posed by AI.

While many new regimes specifically regulating AI are yet to be enacted and/or implemented, AI-related litigation and investigations are being brought under existing regimes governing areas such as data protection and privacy, equality and anti-discrimination, intellectual property (IP), product liability and consumer protection and misrepresentation.

> While lawsuits and investigations concerning AI are currently based on existing regimes, we expect to see a real influx of new cases once new legislation specifically targeting AI comes into effect.

Cat Greenwood-Smith
Partner

AI governance takes center stage

So far, AI litigation remains at a relatively nascent stage. We anticipate a surge in AI litigation with the rapid advancement of AI systems and emergence of new regulatory regimes and potential for diverging approaches across jurisdictions.

In terms of the current landscape:

- The US is leading the way with a number of class actions. Allegations range from unfair and discriminatory outcomes resulting from algorithmic decision making, to breach of privacy in connection with the training of AI models. Other jurisdictions will likely follow suit.
- Outside the US, early cases have been brought primarily against states for their use of AI, eg in relation to alleged biases and invasion of privacy resulting from use of facial recognition software. However, the focus appears to be shifting to companies who develop and/or deploy AI.
- Globally there is already big-ticket IP litigation, where claimants allege their IP is being used by defendants without consent to train their own AI models, or that outputs from defendants' AI models infringe IP.

> Mass claims alleging harms caused by AI are already being brought in the US, but we expect to see a dramatic increase in AI related mass claims both in the US and elsewhere as the development and use of AI rapidly expands.
>
> **Georgina Bayly**
> Associate

We are also seeing regulators taking a more hands-on approach to governing AI, even where specific AI regulations are yet to take effect, for example:

- Data protection authorities are particularly active in the AI space, showing a readiness to issue warnings, launch investigations and bring enforcement action against companies where their development and/or use of AI is suspected to be in breach of data protection regimes.
- Financial regulators, particularly in the US, are clamping down on so-called 'AI washing,' where companies overstate their AI capabilities to investors and consumers. Several warnings and certain enforcement actions have been issued in recent months (we anticipate other regulators will follow suit).
- Competition authorities are showing particular interest in tech companies' position in the AI development market, with investigations into partnerships between large tech firms and AI start-ups launched in both the US and Europe.
- Consumer protection regulators in the US are closely scrutinizing disclosures to users, ensuring that users' understanding and expectations match AI tools' capabilities. These agencies are also using consumer protection standards in their attempts to require companies to recognize new or evolving rights to online content that may be used for training AI systems.

> Regulators have already set their sights on AI, particularly in areas such as data protection and financial regulation in relation to AI washing. Companies should review their governance systems to ensure they stand up to scrutiny and be wary of new requirements coming down the line.
>
> **Zofia Aszendorf**
> Senior Associate

AI governance takes center stage

Key cornerstones for successful AI governance

The right governance around AI is important both to achieving organic growth in this area and to attracting investment (including, for early-stage companies, in the context of investor diligence). Importantly, AI governance shouldn't be seen as being limited to mitigating legal risk – done well it can also help to maximize the value of a company's AI investment, setting up future growth.

> A successful AI governance framework will help mitigate AI-related risk and set up future growth.
>
> **Beth George**
> Partner

A good example in the data space is the importance of appropriate governance processes in ensuring that proprietary datasets are appropriately ringfenced from use by third parties in the AI value chain (through a combination of technical measures, processes and contracting frameworks).

> Effective AI governance should not just be seen through the lens of regulatory necessity but also as part of the strategic imperative that builds trust and ensures integrity in decision making.
>
> **Rachael Annear**
> Partner

Regulatory guidance presents degrees of prescriptiveness around governance structures, including around topics such as the involvement of senior management and monitoring and reporting lines. Getting governance for AI right requires considering: (i) what the governance structures should look like; (ii) who should be staffed within them; and (iii) what those individuals should be responsible for.

Governance structures – key considerations

- Within corporations that are looking to add AI to their existing offerings, we are typically seeing a single person with general oversight – an 'AI leader' – supported by a cross functional 'AI steerco' of senior leaders, including legal and compliance professionals.
- Consider whether the AI steerco and AI leader should report to the board.
- Regular reporting assists the board to carry out an effective task of holding the AI steerco and AI leader to account.
- Consider whether links should be made to any other committees or steercos – we are seeing trends of cyber, risk and audit committees being involved in AI governance.
- Corporate groups need to consider what decisions can be made at divisional/subsidiary level and what decisions need to be centralized.

Staffing of the governance structure

- The people in the governance structure need to be appropriately qualified and ideally will come from a range of disciplines – such as engineers, developers, product specialists and lawyers.
- The EU AI Act contains a specific requirement on providers and deployers of AI systems to ensure AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf. Other guidance around the world also emphasizes the need for adequate training of personnel overseeing AI systems.

AI governance takes center stage

Terms of reference for the AI Leader and Steerco

These can broadly be categorized into three areas:

- Legal and compliance: this remit is broader than just AI-specific regulation. It needs to cover other legal obligations, for example antitrust regimes, sector-specific regulation and data regimes. It also applies more broadly than just in relation to the business' external roll out of AI systems – eg there is a significant interface between the use of AI for internal purposes and labor law compliance, including potential works council obligations. A particularly knotty piece of the legal and compliance aspects of AI governance is determining how to approach any product liability considerations, which will depend on the business's role in the AI value chain.
- AI Product Development: this will include considering the development of AI tools in line with legal and compliance obligations, including 'privacy by design' requirements.
- AI Deployment: key features of deployment should include periodic (perhaps annual) systemic risk assessments and audits of the deployment of AI tools, as well as clear processes for sign-off of new use cases for developed tools.

Organizations may also want to task the AI leader, AI steerco and the board with considering the company's AI-related reputation and appropriate external-facing communications – ie what the business wants to be saying about AI in public and how it wants to position itself with respect to AI. Businesses that can articulate this clearly will gain an advantage although they will also need to be mindful of the increased scrutiny on AI washing (see above).

Underpinning these three cornerstones of a business' AI governance structure needs to be a degree of flexibility and adaptability, in recognition of the fact that both the technology and the law in this space is fast evolving.

> AI governance frameworks should be assessed for structure, staffing and terms of reference – does the business have the right people, in the right place, doing the right thing – but it's equally important that they can adapt to the fast-evolving technology and law in this space.
>
> **Lutz Riede**
> Partner

Looking ahead

As the litigation and regulatory landscape continues to change, it's crucial for businesses to keep a close eye on these developments. Regularly evaluating the effectiveness of your governance systems will be key to mitigating AI-litigation risks.

If your business is developing or deploying AI, now's the time to make sure you have the right governance structures in place. This means ensuring you have the right staffing, resources, and clear terms of reference. But don't stop there. Building in flexibility will help you proactively adapt to future needs, positioning you for future success as the landscape evolves.

2.

International data transfers are under the spotlight

International data transfers are under the spotlight

Rachael Annear
London

Richard Bird
Hong Kong

Madeline Cimino
Washington, DC

Tochukwu Egenti
London

Fan Li
Shanghai

Christine Lyon
Silicon Valley

Philipp Roos
Düsseldorf

Christoph Werkmeister
Düsseldorf

Yvonne Wolski
Düsseldorf

In brief

In 2025, questions around data transfers and localization requirements will still be front and center for businesses. Regulators across different jurisdictions – each with varying requirements – aren't holding back either; they've shown they're ready to impose hefty fines for non-compliance.

This chapter outlines how 2025 could mark the beginning of a significant legal challenge to the EU-US Data Privacy Framework (DPF), potentially jeopardizing data transfers from Europe and the UK to the US. We'll also highlight other key developments and trends that businesses need to keep an eye on when transferring data across borders.

EU/UK data transfers to the US under threat?

The DPF is a landmark mechanism negotiated between the EU and the US which entered into force in 2023 to facilitate the transfer of personal data from the European Economic Area (EEA) to eligible US companies that choose to participate in the DPF (see here for further detail). The two predecessors to the DPF were each invalidated by the Court of Justice of the EU (CJEU) following concerns raised by privacy activist Max Schrems that the schemes did not appropriately protect European's personal data. Max Schrems and other activists have indicated they will challenge the DPF in the CJEU given similar concerns.

While 2024 did not see any actions from these privacy activists regarding the DPF, 2025 may be the year for Max Schrems or others to start the third (and final?) round of battle over data transfers from the EU to the US.

International data transfers are under the spotlight

Since the EU-US DPF's adoption, many US organizations have decided to participate:

> Since the DPF's implementation in July 2023, more than 2,800 enterprises have joined the framework, 70 percent of which are small and medium-sized businesses.
>
> Source: Joint Press Statement: Commissioner Didier Reynders and US Secretary of Commerce Gina Raimondo on the first periodic review of the EU-U.S. Data Privacy Framework – European Commission (europa.eu)

The UK agreed a UK Extension to the DPF shortly after the DPF entered force and, in 2024, Switzerland joined the UK in allowing the transfer of personal data to US-based recipients that are certified under the DPF without the need for other transfer safeguards to be implemented under national data protection laws (see here).

> 2025 will likely be another year with a lot of movement regarding cross-border data transfers subject to the EU's GDPR. Most important, the EU-US Data Privacy Framework might be challenged by privacy activists, requiring clients to closely follow the developments.
>
> **Philipp Roos**
> Principal Associate

The UK is no longer subject to the jurisdiction of the CJEU, which means any successful challenge against the DPF would not immediately affect the UK Extension. However, any successful challenge might be considered by the UK in determining whether to amend or revoke the UK Extension or renew it when it comes up for review.

Further EU and UK adequacy decisions?

2025 might also see an extension of the list of 'adequate' locations personal data can be transferred to without the need for additional transfer safeguards under EU data protection law. In this respect, the EU Commission is currently in discussion with Brazil and California, each of which applies high privacy safeguards similar to the GDPR.

The EU Commission's review of the UK's adequacy decision is expected to be completed in June 2025 and it currently seems likely that this decision will be renewed.

In August 2021, the UK government hailed its ability to make use of its new, post-Brexit, powers to issue equivalent adequacy regulations independent of the EU. However, the UK government is yet to issue any new adequacy regulations in respect of countries that are not already the subject of EU adequacy decisions. 2025 might see the UK government forge a separate path and issue adequacy regulations for additional countries.

