HUNTON
ANDREWS KURTH

APRIL 2024

UK/EU Privacy & Cybersecurity: Current Legislative Trends

INTRODUCTION

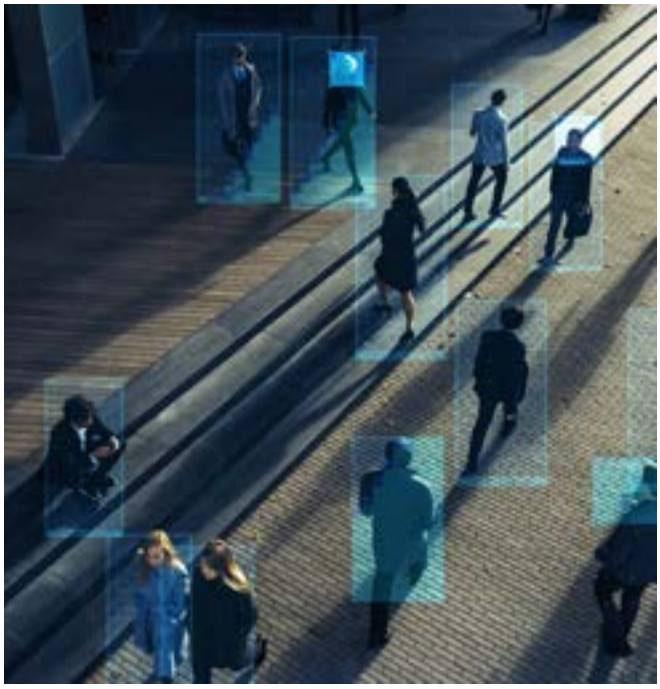
As with recent years, 2024 looks set to be another noteworthy year for the data privacy and cybersecurity legislative landscape in the UK and EU, with potential interesting challenges and considerations on the horizon. Below is a summary of the core legislative trends that have taken shape in 2024 in the UK and EU, and what we anticipate will impact the industry throughout the year. From the increase in legislation around artificial intelligence, to heightened security online and protections from cyber threats, we provide insights on these key issues and discuss the ongoing trends for the following year.

ARTIFICIAL INTELLIGENCE (AI)

Arguably the most talked about topic of recent months in the privacy sphere is AI, and this is not likely to change in the coming months.

The EU

The EU Artificial Intelligence Act (the AI Act), the first comprehensive AI legislation globally, is set to be formally approved in early 2024, with provisions taking effect following a transitional period of between six and 36 months. The AI Act will regulate the development and use of AI systems, including generative AI systems, across all industries in the EU, and will have extra-territorial effect meaning, like the EU General Data Protection Regulation (GDPR), it may apply to organisations outside the EU using AI within the EU. The AI Act places obligations on multiple stakeholders, with the key players being "providers" (i.e., an organisation that develops an AI system or has an AI system developed by a third party but places it on the market under its own name) and "deployers" (i.e., an organisation that uses an AI system under its own authority). The AI Act will operate a risk-based legal framework for AI governance and the obligations that apply to an AI system will differ depending on the risk classification of the particular AI system in question. While the data used within AI systems is not limited to personal data, those developing or using AI with personal data will have to be prepared to comply with both the AI Act and the GDPR. A detailed summary of the AI Act, including further details regarding the obligations for stakeholders, the risk classifications and the potential fines, can be found here.



The UK

The proposed approach to regulating AI in the UK is different from the EU, and we expect to see further traction with this approach during 2024. In 2023, the UK government announced its pro-innovation approach to regulating AI which is based on a framework of five principles to guide and inform responsible development and use of AI in all sectors (a summary of the approach can be found here). The principles will be issued on a non-statutory basis and implemented by existing regulators, such as the Information Commissioners Office (ICO) and the Office of Communications (Ofcom), within their industries.

