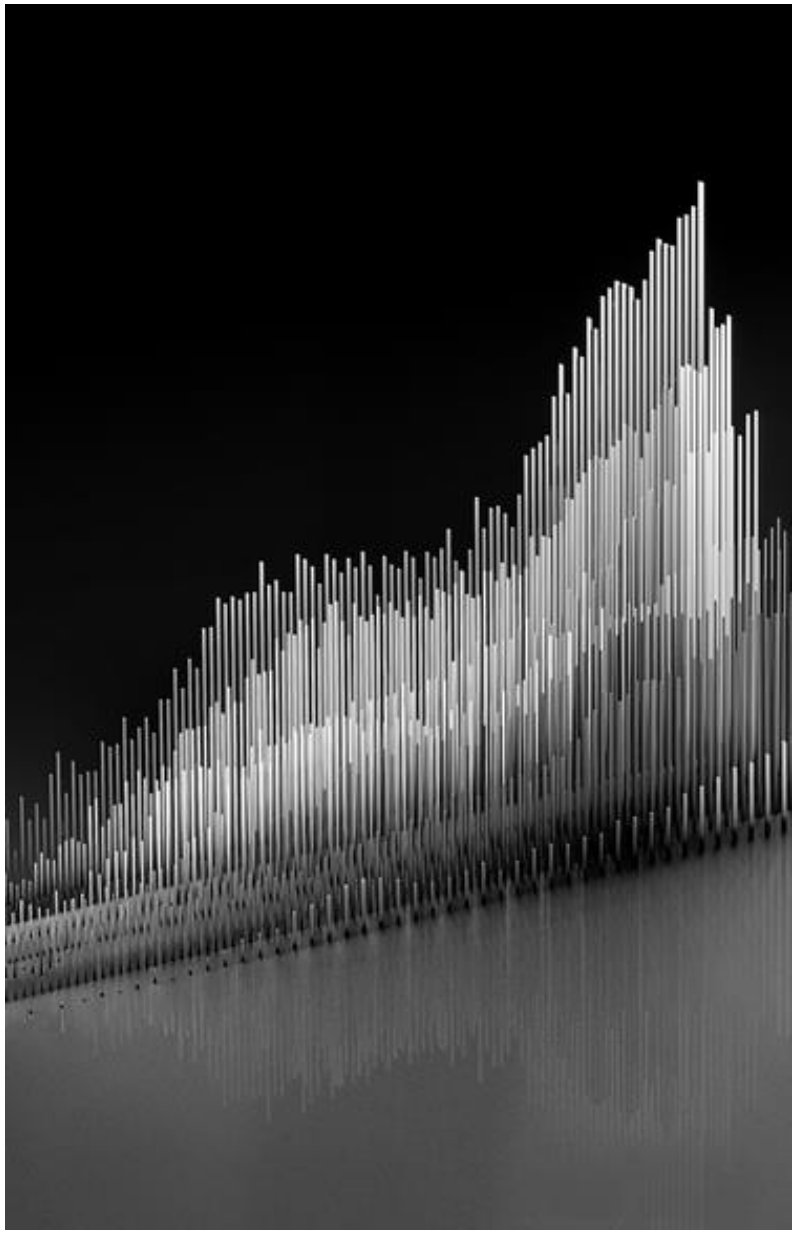
AI in financial services: deploying in compliance

Regulation: cross-perspective with the U.S. and the U.K.

Brice Henry (Partner)

7 NOVEMBER 2024



A&O SHEARMAN

ASSOCIATION EUROPE FINANCES RÉGULATIONS

Comparative regulatory approach between EU, U.S., and U.K.

