King & Spalding

Client Alert

Corporate

MARCH 11, 2025

For more information, contact:

Eve-Christie Vermynck
+ 44 20 3929 5335
evermynck@kslaw.com

Amy Levin
+44 20 7551 7526
alevin@kslaw.com

Kim Roberts
+44 20 7551 2133
kroberts@kslaw.com

Aadam Sattar
+44 203 929 5348
asattar@kslaw.com

Alex Gradinaru
+44 203 929 5361
agradinaru@kslaw.com

Kassi Burns
+1 214 764 4428
kburns@kslaw.com

King & Spalding

London
8 Bishopsgate
London, EC2N 4BQ
United Kingdom
T. +44 20 7551 7500

EU & UK AI Round-up

The first EU & UK AI Round-up, published on 15 January 2025, discussed the important regulatory updates affecting the AI ecosystem in both the EU and the UK that occurred towards the end of 2024. Notably since that update, the first parts of the EU AI Act came into effect on 2 February 2025. These requirements prohibit AI practices that are deemed to pose an unacceptable level of risk (of which there are eight categories specified in the EU AI Act) and require organisations to ensure a sufficient level of AI literacy among staff operating or using AI systems. The previous AI Round-up also discussed the second draft of the General-Purpose AI Code of Practice. This was to be followed by a third draft which was due on 17 February, but publication was delayed and is now expected later this month or in early April ahead of the 2 May deadline for the final version.

Developments in the AI space globally continue to gather pace in early 2025, particularly in the lead up to, and now following the AI Action Summit (10 – 11 February) in Paris. For instance, the UK government announced on 14 February that it will rebrand the AI Safety Institute to the AI Security Institute, switching the focus of the institute to national security concerns posed by AI. Additionally, data protection authorities from the UK, Ireland, France, South Korea, and Australia issued a joint statement on building trustworthy data governance frameworks for AI. The signatories pledged to ensure that AI training data is processed according to respective national privacy legislation and underscored the importance of cultivating public trust and addressing privacy concerns associated with AI.

This edition of the AI Round-up discusses the following major legal and regulatory updates:

1. European Commission Publishes Draft Guidelines on Prohibited AI Practices

2. European Commission Publishes Draft Guidelines on AI System Definition

3. Paris AI Action Summit: Global Collaboration on AI Innovation and Governance
4. CNIL Publishes AI Guidance on EU GDPR Compliance
5. Withdraws EU AI Liability Directive Draft
6. ICO Responds to UK Government's AI Opportunities Action Plan
7. UK Government Publishes International AI Safety Report
8. UK Government Publishes New AI Cybersecurity Code of Practice and Guide
9. Treasury Committee Launches Inquiry into AI in Financial Services
10. Data (Use and Access) Bill Updated with AI Provisions

EUROPEAN COMMISSION PUBLISHES DRAFT GUIDELINES ON PROHIBITED AI PRACTICES

On 4 February 2025, the European Commission ("**EC**") released the first draft of its much awaited guidelines on prohibited AI practices ("**First Guidelines**"). Whilst not legally binding, these First Guidelines aim to promote consistent application of the EU AI Act by clarifying the types of AI practices prohibited under the EU AI Act, including by providing examples for context.

The prohibitions in the EU AI Act relate to the placing on the market, the putting into service, or the use of specific AI systems. AI tools that are at risk of being caught by the prohibitions would likely be those typically used public bodies, governments and law enforcement agencies, however developers through-out the AI value chain will also need to be wary of the limits of their innovation and the technologies they design and place on the market. We highlight the following two prohibitions as most relevant to businesses:

- ***Social Scoring***. The use of AI for classifying people based on their personality traits or behaviour which leads to detrimental or unfavourable treatment is banned. The First Guidelines explain that AI must simply play "an important role" in the social scoring, and so some human intervention does not mean an AI system will not be caught by this rule. The example is provided of a private credit agency using an AI system to "determine the creditworthiness of people and deciding whether an individual should obtain a loan for housing based on unrelated personal characteristics."
- ***Emotional recognition***. An AI system that can perform such a function in the workplace or in an educational setting is banned (except if used for medical or safety reasons, e.g. deploying a digital assistant in the workplace for measuring anxiety based on stress levels so that the employer can determine if use by a worker of a particularly dangerous machine or chemical would be a hazard).

