Data Trends 2024

Welcome to our annual review of the top trends that are expected to impact the data law landscape in coming years.

This report explores eight key themes that we predict will influence the data landscape. The themes have been identified by international specialists from across our global network to help clients plan ahead.

A confluence of emerging capabilities, new regulations and other trends will pose fresh challenges for businesses seeking to make the most of the opportunities of data and allied technologies. We hope this report is a useful guide in helping prepare businesses and their in-house advisors for a rapidly changing environment.

> This forward-looking report is based on our experience of advising on high-profile and business-critical data mandates and the work of our dedicated experts across the US, Europe and Asia advising many of the world's top tech companies. We hope that the learnings from our global network and market-leading expertise are helpful to all businesses seeking to harness the opportunities of data, AI and related technologies, and look forward to navigating the challenges and opportunities for our clients in the year ahead.
>
> **Christine Lyon, Giles Pratt and Christoph Werkmeister**
> Global Co-heads of the Freshfields data privacy and security practice

Trend 1: Accelerating use of AI

The last year saw generative artificial intelligence (AI) take the world by storm, leaving governments and organisations grappling with complex questions about how to adapt to the challenges and opportunities of AI. Many companies have access to troves of data that they may wish to extract additional value or efficiencies from using AI. Our specialists have helped many organisations in aspects of their development and deployment of AI. We highlight steps that businesses developing or implementing AI in the future will need to consider.

Trend 2: Growing complexity and convergence of global privacy laws

2023 saw the continued march of privacy regulation around the world as ever more countries joined the ranks of those with comprehensive privacy laws. While every jurisdiction has continued to apply its own take on privacy regulation, there are many emerging common elements to privacy laws. In our report, we also explain significant regulatory trends that we are seeing across multiple jurisdictions.

Trend 3: Companies confront an ever-evolving cyber risk landscape

Two major risks that businesses need to be increasingly aware of are ransomware and insider threats. We report on those emerging challenges and the actions companies can take that may make a huge difference to their ability to respond to future incidents.

Trend 4: Data portability rights will become more potent

Data portability rights seek to make it easier to transfer data from one company to another. Planned legal reforms in this area could soon raise new challenges and opportunities for EU, UK and global businesses.

Trend 5: Changes in data and cyber enforcement impacting global businesses

We have observed an evolution in enforcement postures across the US, UK, and EU regarding privacy and cyber regulations. The US has extended its focus on non-monetary remedies, the UK has moved from headline grabbing fines to a more outcomes-based approach, and EU data protection authorities have embraced diverse corrective measures as well as record fines. There have also been indications of what areas the relevant authorities will focus enforcement on in the coming years. Understanding those trends will help maximise the prospects of avoiding enforcement.

Trend 6: Growing risk of data litigation

Well-publicised and extensive data breaches have always carried the risk of costly and reputationally damaging mass litigation, and such claims continue apace. We explain why recent trends mean that data litigation should remain a primary area of concern for many organisations.

Trend 7: Acquiring valuable datasets remains a top priority for businesses worldwide

Long-standing issues relating to data, such as data ownership and data protection, will continue to be important in mergers and acquisitions (M&A). We report on new challenges and recent developments impacting the acquisition of data in M&A deals.

Trend 8: Evolving landscape of digital data regulation in the EU

The EU was at the forefront of establishing a legal framework to protect individuals' personal data. Now the EU's wide-ranging 'Digital Strategy' intends to supplement its existing data and digital framework with a new set of rules that are not limited to data, personal or otherwise. Those include new rules to foster data flow, data access and the data economy and enhanced obligations and user protections for online platform services, online hosting services, search

engines, online marketplaces, and social networking services. AI will be another focus of new regulations coming out of Brussels. We explain what changes businesses can expect and how they should respond.

Data protection and privacy laws, which we collectively call 'privacy laws' in this report for convenience, vary around the world—along with their associated terminology and definitions. Given the global influence of EU privacy laws, this report generally utilises 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.

If you would like to discuss any of the topics covered in the report, please reach out to one of the authors or your usual Freshfields contact.

Published: November 2023

> Sign-up to Freshfields' Data and Cyber Newsletter for regular bulletins that will help you keep abreast of the rapidly changing data, cybersecurity, digital markets and AI legal landscapes.

Contents

01.

What to consider when adding data to the AI revolution


Richard Bird
Partner, Hong Kong


Julian Boatin
Associate, Düsseldorf


Brock Dahl
Partner, Washington, D.C./Silicon Valley


Theresa Ehlen
Partner, Düsseldorf/ Frankfurt


Beth George
Partner, Silicon Valley


Adam Gillert
Global Data Knowledge Lawyer, London


Giles Pratt
Partner, London


Katie Sa
Associate, London


Max Smith
Associate, London


Satya Staes Polet
Counsel, Brussels


Christoph Werkmeister
Partner, Düsseldorf

IN BRIEF
Artificial Intelligence (AI) is of growing importance to businesses and in the next few years businesses are widely expected to explore opportunities presented by Generative AI (GenAI). GenAI is capable of processing and analysing large amounts of data and generating new output based on it. Many companies have access to troves of data, from which they may wish to extract additional value or efficiencies by using AI. In this article we highlight why businesses developing or implementing AI in the future should:

- give ample consideration to ensure that any personal data is used and protected in accordance with applicable (and potentially conflicting) global privacy laws;
- pay particular attention to emerging AI-specific regulation in various jurisdictions—which will often overlap with those privacy laws; and
- develop guidelines and strong governance processes for dealing with AI.

GenAI and privacy

GenAI models are trained on large volumes of data, which may include personal data, and will also often rely on the processing of personal data as part of their operation.

In Europe, the EU's General Data Protection Regulation (GDPR), and the UK's GDPR, apply to the use of GenAI to the extent this includes the processing of personal data. For example:

- The collection and use of personal data for training purposes is subject to heightened privacy requirements.
- Organisations using personal data to train AI systems must ensure that personal data in AI training data is accurate in-line with the EU and UK GDPR's requirements.
- Decision-making based solely on automated processing is prohibited in many cases under UK and EU privacy laws (with limited exceptions). Data subjects must also be given certain additional information about many types of automated decision-making, including meaningful information about the logic involved. As explained in this blog post, the UK government has proposed reforms that would liberalise the UK's regime in relation to automated decision making, which may allow greater opportunities to use AI in the UK in coming years. Nonetheless, automated decision-making which results in significant decisions for individuals will remain particularly regulated.
- Various trade-offs may arise in the development of AI, and it is important to find the right balance between aspects such as accuracy, privacy and responsibilities to be able to explain the AI and its output in ways that make sense to people (often called 'explainability').

An increasing number of countries have privacy laws that are similar to the EU's GDPR or which impose other challenging requirements. In the US, companies must be conscious of the state data privacy laws that indirectly influence AI options. Such laws typically contain a range of requirements, such as purpose limitations, data minimisation rules, disclosure limitations, notice and consent obligations, and key sections on automated decision-making. Companies must pay particular attention to these requirements in executing their own AI strategies and designing AI systems.

AI-specific regulation

Many jurisdictions are also in the process of developing laws that specifically target AI. Those laws often overlap with the requirements of privacy laws as well as other legislation (such as those governing copyright, product liability or equalities).

> The rapid evolution of AI capabilities and applications, and the ever-expanding regulatory frameworks governing them, suggests the need for building adaptable compliance frameworks that can manage cross-border complexity.
>
> **Brock Dahl**
> Partner, Silicon Valley

The EU is seen as a leader in this regard and will set out various requirements for the use of AI in the AI Act and the AI Liability Directive. Once they enter into effect, those AI regulations may not only apply to providers but may also affect users of AI within the EU. The multitude of obligations for providers include:

- governance (eg, developing a risk management system);
- transparency (eg, vis à vis the users);
- accountability (eg, generating technical documentation explaining the AI model);
- fairness (eg, implementing safeguards for AI); and
- self-certifying compliance.

Non-compliance may result in a fine of up to €40m or 7% of the total worldwide annual turnover, whichever is higher. A final draft of the AI Act is expected by the end of 2023 at the earliest, which will likely be followed by an implementation period of around 24 months.

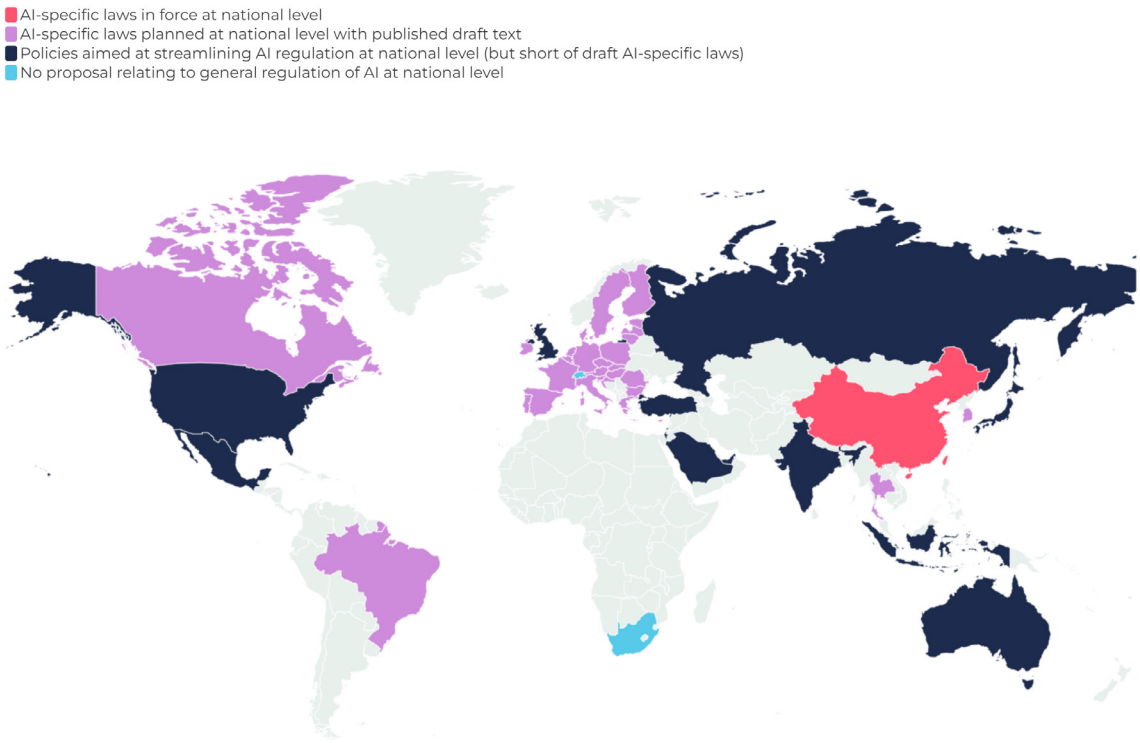
Given the extensive time and investment required to build an AI system, it is vital that AI providers and other impacted businesses begin to consider the

implications of the EU's pending AI laws. Businesses should keep an eye on possible changes to the draft laws as they complete their legislative journeys. This is even more true given that the EU, together with tech companies, is currently working on a so-called 'AI-Pact' to bridge AI governance until the AI Act becomes effective.