New SCCs and data localization requirements in the EU

The EU Commission has announced work on a new set of Standard Contract Clauses (SCCs) for international data transfers to address the situation where a data importer of GDPR personal data is in a third country but also subject to the GDPR. It remains to be seen whether and to which extent these SCCs deviate from the existing SCCs and whether other jurisdictions might (again) follow this approach.

The EU will introduce data localization requirements as part of the European Health Data Space (EHDS) Regulation. The EHDS Regulation aims to establish an EU data space for health data and includes dedicated rules on the primary and secondary use of health data. In particular, given the sensitivity of health data, the EHDS Regulation proposes that certain stakeholders may only store and process health data within the EU or, as an exception, in third countries providing an adequate level of data protection. In addition, EU Member States may impose data localization rules at a national level. The EU may apply similarly strict standards in other data spaces involving sensitive data in the future.

International data transfers are under the spotlight

US tightens rules for data transfers

In 2024, President Biden issued an Executive Order (EO) restricting the bulk transfer of sensitive data to certain countries. EO 14117, signed on February 28, 2024, represents a major shift in US data regulation, particularly regarding sensitive personal and government-related data. The EO aims to address concerns about potential exploitation of such data by 'countries of concern' through new prohibitions and restrictions. By empowering the Attorney General to implement regulations, the EO seeks to prevent the transfer of bulk sensitive personal data to adversarial countries, including China, Russia and others. The scope of this regulatory framework is significant, as it targets not only data transactions but also data brokerage and vendor agreements, further strengthening the national security shield around US sensitive data. See here for further background.

The proposed regulations outlined in the Advance Notice of Proposed Rulemaking highlight efforts by the US Department of Justice (DOJ) to classify certain transactions into prohibited and restricted categories. Prohibited transactions include those involving data brokerage or access to human genomic data, while restricted transactions may proceed if security measures are in place. These rules will require companies engaged in international data transfers to review and potentially overhaul their compliance programs. For businesses involved in sensitive sectors like healthcare, finance or telecommunications, these new regulations may significantly impact their operations and necessitate additional compliance diligence.

Given the far-reaching nature of these proposed regulations, businesses that handle or process large volumes of US personal data must act swiftly to assess their risk exposure.
The expansive definitions of 'bulk sensitive personal data' and 'data brokerage' increase the number of companies that will be subject to these regulations. While certain exemptions are proposed, such as for personal communications and financial services, the overarching authority of the DOJ to regulate sensitive data transfers remains a critical concern. As this regulatory framework develops, it is likely to reshape the way US businesses engage in international data transfers, influencing their global operations and partnerships.

> The Executive Order 'marks the most significant executive action any President has ever taken to protect Americans' data security.'
>
> Source: FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data | The White House

Asia looks both ways

China's strict data transfer regulations have proven to be a significant burden for many multinational companies. New rules relaxing certain of these requirements were introduced in March 2024 – most notably, the exemption of transfers of the personal data of fewer than one million individuals a year from the requirement to undergo security assessment with the Cybersecurity Administration (see here for further detail).

While a large proportion of international companies operating at scale in China will still need to put in place (and file) a standard contract and security impact assessment, complete exemptions have usefully also been introduced for transfers of HR data and to facilitate individual cross-border commerce. A simplified form of standard contract has also been introduced for transfers of personal data within the Greater Bay Area (also without an obligation to file an impact assessment with the contract filing).

Within the last year, Thailand and Indonesia have both either introduced or proposed cross-border data transfer mechanisms that are structurally very similar to those under the GDPR. Thailand and the Philippines (among others) are actively promoting the adoption of the Association of Southeast Asian Nations (ASEAN) model contractual clauses (ASEAN and the EU have also recently published a joint guide to their respective contractual clauses).

International data transfers are under the spotlight

On the other hand, Vietnam has adopted a modified version of China's process for approving personal data exports, allowing for the government to intervene based on security assessment dossiers to be filed within 60 days of the transfer.

In the past few months, Australia has proposed introducing a 'whitelist' (without SCCs) while Malaysia has proposed removing its own whitelist regime (having never issued a list). The Digital Personal Data Protection Act in India will empower the government to issue a 'blacklist'.

Another proposed new Vietnamese law will restrict outbound transfers of categories of non-personal data: 'important data' and 'core data', with these terms defined in a way that approximates to the definitions of the synonymous concepts under China's Data Security Law. It appears that government approval will be required to transfer either category of data out of Vietnam. The equivalent restrictions on transfers of 'important/core data' from China have brought about pre-emptive localization of many operations and systems there.

However, on this topic as well, the past few months have seen a generally more business-friendly approach being taken, especially in the catalogues of 'important data' and approval mechanisms of free trade zones (in Shanghai, Tianjin and Beijing). Some of those rules were developed with the participation of resident international businesses. The EU and China also began discussing a mechanism to facilitate flows of non-personal data in August 2024.

SCCs in other jurisdictions

Like the EU and UK GDPR, various international jurisdictions may require data exporters to conclude SCCs to safeguard certain transfers of personal data to data importers in third countries. For example, in 2024, the Turkish and Brazilian authorities each published a set of updated SCCs including similar provisions as in the EU SCCs for data transfers. Therefore, international organizations must be prepared to both update intra-group agreements and address requests from third-party organizations to enter into such SCCs.

> While most countries in Asia do provide pragmatic data transfer mechanisms, the exact requirements vary a good deal from one jurisdiction to the next.
>
> **Richard Bird**
> Partner

Looking ahead

By staying informed and proactive, you can better manage risks and seize opportunities in the ever-evolving data landscape. It's essential for businesses to be equipped to navigate the complex and rapidly changing requirements around data transfers and localization, which can differ greatly across jurisdictions.

Keep a close eye on developments in cross-border transfer and localization laws, especially those recently introduced in the US, China, and Vietnam. If your business is involved in data transfers from Europe, be prepared for potential legal challenges to the DPF and anticipate likely changes to the SCCs for data transfers from the EU. Planning ahead will be crucial to ensure compliance and maintain smooth operations.

3.

A new wave of cyber threats is here

A new wave of cyber threats is here

Richard Bird
Hong Kong

Laéna Bouafy
Paris

Madeline Cimino
Washington, DC

Brock Dahl
Washington, DC/ Silicon Valley

Tony Gregory
London

Hanna Hoffmann
Düsseldorf

Megan Kayo
Silicon Valley

Jérôme Philippe
Paris/Brussels

Thomas Retière
Paris

Satya Staes Polet
Brussels

Rhodri Thomas
London

Christoph Werkmeister
Düsseldorf

In brief

As global cybersecurity threats continue to evolve, companies are navigating an increasingly complex risk landscape. In this chapter, our cybersecurity experts dive into recent trends in ransomware attacks and the latest regulations around incident response. They also discuss new guidance on fines and damage claims while exploring the intersection of cybersecurity and AI.

Here's what we'll cover:

- The rising frequency and scale of ransomware attacks.
- New incident response obligations.
- GDPR damage claims.
- The role of AI in enhancing and undermining cybersecurity.

Developments in ransomware attacks

In February 2024, several international law enforcement agencies scored a major success in the fight against cybercrime by seizing control of infrastructure used by LockBit, one of the world's most active ransomware groups, while developing decryption keys that could enable the recovery of many LockBit-encrypted systems. However, LockBit has reportedly continued attacking companies using new servers and dark web domains, which demonstrates the persistence of cybercriminals. While law enforcement continues to pursue cybercriminals and companies continue to improve their cybersecurity measures, ransomware remains rampant and attacks are increasing in sophistication and number, not least due to:

- the rise of widely available generative AI; and
- the increasing commoditization of ransomware, particularly through ransomware as a service

A new wave of cyber threats is here

> Recent developments emphasize that cybersecurity should be always higher on the agenda of the leadership of organizations.
>
> **Satya Staes Polet**
> Partner

In 2024, ransomware demands and payments have continued to climb, reflecting the ongoing evolution and aggressiveness of cybercriminals' tactics. The first half of 2024 saw ransomware attacks increase in both frequency and scale, with the average ransom demand reaching over $1.5m in the second quarter of 2024 – a 102 percent increase quarter over quarter. This increase is largely driven by the continued success of multiple-extortion schemes, where attackers not only encrypt data but also exfiltrate it, threatening to release sensitive information if ransoms are not paid.

Attackers may also threaten to deploy distributed-denial-of-service attacks or threaten employees and customers of victims to apply additional pressure on companies. A group of cybercriminals has even been known to lodge a complaint with a regulatory authority to denounce the failure of the company that suffered the data breach to disclose it as required by law, thereby using the law as a means of exerting pressure. The emergence of new groups and ransomware variants of cyberattacks, including rebranded ransomware groups, has also contributed to the record-breaking number of incidents and payments. Despite ongoing law enforcement efforts, the overall threat continues to grow, with 2024 potentially becoming the worst year on record for ransomware payments.

Beyond ransomware attacks, supply chain attacks continue to be a significant issue. Companies rely on third-party vendors, which provide systems and services critical to those companies. Cyberattacks, vulnerabilities or even faulty updates at vendors have resulted in significant losses for numerous customers of those vendors and highlighted the growing importance of integrating cybersecurity into a company's overall risk management. These incidents underscore the cascading effects that supply chain attacks can have, leading to regulatory penalties, breach of contract claims and potential litigation.

Additionally, supply chain attacks can be more challenging to investigate as an affected customer may have limited visibility into an attack on a third-party vendor and limited control over the vendor's investigation. In fact, supply chain risk has become such a significant issue that the US' National Institute of Standards and Technology (NIST) released its first major update of its Cybersecurity Framework, since 2014, to incorporate practices to manage cybersecurity risks within and across organizations' supply chains. Organizations must bolster their cybersecurity measures, ensure their supply chain contracts include robust security provisions and stay compliant with evolving regulations. Legal teams should prepare for complex liability issues and the intricacies of data breach notifications that arise from such multifaceted attacks.

Cybersecurity and AI

Cybercriminals are increasingly using AI to automate and target their attacks. This allows them to carry out individualized mass phishing attacks tailored to their targets, not only greatly increasing the efficiency of the attacks, but also allowing well-organized threat actors to automatically create fake login pages that are virtually indistinguishable from the legitimate pages. Additionally, research has indicated that the use of AI will significantly improve the capability of threat actors to crack passwords.

