

REGULATORY INTELLIGENCE

Data privacy and cybersecurity outlook for 2025: what financial services firms need to know

Published 15-Jan-2025 by

William Long, Francesca Blythe, Max Savoie and Eleanor Dodding, Sidley Austin

Last year saw many developments across the worldwide data privacy and cybersecurity landscape, including in the EU/UK, and this momentum shows no sign of slowing in 2025. The EU [General Data Protection Regulation](#) (GDPR) enters its seventh year in May 2025. New cybersecurity and operational resilience legislation and related guidance are coming into force to regulate new and challenging technologies, several of which will affect financial services firms.

Artificial intelligence

AI is set to continue dominating the data landscape in 2025 and beyond. In the EU, the world's first horizontal and standalone law governing the commercialisation and use of AI, known as the AI Act, came into force on August 1, 2024.

The [AI Act](#) introduced wide-ranging obligations, from conformity assessments to the development and maintenance of technical documentation (depending on the risk posed by the AI system). It applies to firms established inside and outside the EU that place AI systems in the EU market or provide an AI system whose output is intended for use in the EU.

Most of the AI Act's obligations will become enforceable as of August 2, 2026, followed by others in 2027. Some requirements, however, take effect on February 2, 2025, including those relating to AI literacy, such as ensuring a firm has sufficient skill, knowledge and understanding to enable the informed use and operation of AI systems.

It will be interesting to see how the AI Act is enforced in the year ahead. To meet these obligations, firms using AI systems should assess staff knowledge and implement a training program proportionate to employees' roles and AI exposure. For example, staff involved in interpreting AI output or conducting AI risk assessments should receive more specialised training than staff merely engaged in the use of AI.

The UK had previously taken a principles-based approach to regulating AI, but in July 2024, the UK government announced plans to regulate the most powerful AI models. It still intends to follow the proposed sectoral regulation of AI compliance by existing regulators rather than creating a new, central AI regulator.

For example, the FCA will have competence to regulate AI in the financial services industry. The regulator described its approach in an [AI Update](#) outlining its alignment with the UK government's five principles for creating a strong regulatory framework that aims to adapt to the challenges of new technology and ensure the safe and responsible deployment of AI while promoting innovation.

Regarding enforcement and guidance, the European Data Protection Board (EDPB) and national data protection authorities continue leading the way. The EDPB recently published an [opinion](#) on certain data protection aspects related to the processing of personal data in the context of AI models. The opinion addressed, among other points, the application of the legitimate interest legal basis in the context of such models and at what point data used in the models can be considered anonymous.

Firms are also starting to see enforcement action against companies using AI. In June 2024, the UK Information Commissioner's Office published a [decision](#) regarding the compliance of a technology company's AI chatbot. It assessed in detail the requirements for a data protection impact assessment when using AI, among other risk factors.

Other AI and privacy-related enforcement actions will likely follow in 2025. More generally, firms can expect greater regulatory focus on AI governance and responsible AI use, regardless of whether they are subject to specific legislation.

Firms should assess whether they are using AI, whether such systems come under the AI Act and what risks they create. This will enable compliance with obligations coming into effect from February this year. Even if not subject to the EU AI Act, firms should still consider how they should address their use of AI, including the potential introduction of an AI governance program.

EU Digital Operational Resilience Act

[DORA](#), which sets cybersecurity requirements for the financial services industry, will become enforceable from January 17, 2025. It will apply directly to most categories of EU-regulated financial services firms, including investment firms, insurers, insurance intermediaries, credit institutions, electronic money institutions, payment institutions and most types of EU-regulated asset managers. It also applies directly to financial entities authorised in the EU and critical third-party information and communication technology service providers,



THOMSON REUTERS™

© 2025 Thomson Reuters. All rights reserved.

regardless of location. DORA also applies indirectly to non-critical third-party ICT service providers (whether or not located in the EU), as in-scope financial entities must impose certain contractual requirements on such providers.

DORA imposes various obligations on financial entities, including requirements to implement an ICT risk management framework, reinforced incident management measures and provisions related to ICT third-party service providers, including contractual and oversight requirements.

The European supervisory authorities — the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) — published a [joint final report](#) in July 2024 on draft technical standards for ICT subcontracting. The standards address the classification of ICT-related incidents, materiality thresholds and detailed reporting of major incidents; contractual arrangements for ICT services supporting critical and important functions; and ICT risk management tools, methods, processes and policies.

Firms should consider whether they are in-scope of DORA and, if so, take action to comply with third-party ICT risk management and contractual requirements.

Operational resilience in the UK

While DORA is not a UK law, certain categories of regulated financial firms in the UK are subject to Financial Conduct Authority (FCA) rules on operational resilience under [chapter 15A](#) of the Senior Management Arrangements, Systems and Controls sourcebook and, for firms authorised by the Prudential Regulation Authority (PRA), the PRA's Supervisory Statement Operational Resilience: Impact tolerances for important business services ([SS1/21](#)). These set out requirements to identify, map, test and enhance important business services to withstand disruption. The deadline for compliance is March 31, 2025.

In-scope firms must do the following:

- Identify each "important business service."
- Set impact tolerances for each important business service (i.e., the maximum tolerable level of disruption to such service).
- Complete mapping and scenario testing.
- Update internal policies and procedures.
- Prepare a communication strategy to "act quickly and effectively to reduce the anticipated harm caused by operational disruptions."

This is not a "once and done" exercise and should be embedded in a firm's culture, the FCA has said.

Similarly to DORA, the UK [Financial Services and Markets Act 2023](#) introduced a new regulatory regime for the designation and direct supervision of some critical third-party service providers. While the concepts are broadly analogous to DORA, its designation criteria and regulatory scope differ in several important respects. Firms providing critical services to financial firms in the EU and the UK should consider these separately.

Other UK privacy and cybersecurity legislative developments

The UK government [announced](#) plans in July 2024 to introduce a new [Cyber Security and Resilience Bill](#) designed to strengthen UK defences against cyber-attacks and protect critical infrastructure.

An accompanying briefing note suggested the bill would update the UK's cyber regulatory framework by:

- Expanding the scope of current regulation (i.e., the UK [Network and Information Security \(NIS\) Regulations 2018](#)) to cover "more digital services and supply chains" and better align with the expanded scope of the EU's [NIS 2 Directive](#).
- Giving further power to regulators to ensure measures are being implemented.
- Mandating increased incident reporting to provide a better picture of the threat landscape and cyber-attacks.

Observers expect the bill to be introduced to parliament in 2025, and firms should continue monitoring its progress to determine its scope and any corresponding obligations.

It was expected that 2024 would see the introduction of the UK Data Protection and Digital Information Bill as part of the UK government's approach to reforming data protection laws and moving away from the GDPR. The DPDI Bill was not completed before the 2024 General Election and is no longer progressing.

The UK has since introduced the [Data \(Use and Access\) Bill](#), which contemplates similar but less extensive reforms. Importantly, the bill targets data-sharing and non-personal data more generally, drawing parallels to the EU approach found in the Data Act and the Financial Data Access regulation, which aims to create an open finance system. The bill is at the report stage in the House of Lords, and firms should monitor its progress in 2025.

(William Long, Francesca Blythe, Max Savoie and Eleanor Dodding, [Sidley Austin](#))

[Complaints Procedure](#)

Produced by Thomson Reuters Accelus Regulatory Intelligence

16-Jan-2025



THOMSON REUTERS™

© 2025 Thomson Reuters. All rights reserved.