Digital Regulation Cooperation Forum

DRCF Insights: Smart Data Frameworks

An International Comparative Analysis and Strategic Considerations

The research findings presented in this report are the work of British Academy Research Fellows seconded into the DRCF for 2025/26. These findings do not represent the views of any of the DRCF member regulators and should not be interpreted as such. They do not represent a statement or indication of the DRCF members' regulatory policies.

Publication date: 26 March 2026

CMA Competition & Markets Authority · Ofcom · ico. Information Commissioner's Office · FCA Financial Conduct Authority

Contents

1. Executive Summary 3

1.1 Implementation Models 3

1.2 Potential Insights and Considerations 4

2. UK's Smart Data Approach 6

2.1 Legislative Foundation: The Data (Use and Access) Act 2025 6

2.2 Building on the Open Banking Precedent 7

3. An International Review of Smart Data Implementation Models 8

3.1 Regulator-Mandated 8

3.2 Market-Facilitated 17

3.3 Public Infrastructure-Led 26

3.4 Hybrid and Transitioning 31

4. Analysis 37

4.1 Models of Governance and Regulation 37

4.2 The Role of Standards and Interoperability 38

4.3 Consumer Awareness and Consent Journey 39

4.4 Economic and Social Impact 41

5. Considerations for Smart Data in the UK 42

5.1 Designing a Fit-for-Purpose Governance Body 42

5.2 A Framework for Prioritisation, Phasing and Customisation 42

5.3 Fostering Interoperability and a Unified Framework 43

5.4 Mitigating Key Risks: Liability, Costs, Incentives, Security, and Potential Unintended Consequences 43

6. Conclusion 45

1. Executive Summary

This report provides an international review of Smart Data initiatives, offering a comparative analysis of implementation models to inform strategic considerations for the UK. The UK's Data (Use and Access) Act 2025 provides the legal framework to expand on the success of Open Banking and create a cross-sectoral Smart Data economy. The central aim is to empower consumers and businesses to securely share their data with authorised third parties, based on their explicit consent.[1] This process is designed to foster innovation, competition, and the development of new services that offer greater value.[2]

1.1 Implementation Models

The international landscape of data portability reveals a clear evolution from single-sector Open Banking towards economy-wide Smart Data frameworks. However, distinct implementation models have emerged in different jurisdictions, each with inherent strengths and weaknesses. This report categorises these into three main types:

- **Regulator-Mandated:** This model is characterised by comprehensive, government-led legislation that prescribes the scope, standards, participants, and rules of engagement. Jurisdictions such as Australia, with its Consumer Data Right (CDR), and Brazil, with its Central Bank-led Open Finance framework, exemplify this approach. It provides significant legal certainty and can mandate participation, driving rapid ecosystem development. However, it risks imposing high compliance costs, regulatory rigidity, and potentially stifling innovation if not designed with flexibility.
- **Market-Facilitated:** In this model, data sharing initiatives are primarily driven by industry innovation and commercial agreements, with regulators playing a facilitative role. The United States, with its framework rooted in Section 1033 of the Dodd-Frank Act, and Japan, with its API adoption encouraged by the Financial Services Agency, are key examples. This approach fosters innovation and allows market-led solutions to emerge but can suffer from inconsistent standards, slower adoption by incumbents, and regulatory uncertainty, particularly concerning liability.
- **Public Infrastructure-Led:** This model is predicated on the existence of a foundational, government-operated digital public infrastructure (DPI), typically comprising a national data exchange layer and a universal digital identity system.[3] Estonia, with its X-Road platform, and Singapore, with its SGFinDex built upon the Singpass national digital identity, are leaders in this

[1] Readers should note that references to 'consent' and 'explicit consent' in this paper are intended in a general sense and should not be interpreted as invoking the specific legal definitions set out in UK GDPR Articles 6 or 9.
[2] Creating a Smart Data economy, https://www.gov.uk/government/collections/creating-a-smart-data-economy
[3] Digital Public Infrastructure (DPI) refers to a set of shared, secure, and interoperable digital systems designed to support broad access to public and private services. Examples include digital identity, data sharing systems, digital payments and digital post and notifications. (Digital Public Infrastructure for Digital Governments, OECD Public Governance Policy Papers No. 68, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf)

approach. This model provides a trusted, secure, and interoperable foundation that significantly reduces friction for consent and authentication, enabling unified and secure data sharing across both public and private sectors. However, this model typically demands significant upfront investment, sustained political commitment, and strong governance arrangements.