AI also allows threat actors to replicate proofs of concept or other types of successful attacks more quickly. For example, if a zero-day vulnerability is identified, the amount of time for threat actors to identify and target companies with such vulnerabilities in their systems is becoming shorter.

A new wave of cyber threats is here

The dwell time that threat actors are in a company's systems is also decreasing, as AI allows threat actors to identify data that appears to be valuable more efficiently and thus extract that data more quickly.

> As generative AI decreases attackers' dwell time, it's increasingly important to be prepared.
>
> **Megan Kayo**
> Partner

Conversely, AI can also help protect companies. AI can help identify and quarantine suspicious emails that may be phishing campaigns. Additionally, AI can detect vulnerabilities as well as malicious or anomalous activity within a company's systems sooner.

While AI tools and systems can benefit companies, cybersecurity plays a crucial role in ensuring that AI systems are resilient to attempts by malicious third parties to alter the system's behavior, performance or security properties by exploiting the system's vulnerabilities. Cyberattacks against AI systems can exploit AI-specific assets, such as training data sets or trained models, but also vulnerabilities in the AI system's (underlying) digital assets or the underlying ICT infrastructure. To address these risks, the EU AI Act requires certain high-risk AI systems to meet a specific cybersecurity standard.

New regulations on incident response

The EU Digital Strategy comprises several regulations on cyber strategy (eg the Cyber Resilience Act, the latest Network and Information Security directive (NIS2) and Digital Operational Resilience Act (DORA)). For specific sectors, they impose various obligations including registration obligations, specific governance measures, obligations to take technical, operational and organizational measures to manage security risks and specific reporting obligations for significant incidents. Companies in scope of NIS2 must make such reports within 24 hours.

If a cyber incident affects individuals in several European Economic Area (EEA) countries, global companies engaged in cross-border data processing can often benefit from the so-called one-stop-shop mechanism. This allows them to deal with a single lead supervisory authority, for example when reporting a global data breach. Recently, the EDPB has clarified that under the EU's GDPR, a legal entity which is the place of central administration of a group in the EEA can be considered as a main establishment only if it:

- takes the decisions on the purposes and means of the processing of personal data in the EEA; and
- has the power to implement these decisions.

In the UK, the trend is also for increasing cyber security regulation. The new government plans to introduce a new Cyber Security and Resilience Bill, which it says, 'will strengthen the UK's cyber defences, ensure that critical infrastructure and the digital services that companies rely on are secure.' The announcement comes after a number of recent high-profile cyberattacks in the UK including on the National Health Service, Transport for London, the Ministry of Defence and the Royal Mail. While the details of the Bill remain to be seen, according to government briefing notes, the Bill will update the UK's current Network and Information Security (NIS) Regulations 2018, including by:

- expanding their remit to protect more digital services and supply chains, beyond the 'essential services' and 'digital service providers' that are regulated by the current Regulations;
- giving greater powers to regulators to proactively investigate potential vulnerabilities, and ensuring they are better funded; and
- mandating increased incident reporting to give the government better data on cyberattacks, including specifically ransomware attacks.

The Bill follows the entry into effect of the UK's Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, which mandates baseline security requirements for manufacturers of consumer connectable products.

A new wave of cyber threats is here

In the US, the adoption by Securities and Exchange Commission (SEC) of new cybersecurity disclosure rules marks a significant shift in how public companies must manage and report cybersecurity risks. US domestic issuers are required to disclose material cybersecurity incidents within four business days of determining a cybersecurity incident to be material (and foreign private issuers must do so 'promptly' in certain circumstances) and provide annual disclosures on their cybersecurity risk management, strategy and governance. To ensure clarity and consistency in reporting and avoid confusion in the marketplace, the SEC clarified that domestic issuers should only report material cybersecurity incidents under Item 1.05 of Form 8-K, and all others under other sections, such as Item 8.01. US domestic issuers must:

- ensure a process is in place to escalate and carefully assess the materiality of cybersecurity incidents, considering both quantitative and qualitative factors, such as potential reputational harm and the likelihood of regulatory scrutiny; and
- incorporate the new disclosure requirements into their overall risk management strategies, ensuring that they meet regulatory obligations and effectively mitigate potential risks associated with cybersecurity threats.

> Companies are closely monitoring the SEC's evolving cybersecurity regulations, paying particular attention to emerging enforcement trends and their impact on risk management and compliance.
>
> **Brock Dahl**
> Partner

Additionally, the US Federal Trade Commission (FTC) finalized updates to its Health Breach Notification Rule to expand the definition of breach to include unauthorized disclosures of information and to apply to additional health and wellness apps and technologies, such as apps that track fitness, fertility, sleep or diet. The FTC also amended its Safeguards Rule to incorporate reporting obligations for data breaches and other security events.

Fining guidance and damage claims

In recent months, the Court of Justice of the European Union (CJEU) has dealt extensively with claims for damages under Article 82 of the GDPR in connection with data breaches. In this context, the CJEU clarified that:

- data breaches do not lead to an irrebuttable presumption of inadequacy of security measures;
- claims for damages require the existence of (material or immaterial) damage, which is a separate requirement from 'breach of the GDPR';
- inconsequential losses of control over personal data do not constitute damage. However, non-material damages can arise if a data subject fears that their personal data could be misused by third parties as a result of the breach; and
- while the term 'damage' does not provide for a certain threshold, there are two significant restrictions that in practice will impede compensation for fears as non-material damage: (i) fear 'may,' but need not, constitute damage; and (ii) the burden of proof to show that the fear can be considered 'well-founded' falls on the claimant.

In the UK, the Information Commissioner's Office (ICO) has published new fining guidance on how it will exercise its fining powers for breaches of the UK GDPR. The guidance replaces the sections concerning penalty notices in the ICO's Regulatory Action Policy, which was published in November 2018. While much of the guidance reflects existing practice, it includes certain clarifications relevant to UK GDPR breaches, including:

A new wave of cyber threats is here

- the ICO will adopt a five-step approach when calculating any fines, which involves: (i) assessing the infringement's seriousness; (ii) ascertaining the organization's turnover; (iii) determining a starting point for the fine having regard to seriousness and turnover; (iv) adjusting the amount for any aggravating and mitigating factors; and (v) calibrating the fine to ensure it is effective, proportionate and dissuasive;
- in addition to 'special category data' and criminal convictions data, the ICO may consider affected location data, private communications, passport or driving license details and financial data to be sensitive when assessing the seriousness of the infringement, on the basis that these are likely to cause damage or distress to data subjects; and
- among other factors, the ICO may consider the extent to which the organization cooperated with the regulator as an aggravating or mitigating factor. Cooperation that enables the investigation to be concluded significantly more quickly or effectively, or that significantly limits the resulting harms to data subjects may be considered a mitigating factor, although simply performing the legal duty of cooperating with the ICO (for example by responding to requests for information and attending meetings) will be viewed neutrally. On the other hand, persistent and repeated behavior that delays an investigation – including failures to meet deadlines without a reasonable excuse – may be an aggravating factor.

> The good news is that there's often lots that organizations and their legal advisers can do – both before and immediately after a cyberattack – to mitigate the harm caused.

Rhodri Thomas
Partner

Looking ahead

Cybersecurity regulations are tightening, and penalties for non-compliance are on the rise. As cybercriminals become more sophisticated in their use of AI, the need for companies to continually update and bolster their cybersecurity strategies has never been more urgent.

Staying ahead in this rapidly changing environment requires vigilance and adaptability. A strong, proactive cybersecurity strategy can make all the difference, helping you stay ahead of threats and minimize damage if a cyberattack occurs.

4.

New global regulations are changing our digital operations

New global regulations are changing our digital operations

Rachael Annear
London

Richard Bird
Hong Kong

Gernot Fritz
Vienna

Rixa Kuhmann
Hamburg

Janet Kim
Washington, DC

Laura Knoke
Hamburg/Berlin

Tristan Lockwood
London

Christina Möllnitz-Dimick
Munich

Sean Quinn
Washington, DC

Lutz Riede
Vienna/Düsseldorf

In brief

Over the past year, a global push to regulate the safety, accountability, and transparency of online services have begun to crystalize. In late 2023, the EU Digital Services Act came into force alongside the passage of the UK Online Safety Act, signaling a significant shift in how digital intermediaries are regulated.

While the US has yet to pass federal legislation, both state and federal regulators invoking concerns about privacy and consumer rights and state lawmakers focusing on children's safety, have worked to address the gap.

Beyond the EU, UK, and US, laws like the Australian Online Safety Act are contributing to an expanding landscape of digital regulation. The full impact – both intended and unintended – of these developments will unfold over the coming years.

The new frontier of internet regulation

Digital intermediaries have long been subject to general laws and an assortment of targeted obligations. However, the EU Digital Services Act and the UK Online Safety Act reflect first attempts at the comprehensive regulation of online harm, as well as various other perceived risks and challenges arising from digital intermediaries related to transparency and accountability. They come at a time when lawmakers and regulators are also keenly focused on competition and consumer issues in digital ecosystems, with reforms such as the EU Digital Markets Act and UK Digital Markets, Competition and Consumers Act imposing parallel obligations on so-called digital 'gatekeepers.'

New global regulations are changing our digital operations

Adopting the lexicon of Australia's 2021 Online Safety Act – an early, industry-led framework passed by federal lawmakers in Australia – many jurisdictions are increasingly framing the issue of digital risk as a question of online safety, especially that of children.

In the US, the Kids Online Safety Act – a sweeping Bill passed by the Senate that would impose a duty of care on covered platforms, along with various safeguarding, disclosure and transparency requirements – reflects mounting bipartisan efforts at a federal level to regulate in this space. Despite uncertainty as to whether it has the necessary traction to pass the House, the law signals the intent with which many lawmakers are confronting the issue.

> The debate over online safety is just beginning; emerging technologies and processes that are being developed now may well fundamentally change our expectations of the way we participate in life online.

