The UK Data (Use and Access) Act 2025: implications for financial services

Published 30-Jul-2025 by
Francesca Blythe, Eleanor Dodding and Paida Manhambara, Sidley Austin

The new UK Data (Use and Access) Act 2025 came into force on June 19. Applying in phases through June 2026, the Act will reform, in part, how the UK regulates personal and non-personal data.

The legislation is a cornerstone of the UK government's post-Brexit strategy to position the UK as an international tech and innovation hub. It does not specifically target financial services firms, but will apply to personal and non-personal data processed by in-scope entities, including those subject to the UK General Data Protection Regulation (UK GDPR).

Given the sector's deep reliance on data, whether for compliance, risk management, client service and/or product innovation, firms should closely review the Act to assess their compliance obligations. The Act introduces various new obligations aimed at improving data accessibility, security and public trust.

This article highlights the updates which will be of most relevance to firms.

UK GDPR

While the Act is not a wholesale overhaul of the UK GDPR, it introduces meaningful amendments in several key areas. For example:

- International transfers: The Act introduces a new, more flexible test to replace the "essentially equivalent" standard for assessing third-country adequacy. The secretary of state and data exporters can now approve international transfers where the destination country's protections are "not materially lower" than those in the UK.
- Legitimate interests: The Act sets out a list of "recognised legitimate interests" that obviate the need for the firm to conduct a balancing test (i.e., a legitimate interest assessment) provided that the processing is necessary. These include, for example, processing necessary for crime prevention and safeguarding national security. Additionally, certain processing activities, such as direct marketing, intra-group data sharing and network/information security, are now explicitly incorporated into the Act (whereas previously only mentioned in the GDPR's non-binding recitals) and, in turn, it is presumed these activities will be easier to justify as a legitimate interest, though still requiring an assessment.
- Data subject access requests (DSARs): The Act potentially streamlines the efforts expected of firms when responding to DSARs, making it clear that only "reasonable and proportionate" searches are required. It also clarifies that the response deadline clock pauses when a controller needs additional information from the requester.
- Automated decision-making: The Act relaxes automated decision-making rules. Under the prior UK framework, individuals had a right not to be subject to decisions based solely on automated processing, including profiling, where such decisions produced legal or similarly significant effects. Under the act, controllers can now use automated decision-making in most circumstances, as long as they ensure transparency, offer human review and allow individuals the opportunity to challenge outcomes. Automated decision-making involving special category personal data, such as health information, remains tightly restricted.

Firms operating across the UK and the EU should consider the potential regulatory divergence introduced by the Act, particularly in conducting transfer impact assessments for EU/UK transfers. They should also determine whether to apply the EU standard uniformly or to split the assessment between the EU and the UK.

ePrivacy law

The law aligns fines under the UK Privacy and Electronic Communications Regulations, which govern areas such as cookies and direct marketing, to align them with the UK GDPR (i.e., up to £17.5 million or 4% of global turnover). In addition, the dropping of "low-risk" cookies, such as those used for security and certain analytics, will be permitted without explicit consent, provided users have an opportunity to opt out. This may help streamline firms' cookie notices, although divergence from EU requirements may still complicate compliance for cross-border operations.

Complaints procedure

The Act requires firms to implement a clear internal complaints process that includes acknowledging complaints within a 30-day deadline and responding to them "without undue delay," explaining what actions have been taken. Firms should ensure their internal governance protocols and complaint processes are up-to-date to achieve these timeframes. Many of the above requirements commence within two to six months of the law coming into force. As such, firms should prioritise reviewing these provisions to determine if compliance actions are necessary.

Smart data schemes

The Act creates a framework to empower the secretary of state to establish sector-specific "smart data schemes." The framework has been compared to the GDPR's "right to data portability," albeit broader in scope. Unlike the GDPR, which is limited to personal data, the smart data framework extends to non-personal data and information related to goods, services or digital content.

The primary objective of the smart data scheme framework is to build upon the success of open banking, which allows customers to share financial information from their bank to third parties. This should increase competitiveness, reduce costs and provide opportunities for innovation in the UK. It is projected to contribute £10 billion to the UK economy.[1]

Based on the Smart Data Roadmap published by the previous Conservative government, the priority sectors for smart data schemes were banking, finance, energy and road fuels, telecommunications and transport. Retail and home-buying were considered areas of interest. It remains to be seen whether the Labour government will maintain these priorities or adopt a different approach.

The Act is primarily an enabling framework, with the detailed rules and obligations of the smart data schemes to be implemented through secondary legislation. The Act may require firms to:

- Provide customer and/or business data at customers' request, either directly or to third-party services.
- Produce, collect or retain customer and/or business data.
- Make changes to customer data, including rectification of inaccuracies.
- Use specified facilities or services, including dashboards, other electronic communications or application programming interfaces.
- Implement complaint-handling procedures.

The Act also permits the Treasury to require or enable the Financial Conduct Authority (FCA) to develop "interface rules" to support open finance, such as using prescribed digital interfaces and compliance with technical standards. The FCA is further empowered to impose additional directions if firms are non-compliant, collect fees/levies linked to smart data schemes and coordinate with other regulators to supervise and oversee implementation.

Firms will need to consider their data lifecycle management, including storage, portability, sharing protocols and liability for onward transfers. Where firms rely on third-party vendors or data analytics services, they may need to ensure these providers comply with any FCA-prescribed interfaces and standards.

The smart data schemes may create challenges for firms with existing data-sharing models. Many firms have developed bespoke data architectures, legacy IT systems and contractual frameworks to address existing data-sharing obligations. Such legacy systems may not readily align with future FCA-mandated standard interfaces and specifications. Firms will need to ensure that data-sharing practices are transparent and explainable, particularly where automated decision-making is involved, even under relaxed rules. This may necessitate updates to internal governance frameworks and enhanced cross-functional coordination. Maintaining public trust in data usage is a key component of the Act and should guide smart data implementation.

Opportunities and risks

While there are challenges in addressing compliance with the Act, firms may view it as an opportunity to develop the next generation of services through secure, interoperable data use. UK Finance has said smart access schemes could "reduce fraud, improve financial wellbeing, widen access to credit, deliver greater choice in payments and help enable reusable digital identities." Firms that adapt early may find themselves well-positioned in the evolving open finance landscape when discussions begin on how to prioritise and implement this new scheme.

Nevertheless, integration of smart data schemes may be costly. Additionally, the regulatory burden for non-compliance remains high, especially as the enforcement powers of the Information Commissioner's Office (ICO) have been strengthened. The FCA's forthcoming interface standards are expected to impose new technical and compliance burdens.

Practical next steps

The practical impact of certain obligations (e.g., smart data schemes) remains to be seen, given the need for further secondary legislation to provide granular detail, and firms should monitor related developments closely. Other obligations, in particular those amending requirements under UK GDPR, should be prioritised by firms during the next 12 months as the Act is phased in, with firms considering how this affects alignment across EU and UK markets (where applicable).

Despite imposing new compliance obligations, which many can view as a compliance burden, the Act represents a strategic opportunity for firms in an ever-evolving, data-driven business landscape. While the Act does not revolutionise the existing UK GDPR framework, it introduces a targeted data-use regime in one of the most data-reliant sectors of the UK economy. It also attempts to streamline some of the elements of UK GDPR compliance, such as cookies.

(Francesca Blythe, Eleanor Dodding and Paida Manhambara, Sidley Austin)

Complaints Procedure