EUROPEAN COMMISSION PUBLISHES DRAFT GUIDELINES ON AI SYSTEM DEFINITION

On 6 February 2025, the EC published another set of draft guidelines, this time intended to explain the practical application of the definition of an 'AI system' under the EU AI Act ("**Second Guidelines**"). The Second Guidelines delve into the seven main elements that constitute an AI system as defined in the EU AI Act as follows: *'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*.

Below is a summary of insights related to the more distinguishing features of an AI system as opposed to other traditional computer systems:

- ***Adaptiveness***: this refers to self-learning capabilities, allowing the behaviour of the system to change while in use. The new behaviour of the adapted system may produce different results from the previous system for the same inputs.
- ***Capability to infer***: this is arguably the most distinguishing feature of an AI system from traditional computer systems; it is broader than simply the ability to derive outputs from given inputs. It is the derivation of outputs during the building phase through AI techniques that enable inferencing.
- ***Outputs***: this means the ability to generate outputs like predictions, content, recommendations, and decisions through handling complex relationships and patterns in data. AI systems can generally generate more nuanced outputs than other systems, for example, by leveraging patterns learned during training or by using expert-defined rules to make decisions, offering more sophisticated reasoning in structured environments.

The Second Guidelines note that it is not necessary for all elements of the definition to be present throughout all stages of an AI system's lifecycle (pre-deployment / building and post-deployment / use phase) for a system to qualify as an AI system. Also given the risk-based approach and classification system of the EU AI Act, most AI tools, even if they qualify as AI systems will not be subject to any regulatory requirements.

Given the variety and diversity of AI systems, the Second Guidelines do not provide an exhaustive list of all potential AI systems. Every system should be assessed on a case-by-case basis to determine whether it constitutes an "AI system" under the EU AI Act. Despite this guidance, doubts remain regarding the appropriateness of the EU AI Act's definition and whether it raises more questions than it answers due to the difficulty in drawing a boundary around what constitutes an AI system.

In relation to both the First Guidelines and Second Guidelines, the EC will review the drafts and will consider input from various stakeholders, including interpretations from the Court of Justice of the European Union, following which the EC will decide to amend (or withdraw) these draft guidelines.

PARIS AI ACTION SUMMIT: GLOBAL COLLABORATION ON AI INNOVATION AND GOVERNANCE

The AI Action Summit ("**Summit**"), held in Paris from 10-11 February 2025, brought together government leaders and industry stakeholders to discuss AI development, investment, governance and regulation. Key takeaways from the Summit are:

1. ***A move towards deregulation***: Both US Vice President Vance and European Commission President von der Leyen made statements signalling a shift towards deregulating AI and prioritising innovation. For more information on the AI Liability Directive, see below.
2. ***The Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet***: The Statement set out key priorities and actions aimed at promoting diversity, accessibility, openness, and inclusivity in AI. It was signed by over 70 participating nations, including the EU, China, India, Japan, Australia, and Canada. However, both the US and UK declined to sign the Statement, with the UK claiming the statement lacked clarity and did not adequately address national security risks, and the US viewing the statement as the continuation of burdensome regulations and obligations placed on US tech companies.
3. ***Significant investment pledges***: Von der Leyen announced €10 billion (US$10.4 billion) worth of investment in EU "AI factories" and plans to raise €200 billion (US$208 billion) for AI investment across Europe. This follow US

President Trump's January 2025 pledge of US$ 500 billion for the "Stargate" project, which is dedicated to building AI infrastructure and led by major tech giants.

4. ***AI Excellence Centre in Paris***: On 27 February 2025, the World Economic Forum ("**WEF**") announced the launch of the European Centre for AI Excellence ("**CAIE**"). Located in Paris, the CAIE will join the WEF's Fourth Industrial Revolution Network, a group of global centres designed to maximise the societal benefits of technology. The CAIE will be the first AI-specific centre within the network and will have the mission of promoting AI research and policy across Europe, facilitating EU AI research collaboration, fostering AI start-ups, and organizing training programs and events for AI industry leaders.

Following this third instalment of the global AI summit, the fourth will be hosted by India as announced at the Paris summit by Prime Minister Narendra Modi.

CNIL PUBLISHES AI GUIDANCE ON EU GDPR COMPLIANCE

On 7 February 2025, the French Data Protection Authority ("**CNIL**") released two important recommendations focusing on AI and EU GDPR compliance ("**CNIL Guidelines**"). The CNIL Guidelines specifically address the challenges of informing data subjects and facilitating individuals' rights in the context of AI systems. The CNIL's recommendations were shaped by a public consultation involving various stakeholders, ensuring alignment with real-world applications of AI.