	U.S.	EU	U.K.
Specific AI legislation, regulation or policy	◆ No overarching AI-specific legislation at the federal level. ◆ Significant legislative activity at the federal and individual states-level (e.g., stand-alone AI laws and comprehensive privacy laws which apply to automated processing via AI). ◆ White House Executive Order; rulemaking and guidance germane to AI from various regulatory agencies.	◆ EU AI Act. ◆ European Supervisory Authorities statements and reports. ◆ European Commission issued consultation on the use of AI in financial services.	◆ No comprehensive AI-specific legislation. ◆ U.K. AI White Paper (not binding).* ◆ Implementing the U.K.'s AI Regulatory Principles: Initial Guidance for Regulators.* ◆ U.K. financial services regulators strategic approach to regulating AI systems.*
Approach	◆ Highly fragmented legislative and regulatory landscape, involving multiple governmental and regulatory authorities at the federal and state levels.	◆ Requirements for high-risk systems fully prescribed in law by the AI Act, with lighter requirements applying to limited risk systems.	◆ Approach based on common law principles of only imposing legal and regulatory obligations where necessary to address identifiable risks. Responsibility with sectoral regulators to use existing powers to supervise appropriately.
Key principles	◆ Safe, secure and effective systems	◆ Technical robustness and safety.	◆ Safety, security, robustness.*
	◆ Explainability and transparency.	◆ Transparency.	◆ Appropriate transparency & explainability.*
	◆ Bias, algorithmic discrimination protections.	◆ Diversity, non-discrimination and fairness.	◆ Fairness, including data protection.*
	◆ Data protection & data privacy.	◆ Privacy & data governance.	
	◆ Accountability and governance.	◆ Societal and environmental well-being & accountability.	◆ Accountability and governance.*
	◆ Human alternative, consideration and fallback for automated decisions in fundamental services.	◆ Human agency and oversight.	◆ Contestability and redress.*

* Issued by or under the U.K.'s previous government. The principles noted above derive from the AI White Paper, also issued under the U.K.'s previous government.

Comparative AI regulation scope between EU, U.S., and U.K.

	U.S.	EU	U.K.
Scope	◆ The scope of implementation of existing laws and regulations applicable to AI will match the scope of those laws and regulations.	◆ The AI Act defines four main players in the AI sector – deployers, providers, importers and distributors. ◆ It also categorises AI systems according to risk. Differing standards and requirements apply to each identified category. However, most of the obligations apply to high-risk systems and the use of those systems. ◆ There are some derogations for providers and deployers of high-risk AI systems that are financial institutions subject to similar requirements under EU financial services law.	◆ The scope matches the regulatory perimeter of sectoral regulators, such as the U.K. financial regulators, who supervise the use of AI by all U.K. regulated financial firms, and who will also supervise certain third-party service providers to financial firms.
Data governance / processing	◆ Executive Order 14110 encourages regulatory agencies to use their authorities to protect consumer privacy and to consider introducing rules or clarifications and guidance as to how existing rules apply to AI systems. ◆ State laws on data protection and privacy may also apply.	◆ The AI Act provides that EU laws on data protection and privacy, such as the General Data Protection Regulation (GDPR), apply to personal data processing using AI. ◆ The AI Act does not affect the rights and obligations contained in GDPR.	◆ The U.K.'s General Data Protection Regulation (U.K. GDPR) and the Data Protection Act 2018 apply.