Rachael Annear
Partner

	UK Online Safety Act	EU Digital Services Act	Australia Online Safety Act
Extra-territorial scope	Yes	Yes	Yes
In force	Yes – requirements coming into force on a rolling basis until 2026	Yes – all provisions in force	Yes – requirements coming into force on a rolling basis
Key topics	Child safety, illegal content, adult user empowerment, fraudulent advertising	Illegal content, societal risk, digital traders	Child safety and illegal content
Services subject to the most extensive obligations	Categorized services that meet both UK monthly active user and functionality thresholds	Very large online platforms and very large online search engines (< 45 million monthly active EU users)	Social media, electronic messaging, search engines, app distribution
Regulator	Ofcom	European Commission and Member State enforcement agencies	eSafety Commissioner
Fines	£18m or 10% of global annual revenue	6% of the worldwide annual turnover	Up to AU$782,500 (2024)

New global regulations are changing our digital operations

> While the US debates the merits and constitutionality of laws seeking to improve online safety, accountability and transparency, the UK, EU and various other jurisdictions have moved forward with robust reforms that may ultimately drive global standards.
>
> **Tristan Lockwood**
> Senior Associate

Age-gating and age-appropriate design

US state lawmakers have been more successful in passing various narrower online safety reforms, with an increasing number of states adopting laws requiring age verification to access online pornography and requiring age verification and parental consent for minors to access social media. However, constitutional challenges have halted the enforcement of many such laws. In July 2024, the US Supreme Court decided to hear a challenge to a Texas law requiring age verification to access online pornography, potentially set to bring some certainty to the future of such requirements in 2025.

> The prospect of US federal online safety legislation, a growing number of state initiatives and mounting state and federal enforcement actions make for an uncertain compliance landscape in the US.
>
> **Janet Kim**
> Partner

A free speech challenge has also halted the enforcement of the California Age-Appropriate Design Code Act ahead of its July 2024 effective date. The law, which is modelled on the UK's Age-Appropriate Design Code, requires businesses to prioritize children's privacy and protection when designing digital products or services likely to be accessed by under-18s.

Despite constitutional uncertainty surrounding age-gating and age-appropriate design requirements in the US, such laws are gaining traction elsewhere. The UK Online Safety Act and draft Codes of Practice issued by the online safety regulator, Ofcom, seek to impose potentially sweeping requirements to enforce highly effective age assurance to prevent children accessing pornographic and other harmful content. Jurisdictions elsewhere in the world are looking to the UK's design-focused Age Appropriate Design Code as a model. For example, the Singaporean privacy regulator this year adopted Advisory Guidelines for Children's Personal Data that mirror many of its requirements. Likewise, the EU Digital Services Act requires online platforms to introduce measures to ensure a high level of privacy, safety and security of minors, with the European Commission planning to issue detailed guidelines outlining specific expectations in 2025.

> The EU Digital Services Act was a watershed moment. But with a broad interpretation of risk assessment and mitigation requirements, proactive enforcement and codes of practice and guidelines in the pipeline, its full implications remain to be seen.
>
> **Lutz Riede**
> Partner

Looking forward, the debate around the costs and benefits of such laws, especially how they may impact the free speech and other interests of adult users, looks set to intensify.

New global regulations are changing our digital operations

Transparency

A common thread in the legislative efforts canvassed above are increasing requirements to provide user transparency around content moderation rules and outcomes, along with the operation of recommender systems on platforms. In various jurisdictions around the world, a lack of transparency is also increasingly being used as a hook by regulators and private litigants in privacy and consumer cases targeting online platforms.

In the US, the concept of 'dark patterns' has been formalized in several state consumer privacy laws, including prohibitions on the use of dark patterns to obtain consent. Additionally, the Federal Trade Commission has continued to express its keen interest in dark patterns through several actions, public workshops and a staff report titled *Bringing Dark Patterns to Light*, which argues that dark patterns are an unfair or deceptive business practice that may be subject to enforcement action.

This emphasis on transparency is also apparent in the EU's AI Act, which imposes transparency obligations aimed at enabling users to understand that they are interacting with an AI system and to detect synthetically generated content and deepfakes, and deployers to understand the AI systems' design and be informed of their use. This allows accountability for AI-based decisions made by companies and public authorities and ensures additional risk management and transparency of training data for very capable and impactful AI models.

Mounting transparency expectations are also apparent in more traditional contexts, such as the enforcement of privacy laws, with many privacy regulators emphasizing the importance of transparency when issuing guidance on the development and deployment on AI systems.

Looking ahead

As we move forward, we anticipate that more jurisdictions will introduce laws aimed at enhancing the safety, accountability, and transparency of digital intermediaries. As these regulations evolve, we expect regulators to:

- Leverage new laws to tackle perceived risks and address control deficiencies.
- Utilize transparency mechanisms to bridge the information gaps between digital service providers and consumers.
- Focus on service providers that fail to adhere to their terms of service and public statements, particularly regarding content moderation.

With this shifting regulatory landscape, it's essential for providers to consider any structural changes necessary to ensure that their product development, launch, and monitoring processes, along with compliance design and assurance frameworks, are robust and fit for purpose in the medium and long term.

5.

Tougher enforcement is reshaping data and privacy compliance

Tougher enforcement is reshaping data and privacy compliance

Rachael Annear
London

Robert Barton
New York

Richard Bird
Hong Kong

Davide Borelli
Milan

Mark Egeler
Amsterdam

Nina Frant
Washington, DC

Daniel Gold
London

Cat Greenwood-Smith
London

Tim Howard
New York

Sam Kloosterboer
Amsterdam

Joseph Mason
London

Giles Pratt
London

In brief

The spotlight on AI risks is intensifying, and with it comes a surge in data-related regulatory enforcement worldwide. Regulators are not only using existing laws but are also advocating for greater powers to oversee AI development and deployment. In some regions, this includes calls for restrictions on AI-related processing. For organizations developing AI, it's important to integrate compliance and risk management measures throughout the process. At the same time, attention should remain on existing enforcement risks around cyber issues, privacy practices, and consumer and competition laws.

Increased regulatory focus on AI

As AI becomes ever more ubiquitous and powerful, regulators are rushing to manage and mitigate this potentially high-risk technology. Typically, this means relying on privacy laws, including the EU and UK GDPR, where the data processing includes personal data, but consumer protection legislation and antitrust laws are also being used to put guardrails around AI.

Examples of regulatory action in 2024 include:

- Some regulators, including several EU data protection authorities (DPAs), are actively investigating AI companies for alleged breaches of the EU GDPR. The Italian DPA issued OpenAI with a formal notice for violations of provisions of the EU GDPR, having originally banned the use of ChatGPT in Italy until OpenAI complied with a set of interim measures.

Tougher enforcement is reshaping data and privacy compliance

- In the UK, the Information Commissioner's Office (ICO) has been investigating Snap's 'My AI' chatbot but, in July 2024, agreed to close its investigation on the basis that Snap appropriately remedied its alleged breaches of the UK GDPR. However, the ICO noted that its investigation had led to Snap conducting a more thorough review of potential risks posed by the chatbot.
- Some regulators, such as the South Korean Personal Information Protection Commission (PIPC) and the UK's ICO, are aiming to mitigate AI risks through updating existing guidance and regulatory innovation. The ICO launched a consultation series in the first half of 2024 on the intersection of data protection and generative AI, focused on topics such as purpose limitation in the generative AI lifecycle, the accuracy of training data and model outputs and the allocation of controllership. We expect to see updates to ICO guidance in 2025 as a result. South Korea's PIPC has emphasized regulatory sandboxes and introduced a 'Prior Adequacy Review Mechanism,' where it will work together with startups developing innovative AI models or services to ensure that sufficient privacy and data protection measures are embedded in the design of AI systems.

> Data privacy regulators across the world are focused on AI. Businesses need to ensure that they are developing and deploying AI systems compliantly including, where appropriate, engaging closely with regulators as they do so.
>
> **Giles Pratt**
> Partner

- In the US, the Federal Trade Commission (FTC) has increasingly brought investigations and enforcement actions related to AI. In July 2023, the FTC issued a civil investigative demand (CID) to OpenAI covering a range of topics, including public disclosures about AI products, the data it used to train its models and measures taken to mitigate potential risks including false statements about individuals. This follows a settlement with Rite Aide related to the company's use of AI-based facial recognition technology. In addition, the agency recently announced a sweep of enforcement actions concerning AI-related misrepresentations. More CIDs can be expected to be issued in AI investigations, given the FTC's November 2023 approval of a resolution making it easier for officials to issue CIDs.

> The Italian DPA's bold stance against OpenAI reflects the global shift toward stricter AI regulation. AI growth must be matched by strong commitments to data protection and regulatory engagement.
>
> **Davide Borelli**
> Counsel

Looking ahead to 2025, we expect privacy regulators to continue their focus on AI.

In the US, the FTC should be expected to ramp up its rigorous scrutiny of AI products and businesses. The FTC has publicly stated its interest in enforcement relating to advertising claims, AI product misuse to perpetuate fraud and scams, competition concerns and copyright/IP concerns with regards to training AI models and data privacy. The FTC's interest in investigating competition concerns has already resulted in the issuance of orders to five companies requiring them to provide information about recent investments and partnerships involving generative AI companies and cloud service providers. The agency has also announced an investigation into 'surveillance pricing,' the practice of categorizing individuals using their personal information to set pricing targets for goods or services using AI technology.

Tougher enforcement is reshaping data and privacy compliance

> As many companies increasingly become AI companies, they will need to ensure that they are developing and deploying AI systems safely and effectively.
>
> **Joseph Mason**
> Associate

In the UK and EU, we expect ongoing focus on AI products and services, particularly those deemed to be higher risk, and companies should expect a robust approach from regulators if they suspect infringements of EU or UK GDPR. It remains to be seen how plans to reform UK data laws announced by the newly-elected UK government will impact data protection regulation as it relates to AI.