Several other jurisdictions, including (among others) Canada, Brazil and China, have either introduced or are planning to introduce AI-specific laws.

Other countries are taking a less direct approach to AI regulation, but businesses will still need to keep abreast of emerging regulator-led initiatives, and potentially a more complex patchwork of applicable laws.

AI-specific laws: current and pending regulation in selected jurisdictions



Data collected 1 November 2023. Information for EU and federal states (eg US, Canada, Australia) is at EU or federal (rather than constituent state) level.

Unlike the EU, the UK is not planning to introduce any new AI-specific regulations or laws. Instead, the government has proposed a 'pro-innovation' framework based on five overarching principles to guide the development and use of AI: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress. It is envisaged that existing regulators in the UK would be responsible for applying these five principles in practice across sectors. The idea is that the framework should be sufficiently flexible to keep pace with the fast-moving technology involved. The five overarching principles underpinning the UK AI White Paper are broadly aligned with the principles outlined in the UK and EU GDPRs.

> The UK government is taking an agile and iterative approach to regulating the use and development of AI, so we advise clients to keep a watching brief of how this develops. Guidance published by UK regulators will be a key resource in the first instance to understand how they intend to apply the five principles in practice.
>
> **Maxwell Smith**
> Associate

Similar to the UK, the US government (at the federal level) has taken a variety of steps to signal its interest in AI issues; but neither it nor the US Congress have yet pursued legislative requirements. For now, AI applications are more typically governed less directly through the increasingly proliferating state data privacy laws.

At the US federal level, the White House has issued an Executive Order that, if fully implemented, will establish a range of regulatory requirements pertaining to AI. These will include:

- requiring the National Institute of Standards and Technology set new market standards for AI safety and security;
- requiring reporting to the government regarding dual-use foundation models;
- starting the regulatory process for requiring reporting to the government regarding certain infrastructure as a service transactions;
- incorporating the AI risk management framework into critical infrastructure guidelines (and potentially making those formal regulatory requirements); and
- establishing new content labelling and identification standards for the federal government, and more.

Looking ahead

> We look at legal risks along the cycle of an AI use case: input, operation of the model and output. That allows us to address the risks when and where they come up and find appropriate mitigation measures.

Theresa Ehlen
Partner

As explained above, many privacy principles and requirements will be pertinent in considering the development or deployment of AI where personal data is used.

Privacy and AI-specific laws are just one part of a legal jigsaw of issues which those developing or using AI should consider. Other matters may include:

- Intellectual property (IP) rights in the inputs or outputs of the AI—for example, IP issues have arisen where copyright materials have been used to train an AI model.
- The risk that the AI may cause some damage or harm to third parties, and related liability issues.
- Risks that AI systems without appropriate safety mechanisms during their training and deployment may behave in ways that may create or heighten existing bias and toxicity issues. For example, AI models can learn existing biases from training data and have the potential to result in discriminatory or unfair outcomes.

> The opportunities of using AI in the workplace are as fascinating as the challenges it may trigger, given the variety of legal areas that it involves.

Satya Staes Polet
Counsel

Further background on those broader matters is available in our blog post: Generative AI: Five things for lawyers to consider.

A business will often be required to take difficult decisions when deciding how to proceed with AI. Accordingly, it is important for companies using AI to implement strong governance arrangements to ensure a robust process is in place for documenting key decisions and achieving appropriate outcomes where AI is developed, implemented or used.

In relation to privacy, this should include companies considering the implications of using AI as part of existing data privacy and information security assessments. This may include addressing explainability, considering any novel security risks, and ensuring meaningful human review of decisions.

02.

Global trends in privacy laws: different routes taken along the same regulatory pathway

Rachael Annear
Partner, London

Richard Bird
Partner, Hong Kong

Claudia Chan
Associate, London

Hannah Family
Associate, London

Adam Gillert
Global Data Knowledge Lawyer, London

Christine Lyon
Partner, Silicon Valley

Jackson Myers
Associate, New York

Philipp Roos
Principal Associate, Düsseldorf

IN BRIEF
The Economist commented in its 23 September 2023 edition that the EU's General Data Protection Regulation (GDPR) 'became the model for most of the world's 150 privacy laws' after it was proposed in early 2012. But is it this simple?

The GDPR introduced many new approaches to the regulation of data privacy that have now become conventional around the world (such as privacy impact assessments, enhanced transparency and consent requirements and specific governance requirements) and has been the predominant influence over the development of global privacy laws across the past decade. However, every jurisdiction has continued to develop its own take on privacy regulation. While the GDPR has tended to serve as a menu of tools for legislators to choose from, no other major jurisdiction has simply copied this legislation.

In general, there are many more common elements to any selection of privacy laws than there are differences. The overriding theme is that privacy laws have become increasingly onerous for organisations that are collecting and using personal data.

In this article, we highlight several significant regulatory trends that we are seeing across multiple jurisdictions:

- enhanced requirements for data governance and accountability;
- divergence in the role of consent between Europe and many other regions; and
- greater restrictions on cross-border data transfers—including in jurisdictions outside of the EU.

> Privacy laws tend to share several core concepts, such as transparency, legal basis/consent, individual rights (although the extent of individual rights provided can vary a great deal from one jurisdiction to the next), data security and breach notification obligations.
>
> **Christine Lyon**
> Partner

Enhanced requirements for governance and accountability

The GDPR has always rested on the principle of accountability, requiring organisations to take documented measures to demonstrate their compliance. Many countries have been required by the GDPR to implement more formal operational privacy requirements of this nature, such as requiring the appointment of a data protection officer (DPO) in certain contexts and requiring formal impact assessments to be carried out.

(Source: United Nations Conference on Trade and Development)

Data protection impact assessments

A large proportion of major jurisdictions outside of the EU (eg, Japan, China, Brazil, Indonesia, several other countries in Asia and certain US states) have adopted—as either a formal or recommended requirement—the GDPR concept of requiring a documented data protection impact assessment (DPIA) of high-risk processing activities or activities that may have a significant impact on the rights and interests of individuals.

High-risk activities may include the processing of sensitive data on a large scale or using personal data in automated decision-making that could have legal or other significant effects on individuals, and include other personal data processing activities that may have a significant impact on individuals. In a variation on this approach, in India, a class of designated 'Significant Data Fiduciaries' will be required to undertake 'periodic' DPIAs and privacy audits under the recently passed Digital Personal Data Protection Act 2023.

This trend reflects the growing importance for organisations of performing and maintaining documented assessments of privacy risks.

Data protection officers

In the EU, organisations are required to appoint a DPO if their core activities consist of certain high-risk activities such as processing sensitive personal data on a large scale. The DPO has a high level of autonomy. For example, organisations may not give instructions to the DPO on how they should perform their duties or penalise or dismiss the DPO for performing their task. Guidance from EU authorities also makes clear that DPOs cannot undertake any other tasks which can result in a conflict of interest, such as a DPO having a C-suite function.

Other jurisdictions have begun requiring the appointment of DPOs, but the nature of the role can differ. In China, for example, an influential predecessor to the Personal Information Protection

Law (the PIPL) adopted in 2021, namely the Personal Information Security Specification 2020 edition (a government-issued Chinese national standard), provides that the responsibilities of a DPO include taking the lead in preparing internal policies, establishing the organisation's approach to data security, conducting DPIAs, and setting rules and procedures for handling data subject requests. This represents a much more hands-on (and perhaps less independent) role than under the GDPR, even if the core statutory function remains to supervise the organisation's data processing activities and the protective measures taken. The detailed implementing rules for DPOs under the PIPL have yet to be issued, but following the approach seen in most other areas of the PIPL it is expected that the PIPL will retain the broad lines of the Personal Information Security Specification.

Similarly, under the new Law on Personal Data Protection in Indonesia enacted in October 2022, in circumstances where organisations are required to appoint a DPO, the DPO will have direct responsibility for ensuring the organisation's compliance with the law. The new law in India also takes a similar approach to that of China.

Regulation of Artificial Intelligence (AI)

Data governance has been placed at the heart of emerging approaches to the regulation of AI services around the world.

The EU's proposed AI Act is built around key tenets of transparency, human oversight, and accountability. Similarly, the Federal Trade Commission in the US has declared that the use of AI should be 'transparent, explainable, fair, and empirically sound while fostering accountability.'