The CNIL's key recommendations are:

1. ***Transparency***: Advocating for transparency in AI data processing, recommending that information notices regarding training data sources indicate general categories rather than specific sources.
2. ***Data subject rights***: Advising on clear mechanisms for responding to requests for data correction, including the use of version control systems and filtering techniques.
3. ***Data minimisation***: Proposing tailored approaches for ensuring data minimization and retention in AI technologies.
4. ***Privacy by design***: Emphasising the importance of incorporating privacy by design principles in AI systems.
5. ***Anonymization and pseudonymization***: Suggesting consideration of these techniques as alternatives to re-training, particularly in scenarios involving data scraping.

Businesses will likely welcome the CNIL's clarifications on the EU GDPR's applicability to their AI models' use of personal data. Further, the CNIL's recommendations should be read in tandem with the EDPB's guidance on the processing of personal data in the context of AI models (covered in the previous AI Round-up).

EUROPEAN COMMISSION WITHDRAWS EU AI LIABILITY DIRECTIVE DRAFT

On 11 February 2025, the EC announced the withdrawal of the proposed AI Liability Directive ("**Directive**") in an annex to its 2025 work programme. The Directive, proposed by the EC as far back as September 2022, was designed to harmonize non-contractual civil liability rules for damages caused by AI systems across the EU. It seeks to ensure that individuals harmed by AI receive the same level of protection as those affected by other technologies and includes provisions such as a rebuttable presumption of causality to ease the burden of proof for victims, allowing national courts to order the disclosure of evidence related to high-risk AI systems.

However, the Directive's progress has been slow, previously due to the focus on finalising the EU AI Act. There have now also been discussions about whether specific AI liability rules are necessary, given the revisions to the EU Product Liability Directive ("**Product Liability Directive**"), which now covers software and AI systems as of 8

December 2024. Under the Product Liability Directive, AI system providers (treated as manufacturers in the legislation) are liable for defects in AI systems and software that cause harm, including post-deployment. However, critics of the planned withdrawal point out there are AI harms that the Directive would have dealt with, that are otherwise not addressed by the Product Liability Directive, such as errors made, for example, by an algorithm that would lead to discriminatory output from an AI system. Despite the withdrawal plans, the Directive remains in the first reading in the European Parliament with ongoing debates and amendments being considered.

The European Parliament is expected to continue debating the Directive, with key upcoming milestones including a draft report by the rapporteur in June 2025 and potential votes in the JURI Committee and the European Parliament's plenary session in early 2026. The Directive's fate remains uncertain, with some arguing that existing product liability laws may suffice for AI-related damages, while others advocate for specific AI regulations to address unique risks such as algorithmic errors leading to discriminatory outcomes. This is certainly an interesting development given AI companies claims about the growing list of liabilities to which developers in particular are exposed.

The current version of the Directive is available here.

ICO RESPONDS TO UK GOVERNMENT'S AI OPPORTUNITIES ACTION PLAN

On 16 January 2025, UK Information Commissioner John Edwards welcomed the UK government's AI Opportunities Action Plan in a letter to the government ("**ICO Letter**"). The ICO emphasized its commitment to supporting businesses operating in the AI sector and announced a number of initiatives to strengthen the UK's AI landscape.

Key AI-relevant points from the ICO Letter are as follows:

1. **Giving business regulatory certainty on AI**: The ICO will produce a single set of rules for the development and use of AI products and will support the government in legislating the rules into a statutory Code of Practice on AI. The ICO will also support government rollout of AI in the public sector to encourage public trust in AI and improve efficiency across public services.
2. **Cutting costs for SMEs through AI**: The ICO will work on using generative AI to create tailored advice for businesses and will launch a "Data Essentials" training and assurance programme for SMEs in 2025/26.
3. **Enable innovation through the Regulatory Sandbox and Innovation Advice services**: Following recommendations in the AI Opportunities Action Plan, the ICO will seek to implement an experimentation regime to give businesses a time-limited derogation from specific regulatory requirements to test their new ideas under strict governance controls supervised by the ICO.
4. **Cut cost of engaging with multiple regulators**: The ICO will work with the UK's other digital regulators such as the Digital Regulation Cooperation Forum to promote efficiency and ease regulatory burdens. The ICO will also work with other regulators to deliver the AI and Digital Hub to provide joined-up advice to businesses, and continue to support the development of the AI Security Institute, as set out in the AI Opportunities Action Plan.