> Working out how to approach AI enforcement is fast becoming a global priority, reflecting a collective commitment to harnessing the power of AI responsibly.
>
> **Rachael Annear**
> Partner

Novel regulatory approaches to match new challenges

In the EU, there is increased regulatory focus on consistent enforcement of GDPR by DPAs in cross-border cases. Following its 2024-27 strategy, the European Data Protection Board (EDPB) aims to 'reinforce a common enforcement culture and effective cooperation.' This partly reflects the realization that data processing is an increasingly cross-border activity, and that greater collaboration between DPAs is therefore necessary. The EU is taking the following steps to improve data regulation across the EU:

- Updates to the one-stop-shop mechanism (OSS):
  - Despite being a cornerstone of the EU's GDPR, the OSS mechanism has not fully met expectations, with delays in enforcement arising when the lead DPA was unable to reach a consensus with other DPAs. The European Commission has proposed a Regulation containing new procedural rules which aim to further harmonize enforcement and improve the efficiency of cross-border cases. The regulation is currently still in the legislative pipeline. The EDPB and the European Data Protection Supervisor (EDPS) jointly issued an Opinion on this proposal, welcoming many aspects aimed at improving the handling of cross-border claims.
  - In a recent Opinion, the EDPB clarified that, in relation to the OSS:
    - a controller's central administration can only be considered its 'main establishment' if it makes and implements the decisions on the purposes and means of the processing of personal data; and
    - the OSS mechanism is applicable only if one of the controller's EU establishments makes and implements those decisions; without such an establishment, the OSS cannot be applied.
- There is an increased use in the 'regulatory toolbox' by EU DPAs and an increase in the amount and height of fines (following implementation of EDPB Guidelines on the calculation of fines). In 2023 alone, DPAs collectively imposed an amount of over €1.97bn across 1,690 fines. This trend is continuing in 2024 (eg a recent €290m fine for Uber by the Dutch DPA), while regulators are increasingly using other regulatory powers such as enforcement orders.
- Specific focus areas of EU DPAs include the use of tracking cookies (and ePrivacy in general), data trading (brokers), shadow banning and similar technologies and the use of biometric data including facial recognition.

Tougher enforcement is reshaping data and privacy compliance

Similarly, US regulators have interpreted their existing investigative authority in novel ways to allow it to address new data privacy issues.

- The US Department of Justice (DOJ) continues to bring actions under its Civil Cyber-Fraud Initiative against federal contractors that fail to implement appropriate security controls required by government contracts, including one recent settlement of over $10m against consulting companies associated with New York State's implementation of federal COVID-19 Emergency Rental Assistance programs.
- The US Securities and Exchange Commission (SEC) has had mixed success in attempting to broaden an existing rule that requires companies to maintain sufficient accounting controls to apply in the data privacy and cybersecurity context. The agency recently secured a settlement of over $2m in part on the basis of this broader interpretation of the rule. But just one month later, a court dismissed similar claims in a separate lawsuit, holding that the rule did not provide the SEC with authority to regulate data privacy and security.
- The FTC continues to investigate and (in coordination with the DOJ) sue for alleged infractions of federal law protecting children's digital privacy. In August 2024, following an investigation, the DOJ sued TikTok and affiliates for allegedly failing to obtain parental consent before collecting children's personal information, in violation of a federal statute.

While the UK's ICO is continuing to take regulatory action for alleged data privacy infringements, it has suffered several recent adverse decisions.

- In October 2023, Clearview AI successfully appealed against the ICO's £7.55m fine and processing ban, with the court holding that the processing of UK data subjects' photos by non-UK/EU criminal law enforcement and national security agencies was outside the material scope of both the EU and UK GDPRs.
- In April 2024, a second instance court dismissed the ICO's appeal against the first instance court's 2023 judgment, which largely overturned the ICO's 2020 enforcement action against Experian regarding its processing of user data for its marketing services.

In August 2024, the UK Government announced a proposed uplift to the annual data protection fees by 37 percent, in what could be seen as a recognition that the ICO may need additional resources to take as much regulatory action as it might wish.

Data litigation continues to develop

In addition to regulatory enforcement in the EU, there is an increase in 'private enforcement' through class action litigation as EU case law on material and non-material damages further develops.

In the UK, opt-out mass claims alleging infringements of the UK GDPR have become much harder to bring since the Supreme Court's 2021 judgment in *Lloyd v Google*. However, case law in this area is still embryonic and several funders and plaintiffs are testing this, including by using alternative collective redress mechanisms, such as the opt-in Group Litigation Order and the antitrust-specific 'Collective Proceedings' model.

Plaintiffs in the US continue to bring class action claims arising from data breaches. Questions remain about whether such claims give rise to standing to sue in federal court under recent US Supreme Court jurisprudence, but companies may face pressure to settle such claims rather than prolong litigation by disputing plaintiffs' alleged injuries or damages. Earlier this year, Cash App and its parent company reached a $15m class settlement arising from data breaches that took place in 2021 and 2023, exposing customers' personal information.

Tougher enforcement is reshaping data and privacy compliance

Looking ahead

As we look to 2025 and beyond, companies should brace for an intensified regulatory focus on data enforcement, particularly concerning the development and deployment of AI systems. Regulators have shown a readiness to take strong actions against suspected privacy law violations, including halting the launch of AI solutions or pausing ongoing AI development.

However, these regulatory measures also serve as valuable guidance for safe and effective AI deployment. To navigate this landscape, companies should:

- Ensure they maintain comprehensive documentation, including detailed data protection impact assessments for high-risk processing.
- Stay informed about the latest guidance from DPAs, such as the UK's ICO and the EU's EDPB.
- Prioritize the integration of privacy protections into their AI systems from the outset of the development process.

Beyond AI, changes to the EU GDPR's OSS mechanism are likely to facilitate more enforcement of cross-border processing within the EU. We also anticipate an uptick in global enforcement actions related to alleged breaches of privacy, cybersecurity, and consumer protection laws.

6.

US state consumer privacy laws are expanding

US state consumer privacy laws are expanding

Christine Chong
Silicon Valley

Christine Lyon
Silicon Valley

In brief

Consumer privacy legislation in the US has reached a critical turning point. With no comprehensive nationwide privacy law in place, individual states have begun enacting their own laws to safeguard consumer privacy. Currently, over 40 percent of US states have implemented consumer privacy laws, and momentum continues to grow as additional states propose and consider their own legislation.

While these new state laws share some commonalities, their unique obligations contribute to a complex compliance landscape. Furthermore, certain states are also introducing specialized privacy laws, such as those focused on consumer health data. In this chapter, we explore the current status of US state consumer privacy laws, highlight key areas of alignment and divergence, and offer predictions regarding upcoming enforcement priorities.

Current status of state consumer privacy laws

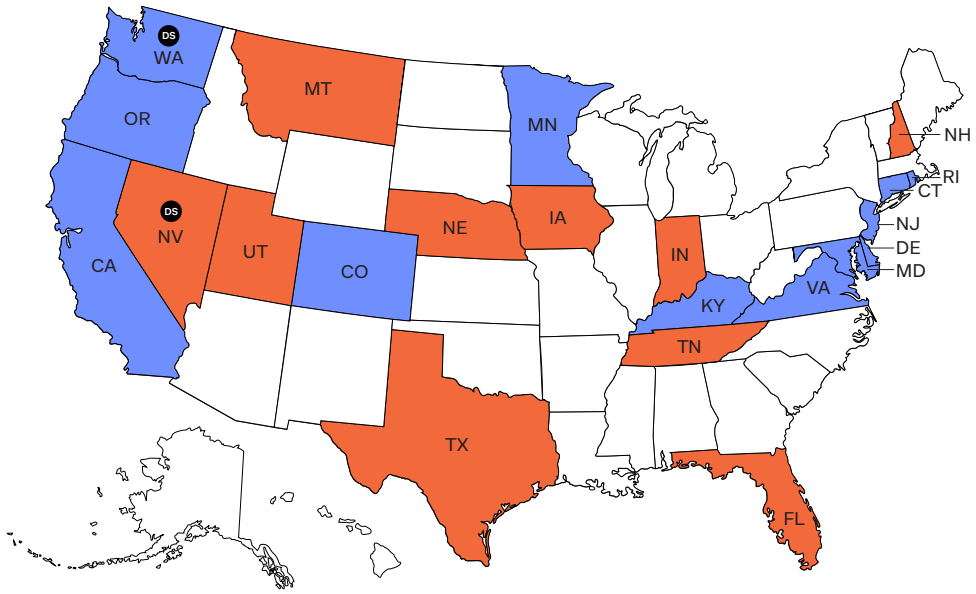
California was the first state to pass a comprehensive consumer privacy law, called the California Consumer Privacy Act (CCPA), in 2018. Since then, other states started to pass their own laws and the first half of 2024 saw a surge of states passing these laws; at one point, a new state law seemed to pass weekly. These state consumer privacy laws are either in effect or shortly coming into effect through 2026.

US state consumer privacy laws are expanding

As of the end of August 2024, 20 states had passed consumer privacy laws, and two further states had passed consumer health data laws. Notably, these laws have gained support on both sides of the political aisle, from both Democrat and Republican legislators.

The chart below shows the degree of bipartisan support for these privacy laws, reflecting, in blue, the states with consumer privacy laws with Democratic-party affiliated governors, and red for states with Republican-party affiliated governors.

State consumer privacy laws



Key

- Democratic
- Republican
- DS Consumer health data specific

Consumer health data specific laws

1. Nevada Act Relating to Data Privacy
2. Washington My Health My Data Act

Laws passed as of August 31, 2024

Consumer Privacy Laws

CA	–	California
CO	–	Colorado
CT	–	Connecticut
SE	–	Delaware
FL	–	Florida
IN	–	Indiana
IA	–	Iowa
KY	–	Kentucky
MD	–	Maryland
MN	–	Minnesota
MT	–	Montana
NE	–	Nebraska
NH	–	New Hampshire
NJ	–	New Jersey
OR	–	Oregon
RI	–	Rhode Island
TN	–	Tennessee
TX	–	Texas
UT	–	Utah
VA	–	Virginia

US state consumer privacy laws are expanding

While there initially appeared to be momentum in Congress toward a federal privacy bill, including for the American Privacy Rights Act of 2024 (APRA) being deliberated in this 118th Congress, support for the APRA has appeared to cool and commentators now think it's unlikely that the APRA will pass in its current form in this legislative session.

> We have reached a turning point in US privacy regulation, and there is no going back: the future involves greater regulation and protection for consumers.
>
> **Christine Lyon**
> Partner

This means that, for the foreseeable future, the state-level privacy laws are here to stay. Notoriously, the US has 50 different state data breach laws, and in principle, we could potentially end up with 50 different state consumer privacy laws as well.

Where do the laws align or differ?

The state consumer privacy laws share many core elements, including requirements related to:

- notice (eg additional detailed notices required in certain states);
- consumer rights (eg access, correction and deletion rights, as well as rights to limit processing of sensitive personal information and to opt out of certain activities, such as sale or sharing/use of personal information for targeted advertising);
- oversight of service providers/processors; and
- governance and accountability (eg data protection assessments, training and record-keeping).

While the state consumer privacy laws have started aligning in certain areas, none of these laws are exact duplicates, and the detailed requirements vary from state to state. Below, we highlight a few of the key areas where the laws differ more fundamentally in approach.