It should be noted that in some jurisdictions, a combination of the models may have been leveraged in the development of data sharing schemes. These are described in Section 3.4.

1.2 Potential Insights and Considerations

Drawing on international experiences, this report explores potential strategic avenues for the UK as it works through the implementation of the Data (Use and Access) Act 2025:

- **A Central Governance Body is essential:** Consider a central Smart Data governance body to coordinate the development of all schemes, ensuring cross-sectoral interoperability, setting common baseline standards, and providing a unified strategic vision.
- **Adopt a Phased, Use-Case-Driven Rollout:** Prioritise sectors for designation based on clear consumer benefits and alignment with wider government policy objectives, such as energy for Net Zero, allowing for an iterative and learning-based approach.
- **Tailor Implementation Models to Sectoral Contexts:** Recognise that different sectors may be better suited to different implementation models, with some lending themselves to a more Regulator-Mandated approach and others to a more Market-Facilitated one, depending on their digital maturity, market structure, and regulatory landscape. This enables sectors to progress at different paces while maintaining a unified strategic vision.
- **Ensure Interoperability and Integrate Digital Identity:** Smart Data schemes should adhere to common technical and security standards. Aligning these schemes with the UK's Digital ID and Trust Framework presents an opportunity to establish a secure, trusted, and unified consent architecture.
- **Strategic Alignment with International Standards:** Strategic alignment with leading international developments such as Gaia-X in the EU could be considered to manage international digital trade costs and maintain influence in global markets. Embedding cross-national interoperability in Smart Data schemes can safeguard market access and minimise compliance burdens for internationally active businesses.
- **Build Industry Confidence Through Predictable Rules:** Establish a clear liability framework in secondary legislation that fairly apportions responsibility between data holders and third parties. Define robust security standards and unified data breach protocols. Conduct transparent cost-benefit analyses for all new rules, actively soliciting industry feedback on implementation costs.
- **Foster Consumer Awareness and Understanding:** The success of Smart Data schemes is fundamentally linked to active consumer participation. This requires clear, accessible communication regarding the benefits and risks of data sharing, alongside initiatives to improve digital literacy, ensuring that consumers can make informed decisions and maintain control over their data.

- **Safeguard Against Potential Anti-Competitive Risks** While designed to enhance competition, there is a risk that Smart Data schemes could inadvertently facilitate easier monitoring of key competition variables, such as rivals' pricing, potentially leading to tacit collusion. Safeguards could be built into the design to monitor and mitigate such adverse market outcomes.

2. UK's Smart Data Approach

The UK's approach to Smart Data represents a strategic effort to build upon its pioneering work in Open Banking and extend the principles of consumer-centric data portability across the wider economy. This vision is underpinned by a new legislative foundation and driven by economic and social policy objectives.

2.1 Legislative Foundation: The Data (Use and Access) Act 2025

A cornerstone of the UK's Smart Data policy is the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent in June 2025.[4] This Act formalises the government's power to establish and regulate data-sharing schemes. Rather than prescribing the detailed rules for every sector, the Act empowers the Secretary of State of government departments to introduce sector-specific Smart Data schemes through secondary legislation.[5]

This legislative architecture provides the government with considerable flexibility to tailor schemes to the unique characteristics of different markets. The secondary regulations will define the operational mechanics of each scheme, including, among others: the parties required to share data (data holders); the types of customer and business data to be shared; the technical standards for data formatting, security, and transfer mechanisms; the conditions for authorising third-party providers (ATPs); provisions for fees, financial assistance, and redress mechanisms.

The Department of Business and Trade (DBT) own the centralised Smart Data policy, and are working on how to unlock the value of cross-sector Smart Data schemes, while individual government departments are exploring the value in their sector.

While this legislative architecture enables bespoke, sector-specific regulation, it also introduces the risk of regulatory and technical fragmentation. This creates a timely opportunity to examine international approaches, assessing the risks and benefits of different implementation models to help inform the UK's strategic direction.