Targeting AI stakeholders anywhere

	U.S.	EU	U.K.
Extraterritoriality	◆ The U.S. financial regulatory scheme has various laws and regulations that have extraterritorial effect, or which apply when non-U.S. persons deal with U.S. persons. The U.S. has already imposed restrictions on AI that will have an extraterritorial effect, such as limitations on the exports of emerging technologies like AI.	◆ The AI Act will apply to providers regardless of whether the provider is physically present or established within the EU or in a third country. Third-country providers must appoint an EU representative. ◆ The AI Act will also apply to providers and deployers of AI systems that are located or established in a third country, where the output produced by the system is used in the EU. ◆ EU GDPR has an extraterritorial reach that could impact firms using or deploying AI systems.	◆ In general, the exemptions from the licensing (e.g., the U.K.'s overseas persons exclusion) and financial promotions requirements will be available to third-country financial institutions, including their use of AI systems, when dealing with U.K. wholesale (large corporate) users. Retail business with U.K. customers is generally regulated, including when the supplier is overseas. ◆ U.K. GDPR has an extraterritorial reach that could impact firms using or deploying AI systems.
Third-party providers	◆ Executive Order 14110 suggests that financial institutions should expand their typical third-party due diligence and monitoring to account for AI-specific factors. ◆ Existing guidance and proposed new rules for U.S. financial institutions apply to their management of risks arising from third-party arrangements.	◆ EU financial institutions remain responsible for any functions that are outsourced and must manage the risks arising from outsourcing critical functions. ◆ The Digital Operational Resilience Act (DORA) will strengthen that framework from 2025, with additional requirements for IT providers to financial services entities and direct regulation of critical third-party providers. ◆ EU GDPR imposes obligations on both data controllers and data processors, including where the data processing is undertaken by a third party.	◆ U.K. financial institutions remain responsible for any functions that are outsourced and must manage the risks arising from outsourcing critical functions. ◆ The U.K. recently introduced direct regulation of critical third-party service providers to financial institutions. ◆ U.K. GDPR imposes obligations on both data controllers and data processors, including where the data processing is undertaken by a third party.

Comparative sanction and remedy regimes in the EU, U.S., and U.K.

	U.S.	EU	U.K.
Fines/ enforcement	◆ No specific AI regulatory enforcement regime. However, U.S. agencies have used their existing powers to enforce laws and regulations concerning AI.	◆ Enforcement of the AI Act will be at national member state level. The AI Act sets maximum levels of fines. ◆ EU data protection authorities have already taken enforcement action against companies infringing the data protection laws while using AI.	◆ No specific AI regulatory enforcement regime. ◆ Various regulators have enforcement powers, including the financial services regulators for financial regulations, the Information Commissioner's Office (ICO) for data protection matters and the Competition and Markets Authority for antitrust matters.
Remedies	◆ No AI-specific legislation. ◆ Companies, including regulated financial institutions, are liable to consumers for any breach of applicable federal or state laws.	◆ Individuals and legal persons may lodge infringement complaints with the relevant authority under the AI Act, and the same applies under EU GDPR.	◆ No AI-specific legislation. ◆ Regulated financial institutions are liable to retail consumers for any breach of the regulatory regime. Firms are also required to have complaints handling procedures. The Financial Ombudsman Service hears retail complaints which are not resolved through such processes. ◆ Individuals and legal persons may lodge infringement complaints with the ICO under U.K. GDPR.
Liability	◆ No AI-specific liability legislation at federal level. Potential liability under various existing federal or state-level statutes.	◆ Specific legislation in the draft AI Liability Directive. ◆ The draft Directive Liability for Defective Products will replace the existing Product Liability Directive, and the scope will be extended to AI. ◆ Individuals have a right, for material or non-material damages arising from an infringement of EU GDPR, to compensation from the controller and data processor. Damages cover pecuniary and non-pecuniary losses.	◆ No AI-specific liability legislation. ◆ Liability may arise under various statutes as well as under the common law, e.g., negligence claims. A data controller and data processor may be liable to compensate an individual for losses suffered as a result of material damage or non-material damage (e.g., distress) arising from an infringement of the requirements in U.K. GDPR.

A&O SHEARMAN

A&O Shearman is an international legal practice with nearly 4,000 lawyers, including some 800 partners, working in 29 countries worldwide. A current list of A&O Shearman offices is available at aoshearman.com/global/global_coverage.

A&O Shearman means Allen Overy Shearman Sterling LLP and/or its affiliated undertakings. Allen Overy Shearman Sterling LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen Overy Shearman Sterling (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen Overy Shearman Sterling LLP (SRA number 401323) and Allen Overy Shearman Sterling (Holdings) Limited (SRA number 557139) are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen Overy Shearman Sterling LLP or a director of Allen Overy Shearman Sterling (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen Overy Shearman Sterling LLP's affiliated undertakings. A list of the members of Allen Overy Shearman Sterling LLP and of the non-members who are designated as partners, and a list of the directors of Allen Overy Shearman Sterling (Holdings) Limited, are open to inspection at our registered office at One Bishops Square, London E1 6AD.