As was the case with the GDPR, the draft EU AI Act is already having an influence on the development of AI regulation in other countries. China's new AI regulations in effect since August 2023, Brazil's AI Law published in December 2022, and Canada's proposed Artificial Intelligence and Data Act (AIDA) issued in June 2022 are all strongly orientated towards the approach being proposed in the EU's AI Act.

At the end of October 2023, the Biden Administration issued an Executive Order that instructs US government agencies to implement rule-setting. The Executive Order picks up on many of the same themes as the Chinese and EU approaches and represents a further pointer that a consensus is beginning to emerge in at least the key tenets of the regulation of AI. But with no prospect of genuine international harmonisation of laws in the short-to medium-term, it will be important for companies to track these rapid developments closely and to identity the areas of difference that affect them most in the markets in which they operate.

For further details, please see Chapter 1 (AI chapter).

Diverging role of consent between the EU/ UK and other jurisdictions

Privacy laws typically require an organisation to establish a legal basis for any processing of personal data, which may include the individual's consent to that processing activity. The GDPR has made it more difficult for organisations to rely on consent, by setting high standards for obtaining a valid consent (eg, requiring a separate consent for each processing activity for which consent is needed, rather than seeking a single blanket consent to the privacy policy).

In contrast, privacy laws in many countries (particularly in Asia and Latin America) still rely heavily on consent as the primary basis for processing personal data (and consent may also be withdrawn). The standards of transparency and explicitness that need to be met for a valid consent have nevertheless often also been raised in line with those of the GDPR.

That said, many newly introduced or recently revised privacy laws have added more flexibility in the range of permissible legal grounds for the collection and use of personal data. This flexibility is achieved by bringing in some combination of the more expansive grounds from the GDPR of 'legitimate interest' and of processing required to fulfil a contractual obligation with the individual (or related grounds), eg, Indonesia, Korea,

India, the Philippines and Thailand. By contrast, both China and Vietnam, still mandate that an individual's consent is to be obtained in most cases. Similarly, various countries in Latin America, such as Argentina and Uruguay, continue to require consent in most cases, and do not provide the same type of 'legitimate interests' basis as the GDPR for processing of personal data without consent despite looking significantly to EU privacy principles in other respects in creating their privacy laws. By contrast, consent is only one of the six lawful bases for processing personal data in the UK and EU. In most cases, consent is often used in the UK and EU for processing special category data or processing data in a potentially intrusive way.

Singapore has permitted processing based on either deemed consent in an expanded range of circumstances or legitimate interests since early 2021. However, in conjunction with this, Singapore law requires organisations to conduct a specific DPIA when planning to rely on either of these bases for processing.

Greater restrictions on cross-border data transfers and separate data localisation requirements

(Source: Freshfields data collected July 2023)

Cross-border data transfers have been a particular focus of EU data protection authorities, and cross-border data transfers are a growing focus of regulation in other jurisdictions as well.

The EU standard contractual clauses remain the most common mechanism for cross-border data transfers of personal data out of the EU, and many other countries have now issued or proposed to issue their own model clauses for cross-border transfers of personal data (eg, the UK, Brazil, China, the ASEAN, Hong Kong and Thailand).

Separately, a smaller subset of countries (such as China, Russia, Indonesia, Vietnam and certain countries in Africa) impose data localisation requirements for certain categories of data or applicable to certain categories of organisation/sector. These rules generally require copies of data to be maintained in-country, or prohibit the transfer of data out of the jurisdiction without government approval.

These data localisation requirements can prevent the cross-border transfer of covered data even if the requirements under privacy laws have been met. For example, even if an organisation uses China's approved standard contract for cross-border transfers of personal data under the PIPL, the organisation may still be prohibited from transferring personal data above certain volume thresholds or if the organisation has been designated an operator of critical information infrastructure.

> "As a result of the growing role of data transfer and localisation restrictions, organisations need a holistic understanding of a jurisdiction's data laws, rather than focusing exclusively on privacy laws.
>
> **Philipp Roos**
> Principal Associate

However, the march of restrictions on cross-border data transfer may already be in retreat.

Earlier versions of what eventually became the India Digital Personal Data Protection Act 2023 had proposed a combination of the Russian and Chinese approaches; namely a requirement to maintain a copy of all personal data on a server in India (ie, as is the case in Russia), coupled with powers for the government to notify certain categories of critical personal data that could only be processed in India (ie, similar to the Chinese rules). Both proposed requirements were dropped before the final legislation passed in August 2023. The final Act instead adopts a 'black-list' approach that would prohibit transfers of personal data to certain jurisdictions designated by the government.

Vietnam's expansive requirement for local data storage by organisations providing services over networks (including the internet)—which has been in place since 2019—was narrowed down in August 2022 to apply only to ten digital sectors and only to certain types of user and service data. The impact of the rule does nevertheless remain significant, and uncertainty remains as to whether these kinds of data can only be stored in Vietnam. The new Vietnamese Decree No. 13 on the Protection of Personal Data issued in April 2023 allows personal data to be transferred overseas by mere notification to the government. The government does, however, reserve the right to discontinue specific data transfers, including on national security grounds. This indicates a further liberalisation in Vietnam's thinking, although the 2019 rule remains in force.

Similarly, while Indonesia has certain sectoral data localisation rules, it relaxed the key restriction in 2019 as it had applied to private networks and information systems (GR 71/2019). The new privacy law has also avoided imposing any unusually strict restrictions on cross-border data transfer.

In a surprise announcement on 28 September 2023, China also revealed that it was planning to relax its rules on cross-border data transfers in certain circumstances. See here for further details of the new proposal.

Looking ahead

"While the EU's GDPR continues to assert a strong influence over other global privacy regimes, as the number and sophistication of privacy laws grows around the world, we are seeing growing divergence and diversity, not least in Asia.

Richard Bird
Partner

Privacy laws do tend to share several core concepts, such as:

- Transparency.
- Legal basis/consent.
- Individual rights (although the extent of individual rights provided for can vary a great deal from one jurisdiction to the next).
- Data security.
- Breach notification obligations.

As new privacy laws and regimes expand and mature, we expect to see countries continuing to take inspiration from other jurisdictions' privacy laws, and it can be expected that the GDPR will remain a primary reference point. At the same time, we will continue to see many examples of jurisdictions tailoring their legislation to their own political, historical, and cultural contexts.

When it comes to data regulation, no two journeys are exactly alike. A 'GDPR is the high watermark' approach to compliance is therefore unlikely to achieve complete compliance across any basket of jurisdictions in which an organisation operates. Compliance programmes that do not also recognise the nuances on common privacy questions in certain jurisdictions will generally fall short of an ideal standard.

03.

Preparing for the cyber risks of today, and tomorrow


Richard Bird
Partner, Hong Kong


Claudia Chan
Associate, London


Brock Dahl
Partner, Washington, D.C./Silicon Valley


Tochukwu Egenti
Associate, London


Beth George
Partner, Silicon Valley


Adam Gillert
Global Data Knowledge Lawyer, London


Megan M. Kayo
Partner, Silicon Valley


Philip Kroner
Associate, Düsseldorf


David Mendel
Partner, London


Rhodri Thomas
Partner, London


Christoph Werkmeister
Partner, Düsseldorf

IN BRIEF
Companies confront an ever-evolving risk landscape when it comes to global cybersecurity threats. In this chapter, our cybersecurity specialists outline two major risks that businesses need to be increasingly aware of: firstly ransomware, which is an ever-growing global scourge; and secondly, insider threats, which should be high on any company's cyber risk awareness, but are often overlooked (until it is too late). We outline:

- how regulators and governments around the world have placed new reporting obligations on companies;
- the risks of paying ransoms;
- actions companies can take that may make a huge difference to their ability to respond to an attack;
- how companies can tackle those threats by establishing robust procedural controls; and
- the latest information on the regulatory and claims risk faced by organisations that succumb to such threats.

Increase in ransomware attacks and developing regulatory response

Ransomware, a particularly pernicious threat, has grown unabated. Ransomware actors have continued to pursue private companies and individuals relentlessly.

By some estimates, there has been a **30% growth** in **ransomware related damages** year over year for the **past decade**

(Source: Cybersecurity Ventures, CyberCrime Magazine)

In the US, regulators are taking a more aggressive approach to compulsory reporting. For example:

- In the summer of 2023, the Securities and Exchange Commission (SEC) released rules that require registrants, including foreign private issuers under certain circumstances, to report cybersecurity incidents within four days of making a determination that such incidents are material under US securities law.
- Similarly, the US Department of Homeland Security will be releasing regulations in 2024 requiring covered critical infrastructure entities to report covered incidents within 72 hours of their occurrence (whether or not they are deemed material).
- In the EU and UK, companies must report personal data breaches without undue delay, and usually within 72 hours, to the relevant data protection authority.
- In the EU and UK, operators of essential services and relevant digital service providers must notify the applicable competent authority of a relevant cyber incident without undue delay, and within 72 hours. Similar reporting obligations exist for other regulated companies (eg, those in the financial sector). Both the EU and UK are implementing reforms which will soon expand the scope of businesses caught by such requirements (such as to managed IT service providers).

> “Unlike many other regulations, the SEC’s reporting rules require public reporting of a cybersecurity incident in the days following its discovery, rather than confidential reporting. This new requirement will force companies to think through reputational issues on a tight timeline and increase pressure to provide more detailed information sooner than most companies may be prepared to share.
>
> **Beth George**
> Partner

Preparation is key

Ransomware payments during **the first six months of 2023** have reportedly already almost equalled **the whole of 2022**

(Source: Wired Magazine)

When an attack occurs, several preparatory factors can make a crucial difference to the company's ability to respond to an attack:

- **Backup and recovery capabilities.** Sufficient data backups can ensure that offline copies are readily available to restore company operations to sufficient operating capacity notwithstanding the loss of access.
- **Data and system mapping.** Companies that have mapped data and system infrastructure are in a strong position to assess the potential implications of an attack and understand what their options may be given those implications.
- **Sufficient logging and monitoring.** Once an attack occurs, visibility into the systems can make a crucial difference as to confidence levels about impacted information. Logging and monitoring provides visibility to experts to help assess implications and options.

