The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Artificial Intelligence regulation in the UK	To date, the UK government has adopted an agile, pro-innovation, sector-based approach to AI regulation. In March 2023 the Government published the AI White Paper, setting out a cross-sectoral, principles based approach with light-touch government involvement – empowering relevant regulators to develop flexible and proportionate guidance to address the use of AI in their sectors. In spring 2024, the regulators reported on their work to date and released their 12 month forward plans – including, among others, the Information Commissioner's Office ("**ICO**"), the Financial Conduct Authority ("**FCA**") and Bank of England (including the Prudential Regulation Authority), the Competition and Markets Authority and Ofcom. The UK also hosted the first AI Safety Summit in November 2023 which produced the Bletchley Declaration signed by 28 countries (including EU, China and the US), affirming a number of principles with regard to the safe and responsible use of AI. An Artificial Intelligence Bill was brought as a private members' bill in the House of Lords, but subsequently dropped from the parliamentary agenda when the general election was called for 4 July 2024. In addition, the Trade Unions Congress has published a draft AI (Employment and Regulation) Bill concerning the use of AI for making high risk decisions affecting employees in the work place.	It remains possible that the UK may legislate for AI. The UK's general election, scheduled for 4 July 2024, may herald a shift in approach. In its response to its AI White Paper consultation, the current Conservative government identified areas requiring possible future regulation, including in relation to "highly capable general-purpose AI systems" to manage safety risks if deployed across multiple sectors. In any event, the elected government will need to continue keeping pace with rapidly developing AI technologies, and addressing risks and challenges associated with them. Technology developers and deployers should keep an eye out for new legal and regulatory updates against the UK's evolving political landscape.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Artificial Intelligence regulation in the UK (continued)	Other notable UK AI regulatory developments for organizations in the TMT sector include: — The ICO's consultation series on how aspects of data protection law should apply to the development and use of generative AI models — The Department for Science, Innovation and Technology is consulting on a two-part intervention, including a voluntary Code of Practice on AI cyber security which will be taken into a global standards development organisation for further development and sets baseline security requirements for stakeholders in the AI supply chain	
Data Protection and Digital Information Bill dropped from parliamentary agenda	The Data Protection and Digital Information Bill has been dropped from the parliamentary agenda in light of the announcement that there will be a UK general election on 4 July. The Bill was introduced in Parliament on March 8, 2023, replacing the first bill published in July 2022 which followed a public consultation on data protection law reforms, "Data: A new direction". The Bill aimed to update and simplify the UK's data protection regime, which comprises the UK General Data Protection Regulation, the Privacy and Electronic Communications Regulations, and the Data Protection Act 2018. The UK government hoped the Bill would help deliver a "Brexit dividend" by empowering data-driven activity and providing flexibility for businesses while still maintaining a high standard of protection for data subjects.	The Bill will make no further progress. Changes to the current rules governing data protection may be picked up and progressed in some form following the election, despite any change in government – for example, provisions offering flexibility, pragmatism and arguable additional opportunity for UK business – but the detail of those will depend on who exactly will be holding the pen at that point. Organizations should continue to monitor the UK political landscape for developments in this regard. You can read our briefing for further details.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Network and Information Systems Regulations 2018 **Activation date:** In force May 10, 2018.	The NIS Regulations aim to enhance the security and resilience (cyber and physical) of network and information systems that are critical for the supply of digital services and essential services in the UK. The organizations in scope are relevant digital service providers (comprising online marketplaces, online search engines, and cloud computing services) and providers of essential services (in the transport, energy, water, health, and digital infrastructure sectors). The NIS Regulations are derived from the EU's NIS Directive and seek to (1) establish a national framework equipped to manage cybersecurity incidents (including a National Cyber Security Strategy, a Computer Security Incident Response Team, and NIS- competent authorities), and (2) ensure that providers of essential services and relevant digital services are obliged to take appropriate and proportionate security measures to manage risks to their network and information systems and notify the relevant competent authority about serious incidents.	In November 2022, the government confirmed that it was moving forward with plans to update the NIS Regulations (UK NIS) as they apply to the UK. Its consultation outcome for a proposal to improve the UK's cyber resilience suggests that some, if not most, of the changes would be very similar to the EU NIS 2 Directive. Details of the reforms are yet to be published, and the extent to which they will be picked up by new government post-election remains unclear. In addition, in December 2023, the government launched a consultation for views on a separate proposed regulation to improve the security and resilience of data infrastructure, including data centres. In the consultation, the government called for views on whether data centres owned and operated by cloud or managed service providers should continue to be covered under the "Relevant Digital Service Provider" category in the NIS Regulations or brought within scope of this proposed new framework. Organizations should continue to monitor the UK political landscape for developments in this regard.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Product Security and Telecommunications Infrastructure Act (PSTIA) 2022 **and** **Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations (PSTIRs) 2023** **Activation date:** December 6, 2022 (Royal Assent), regime applies from April 29, 2024.	