For a summary on the AI Opportunities Action Plan, please view the first AI Round-up of 2025 here.

UK GOVERNMENT PUBLISHES INTERNATIONAL AI SAFETY REPORT

In January 2025, ahead of the Summit in Paris, the UK government published the International AI Safety Report ("**AI Safety Report**"), the world's first comprehensive synthesis of current literature on the risks and capabilities of general-purpose AI systems. Following an interim publication in May 2024, the AI Safety Report, chaired by Turing-award winning computer scientist Yoshua Bengio, is the culmination of work by a diverse group of 96 AI experts to advance a shared international understanding of AI risks and AI safety.

The 300-page AI Safety Report summarises the scientific evidence on three core questions: What can general-purpose AI do (i.e., its capabilities, which are wide ranging)? What are risks associated with general-purpose AI? What mitigation techniques are there against these risks?

Key risks identified – which are categorised as either (a) arising from malicious use, (b) a result of malfunction, or (c) systemic to the technology itself – include labour market disruption, cyberattack, manipulation of public opinion, risks to privacy and a global AI research and development divide. The AI Safety Report emphasises the uncertainty surrounding the development and impact of AI, making it challenging to prioritise and mitigate risks effectively.

The AI Safety Report does not offer policy recommendations but aims to inform policymakers by summarising scientific evidence on AI safety. It underscores the need for further research into how AI systems work internally and how they can be designed to behave reliably. A critical issue for policymakers due to the pace of AI advancements is an "evidence dilemma" – balancing the need for early risk mitigation and legislation (due to potential sudden leaps in capabilities that may amplify potential harms) with the risk of acting prematurely (and ineffectively) based on limited evidence.

The UK government intends for the AI Safety Report to become the “global handbook” for AI safety. The conclusions in the AI Safety Report advocate for the need for international agreement on the development and use of general-purpose AI, given its ability to impact so many aspects of people’s lives and at an accelerating pace. The AI Safety Report is an example of how to build a shared understanding of general-purpose AI grounded in research and science which can lead to more informed policy, enabling society to reap the rewards.

UK GOVERNMENT PUBLISHES NEW AI CYBERSECURITY CODE OF PRACTICE AND GUIDE

On 31 January 2025, the Department for Science, Innovation and Technology (“**DSIT**”) published a new Code of Practice for the Cyber Security of AI (“**Code**”) and introduced an accompanying Implementation Guide (“**Guide**”). The UK government introduced the Code because it believes stakeholders in the AI supply chain require clarity on what security mechanisms they should implement to protect AI systems. The (voluntary) Code provides recommended baseline security requirements for organisations developing and using AI tools and is to be treated as an addendum to the Software Code of Practice, reflecting the DSIT’s modular approach to cybersecurity codes of practice.

The Code is structured into thirteen principles and covers five separate phases to reflect the AI lifecycle, and these are: secure design, secure development, secure deployment, secure maintenance and secure end of life. The Code focuses on AI systems, including generative AI, and sets out high-level cyber security requirements for the entire lifecycle of AI, though the DSIT acknowledges that there is currently a lack of international consensus on what constitutes the ‘AI lifecycle’. The DSIT has listed five stakeholder groups that form the AI supply chain (as those who should review and implement the Code): developers, system operators, data custodians, end-users, and affected entities – though it is important to note that a single entity may hold more than one stakeholder role.

With respect to the thirteen principles, these include: raising awareness of AI security threats; designing for security; evaluating threats; enabling human responsibility; and documenting data, models and prompts. It will be intriguing to watch how businesses grapple with the Code in light of trends such as the rise of agentic AI technology which poses significant risks to privacy and cybersecurity; the Guide briefly notes the particular dangers posed by the hacking of an agentic AI system.

Going forward, the DSIT intends to submit the Code and Guide to the European Telecommunications Standards Institute (ETSI) where it will be used as the basis for a new global standard (TS 104 223).

TREASURY COMMITTEE LAUNCHES INQUIRY INTO AI IN FINANCIAL SERVICES

On 3 February 2025, the House of Commons Treasury Committee ("**Treasury Committee**") launched a call for evidence on AI in financial services ("**Inquiry**"). The Inquiry aims to explore how the UK financial services industry can leverage AI opportunities while mitigating risks to financial stability and protecting consumers, particularly those in the vulnerable category. Figures recently published from the Bank of England show that 75% of financial services firms are already using AI, with a further 10% planning to use it over the next three years. The Treasury Committee plans to decide on areas of focus once it has received written evidence from the finance industry, AI sector, consumers and experts.