Whether to pay ransoms

Independent of the operational facets of a ransomware attack, paying ransoms always carries certain legal risks for which companies must be prepared to establish procedural controls.

In particular, many jurisdictions have sanctions regimes that prohibit economic commerce with certain specified actors. In the US and UK, it is a strict liability criminal offence to make payments to sanctioned individuals. This means that the liability attaches regardless of whether a company actually knew the actor was sanctioned. EU sanctions may be similar in many regards to US and UK sanctions but can also be more or less extensive for individual groups or persons. Regulators are becoming more proactive with sanctions designations, so the risk of committing a sanctions offence is more than just theoretical. For example, in early 2023 individuals connected with Trickbot (a Russian ransomware group) received sanctions designations in both the UK and US.

> Companies sometimes seek to mitigate sanctions risks associated with paying ransoms by performing sanctions checks through outside counsel for relevant jurisdictions, working with ransom negotiators offering thorough vetting and market intelligence on threat actors, and liaising with law enforcement and other authorities.
>
> **Rhodri Thomas**
> Partner

Insider threats

While organisations should always be wary of the threat of malicious hackers, it is important not to underestimate the risk of insider threats to personal data. In particular, we continue to see:

- Disgruntled employees, who consider themselves whistle-blowers, leak information about their employers to third parties.
- Individuals who make it their moral duty to alert the public of how allegedly unsecure their organisation's systems are, and inadvertently cause a personal data breach in the process.
- Simple human error (eg, clicking on phishing links or attaching the wrong documents in emails to external contacts).

Once again, there are steps that can be taken to mitigate these risks. For example, organisations can:

- Monitor for any surge or irregular patterns that might indicate employees exfiltrating data via email or otherwise.
- Restrict access to the most sensitive data.
- Place limits on how much data individuals can send externally without relevant approvals.
- Implement regular training on privacy and cybersecurity obligations. While this might not stop insiders that are determined to exfiltrate personal data, it might reduce the occurrence of human error and assist with manual detection.

> "Employee training is an essential component in helping to prevent cyber incidents. When it comes to disgruntled employees, the recent changes in whistle-blower rules and protections in the EU add a layer of complexity to how these incidents must be addressed.
>
> **David Mendel**
> Partner

Development in fine sizes and increased litigation risk

The damage suffered by companies affected by a cybersecurity incident is not always immediate. Often, the looming damage goes beyond the incident. If employee, customer, or other sensitive data is lost, authorities regularly initiate proceedings for privacy violations, which may grow to full-scale audits—even onsite—of the entire organisation.

In the EU and UK, for example, these proceedings can result in substantial fines where there have been inadequate protective measures against cyber breaches. This reflects the fact that many regulators have developed their own cyber and data privacy expertise in recent years.

In the UK, **four of the top seven largest GDPR fines** handed out by the **UK data protection authority**, the **Information Commissioner's Office (ICO)**, between May 2018 and September 2023 have been for **data breaches**

While the highest fines issued by EU regulators tend to concern data privacy violations that are not related to cyber attacks, many European data protection authorities are no less proactive (and in some cases, more proactive) than the UK's ICO in pursuing enforcement action against organisations that suffer cyber attacks.

> "Once the security risk has been contained and systems have been secured, an organisation's focus quickly turns to managing regulatory engagement and mitigating legal risks. In-house counsel invariably have a critical role to play here.
>
> **Brock Dahl**
> Partner

At the beginning of 2023, the UK ICO started publicising information regarding various complaints and concerns brought to its attention and reprimands it had issued, possibly providing more fuel for claimant law firms to find non-compliant organisations to target. As part of a new approach the ICO has also pledged to 'do more' to publicise cases so that there is wider learning.

In the US, litigation risk originates from multiple potential sources. The Federal Trade Commission (at the federal level) and state Attorneys General typically have authority to bring various categories of actions related to breaches. The SEC is also expected to increase its inquiries and potential actions in light of new cybersecurity rules that come into effect in December 2023. Finally, private litigants of various stripes have the ability to bring actions against a company, whether because their personal data is directly affected by the breach (under certain regimes), or as interested shareholders via securities class and derivative actions.

Looking ahead

The cyber risk landscape will continue to evolve, particularly in light of emerging risks associated with AI and quantum computing. Regulatory frameworks that cover cybersecurity are also likely to develop in the coming years, though perhaps not at the same pace.

There is undoubtably a correlation between the extent to which an organisation prepares for cyber attacks and the harm (operational, financial, and legal) caused by an incident. The most effective preparation often involves co-ordination of internal stakeholders, refreshing incident response plans, testing crisis management processed with simulated attacks, and a good understanding (and mapping) of critical assets and data.

04.

New data portability rights: challenges and opportunity


Richard Bird
Partner, Hong Kong


Aedan Collins
Associate, New York


Theresa Ehlen
Partner, Düsseldorf/ Frankfurt


Adam Gillert
Global Data Knowledge Lawyer, London


Christine Lyon
Partner, Silicon Valley


Jan Niklas di Fabio
Associate, Berlin


Giles Pratt
Partner, London


Philipp Roos
Principal Associate, Düsseldorf

IN BRIEF

Data portability rights seek to make it easier for a natural or legal person to transfer their data from one company to another, by giving them the right to request a copy of their data in a structured, commonly used, and machine-readable format, and to transmit their data to another company. Examples might include a consumer seeking to move their content to a different social networking platform, or a company seeking to migrate its business data to a different cloud services provider.

At present, data portability rights (such as those found in privacy laws) generally do not play a major role in practice due to legal and technical limitations. This may soon change with the introduction of new laws in the EU and UK.

> Although more US states are adopting data portability rights in the B2C context, new laws in the EU and UK will likely increase the practical impact of data portability well beyond what we are seeing in the US, by expanding data portability rights in B2B as well as B2C contexts.
>
> **Christine Lyon**
> Partner

Data portability under existing data privacy laws

Existing data privacy-related laws, such as the EU GDPR, UK GDPR, and newer US state consumer data privacy laws like the California Consumer Privacy Act, already provide individuals with various data portability rights for their personal data. In practice, however, the data portability rights under these laws

have not always led to the benefits that may have been envisioned by lawmakers. For example, these data portability rights are subject to various restrictions, such as technical feasibility. Consequently, individuals may find it difficult to move their data from one organisation to another given different technical set-ups of the relevant services.

Data portability under newly enacted EU legislation

> New and pending EU and UK laws regulating the use and control of data have the potential to change the practical relevance of data portability rights, including by giving new data portability rights to organisations and imposing new data portability obligations on providers of certain types of online services.
>
> **Philipp Roos**
> Principal Associate

Under the Digital Markets Act (DMA), so-called 'gatekeepers' (ie, companies that provide core platform services, such as online search engines, online marketplaces and social networking services) must provide users with effective portability of data provided by the end user or generated through the activity of the user in the course of using the relevant service.

In particular:

- The DMA provides that these new data portability rights apply not only to individual end users but also to enterprise users of these services.
- Unlike its GDPR equivalent, the data portability right under the DMA is not restricted to personal data. Other types of data covered by the DMA may include technical or performance data without any personal reference to the user.
- Gatekeepers are required to provide free of charge tools to facilitate the effective exercise of data portability and the provision of continuous and real-time access to the data.

Another recent EU data access right, which could also be used by consumers to move their data from one service provider to another, is included in the Digital Content Directive. This specifically targets the relationship between consumers and organisations that act for purposes relating to their trade, business, craft, or profession in relation to digital content and digital services contracts (traders). In particular, if a B2C contract regarding the supply of digital content or a digital service is terminated, the trader must make available to the consumer any content other than personal data (since that is governed by the EU's GDPR) that was provided or created by the consumer during the supply of the digital content or digital service. Such content may include user-generated technical or performance data.

Additional proposed data portability in draft EU and UK legislation

Data portability will also play a key role in various upcoming EU proposed laws that are part of the EU Digital Strategy.

The EU's draft Data Act, aiming to facilitate data sharing between organisations, includes several mechanisms which look to ensure data portability by users, whether the users are consumers or businesses:

- Granting users of Internet of Things (IoT) products and related services the rights to access and use data generated by using IoT products and, if requested by the user, to share such data with third parties, eg, other IoT service providers.
- Requiring IoT products to be designed and manufactured in a manner that data generated by their use is, by default, easily, securely and, where relevant and appropriate, directly accessible to the user. Where such data cannot be directly accessed by the user, the relevant data holder must make

available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time.

- Obliging providers of certain data processing services (eg, those providing infrastructure, platforms or software as a service) to enable users to efficiently switch between these services. This includes obligations to remove commercial, technical, contractual and organisational obstacles that might inhibit customers from moving data, applications and other digital assets to another provider.

> The Data Act forms a key piece of the EU data strategy aiming to unlock industrial data and facilitate switching between data processing providers.
>
> **Theresa Ehlen**
> Partner

Closely connected to the Data Act, the European Commission envisages establishing so-called 'Common European data spaces' for several key sectors. For the health and finance sector, the European Commission has already published drafts regulating such data spaces. In line with the goal of granting patients and customers of financial institutions further control over their data, the drafts suggest sector-specific data portability rights.