The Product Security and Telecommunications Act 2022 and Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (together, the "regime") raise the bar for the safety and cybersecurity of consumer, connectable devices (aligning the UK with EU cyber resilience). The regime applies from April 29, 2024 and places greater responsibility on manufacturers, importers and distributors. A product may meet the definition of a UK consumer connectable product even if it is solely aimed at business customers, e.g. if identical products have been made available to UK consumers by another distributor.	It is vital that manufacturers, distributors and importers of consumer connectable products are aware of the requirements, implement such requirements where applicable, and that relevant obligations are flowed down through supply chain contracts. Impacted products include: smartphones, wearable tech, cameras, home automation, IoT base stations/hubs, alarm systems, smart TVs, speakers and toys. Please read our briefing for further details.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Digital Markets, Competition and Consumers Bill **Activation date:** May 24, 2024 (Royal Assent).	The Digital Markets, Competition and Consumers Act 2024 introduces a wide-ranging new competition regime for digital markets, which will put the Competition and Markets Authority ("**CMA**") at the heart of the UK government's policy to regulate large digital platforms, providing for a proactive and interventionist regulatory regime — similar to the regulation of financial institutions and utilities — for some of the major big tech companies. The Act contains substantial reforms to UK competition law more generally, which will impact all sectors, not just digital markets. The CMA's enforcement powers to intervene in anti-competitive conduct are expanded, and reforms proposed to the UK's merger control regime introduce new ways in which the CMA can intervene in M&A deals. Importantly, the Act provides the CMA with the explicit ability to intervene in conduct that takes place outside the UK and to review M&A deals that have a very limited impact on the UK economy. Finally, the CMA has a new suite of tools to enforce consumer law, including the ability to impose fines of up to 10% of global turnover on companies that break the law. This means that the Act substantially strengthens the role and powers of the CMA for the future.	The Act bears many of the hallmarks of the FCA's supervisory regime for financial institutions. For example, the Act creates a senior manager regime whereby a senior manager within a regulated company can be required to take responsibility for compliance with the Act — a fundamental change in role for the CMA and its new DMU and a substantial change in the way in which digital platforms are regulated in the UK. The need to comply with investigations is ever more important as the penalties for failure to comply with, for example, information requirements will result in potentially very substantial fines of up to 1% of annual global turnover or 5% of daily global turnover, which can be imposed on businesses both in and outside the UK. The merger-control-related changes enable the CMA to continue to focus on digital markets, where it has recently prohibited a number of global deals. The CMA's new "teeth" in relation to consumer protection law will require businesses to take compliance much more seriously — as they have done with regard to UK competition and privacy laws. Please listen to our DMCC podcast series for further details.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Automated Vehicles Act **Activation date:** May 20, 2024.	The Automated Vehicles Act became law in May 2024. The law prioritises road safety, expecting to reduce the number of accidents caused by human error. It mandates that autonomous vehicles must be as safe as human drivers and pass strict safety checks. This could significantly lower incidents caused by drink driving, speeding, fatigue, and distraction. Among other things, the Act: — sets up a licensing system for self-driving vehicles and introduces the concept of an 'authorised self-driving entity' who will hold legal responsibility; — defines the 'user-in-charge', their liability, and conditions for immunity; — grants powers to stop and seize automated vehicles and introduces 'automated vehicle incident inspectors' to determine the cause of incidents; and — lets the Secretary of State decide which words or symbols can only be used for self-driving cars that are allowed on UK roads - cars that are not allowed to self-drive cannot use these special words or symbols in their marketing (this is to stop misleading ads)	The success of this Act depends on the introduction of additional laws. These laws will make it clearer how self-driving technologies can be used from 2026 onwards. Further regulatory work is expected in 2024-25: consultations on regulations against deceptive marketing will start later this year. Work on digitising traffic orders will begin in autumn, with the goal of implementing the law by spring 2025. Initial work on the Safety Principles Statement will also start this year, with consultations planned for 2025. Detailed rules on authorisation, operator licensing, and in-use regulation will be developed later. Please read our briefing for further details.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Online Safety Act **Activation date:** October 26, 2023 (Royal Assent).	The Online Safety Act 2023 became law in October 2023 and will come into force on a phased basis. The Act imposes duties of care on providers of services that host user-generated content and search engines. The duties of care include requirements to: — undertake illegal content risk assessments — remove illegal content — use age verification to ensure that users of sites publishing or hosting pornography are at least 18 years old — undertake separate risk assessments in respect of services accessed by children and to protect children's online safety — operate systems and processes that allow affected persons to report illegal content	Service providers with a large user base will have the most obligations. Fines of up to £18m or 10% of qualifying revenue (whichever is greater) will be imposed for compliance failures. Ofcom will also be able to impose "business disruption measures" to stop payment providers, advertisers and internet service providers working with a site, preventing it from generating money or being accessed from the UK. Secondary legislation and guidance by Ofcom, the Act's regulator, is required before the Act can fully come into force. Illegal content duties are currently expected to be in force by the end of 2024, followed by child safety duties in 2025 and additional duties in late 2025/2026. In-scope businesses should closely monitor Ofcom's activities in respect of online safety over the coming year, and respond to consultations on codes of practice and guidance, as relevant.