Applicability Thresholds

The laws generally apply to companies that conduct business in that state or produce goods or services that are targeted to residents of that state and meet certain thresholds, such as the number of consumers whose personal information they process each year and the level of revenue (if any) they derive from sale of personal information.

For example, the Virginia Consumer Data Protection Act (the Virginia law) applies to businesses that produce products or services that are targeted to Virginia residents and (i) during a calendar year, control or process personal information of at least 100,000 consumers, or (ii) control or process personal information of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal information.

In contrast, other laws apply only to companies that reach an annual revenue threshold (such as the CCPA) or exclude small businesses as defined by the US Small Business Administration. These laws also may apply to varying degrees to non-profit organizations.

Scope of Covered Individuals

Most of the laws apply only to consumers acting in an individual or household context and exclude individuals acting in an employment or professional/B2B context. However, the CCPA applies to all California residents, including those acting in an employment or professional/B2B context.

Sensitive Data Opt-in versus Opt-out; Health Data

The laws provide heightened protections for a wide range of data defined as 'sensitive' under these laws, such as:

- government issued identification numbers (eg Social Security Number);
- precise geolocation;
- data revealing racial or ethnic origin;
- genetic or biometric information; and
- personal information concerning a known child.

Certain laws include additional types of data as sensitive, for example, under the CCPA, sensitive personal information includes union membership, as well as the contents of a consumer's mail, email and text messages (unless the business is the intended recipient of the communication).

US state consumer privacy laws are expanding

The Oregon Consumer Privacy Act includes a consumer's status as transgender or nonbinary, or status as a victim of crime, as 'sensitive' data.

While some may assume that California's CCPA has the highest requirements among the state privacy laws, the CCPA takes a less restrictive approach to sensitive data than many of the later state consumer privacy laws: the CCPA requires businesses to allow California residents to limit the processing of their sensitive personal information (similar to an opt-out approach), while many of the other state consumer privacy laws require businesses to obtain opt-in consent to process a consumer's sensitive personal information.

New health data laws, have novel requirements for consumer health data, with distinct notice and consent requirements. For example, the Washington My Health My Data Act requires that businesses provide a separate and distinct link to a Consumer Health Privacy Policy that may not contain additional information not required under the law.

Sale of Personal Information; Use for Targeted Advertising

The laws give consumers varying rights to opt out of the 'sale' of their personal information, and to opt out of the use of their personal information for targeted advertising.

California's CCPA obligations are particularly broad-reaching and administratively burdensome, given the CCPA's expansive definition of 'sale' and requirement to include a specific 'do not sell or share my personal information' link if a company engages in covered 'sales' or 'sharing.' Differing definitions of 'sale' among these laws also can complicate attempts to take a cohesive approach across states.

Governance

The laws generally require that businesses conduct a data protection assessment for processing activities that present a heightened risk of harm to a consumer.

The Minnesota Consumer Data Privacy Act goes further and requires that companies maintain an 'inventory' of personal information, and separately document and maintain a description of policies and procedures to comply with the law, including where applicable, the name and contact information for the chief privacy officer or other individual with primary responsibility.

California's CCPA also includes training requirements for personnel handling privacy-related inquiries or requests.

Predictions on enforcement priorities

State attorneys general and regulatory agencies can initiate investigations and enforcement actions against both controllers and processors. For example, the CCPA regulations provide that the California Privacy Protection Agency (CPPA) may audit a 'business, service provider, contractor or person,' and that the audit may be announced or unannounced as determined by the CPPA. The Virginia Law also explicitly states that the Attorney General has authority to enforce the provisions of the law on controllers and processors.

> Regulators, including attorneys general and privacy enforcement agencies, have newfound powers under these state consumer privacy laws – and they are prepared to exercise those powers.
>
> **Christine Chong**
> Associate

As the state privacy laws are relatively new, we focus on predictions, including based on past actions from enforcement activities and guidance on the oldest of the state privacy laws.

- **2025 will come with more enforcement actions and continued 'sweeps.'** State attorneys general and regulators have initiated investigative 'sweeps' of certain industries under these laws, in which the regulator sends information requests to companies and may initiate further investigations based on their responses. Examples include California's CPPA launching investigative sweeps with letters to businesses with popular streaming apps and devices, as well as on topics such as employers and HR-related data, mobile applications and loyalty programs. In July 2023, the CPPA initiated an inquiry into privacy practices of connected vehicles and related technologies, which is understood to be understood to be ongoing.

US state consumer privacy laws are expanding

- **2025 enforcement actions will focus on processing of sensitive data.** Colorado has announced an investigative sweep focused on collection and use of sensitive data, including on the requirements to obtain consent prior to collecting sensitive data, and allow consumers to opt out of targeted advertising and profiling. Additionally, the Texas Attorney General launched a major data privacy and security initiative earlier this summer to establish a team that is focused on 'aggressive enforcement' of Texas' privacy laws. The statement noted that the data privacy enforcement team will focus on several privacy laws to protect Texans' sensitive data.
- **2025 enforcement actions will be responsive to consumer complaints.** State attorneys general and regulators have emphasized that they are listening to consumer complaints and taking action informed by these complaints. For example, the CPPA has detailed its process to review and evaluate every complaint that it receives, and over 2,000 consumer complaints were received from July 6, 2023 to June 30, 2024. The California Attorney General also noted that one of its major recent CCPA actions arose in part from a consumer's complaint on social media about the company's processing of their personal information. The volume of complaints will likely increase over time, as a number of the state consumer privacy laws now require a business to provide the consumer with a mechanism or information through which the consumer may contact the Attorney General to submit a complaint if the business has denied the consumer's request even in part.

Looking ahead

As the number of US state consumer privacy laws continues to grow, it's crucial for companies to take proactive steps to navigate this evolving landscape. Here are three key actions to consider:

1. Develop a Compliance Strategy: Collaborate with your business teams to create a comprehensive approach for complying with state privacy laws. With new legislation emerging regularly, having a robust privacy compliance strategy will help you establish sustainable policies and procedures.
2. Review Consumer Rights Mechanisms: Take a close look at the rights mechanisms available to consumers. This includes evaluating the methods you have in place and ensuring you're ready to respond effectively. Keep in mind:
   - This area is under high scrutiny, with significant volumes of complaints reported by the CPPA.
   - Consumer rights mechanisms are highly visible to regulators, making it easy for them to spot potential deficiencies (for example, companies receiving CCPA notices of violation for failing to include a 'Do Not Sell or Share My Personal Information' link on their sites).
   - Prioritizing these mechanisms is essential, as they are a focal point of US state privacy laws and play a crucial role in building customer trust.
3. Educate and Engage Your Team: Share updates on new privacy laws and provide training for employees on how to handle data subject requests and the importance of compliance. Keeping your team informed and engaged is vital for fostering a culture of privacy within your organization.

7.

Asia's privacy laws are maturing

Asia's privacy laws are maturing

Richard Bird
Hong Kong

Harshavardhan Ganesan
Singapore

Fan Li
Shanghai

In brief

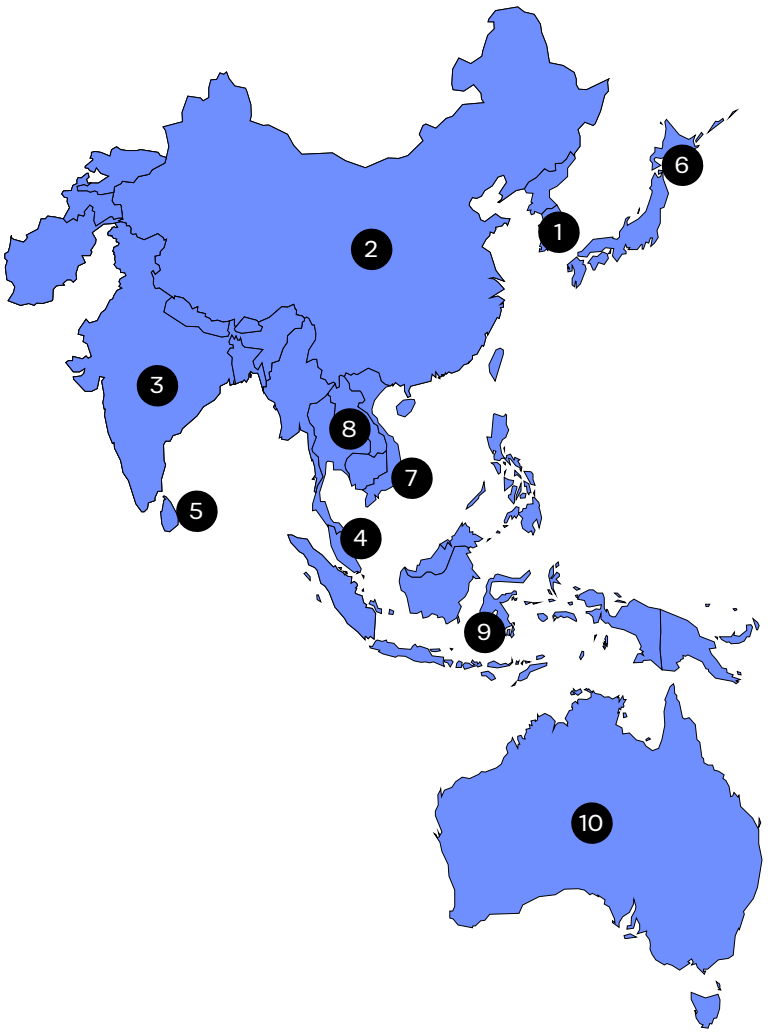
In recent years, many countries across Asia have either rolled out new comprehensive privacy laws or made significant amendments to existing regulations. Notable examples include China, India, Indonesia, Japan, Malaysia, South Korea, Sri Lanka, Thailand, and Vietnam. Currently, Indonesia, India, and Malaysia are working toward the full implementation of their newly amended laws. Additionally, Australia has announced the first phase of a comprehensive reform of its Privacy Act after a thorough government review.

Common themes in Asian privacy laws

- Consent remains the primary legal basis for processing personal data in China, India and Vietnam. In addition, Australia, China, Malaysia, Philippines, Taiwan and Thailand all require consent for the collection of sensitive personal data (and this will require a separate reputational assessment to be made under Vietnam's new Personal Data Protection Law). Deemed consent is also a permitted legal basis in Singapore (subject to certain constraints), and to a more limited degree in India as well.
- Indonesia, the Philippines, Singapore and Thailand permit data processing based on an organization's legitimate interests. China, Indonesia, Korea, Malaysia, the Philippines, Singapore, Taiwan and Thailand allow processing where necessary for the performance of a contract with the data subject. Clarification is needed whether Vietnam will also allow processing on this basis under the new law, in particular for online services. Neither legal basis is available for the processing of sensitive personal data in those countries that require consent.