Over 6 million
active users of the UK's '**Open Banking**' scheme to open up customer data using **secure protocols**

(Source: UK Competition and Markets Authority)

Similarly, UK lawmakers are also considering various government-backed draft laws that seem likely to create new data portability rights and obligations, such as:

- The UK's equivalent of the EU's DMA, the draft Digital Markets, Competition and Consumers Bill. The Bill would create new powers for the UK competition authority, allowing it to make various interventions in digital markets to encourage competition, especially targeting larger companies designated as having 'Strategic Market Status' (SMS). The UK government has suggested those new powers might be used to require SMS businesses to allow greater interoperability or data access.
- The UK's draft Data Protection and Digital Information (No.2) Bill, which would allow the UK government to introduce 'smart data schemes' across the UK economy in the hope of replicating the perceived success of the UK's existing 'Open Banking' scheme. These new schemes envisage both business and consumer customers being able to require that traders share certain data with the customer or its third-party providers. The Bill's Impact Assessment suggests the financial services (including pensions and insurance), energy and telecommunications sectors are likely to be early candidates for a UK smart data scheme.

Looking ahead

Lawmakers in the EU and the UK are currently introducing laws which include new data portability rights going beyond the data portability rights under existing privacy laws.

This is a trend other jurisdictions might follow, just as the EU GDPR led to reforms.

> Strengthened data portability rights can, in principle, lead to increased competition and consumer choice, stimulating data-driven innovation. But data portability rights also risk undermining incentives to invest in data-driven businesses, particularly if the scope of data that must be shared includes valuable analytics data.

Giles Pratt
Partner

The practical effects of each data portability right can be quite different, especially given their different scope and the possible limitations under each of the relevant laws.

Organisations should start assessing:

- the necessary updates to their processes to comply with these rights; and
- to what extent they might benefit from new data portability rights allowing them access to data they were previously not able to receive and use.

05.

Changes in data privacy and cyber enforcement


Rachael Annear
Partner, London


Robert Barton
Associate, New York


Richard Bird
Partner, Hong Kong


Laéna Bouafy
Associate, Paris


Tochukwu Egenti
Associate, London


Adam Gillert
Global Data Knowledge Lawyer, London


Timothy Howard
Partner, New York


Michael Schwaab
Principal Associate, Frankfurt


Christoph Werkmeister
Partner, Düsseldorf

IN BRIEF

The digital age has brought about intensified scrutiny of data privacy and cyber regulations globally. From varying penalty systems to emerging legislative patterns, these trends signify the evolving priorities of regulators safeguarding data privacy and cybersecurity. Understanding recent privacy and cyber enforcement trends across the US, UK, and EU, provides critical insight for businesses navigating this intricate regulatory landscape.

Over the past year, we have observed an evolution in enforcement postures across those jurisdictions. The US has extended its focus on non-monetary remedies, including the deletion of algorithms developed from improperly obtained data and personal consequences for executives. The UK has moved from headline grabbing fines to an outcomes-based approach, emphasising enforcement variety rather than just monetary penalties. Meanwhile, the EU continues to grapple with the maturation of the GDPR, with enforcement including not only (record) fines, but also diverse corrective measures.

US—beyond monetary penalties

> Federal regulators in the US have recently pursued creative and sometimes controversial remedies in enforcing data and cyber regulations.
>
> **Timothy Howard**
> Partner

Deletion of data and algorithms

In a March 2022 settlement with the Federal Trade Commission (FTC), in addition to paying a US$1.5m penalty, a company agreed to delete both the personal data of children that it had allegedly improperly obtained and any algorithms and models developed using that personal data. This follows on a similar consent order issued in 2021 against a photo storage service.

Personal consequences for executives

As part of its January 2023 consent order with Drizly Inc. and CEO James Rellas involving the company's alleged failure to use appropriate information security practices, the FTC issued detailed requirements for the information security program of any company for which Rellas is a majority owner or senior officer for ten years following the entry of the order.

Criminal liability

In May 2023, a former Chief Information Security Officer (CISO) was sentenced to three years' probation and fined after being convicted of charges related to obstruction in connection with an FTC investigation. The CISO is alleged to have taken steps to conceal information from the FTC regarding a second breach that he learned of during the agency's investigation of a prior breach, both of which exposed personal data.

UK—a move to an outcomes-based approach

The anticipated flurry of major fines, which was expected after the UK data regulator, the ICO, imposed double-digit million-pound fines in 2020, has not materialised and, instead, the ICO's recent approach has been to focus on outcomes, rather than punishment.

Focus on outcomes based approach

In a speech in November 2022, John Edwards, the Information Commissioner since January 2022, stated that:

There's nothing in the law that says that enforcement must equal fines. Enforcement happens across a spectrum. Rather than being one thing, it's a series of graduated responses to non-compliance.

This indicated the shift in approach from heavy fines for non-compliance, to an outcomes-based approach where the most appropriate enforcement steps are taken to ensure that the best outcome is chosen. Under this approach, where a company takes the right remedial steps in good time to correct their privacy shortcomings, a public reprimand may be deemed more appropriate than a large fine. However, where the same company has repeatedly breached their obligations under privacy laws, or where there is a particularly serious breach, reprimands alone may not be sufficient. In John Edwards' words, 'monetary penalties remain an important regulatory tool and we will use them in instances where they are truly needed'.

As of **early September 2023**, the ICO has only publicly reported **one new monetary fine in 2023** for breach of the UK General Data Protection Regulation (GDPR) (**£12.7m**)

Cookie banners

In November 2022, the ICO published its ICO25 strategic plan and its regulatory approach, which focuses on a number of priorities, including safeguarding vulnerable individuals. Reflecting this focus, in August 2023, the ICO announced that it will evaluate the cookie banners of the most frequently visited websites in the UK and take action where it finds that harmful design is impacting users.

> We expect UK enforcement action against cookies to be focused on complicated privacy controls, default settings that give less control over personal data, and bundling of privacy choices to nudge consumers to share more data.
>
> **Tochukwu Egenti**
> Associate

In the UK the use of cookies is primarily regulated by the Privacy and Electronic Communications Regulations (PECR). One of the changes being introduced by the UK Data Protection and Digital Information Bill is to increase the maximum level of fines the ICO can issue for breaches of PECR, from £500,000 to the higher of 4% of worldwide turnover, or £17.5m (ie, the maximum penalty under the UK GDPR). Therefore, if this Bill is passed, we can expect to see much higher fines for breaches of PECR, especially with the ICO's renewed focus.

> Recent decisions confirm the French DPA's severity with regard to cookie and other tracers' violations and remind companies of all sizes of the importance of compliance with applicable requirements. The French DPA is paying particular attention to 'dark patterns', 'tracer walls' and alternatives to third-party cookies used to circumvent limitations on the deposit of cookies ('fingerprinting', 'single sign-on' etc). See our blog post on this for further background.
>
> **Laéna Bouafy**
> Associate

EU—GDPR's five-year journey: fines, corrective measures, and current trends

(Source: Freshfields data)

Since the introduction of the EU's General Data Protection Regulation (GDPR) five years ago, the EU GDPR's enforcement regime has exhibited an evolving maturity with an impressive record of financial sanctions but also a broader spectrum of corrective measures on the horizon. Fines have particularly impacted technology companies. While fines have made headlines, the EU's GDPR empowers DPAs with diverse corrective measures. Limitations on processing, for instance, could have a more profound business impact than financial penalties.

Data transfers to the US

Data transfers to the US have been heavily scrutinised by EU DPAs in recent years, given the conclusion of the EU Court of Justice in 2020 that the US does not offer a sufficient level of protection for personal data. In this context, DPAs raised the concern that organisations often do not implement sufficient additional technical and/or organisational measures when relying on standard contractual clauses (which are one of the most common transfer mechanisms relied on).

A new EU-US Data Privacy Framework (EU-US DPF) was adopted in July 2023 to facilitate personal data transfers to US entities participating in that scheme. Given the continued uncertainty over whether the EU-US DPF will survive an expected legal challenge (and other limitations) it is likely that many personal data transfers to the US will continue to rely on other mechanisms such as standard contractual clauses.

It remains to be seen how the various additional safeguards and recourse mechanisms introduced by the US to support the new EU-US DPF, but which also have relevance to other common transfer mechanisms, will be reflected in future regulatory decisions.

Cookie banners

Regarding cookie banners, in particular various forms of nudging are regularly criticised by EU DPAs. Examples include cookie banners that use a traffic light-like colour and design scheme ('accept all' = green button; 'reject all' = red button) or which make rejection of cookies more onerous than accepting them.

The French DPA has been particularly pro-active in enforcing against cookie banners and imposed over €400m of fines in recent years in relation to alleged violations of cookie laws.

Companies, especially those with a French user base, should therefore consider auditing their cookie banners to ensure they are compliant.

Looking ahead

The enforcement trends outlined above show the importance of companies and other organisations continuing to place emphasis on compliance with privacy and related laws. There is ample opportunity for regulators on both sides of the Atlantic to impose onerous non-monetary penalties on organisations in addition to, or instead of, heavy fines.

The risk of personal liability for CISOs and other corporate officers not only elevates the stakes for organisational compliance but makes it a personal imperative for executives.

Regulators are demonstrating a concentrated effort to shield the rights of vulnerable individuals, especially children. Companies need to be particularly diligent with data concerning minors, ensuring that any data collection practices are transparent and consensual.

In addition, those companies leveraging AI must maintain their data sources' integrity and ensure algorithms are built in accordance with privacy law standards.

More generally, companies can expect continued regulatory scrutiny of their online practices, with the UK and EU focusing on cookie-banners and user consent—areas which are often overlooked.

Finally, in the EU, international data transfers are likely to remain a major area of focus from regulators.

06.