*Last updated June 2024

View the details of the contacts for this region

The roadmap continues ...

United Kingdom

Legislation	Summary of scope	Impact
Online Safety Act (continued) **Activation date:** October 26, 2023 (Royal Assent).	Providers of user-to-user services that are categorised as Category 1 services (on the basis of user numbers and functionalities) will also be subject to enhanced duties. These include: — taking down material that breaches their own terms of service (so if those terms ban certain types of legal but harmful content, they will be required to take that type of content down) — offering adult users the option of verifying their identity — giving adult users the ability to block people who have not verified their identity — providing tools for adult users to choose whether or not they see legal but harmful content — protecting content of democratic importance and journalistic content	

*Last updated June 2024

View the details of the contacts for this region

Our contacts

APAC countries

Rhys McWhirter
APAC Technology Lead
T: +852 2186 4969
M: +852 6415 1739
rhysmcwhirter@eversheds-sutherland.com

Frankie Tam
Partner
T: +852 2186 4919
M: +852 9252 5819
frankietam@eversheds-sutherland.com

European Union

Marie McGinley
International Head of Technology Sector
T: +35 3 16 44 14 57
M: +35 386 170 6507
mariemcginley@eversheds-sutherland.ie

Olaf Van Haperen
European TMT Sector Lead
T: +31 1 02 48 80 58
M: +31 6 17 45 62 99
olafvanhaperen@eversheds-sutherland.com

Middle East

Geraldine Ahern
Partner
T: +97 12 494 3632
M: +97 15 022 05 983
geraldineahern@eversheds-sutherland.com

Nasser Ali Khasawneh
Global Head of TMT & AI
T: +97 1 43 89 70 03
M: +97 1 50 65 53 198
nasseralikhasawneh@eversheds-sutherland.com

continued ...

*Last updated June 2024

Our contacts continued

United Kingdom

Paula Barrett
Global Co-Head of Data Privacy & Cyber Security
T: +44 20 7919 4634
M: +44 777 575 7958
paulabarrett@eversheds-sutherland.com

Philip James
Partner
T: +44 207 919 0700
M: +44 788 423 3723
philipjames@eversheds-sutherland.com

United States

Rachel Reid
Partner
T: +1 404 853 8134
rachelreid@eversheds-sutherland.com

Mary Jane Wilson-Bilik
Partner
T: +1 202 383 0660
M: +1 202 302 4988
mjwilson-bilik@eversheds-sutherland.com

*Last updated June 2024