The Inquiry seeks views on the following questions, with the deadline for responses being 11 April 2025:

1. How AI is currently used in different sub-sectors of financial services and how this is likely to change over the next ten years.
2. The extent to which AI can improve productivity in financial services.
3. The risks to financial stability arising from AI and how they can be mitigated.
4. Benefits and risks to (vulnerable) consumers arising from AI.
5. How the government and financial regulators can strike the right balance between seizing opportunities and protecting consumers.

With the financial services sector contributing 8.8% of the UK's total economic output in 2023, this Inquiry highlights the need for policymakers to understand not only the use of AI in critical sectors in driving modernisation, but also the potential negative impacts on consumers and if such innovation poses a risk to financial stability.

DATA (USE AND ACCESS) BILL UPDATED WITH AI PROVISIONS

In February, the Data (Use and Access) Bill ("**Bill**"), which has reached the final stages in Parliament was subject to amendments submitted to Parliament to capture recent developments in AI. The Bill introduces several AI-specific provisions which mark the UK's first statutory departure from the EU's regulatory framework.

The first notable change to the current AI landscape is to the permitted uses of automated decision- making. Currently, data subjects have a right under the UK GDPR to not be subject to decisions based solely on automated processing, which produce legal or similarly significant effects on them. Exceptions to this general prohibition exist under the UK GDPR, but apply only in limited circumstances, if the processing is:

- necessary for entering into or performing a contract between a controller and the data subject;
- explicitly required or authorised by law; or
- explicitly consented to by the data subject.

The Bill significantly changes the current position. It provides that the general prohibition and exceptions above only apply in respect of decisions involving special categories of personal data, meaning that automated decision-making with significant effect will otherwise be permissible without the need to rely on exceptions if only non-sensitive personal data is involved. However, regardless of the type of personal data processed, the usual safeguards on the use of automated decision-making with significant effect, such as the provision of information and the right to make representations, obtain human intervention and contest the decision, will still be necessary. The proposed change to the automated decision-making regime under the UK data protection laws is one of the Bill's most controversial areas and has been met with some concern in both houses of Parliament.

Finally, the Bill defines 'scientific research', which is a special purpose that is granted various exemptions under the UK GDPR, as "any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity". This is particularly important in relation to justifying the processing of special category data under the UK GDPR and will empower organisations looking to train, develop or deploy AI tools which process personal data for scientific research.

Going forward, businesses can already consider the implications of the changes brought by the Bill, such as identifying if their business operations could benefit from the roll-out of solely automated decision-making tools, or the increased flexibility provided by the definition of 'scientific research'.

The current version of the Bill is available here.

LOOKING AHEAD

As the obligations of the EU AI Act take shape, and governments commit to further investment in AI research, development, innovation and infrastructure, the AI industry is demonstrating its ability to be a battle ground of numerous competing interests. From debates between the creative industry and technology companies, and between policymakers, civil society groups and scientists, observing how the technology evolves and how it will be regulated promises to produce many interesting discussions.

The next few months will also see the publication of the third and final drafts of the General-Purpose AI Code of Practice, and the EC is also expected to opine on the above-mentioned draft guidelines prior to finalisation. Given that the first requirements of the EU AI Act have taken effect, enforcement plans will follow suit and EU member states are in the process of designating their respective national competent authorities, e.g. the Irish government has recently announced plans for an AI bill that will regulate how the EU AI Act is enforced in Ireland.

While in the UK, plans for a government-led AI legislation, which was initially expected to be introduced by the end of 2024, have been pushed back until the summer of 2025, if a draft law proceeds at all. The UK government is likely taking a cautious approach to ensure that any proposed legislation effectively addresses the evolving landscape of AI technologies and their potential impacts on society (as discussed in the AI Safety Report). It will also provide additional time for stakeholders, including industry leaders, researchers, and policymakers, to engage in further discussions and assist in developing the legislative framework. Finally, it enables the UK government to consider international developments, such as the EU's AI Act and its enforcement, deciding on its approach to AI regulation.

The last few months have seen examples of international cooperation on AI innovation and governance but also examples of diverging priorities between various governments. It will be interesting to observe how organisations deal with these differences or fragmentation in regulation as they consider their global AI governance and compliance.