Growing risk of data litigation


Richard Bird
Partner, Hong Kong


Mark Egeler
Senior Associate, Silicon Valley


Adam Gillert
Global Data Knowledge Lawyer, London


Daniel Gold
Associate, London


Catherine Greenwood-Smith
Partner, London


Timothy Howard
Partner, New York


Severin Kehrer
Principal Associate, Frankfurt


Fiona McHugh
Associate, London


Adam Silow
Associate, New York


Rhodri Thomas
Partner, London


Christoph Werkmeister
Partner, Düsseldorf

IN BRIEF
Well-publicised and extensive data breaches have always carried the risk of costly and reputationally damaging mass litigation, and such claims continue apace. Add into the mix recent trends—such as the rise in other data-related litigation (where no data breach occurred), an increasingly onerous regulatory environment, more active plaintiff law firms, and companies going on the offensive to protect their data—and it is clear why data litigation has, and will remain, a primary area of concern for many general counsel.

This article identifies four recent trends that have increased the risk of data litigation for global businesses, and explores what actions organisations should take to address them.

Data breaches, and plaintiff recruitment, becoming more high profile

Companies suffering data breaches have always faced a risk of litigation, but this risk has markedly increased in recent years.

Plaintiff law firms are becoming more active in this field, in part due to the significant increase in plaintiff-side mass claims funding and the ease of identifying and recruiting potential plaintiffs. It is becoming increasingly common for litigation proceedings to be issued earlier, and in parallel with regulatory proceedings.

In addition, plaintiff firms, particularly in Germany and Austria, often bring hundreds, or even thousands, of individual actions in parallel; thereby creating, in effect, an informal class action and an immense administrative burden on businesses and courts.

> “Companies often underestimate the risk of having to defend hundreds or thousands of separate claims. With such large numbers, it is likely that in at least a handful of cases the plaintiffs will win (at least at first instance), which plaintiff firms publicise to help their recruitment campaigns. In Germany, this is fuelled by the majority of individuals having legal claims insurance, which covers any litigation-related costs regardless of the outcome. This means that for plaintiffs, litigation is a win-win.
>
> **Severin Kehrer**
> Principal Associate

This trend is likely to be exacerbated in the US by the Securities and Exchange Commission's (SEC) new cybersecurity disclosure rules, which require all US reporting companies to disclose material cybersecurity incidents within four business days of the company's determination that they experienced such an incident.

The new rules also require foreign private issuers to disclose material cyber incidents to the SEC if they are already required to:

- disclose the incident under the laws of their home jurisdiction;
- report it pursuant to stock exchange requirements; or
- disclose it to their shareholders.

As part of the disclosure, companies must describe material aspects of the nature, scope, and timing of the incident, as well as the material (or reasonably likely) impact on the company, including its financial condition and results of operations. Companies making such mandatory disclosures are likely to face an increase in scrutiny and litigation risk from investors and consumers.

Evolving case law and legislation

The UK Supreme Court decision in *Lloyd v Google* made opt-out UK General Data Protection Regulation (GDPR) mass claims much harder to bring in England & Wales and few opt-out claims in England & Wales have got off the ground since this judgment. However, case law in this area is still embryonic and several funders and plaintiffs are testing where the courts will set the boundaries and parameters.

The recent EU Court of Justice decision in *Austrian Post* was, in some senses, a blow to low-value claims in the EU, since it determined that the mere infringement of the EU's GDPR does not in itself confer a right for compensation. However, the court declined to set an EU-wide minimum threshold for the seriousness of non-material damage required to bring a claim, leaving it open for national courts to decide.

In the US, a frequent threshold hurdle for data breach plaintiffs is satisfying the federal standing requirements, specifically that of 'injury-in-fact'. Recently, US courts have applied the 2021 US Supreme Court's holding in *TransUnion v Ramirez*—that the mere risk of future harm on its own cannot qualify as a

concrete harm—in the data breach context to dismiss data breach claims that are insufficiently concrete. However, we are seeing a divergence among federal courts in the US. Some courts are distinguishing *TransUnion* on procedural grounds or finding sufficiently concrete harm, to allow data breach claims to proceed.

> The nascent nature of jurisprudence in this area creates fertile ground for plaintiffs looking to test the boundaries of privacy law. Many funders are aware of this and the opportunities it creates.
>
> **Rhodri Thomas**
> Partner

Although these recent UK, EU and US judgments have posed a challenge to data-related mass claims, a number of new laws have been passed that are in a potential claimant's favour.

In the US, new state laws incentivise plaintiffs to bring claims by providing an avenue to obtain statutory damages for data breaches even in the absence of damages to the individual. For example, the California Consumer Privacy Act provides plaintiffs with statutory damages of up to US$750 per impacted individual where they can show that the breach was the result of a business's failure to maintain reasonable security procedures and practices.

The new Representative Actions Directive (RAD) requires EU Member States to have a domestic procedural mechanism for collective redress and is expected to increase the number of data-related collective actions. Nevertheless, the need to evidence non-material damage may still be a major obstacle in some cases.

> The Netherlands in particular is becoming a go-to-jurisdiction for plaintiff lawyers in data-related litigation. A commonly heard saying is 'the data protection regulator cannot do it alone', and that private enforcement must become more mainstream—this is obviously concerning for companies that are working on complying with a patchwork of data-related legislation.
>
> **Mark Egeler**
> Senior Associate

Rise in non-data breach litigation

While hacks, cyber attacks and ransomware often grab the headlines, that is far from where data litigation ends.

There has been a rise in litigation relating to cross-border data transfers, misuse of personal data, online safety and shortcomings in privacy policies. Data scraping is another area that litigants have focused on recently; from third parties scraping data from websites, to privacy and digital rights organisations filing complaints against companies for scraping images for facial recognition technology. In the US, recent class actions have been brought for the use of mass data scraping for the purpose of training artificial intelligence (AI) large language models.

As data-related laws and regulations (such as those concerning AI) develop, the scope for new grounds of legal challenges are likely to emerge.

Corporate victims go on the offensive

While plaintiffs in data litigation cases are often consumers or privacy campaigners, it is increasingly common to see businesses affected by breaches, unauthorised data scraping or hackers acting against malicious third-party actors.

There are a wide variety of protective and reactive steps available to businesses, depending on the nature of the incident. These include:

- limiting the accessibility to stolen data through take-down notices and injunctions;
- suing bad actors for breaching a website's terms; and
- cooperating with law enforcement to recover data. Co-operation with US federal law enforcement in particular has proven beneficial to victims of data-related crimes, especially where US authorities have been able to share threat intelligence information and, in some cases, use their own powers to seize data and recover stolen funds.

Looking ahead

The potential risks arising from data-related litigation are complex and wide-ranging, and the legal and regulatory landscape is changing rapidly.

Litigation risk is often understandably low on an organisation's worry list in the immediate aftermath of a data-related incident. However, there is often much that can be done in that time and the following weeks in order to mitigate litigation risk.

Responding to complex legal claims and regulatory inquiries in parallel:

- can impose a significant burden on the resources of a company's internal functions, and not just legal teams; and
- requires careful management to ensure that the output of regulatory and litigation workstreams are aligned.

The difficulties in handling regulatory inquiries and litigation in parallel are not to be underestimated.

In our experience, businesses that turn their minds quickly to these issues, including taking offensive steps where helpful, are often the ones that have the best prospects of defending claims, or avoiding being sued altogether.

07.

Data deal trends

Richard Bird
Partner, Hong Kong

Brock Dahl
Partner, Washington, D.C./Silicon Valley

Theresa Ehlen
Partner, Düsseldorf/ Frankfurt

Tony Gregory
Senior Associate, London

Annabelle Hamelin
Associate, Berlin

IN BRIEF
Acquiring valuable datasets remains a top priority for businesses worldwide. Long-standing issues relating to data—such as data ownership and compliance with privacy laws—will continue to be important in M&A deals.

However, new challenges have also emerged, such as when a buyer is seeking to acquire artificial intelligence (AI) related assets. Additionally, recent developments in international data transfers often require consideration.

AI acquisitions and the dawn of a new era

To navigate legal complexities and mitigate unknown risks, buyers must address specific legal issues associated with acquiring AI assets. This involves assessing potential target liabilities and risks, with a focus on AI inputs, the relevant AI system(s), AI outputs and evolving AI regulation.

Below are some examples of the related legal risks buyers should due diligence and address:

> With the increased public spotlight on AI, we're also seeing even more AI and data deals and a new focus on data risks. While for many, the GDPR has become part of standard compliance due diligence, AI and data ownership have moved to the forefront of some buyer's risk and benefit analysis. A lot of our clients are concerned whether they can actually make use of the data and the AI model and how to protect themselves against the risks in this area. Never have regulation, IP and reputation been so closely linked as we're now experiencing with AI.
>
> **Theresa Ehlen**
> Partner

AI inputs

AI training often involves data that is protected by copyright and/or database rights, making the navigation of intellectual property (IP) rights a central consideration for buyers. Additionally, compliance with privacy laws—such as the UK or the EU's General Data Protection Regulation (GDPR) or relevant US state laws, such as California Consumer Privacy Act—is essential when AI applications involve personal data. For example, developing or using AI applications in compliance with the EU's GDPR may require complying with information obligations towards data subjects.

Privacy compliance in the US and globally is becoming increasingly complex. A dozen US states have now completed legislative processes on comprehensive consumer privacy laws. China's landmark Personal Information Protection Law (PIPL) entered effect in 2021, and India's parliament also recently passed its long-awaited privacy law.

AI systems and their outputs

Determining copyright protection for AI outputs hinges on human intervention. Buyers must assess whether the AI system or the human operator can be considered the 'author' of the content. Patentability of AI inventions, including the AI system itself, should also be examined. However, the patentability of software is generally limited, and the debate continues over whether AI systems can be considered inventors under patent law.

Organisations must also ensure the handling of AI outputs, and that decisions or actions taken in reliance on them, comply with other applicable laws such as those relating to privacy, consumer regulation and sector specific-laws (such as in financial services).

We are likely to see certain countries liberalise their existing IP and privacy regimes in order to make their jurisdictions more attractive for AI development and use. For example, the UK government is currently seeking to change existing laws regarding automated decision-making in relation to personal data, which may create new opportunities for businesses to use automated decision-making and AI in the UK.