The principles are: (i) safety, security and robustness; (ii) appropriate transparency and explainability; (iii) fairness; (iv) accountability and governance; and (v) contestability and redress. Principles of this nature are well-known and understood by privacy practitioners as they are very similar to the principles of the GDPR and UK GDPR. However, for those business teams working with AI from other areas of expertise, the principles may not be as clear, meaning more guidance from the existing regulators will be required.

The approach was subject to a consultation and on February 6, 2024, the UK government published the response to the consultation. According to the publication, the response to the approach was generally supportive and the version proposed in 2023 is largely unchanged (a summary of the response can be found here), although there is a clear indication that the government is not ruling out the requirement for some, more formal, regulation in due course. During 2024, we will see the approach to AI regulation evolve in the UK, including further policy development, building of a central function and the emergence of guidance from existing regulators.

SPOTLIGHT ON THE EU

In addition to the AI Act, there are several other items on the EU legislative agenda that practitioners should be aware of as 2024 progresses.

Digital Services Act

The Digital Services Act (DSA) aims to foster protection against the spread of illegal content and protect users' fundamental rights. In this respect, not only does it implement online safety legislation, but also certain related consumer law protections. The legislation applies to online intermediary services such as hosting services (including online platforms like social media sites, online marketplaces and cloud storage services), as well as caching services, mere conduit services and online search engines. Depending on the specific type of online intermediary, the DSA may impose measures such as the implementation of mechanisms allowing users to flag illegal content online, reinforced transparency, safeguards and rights for users and additional rules on the protection of minors.

"Very large online platforms" and "very large online search engines", defined as online platforms and search engines with more than 45 million active monthly users, are also subject a number of additional obligations, including the requirement to mitigate systemic risks, conducting annual audits and either implementing or justifying the non-implementation of the audit recommendations, and establishing a compliance function, which is independent from their operational functions to monitor DSA compliance. A summary of the DSA is available here.

The DSA became fully applicable on February 17, 2024, so those organisations subject to the DSA should be taking steps to comply with the DSA.

Cyber Resilience Act

The Cyber Resilience Act[1] establishes horizontal rules to protect digital products in the EU against cyber threats. The Regulation regulates the design, development, production and making available on the market, of hardware and software products that are connected either directly or indirectly to another device or to a network. The Cyber Resilience Act will also impose certain reporting obligations regarding actively exploited vulnerabilities and incidents. The European Institutions have reached a political agreement on the final text and its final approval is expected mid-2024 ahead of the European Parliament elections.

NIS2 Directive

Replacing the NIS Directive, the NIS2 Directive is broader in scope. It defines which organisations will be in scope, including organisations that are considered part of "essential sectors" (e.g., energy, transport, banking, financial markets, health, drinking water, digital infrastructure, B2B ICT service management, public administration and space) and "important sectors" (e.g., waste management, postal services, chemicals, food, medical device manufacturers, digital providers and producers of electronics). EU Member States will also be given some flexibility to impose the NIS2

1 Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. The final text of the Cyber Resilience Act is not yet available at the time of this writing.

Directive's rules on entities not expressly included in the NIS2 Directive's scope through national law.

In addition to stringent rules on governance, cyber risk management and other areas, the NIS2 Directive introduces new notification requirements for any incident affecting a relevant organisation having a significant impact on the provision of their services. This notification must be made to the national computer security incident response team, or applicable competent authority, without undue delay and there are several timeframes to comply with in this respect, including an "early warning" notification within 24 hours of becoming aware.

The NIS2 Directive also provides EU national competent authorities with a robust set of enforcement and investigation powers, such as the ability to conduct raids and the ability to impose considerable fines of up to €10 million or 2 percent of the worldwide annual turnover for "essential entities" and up to €7 million or 1.4 percent of the worldwide annual turnover for "important entities".

As a Directive, EU Member States have until October 17, 2024, to transpose the NIS2 Directive into national law, replacing the transposed version of the NIS Directive. While awaiting national laws, organisations that fall within the scope of NIS2 should be taking initial steps to assess their compliance obligations against the information available in NIS2. A summary of the NIS2 Directive can be found here.