Examples of Asia-Pacific data privacy developments

1. Extensive amendments to **South Korea**'s Personal Information Protection Act in 2023.
2. **China:**
   - Cyber Security Law
   - Personal Information Protection Law
   - Data Security Law
3. Digital Personal Data Protection Act in **India** passed in August 2023. Not yet in force.
4. Limited amendments to **Malaysia**'s Personal Data Protection Act pending.
5. **Sri Lanka**'s Personal Data Protection Act enacted March 2022.
6. Amendments to the Act on Protection of Personal Information in **Japan** effective April 1, 2022.
7. Personal Data Protection Law in force January 1, 2026 in **Vietnam** (Decree 13 in force).
8. Multiple data protection guidelines have been issued to supplement the Personal Data Protection Act in **Thailand**, which became fully effective on June 1, 2022.
9. New Personal Data Protection Law introduced in **Indonesia** with a two-year transition period ending in October 2024.
10. Major overhaul of privacy law in **Australia** underway following the Attorney-General's report.



Asia's privacy laws are maturing

- While South Korea also permits processing based on legitimate interests, the GDPR standard (and that adopted elsewhere in Asia) it flipped by instead requiring that the organization's legitimate interests clearly override an individual's rights in order for this legal basis to be relied upon.
- GDPR-style data subject rights have been widely adopted across Asia, particularly the rights to access and rectification, erasure and cessation of processing. The right to object to automated processing (China, Indonesia, Philippines and Vietnam (pending)) and the rights of data portability are less well cemented at this point in time. Only China, the Philippines and South Korea grant both (the portability right is not yet in force in Korea). Singapore and Malaysia have also recently extended their data subject rights to include a right of portability, although neither amendment is in effect yet.
- Privacy impact assessments are either required or recommended in many Asian countries – although the specific triggers for these assessments vary.
- Mandatory breach reporting obligations are the norm across the region (as discussed further below), with an additional annual security incident reporting requirement in the Philippines. Reporting timelines typically follow the GDPR standard of 72 hours. Several countries require organizations to implement formal security incident management processes (eg China, Indonesia and Malaysia) as a specific organizational measure to protect personal data, and this has been proposed in Australia as well.
- Maximum penalties range quite considerably across the region, although with maximum penalties set as a percentage of revenue/turnover having recently been introduced in several countries (eg China, India, Indonesia and Singapore) and proposed in Australia. Overall, both maximum and awarded penalties are trending markedly upwards.
- Varied rules on cross-border data transfers are also increasing compliance burdens on multinational companies (see Chapter 2 for recent developments in the related rules in Asia).

> New privacy rules have been taking shape across Asia the past few years. While there is a good degree of conceptual alignment with the GDPR, no country has taken a copy and paste approach either, and in some areas there is significant departure.
>
> **Richard Bird**
> Partner

Yet significant divergence in Asian privacy laws, too

While Asia's privacy laws reflect a relatively high degree of general consensus in approach (as outlined above), each has its unique requirements and idiosyncrasies. These points of difference can have significant practical impacts on compliance programs.

The absence of any true harmonization in the permitted legal basis for processing, and the greater reliance on consent as the primary and preferred basis for processing creates a significant impediment by itself to organizations taking a single regional approach to privacy compliance.

It is important that international companies maintain awareness of all important local requirements in those Asian jurisdictions in which they operate, given the significant penalties that attach to non-compliance in many, and the generally increasing levels of enforcement also.

For examples, while it was noted above that most countries in Asia have either introduced or are proposing (ie Malaysia) mandatory data breach reporting requirements, the basis for reporting may vary significantly from one jurisdiction to the next.

Asia's privacy laws are maturing

There are notable differences in data incident reporting thresholds across the region – harm or scale standards are often set up differently, for example, or with differing deeming criteria. In other jurisdictions, reporting requirements can be triggered depending on the nature of the incident, for example whether it involves unauthorized access from outside the organization. Specific sectoral reporting obligations may also apply.

The assessment of reporting requirements for data security incidents that implicate personal data that was either collected in or relates to the residents of multiple countries/territories is made more complex still by the large amount of variability in the jurisdictional basis for the application of local law to data that is processed in another country or for purposes related to activities in another country (eg an overseas purchase or booking). Mandatory (ie standard form) contractual mechanisms for cross-border data transfers may include their own reporting obligations on either transferor or transferee (or both).

These assessments also need to be made against relatively strict reporting deadlines, typically within a reporting window of 72 hours or less. The prevailing standard for reporting to privacy authorities and for notifying individuals can be different within a single jurisdiction.

An early report in one country – reflecting a more limited understanding of the incident available at the time – may impact the reporting strategy in another country where the report is due later. Reporting may precipitate a privacy authority to start an investigation before reports have been filed in other countries. Those earlier filed reports and regulatory submissions may also be discoverable in the context of investigatory processes and court proceedings in other countries around the world. Risk calculations may therefore need to be made.

> Given the pace of change in privacy laws in Asia, international companies active in the region should make it a priority to stay updated.
>
> **Fan Li**
> Senior Associate

Practical implications for businesses

Given the rapid evolution of privacy laws in Asia, it is advisable for organizations to take stock of the increasing compliance burden by conducting a gap analysis and updating existing data protection notices and policies and their internal technical and organizational controls, especially if these have not been reviewed in the past few years. Many of the new or amended laws in the region also require a data protection officer (DPO) to be appointed.

Conducting regular staff training will be another important measure to take to ensure that the requirements of new laws and internal policies are well understood and embedded in organizational processes.

> Whereas in the past Asia may not always have been at the forefront of companies' minds in their global privacy compliance programs, increasing fines and enforcement call for a sharpened focus on the region.
>
> **Harshavardhan Ganesan**
> Associate

Asia's privacy laws are maturing

Looking ahead

Exciting changes are on the horizon across several countries in Asia.

- In India, the Digital Personal Data Protection Act (DPDP) passed in August 2023 and is set to be enforced soon now that the general elections have concluded. One key aspect to watch is how the government will define 'significant data fiduciaries.' These organizations will face additional responsibilities, including conducting regular privacy impact assessments, undergoing external audits, and appointing a DPO who must be based in India. This DPO will report directly to the board and act as the main contact for grievance redressal under the DPDP. The government will determine which data fiduciaries are deemed 'significant' based on factors like the volume and sensitivity of personal data processed and the associated risks. Additionally, keep an eye out for the government's forthcoming 'blacklist' of countries where organizations won't be allowed to transfer personal data.
- Malaysia's parliament approved substantial updates to the Personal Data Protection Act in July 2024. The government is also working on new rules regarding data breach reporting, DPO appointments, and the right to data portability.
- Vietnam has recently announced a draft Data Law. This law takes cues from China's regulations, including stricter protections for 'core' and 'important' data, along with a security assessment process for data exports. A new Personal Data Protection Law is also set to take effect on January 1, 2026, reinforcing most provisions from the existing Decree 13 while adding several new requirements.
- In Japan, the Act on Protection of Personal Information is under a three-year review. The Personal Information Protection Commission shared an interim summary in June 2024, hinting at proposed reforms concerning biometric and children's data. They plan to ban certain improper uses of personal data and expand individuals' rights to request the suspension of their data usage.
- Australia has taken the first steps toward implementing a series of changes to its Privacy Act. The first round of amendments was introduced in mid-September 2024, and the government is expected to roll out many of the 166 reforms suggested in the Attorney-General's 2023 review of the law.

8.

New EU data access regulations are shaping the future

New EU data access regulations are shaping the future

Davide Borelli
Milan

Estella Dannhausen
Vienna

Enrico De Jong
Amsterdam

Mark Egeler
Amsterdam

Theresa Ehlen
Düsseldorf/ Frankfurt

Gernot Fritz
Vienna

Daniel Klingenbrunn
New York/ Frankfurt

Julia Utzerath
Düsseldorf

Christoph Werkmeister
Düsseldorf

In brief

The European Commission's Data Strategy 2020 has paved the way for new data access regulations that will significantly impact businesses across Europe. In this chapter, we dive into the data access rights established by the EU's Data Act, along with two pivotal Common European Data Spaces: the European Health Data Space (EHDS) and the Financial Data Access (FIDA) framework.

These new regulations are set to affect many businesses operating in the EU market. If you offer connected products in the EU (eg smart devices) or software that connects to devices being used there and that enables the devices to perform their functions (eg certain apps), the Data Act applies to you, regardless of where your organization is based. The EHDS and FIDA introduce complex obligations for various stakeholders in the health data and financial services ecosystems.

We'll explore the challenges and opportunities these data access regulations present for businesses and provide practical advice to help you navigate the new compliance landscape.

What the Data Act, FIDA and EHDS have in common

The primary objective of the new data access rights under the Data Act, EHDS and FIDA is to foster the development of a unified data market in the EU. This entails making all data produced in this unified data market, whether personal or non-personal, accessible to all market participants, irrespective of their size or influence, in accordance with fair, transparent, proportionate and non-discriminatory access rules. Entities and individuals possessing data, such as data generated via connected products or digital services, will be empowered to share this data for reuse, either freely or for compensation.

New EU data access regulations are shaping the future

However, while all three laws contribute to a major shared objective, the Data Act aims to enhance data access across sectors, particularly for Internet of Things (IoT)-generated data, while the Common European Data Spaces create a framework for data sharing in key areas like health (EHDS) and finance (FIDA).

New obligations that come with the new data access rights

Data Act obligations

The Data Act, being a key pillar of the European Data Strategy, aims to create a horizontal framework for the access to, and sharing of, data generated through smart products and digital services. It also introduces new requirements for redistributing data access and use.