AI regulation

Businesses are likely to encounter a range of approaches to the regulation of AI in different jurisdictions. For example, the upcoming AI Act in the EU, currently expected to be finalised by the end of 2023, adopts a prescriptive approach to the use of AI including obligations on providers relating to governance, transparency, accountability and fairness. On the other hand, the UK is not currently planning to introduce AI-specific regulations but has proposed a 'pro-innovation' framework based on certain overarching principles to govern the development and use of AI, which it is envisaged will be applied by existing regulators. For further details, please see Chapter 1 (AI chapter).

China has introduced several laws targeting specific types or applications of AI, including its 'Interim Measures for the Management of Generative AI Services', which entered into force in August 2023.

There will also be other existing laws that are applicable to AI, for example in relation to privacy, IP, and product liability. Buyers will therefore need to consider a patchwork of overlapping legal regimes when assessing a target's current and planned AI use.

Regarding liability, the EU's proposed AI Liability Directive would make it easier for individuals to seek redress for AI-related damages if companies fail to provide sufficient documentation of their AI system's robustness. Therefore, evaluating AI documentation as part of M&A due diligence is crucial to assessing potential litigation risks.

The crucial issue of data ownership and protection

Statutory laws have not yet established comprehensive protection for data rights. Consequently, the target company's approach to protecting data assets is pivotal. Buyers should identify business-critical data and evaluate its protection through:

- potential IP rights (including database rights);
- contractual means; and
- technical and organisational measures to protect the data from access and usage by third parties, including malicious access (such as use of secure interfaces and use of encryption techniques).

Buyers will often want to ensure they can prevent:

- sellers from reusing critical data for new ventures; and
- undesired third-party access that could impact the business and its competitive position.

In particular, attention should be paid to:

- prior rights which may have been granted when assessing how the transaction should be priced; and
- reviewing agreements which may grant ongoing access, including after the close.

Facilitating cross-border transatlantic and Chinese M&A deals

While cross-border data transfers have become increasingly challenging, for transatlantic M&A, 2023 represents something of a turning point. The European Commission's adequacy decision for the EU-US Data Privacy Framework (the DPF) in July 2023, and the agreement between the US and UK governments on a UK extension to the DPF (the UK Extension), have the potential to better facilitate personal data transfers from the EU and UK to the US. Subject to detailed requirements of the respective regimes, reliance on the DPF and the UK Extension will be possible for M&A deals if the data importer is certified under the DPF or the UK Extension, eliminating the need for additional transfer instruments or measures.

However, because of uncertainty about potential legal challenges, many companies are continuing to rely on existing mechanisms (such as Standard Contract Clauses (SCCs) for the EU, and International Data Transfer Agreements and the UK Addendum to the EU SCCs for the UK) for now. The DPF and UK Extension unfortunately will also not simplify data transfers from the EU/UK to countries other than the US.

On the other hand, China's strict rules on cross-border data transfer continue to create headaches at all stages of an M&A transaction. These rules require specific notification to be given, and consent obtained, for a cross-border data transfer of personal data—with the notification to include the name and contact information of the overseas recipient; a rule that is incompatible with deal confidentiality during a diligence phase. The same requirement applies on a domestic transfer.

Depending on the volumes of data held by the target and being transferred out of China, a cross-border transfer of personal data will need to be supported by a standard contract (in a mandatory form) or to undergo an onerous and time-consuming government security assessment process, with an uncertain outcome. The standard contract itself needs to be filed with the government, along with a detailed impact assessment report.

These rules are leading to more aspects of diligence processes being conducted solely onshore in China and to very close attention being paid to redaction of personal particulars in disclosed materials. An additional layer of national security-type concerns will also arise when conducting diligence in sensitive

sectors of the economy that may involve the new categories of 'important data' or 'core data' that are regulated by the Data Security Law.

Cybersecurity risks on transactions

Cyber risks such as **ransomware attacks** or **data breaches**, rank as the **most important risk globally**

(Source: Link to Allianz Risk Barometer 2023 Allianz Risk Barometer 2023 – Cyber incidents | AGCSs)

Cybersecurity continues to be a significant issue for businesses. Organisations are processing increasing volumes of data, which elevates the risk of a data breach occurring in the context of a cyber attack. Where such an attack comes to light after an M&A transaction has completed, privacy regulators are increasingly willing to investigate the due diligence and post-closing steps taken by the buyer, and take enforcement action.

Shortcomings in this area can lead to unexpected material financial exposure, including review and remediation costs, regulatory fines, and potentially mass claims, as well as reputational data. Therefore, it is important for buyers to properly identify, assess, and remediate cyber issues during and after M&A transactions.

A first step for buyers is to assess the risk profile associated with the target, in order to properly scope cyber and data due diligence. Enhanced due diligence is more likely to be required where the target:

- processed large volumes of customer data;
- undertakes high-risk processing activities (such as analytics and profiling);
- is subject to more onerous privacy regimes (such as the EU's GDPR); or
- has a history of cyber incidents.

Buyers should look to align their due diligence with areas of regulatory focus, such as in particular relevant technical and organisational measures identified in regulatory guidance and decisions, which include:

- multi-factor authentication;
- system monitoring and logging;
- encryption;
- data/cyber policies; and
- procedures and assessments.

Depending on the findings, a buyer might require the seller to remedy security issues before closing and/or seek indemnities in respect of regulatory fines and compensation claims for disclosed incidents.

> "The increasing pace of technology adoption and complexity of cybersecurity risks is making cyber diligence a fundamental component of transactional diligence. It is critical for companies to have frameworks for assessing and managing the associated risks.
>
> **Brock Dahl**
> Partner

Regulators are also likely to review what steps were taken post-closing to identify and remediate cyber issues. For example, if in-depth cyber and data due diligence was not possible before signing (eg, where the buyer and seller are competitors), then regulators will generally expect greater due diligence to take place after closing of the transaction.

Buyers will also need to ensure that the target complies with privacy laws post-closing. For example, under the UK and EU GDPRs this may include the data security principle when integrating the target's IT systems and data, the data minimisation principle when deciding whether to retain all acquired data, and the transparency principle if the buyer wishes to use the target's data for new purposes.

Looking ahead

Companies face extremely varied and complex challenges while carrying out data-related transactions. Despite those challenges, investment and transactional operations relating to data remain very numerous.

Companies should, therefore, continue to prepare as far as possible to be able to tackle all issues likely to arise at every stage. While pursuing the 'new gold' of data, organisations should:

- think globally;
- secure appropriate rights;
- not forget about cybersecurity risks and privacy laws; and
- consider any post-closing issues.

08.

GDPR reloaded: The EU's comprehensive approach to regulating data-driven industries

Rachael Annear
Partner, London

Richard Bird
Partner, Hong Kong

Elena Brandt
Principal Associate, Düsseldorf

Mark Egeler
Senior Associate, Silicon Valley

Theresa Ehlen
Partner, Düsseldorf/ Frankfurt

Christine Lyon
Partner, Silicon Valley

Christina Möllnitz-Dimick
Associate, Munich

Jérôme Philippe
Partner, Paris

Julia Utzerath
Senior Knowledge Lawyer, Düsseldorf

Christoph Werkmeister
Partner, Düsseldorf

IN BRIEF

In the ever-evolving landscape of digital data regulation, the EU has been at the forefront of establishing a legal framework to protect individuals' personal data, in particular with the introduction of the General Data Protection Regulation (GDPR). Now, under the EU Digital Strategy, the EU intends to supplement the existing data and digital framework with a new set of rules that are not limited to personal data or even to data, for that matter.

The EU Digital Strategy introduces new rules to foster data flow, data access and the data economy—introduced by the Data Act and the Data Governance Act—which will apply to both personal and non-personal data, including machine and product data. The EU is also introducing enhanced obligations and user protections for online platform services, online hosting services, search engines, online marketplaces and social networking services under the Digital Markets Act (DMA) and the Digital Services Act (DSA). Artificial intelligence (AI) is another focus of the new regulation coming out of Brussels (see Chapter 1 on AI for more details). In addition, companies offering IT-based services must keep an eye on the proposed e-Privacy Regulation.

Some of the new rules aim to create a single market for data—making it easier for companies to share and get access to data—while the key goal of other newly introduced rules is to create a safe digital environment for the users of the relevant services. Below we explain what changes businesses can expect and how they should respond.

> The EU wants businesses to take the reforms seriously: fines for non-compliance with the new regulations can range from 4% up to 20% of global annual turnover.
>
> **Theresa Ehlen**
> Partner

What changes and impacts to expect?

The DSA—broad scope and global reach coupled with increasing transparency and accountability obligations.

The DSA aims to improve user safety and to protect fundamental rights in digital environments. The scope of services that the DSA covers is broad, capturing a wide range of 'intermediary service providers' such as hosting services, online platforms and online marketplaces. For example, every B2B online platform which showcases third party content, products or services is captured by the DSA, even if the product or service itself cannot be bought on the platform. The DSA applies regardless of the relevant provider's place of establishment as long as their services are offered to recipients that have their place of establishment or are located in the EU.

The DSA creates a layered set of obligations tailored to the different categories of digital services; it introduces a set of baseline obligations which apply to all online intermediaries and requires, for example, the designation of single points of contacts for authorities and users, annual transparency reporting, and transparent terms and conditions. Increased obligations apply to online platforms connecting customers with goods, services and content; those obligations require providers to implement a notice and action mechanism, adopt adequate measures to combat the dissemination of illegal content online, and increase the transparency of their platforms for users.