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) aims at strengthening the IT security of financial entities and ensuring that the financial sector in the EU is able to stay resilient in the event of a severe operational disruption. DORA applies to all financial institutions in the EU. Traditional financial entities, such as banks, investment firms, insurers and credit institutions, and non-traditional entities, like crypto-asset service providers and crowdfunding platforms, are all within scope. Under DORA, financial institutions will be subject to new requirements on matters such as risk management and third-party risk management, incident management and reporting, and resilience testing.

Notably, DORA also applies to some entities typically excluded from financial regulations. This includes, for example, third-party service providers that supply financial firms with ICT systems and services, such as cloud service providers and data centres. DORA adopts a risk-based approach regarding third-party service providers, with service providers that support more relevant functions or those considered as critical to financial entities, being subject to more stringent rules.

DORA entered into force on January 16, 2023, and will apply as of January 17, 2025. EU regulators that oversee the financial system are still finalizing certain key steps required for the adequate implementation of DORA, including drafting regulatory technical standards and implementing technical standards that covered entities must implement. These standards are expected to be finalized in 2024.

Data Act

The Data Act, which will become applicable on September 12, 2025, was designed to ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible. The focus of this law is on reinforcing access to data and data portability by allowing connected device users to gain access to, and share with third parties, data generated by connected devices (e.g., smart devices). The Data Act also grants public sector bodies the authority to access and use data held by private companies in circumstances of high public interest, such as natural disasters, subject to specific conditions.

DEVELOPMENTS IN THE UK

In addition to AI, as discussed above, there are several legislative developments on the horizon for 2024 in the UK.

Online Safety Act

The Online Safety Act (OSA) came into effect in October 2023, with Ofcom as the regulator responsible for ensuring compliance with the OSA. It imposes obligations on online platforms, such as social media providers, that allow users to generate, upload and/or share content and search engines,

and aims to protect children from online harm, while empowering adults with more choices regarding what they see online. For example, the OSA requires that organisations remove illegal content quickly or prevent it from appearing in the first place and prevent children from accessing harmful and age-inappropriate content. During 2024, Ofcom is expected to finalise certain guidance and codes of practice, whilst releasing new drafts on how in-scope organisations can comply with their obligations under OSA. The guidance and codes of practices are based on the following three phases, as set out in the Act: (i) illegal harms and duties; (ii) child safety, pornography and the protection of woman and girls; and (iii) transparency, user empowerment and other duties. A summary of the OSA can be found here.

UK Data Protection and Digital Information Bill

In March 2023, the Data Protection and Digital Information (No. 2) (Bill) was introduced to the House of Commons, replacing the original Bill proposed in 2022. The Bill is intended to overhaul data protection law in the UK by departing from the GDPR in certain respects, for example by introducing a risk-based approach to assessing the impact of international data transfers, introducing a list of activities which would be considered legitimate interests of a controller by default, and increasing the fines for nuisance calls and texts. As of March 2024, the Bill is being considered by the House of Lords. It is not known whether any further changes will be made and/or whether the text will be finalised. However, subject to the UK political landscape, it is likely progress will be made towards finalising the Bill during the course of 2024.

CONCLUSION

The coming months will continue to be busy for practitioners in the field, with many interesting considerations and challenges on the horizon. Organisations operating in the EU and the UK should be aware of and continue to monitor upcoming new laws, regulator focus points and other developments and changes in this rapidly evolving area of law. With decades of experience, Hunton Andrews Kurth's Global Privacy and Cybersecurity practice is well-equipped to help organisations navigate the upcoming risks and challenges.

David Dumont
Partner, Brussels
ddumont@HuntonAK.com
+32 2 643 58 18

Sarah Pearce
Partner, London
spearce@HuntonAK.com
+44 (0) 20 7220 5722

For more information on the latest developments, visit our

Privacy and Information Security Law Blog

HUNTON
ANDREWS KURTH