Right	Requirements
Data access by design	▪ Manufacturers must ensure that connected products and digital services in relation to the connected products are designed to allow users easy and secure access to product data. Such data needs to be provided in a comprehensive, structured, commonly used and machine-readable format. ▪ Manufacturers may decide to make product/digital services data 'directly' available, ie so that the user is able to access the data without the intervention of any other party.
Data access by request	▪ While manufacturers must design their connected products to provide direct access to data, the Data Act recognizes this may not always be feasible. When direct access is unavailable, businesses that have lawfully obtained the data, (ie data holders) must promptly make it available to users of relevant products or services upon request, at the same quality as they receive it themselves. ▪ Users of relevant products or services are prohibited from utilizing the data to create a competing product or sharing it with third parties for that purpose. They must also refrain from using the data to gain insights into the economic status, assets or production methods of the manufacturer or the data holder.
Data sharing by request	▪ The Data Act requires businesses to share data with third parties, even competitors, if a user of a relevant product or service requests so, highlighting the EU's aim to promote a competitive digital environment. However, so-called 'gatekeepers' are excluded from receiving such data. ▪ When both the data holder and the third party are businesses, they must establish a contract that governs the data-sharing arrangement under fair, reasonable and non-discriminatory (FRAND) terms. ▪ The data holder may charge a non-consumer data recipient a fee for accessing data. The fee should be FRAND, possibly varying based on the data's volume, format and nature, and may include a margin.
B2G data sharing	▪ In cases of exceptional need, businesses will be required to make data available to a national public sector body or an EU body. This covers data from connected products, related services and any other business data. ▪ In general, the data will have to be made available free of charge, but under certain conditions businesses are entitled to fair compensation.

New EU data access regulations are shaping the future

EHDS obligations

The EHDS imposes a complex array of obligations on various actors within the health data ecosystem, including health data holders and users, and manufacturers, importers and distributors of Electronic Health Records (EHR) systems. Key requirements in relation to data access rights include:

> With the Data Act, the EU addresses the rapid growth in the use of connected products, leading to enhanced data utilization, flexibility in service selection, and new business opportunities.
>
> **Gernot Fritz**
> Counsel

Actor	Requirements
Health data holders	▪ Health data holders – such as hospitals, healthcare providers, public health authorities, pharmaceutical companies and research organizations – will have certain responsibilities under the EHDS. ▪ Upon request, they must provide relevant electronic health data to designated health data access bodies, which are public sector organizations designated by each EU Member State that are responsible for the operationalization and oversight of the EHDS within their respective jurisdictions. Data holders are required to supply the requested data within a period not exceeding three months from the date of the request. ▪ Regardless of data permits or data requests, data holders are also required to proactively disclose to the health data access body a detailed catalogue of all the datasets they maintain.
Health data users	▪ Health data users – such as academic research institutions, public health authorities, governmental agencies, private sector entities involved in health research and innovation and non-governmental organizations focused on public health – are also subject to various obligations under the EHDS. ▪ They may only access and process electronic health data for secondary use, like research or innovation, after they have obtained data permits, data requests or data access approvals. ▪ Upon obtaining access, health data users are required to make public the results, findings or outputs derived from their secondary use of electronic health data. ▪ They must notify the relevant health data access body immediately of any significant findings or results that have the potential to impact the health of individuals whose data was included in the analysis. ▪ In addition to these specific obligations, health data users must also comply with a range of privacy and data protection requirements and cooperate with health data access bodies.

New EU data access regulations are shaping the future

The FIDA obligations

The FIDA aims to grant effective control to customers over their financial data and to give the opportunity to benefit from new business models and products based on data sharing. As the FIDA is still under negotiation, this chapter summarizes the European Commission proposal of June 28, 2023.

The FIDA applies to credit institutions, insurance firms and most other EU financial sector entities. All of them can act as 'data holder' or 'data user.' Among others, the FIDA applies to customer data on loans, (non-payment) accounts, savings, investments, crypto-assets, real estate, non-life insurance products and data forming part of creditworthiness assessments of firms for loan application processes. Data on sickness and health insurance products, including data collected for related assessments, and data that forms part of creditworthiness assessments of consumers are excluded from the FIDA.

Important requirements in relation to data access rights include:

Actor	Requirements
Data holder	▪ Financial sector entities storing customer data (data holders) are required to share financial data with customers and with third parties upon a customer's request. They must maintain a 'permission dashboard' so that customers can monitor and manage the permissions. ▪ The data holder and data user must establish or join financial data sharing schemes. Scheme members must agree the main parameters for sharing of data (eg technical interfaces, maximum compensation and liability). Scheme rules are subject to review by financial sector authorities.
Data user	▪ Financial data can only be shared with other licensed entities (data users), either a financial sector entity or a 'financial information service provider,' a type of license established under the FIDA. ▪ Data users will become subject to legal restrictions when they intend to process data they have received, to offer consumer products related to credit scoring or to life, health and sickness insurance; this is intended to protect consumers and their fundamental rights.

New EU data access regulations are shaping the future

New opportunities for data-based business models

The Data Act, EHDS and FIDA open up new possibilities for different stakeholders, as summarized below:

Data Act

Stakeholder	Benefit
Users of connected products	Can leverage data for various purposes, while (third-party) data recipients also benefit from gaining access to diverse, high-quality data sources.
Small and medium-sized enterprises (SMEs)	Benefit from fair contractual terms for data access, encouraging their participation in the data economy.
Businesses investing in data-generating products	Data collected by a user or (third-party) data recipient cannot be utilized to create a competing connected product. The Data Act does not, however, restrict competition in related or aftermarket services.
New business models, such as aftermarket services	The Data Act provides access to more data to improve product support and drive service innovation.

EHDS

Stakeholder	Benefit
Businesses in the healthcare and pharmaceutical sectors	Will benefit from easier access to health data across the EU, potentially leading to more efficient drug and vaccine research and faster development of other medical products. This may be especially true for companies specializing in healthcare analytics and AI-driven tools, which can leverage the harmonized health data pool for their initiatives, enhancing the effectiveness of their projects and reducing costs associated with data access.
SMEs	Can access and reuse high-quality health data for innovation and research, contributing to broader health research, improved health outcomes and greater innovation.
Providers of telehealth services	Will be able to expand their services to a broader customer base thanks to more standardized data practices across EU countries.
Individuals	Individuals will have secure, direct access to their personal health data across all EU Member States. They will also be able to provide feedback and file complaints regarding the use and handling of their health data.
New business models, such as aftermarket services	The Data Act provides access to more data to improve product support and drive service innovation.

New EU data access regulations are shaping the future

> All businesses within the health data ecosystem must explore the relevant opportunities and obligations arising out of the EHDS and other new EU data laws.
>
> **Davide Borelli**
> Counsel

FIDA

Stakeholder	Benefit
Businesses in the financial sector	Establishing standardized and safe means of financial data-sharing may open up new opportunities for data sharing business models – beyond payment account related models – due to increased trust from the customers who may be willing to share more financial data.
Customers	The use of financial data by data-driven tools can help customers to compare offered products that match their preferences based on their data and support them to make informed choices.
SMEs	SMEs may benefit from a particularly favorable regulation regarding compensation for financial data.

How to prepare for the new data access compliance requirements

Preparing for the Data Act

- Establish robust data governance processes and, in particular, evaluate existing product designs and contractual frameworks to ensure alignment with the Data Act's provisions.
- Identify key datasets affected by the legislation and developing a comprehensive data strategy are critical steps towards compliance. By doing so, businesses can explore possible avenues for opening access to data and adapt manufacturing and design processes accordingly.
- In addition to risk mitigation, businesses could also explore the potential opportunities presented by the Data Act. By strategically leveraging the Data Act's provisions, businesses may uncover new possibilities for growth and innovation.

Preparing for the EHDS

- Data holders must find effective ways to separate data that is commercially sensitive or subject to intellectual property restrictions from other health data to prevent unauthorized disclosure. This segregation is crucial to comply with transparency and privacy obligations under EU data protection law and the EHDS, which mandates robust mechanisms for safeguarding sensitive information while still allowing health data to be shared for broader purposes such as research and innovation.

New EU data access regulations are shaping the future

- Data users should familiarize themselves with the processes and prerequisites set out in the EHDS for obtaining data permits, data requests and data access approvals. They should also set up a process for the timely publication of the results or output of their secondary use that complies with the anonymization requirements of the EHDS and aligns with data protection law.
- Manufactures, importers and distributors of EHR systems should ensure that their products meet the comprehensive requirements laid down in the EHDS. This is necessary to guarantee their systems comply with EU market standards and can be legally sold and used across EU Member States. Additionally, importers, distributors and users of an EHR system should also assess whether they might be considered a manufacturer of an EHR system according to the EHDS and thus subject to the obligations set out for manufacturers.

Preparing for the FIDA

While most details on the FIDA must still be settled during the legislative process, it has already become clear that the FIDA will (after the EU's Digital Operational Resilience Act) be the next fire drill for financial sector entities in which IT and data departments will need to collaborate with their legal and compliance counterparts to ensure day-one readiness.

- IT and data departments should focus on the availability of IT assets that permit compliance with the ambitious data sharing standards.
- Legal and compliance will be involved in selecting or negotiating key terms of financial data sharing schemes.
- As part of their risk management, financial sector entities will need to consider strategies to shield themselves from liability risks due to loss or incorrect handling of financial data, including customer data that falls within the remits of data protection law.

> FIDA will be the next fire drill for financial sector entities who must ensure day-one readiness.
>
> **Christoph Werkmeister**
> Partner

Looking ahead

Now is the perfect time to embark on your compliance journey and get ready for the upcoming data access requirements under the Data Act, which will take effect on September 12, 2025 (though keep an eye out for certain provisions with different application dates). Recent guidance from the EU Commission has clarified some of the previously ambiguous terms in the Data Act, making practical implementation more straightforward (check out our Freshfields blog post for more insights).

The EHDS is nearing its final stages, with adoption expected in autumn or winter 2024. This gives affected stakeholders two more years to work towards compliance.

On the other hand, the FIDA is still in the early stages of its legislative journey. It's definitely one to watch, as it holds great potential for new data business models in the financial sector – something that's a key aspect of all the new data access regulations coming out of Brussels across various industries.

FRESHFIELDS

Data protection and privacy laws, which we collectively refer to as 'privacy laws' in this report, vary around the world – along with their associated terminology and definitions. Given the global influence of EU privacy laws, especially the General Data Protection Regulation (GDPR), this report generally uses EU privacy law terminology to refer to similar concepts (eg 'personal data', 'data protection impact assessments', 'data protection officers' and 'data subjects') since readers will often be most familiar with those terms.

Law stated as at 1 October 2024

October 2024, 486053

freshfields.com