Additional specific obligations apply for online marketplaces and look to ensure the traceability of traders and safeguarding of users' rights. The most stringent rules apply to 'very large online platforms' (VLOP) and 'very large online search engines' (VLOSE), which are designated by the European Commission depending on whether their monthly average user numbers in the EU are above 45m. For most companies, the majority of the obligations under the DSA will start to apply in March 2024. In addition, for those VLOPs and VLOSEs initially designated by the Commission, the key obligations started to apply on 25 August 2023. Enforcement rules under the DSA are severe with, for example, fines of up to 6% of total worldwide annual turnover.

In a nutshell, all companies covered by the DSA—and not only the largest online platforms and search engines—will face comprehensive compliance tasks. Companies should therefore start with reviewing online business models and potentially adapting and redesigning those to comply with the new set of rules (eg, to design interfaces in ways which omit dark patterns). Their compliance work may need to continue and require additional resources, including for the implementation of complaints systems and changes to T&Cs.

Last but not least, companies are well-advised to set up a solid strategy for dealing with transparency and compliance requests from national authorities and, in case of VLOPs and VLOSEs, the European Commission.

> While the European Commission is the sole authority responsible for DMA enforcement, the DMA framework provides various ways in which EU Member States, and their respective laws, can become involved in those investigations. In particular, the DMA explicitly provides that national competition authorities—after having informed the European Commission—may conduct investigations into possible non-compliance. Therefore, despite the DMA's aim of avoiding regulatory fragmentation across the EU, it remains to be seen how the relationship between the European Commission and Member States and the consistent enforcement of the DMA across the EU will play out in the future.
>
> **Jérôme Philippe**
> Partner

The DMA—enhancing fairness in the digital market

The DMA is intended to promote fair competition and to address certain practices of so-called gatekeepers (ie, providers of very large digital services) which are potentially harmful to the overall EU digital market. Most of the DMA's obligations will start to apply in March 2024.

The DMA introduces a framework which defines certain practices that are inherently considered as anti-competitive and which can be addressed by the regulator without the need to conduct a lengthy investigation into the relevant practices. It is presumed that this will significantly speed up competition enforcement in the digital space.

The set of potentially harmful practices addressed by the DMA includes certain data practices (ie, certain cross-service processing of personal data) which may now require consent under the DMA.

The DMA will also impose obligations on gatekeepers to facilitate access to end user and business user data, and impact the extent to which gatekeepers may use business user data in competition with those business users. As such, the DMA will not only impact the relevant gatekeepers, which will need to review their current practices, but will also have an impact on the end users and business users of the relevant services who may be provided with broader access to their data. Other obligations relate to bundling, self-preferencing, interoperability of services, and transparency (eg, in relation to advertising services).

Fines for DMA infringement are up to 10% of the gatekeeper's worldwide turnover in case of non-compliance, and up to 20% in case of repeated infringements.

The Data Act—regulating the internet of things and data processing services

The Data Act aims to introduce rules for the Internet of Things and for enabling users to easily switch between cloud providers. It is designed to improve access, exchange and use of valuable data generated by connected devices so that more public and private stakeholders can benefit from big data and machine learning.

The Data Act applies to personal and non-personal data and introduces data sharing obligations to companies that manufacture or offer connected products or related services in the EU. Users of a connected product or a related service will be entitled to access data generated by the connected product or service and can even ask the product's manufacturer or seller to transfer this data to a third party. These rules will

apply in B2B, B2C and B2G contexts. There are some exceptions which limit data sharing, for example, if the relevant data includes trade secrets then those shall be preserved and only be disclosed where technical and organisational measures necessary to preserve the confidentiality of the shared data have been agreed in advance.

Implementing these new rules will come with a variety of challenges and considerable compliance work for companies. For example, the data access and data portability rights will require companies to include into the design of their products interfaces that make data easily retrievable. In practice, companies must not only put in place stringent governance and procedures to comply with the data sharing obligations, but also implement the limitations regarding trade secrets and track any infringements of these by their customers or competitors.

> "Where the GDPR has sparked numerous consumer class actions and individual litigation, the Data Act may cause B2B actions where companies request access to non-personal data. This will make the competition and privacy legal teams quite nervous; without proper data mapping, companies can find themselves caught between a rock and a hard place.
>
> **Mark Egeler**
> Senior Associate

Data processing services, like cloud services providers, infrastructure as a service providers, or platform as a service providers must allow users to easily switch their services and to improve portability between different data processing services providers. The scope of interoperability obligations is not completely clear, and it is yet to be determined how the requirements will function regarding the practical challenges of IT migration. Likewise, the obligation to limit switching charges is not clear cut, with uncertainties about which costs will be in scope.

Service providers will also have to cope with another compliance burden by being subject to safeguards for the international transfer of non-personal data, similar to those from the so-called *Schrems II* ruling of the EU's Court of Justice for personal data.

Infringement of the Data Act may lead to GDPR-level fines of up to €20m or 4% of the company's annual turnover—whichever is higher.

To prepare for the different compliance tasks that will come with the Data Act, especially for connected products, companies should start data mapping to gain an overview of the types of data their products generate. In addition, starting to plan the technical elements for data sharing/data portability into products will help to minimise the amount of rework required if product design subsequently changes.

The Data Governance Act—facilitating data sharing

The Data Governance Act (DGA) is a cross-sectoral regulation designed to enhance trust in and facilitate voluntary data sharing for the benefit of businesses and citizens.

While the aim of the Data Act is to determine who is entitled to generate economic value from data and under which conditions, the DGA sets up the process and framework to enable data sharing.

The DGA applies to public sector bodies, providers of data intermediation services (ie, companies which do not sell data themselves but bring together other companies interested in monetising and reusing data), and data altruism organisations which facilitate data sharing for public benefit purposes.

Among other things, the DGA aims to:

- create shared data spaces and mechanisms for reusing certain categories of protected public sector data;
- ensure trust in data by establishing neutral data intermediaries;
- establish data altruism mechanisms which facilitate data sharing for companies, individuals, and public organisations for public benefit purposes; and
- introduce obligations for data intermediation services providers to guarantee their neutrality and prevent conflicts of interest (eg, structural separation of data intermediary services from other services and an obligation to notify a national authority of their intent to provide data intermediation services). Once the notified authority has confirmed, such providers will then be able to use a label and a common logo to show they are a recognised data intermediary in the EU.

Non-compliance with these obligations may lead to fines which are yet to be determined by national law.

The proposed e-Privacy Regulation—updated framework for OTT communication services?

The EU's e-Privacy framework, which primarily aims to address the confidentiality of communications and the online privacy of individuals, currently consists of the ePrivacy Directive and its national implementations. The result is a broad set of regulations which also require businesses to consider variations in EU member state laws when introducing new features to their services.

Besides the fragmentation issue, the main challenge is that the current ePrivacy Directive (introduced in 2002 and last updated in 2009) was originally meant to address traditional telecoms operators; it was never meant to capture so-called over-the-top (OTT) communication service providers. This has changed with the EU Electronic Communications Code (the EECC) which has altered the definition of 'electronic communications services' so that it also covers OTT messaging services. However, the original ePrivacy framework has not been updated, creating legal uncertainty as to which of the obligations also apply to OTT services. In the absence of an updated EU-level framework, some national regulators have adjusted their national ePrivacy rules to account for OTT, at the same time creating an even more fragmented legal framework.

The ePrivacy Regulation is supposed to account for the broader set of players which are now covered by the ePrivacy framework and to keep up with the fast pace at which IT-based services are developing and evolving. Furthermore, the updated framework will impose a more harmonised approach across the EU.

That said, at the time of writing, the proposed ePrivacy Regulation is still under negotiation, and it remains uncertain if, or when, it will be finalised given that initially it was intended to enter into force in parallel to the GDPR in 2018.

Looking ahead

Businesses should check whether they are captured by the new laws under the EU Digital Strategy and start to prepare for it, especially as some of the major laws are already in force and come with hefty fines.

This will require a careful assessment of the applicability of the new regulations to specific services and business models, and a detailed evaluation of how this will impact current practices. Businesses in scope of the relevant framework will have to develop a comprehensive compliance strategy which allows them to continue operating in compliance with the new requirements.

"It will be interesting to see to what extent the EU's approach to digital regulation is copied by other jurisdictions, and whether it becomes globally influential in a similar manner to the EU's data protection laws. The UK is progressing various reforms that cover similar ground to the EU Digital Strategy, such as an Online Safety Act (the UK's equivalent to the DSA) and a Digital Markets, Competition, and Consumer Bill (the UK equivalent to the DMA)—although there are significant divergences in the UK's approach as compared to the EU.

Rachael Annear
Partner

One of the legal challenges in that context is to figure out how the interplay between the GDPR and the relevant piece of the EU Digital Strategy, as well as the interplay between the new laws themselves, works. This is because the relationship between the different EU frameworks is still unclear, both in terms of the scope of the relevant obligation and enforcement.

Similar to the approach that was required following adoption of the GDPR, companies will need to set up compliance programmes for the new digital regulations to ensure their products and processes align with the multi-layered rules, some of which will start to apply already early next year. This may require the implementation of new principles in the very early stages of product development ('compliance by design'), akin to the approach that already exists under the GDPR. Generally, companies can benefit from reviewing their GDPR compliance programmes and considering how the new requirements can fit in or complement the existing programmes.

> Due to the high complexity of the new laws, in addition to their overlaps with each other and with existing regulations, we recommend a holistic approach to the upcoming compliance exercise. Thinking in silos fails to recognise the complexity and interlocking nature of the new regulations that are already in force and will come into force in the coming months and years.
>
> **Elena Brandt**
> Principal Associate

The new frameworks are likely to undergo further refinements and adjustments, as implementing acts and delegated acts of the Commission, as well as related national legislation, are still on their way. Businesses should closely monitor these developments to ensure compliance, and leverage opportunities for growth in the digital marketplace.

We will keep you up to date with the latest developments on our Freshfields EU Digital Strategy Hub.

freshfields.com