[4] Data (Use and Access) Act 2025: data protection and privacy changes, https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes

[5] UK data reforms unpacked: the new smart data schemes and what businesses need to know, https://technologyquotient.freshfields.com/post/102kq6j/uk-data-reforms-unpacked-the-new-smart-data-schemes-and-what-businesses-need-to

2.2 Building on the Open Banking Precedent

The government's vision for Smart Data is to "replicate and extend the success of Open Banking" to other sectors of the economy.[6] Open Banking, widely regarded as a technological and economic success, serves as the foundational proof of concept for the broader Smart Data initiative. Its growth has been substantial: as of May 2025, one in five UK consumers and small businesses were actively using Open Banking services, a significant increase from just one in seventeen in March 2021.[7]

In a nutshell, the UK's Open Banking system functions through a standardised framework that allows consumers and small businesses to share their financial data (such as transaction history) and initiate payments directly from their bank accounts through regulated third-party providers. This is achieved via Application Programming Interfaces (APIs), which act as secure digital "bridges" between a bank's internal systems and external applications. To ensure security and consistency, the Open Banking Standard was created, which dictates the technical specifications, security profiles, and customer experience guidelines that all participating institutions must follow.

The UK Open Banking system operates under the Regulator-Mandated model. Its foundation was established by the Competition and Markets Authority (CMA) in 2017 following a market investigation that found a lack of competition in retail banking. To remedy this, the CMA issued a legally binding "Order" that mandated the nine largest UK banks (the CMA9) to fund and create the Open Banking Implementation Entity (OBIE).

Building on Open Banking as a prototype, the government aims to develop a world-leading Smart Data economy defined as an interoperable cross-sector ecosystem that empowers consumers and businesses, ultimately aiming to turbocharge competition, innovation and growth. As with Open Banking, the central mechanism to achieve this is the secure sharing of customer data, at the customer's request, with authorised third parties who can then use that data to provide innovative and personalised services.[8] The government's "Smart Data Roadmap" identified initial priority sectors for expansion, including finance, energy, and telecoms, with retail and home buying also noted as sectors of interest.[9]

---

[6] Developing an energy smart data scheme, https://assets.publishing.service.gov.uk/media/68809addf2ecaeb756d0e288/smart-data-government-response.pdf

[7] OBL Impact Report 7: open banking delivers real-world impact as adoption accelerates year-on-year, https://www.openbanking.org.uk/insights/obl-impact-report-7-open-banking-delivers-real-world-impact-as-adoption-accelerates-year-on-year/

[8] Developing an energy smart data scheme, https://assets.publishing.service.gov.uk/media/68809addf2ecaeb756d0e288/smart-data-government-response.pdf

[9] The Smart Data Roadmap - Action the government is taking in 2024 to 2025, https://assets.publishing.service.gov.uk/media/66190f98679e9c8d921dfe44/smart-data-roadmap-action-the-government-is-taking-in-2024-to-2025.pdf

3. An International Review of Smart Data Implementation Models

To inform the UK's approach to Smart Data implementation, this section offers an analysis of Smart Data equivalent data-sharing frameworks in key international jurisdictions, based on secondary research. Each jurisdiction's approach is examined consistently, focusing on its legal framework, implementation model, and an assessment of its successes and challenges.

3.1 Regulator-Mandated

The following jurisdictions fall primarily into the regulator mandated model of implementation.

3.1.1 Australia

3.1.1.1 Regulatory Framework

Australia has one of the most comprehensive and legally defined data-sharing frameworks in the world, known as the Consumer Data Right (CDR). The legal basis for the CDR is established under the Competition and Consumer Act 2010. Notably, the framework was designed from the outset to be economy-wide, with a mechanism for the responsible Minister (advised by the Treasury) to designate new sectors over time through legislative instruments.[10] This provides a clear, predictable, and legally robust foundation for expanding data portability across the Australian economy.

3.1.1.2 Implementation Model and Active Schemes

The Australian model is a highly structured, regulator-mandated "top-down" system.

- **Active Schemes:** The CDR was first implemented in the banking sector in July 2020, where it is commonly referred to as Open Banking. It has since been expanded to the energy sector and is being progressively rolled out to non-bank lending.[11]

  A landmark reform in August 2024 introduced "action initiation" (or "write access"), which significantly expands the CDR's scope beyond read-only data sharing. This enables consumers to instruct accredited third parties to initiate actions on their behalf, such as making payments, switching providers, or opening and closing accounts.[12]
- **Role of Regulators:** The governance of the CDR is shared across four key government bodies, creating a multi-agency oversight structure:[13]

[10] Consumer Data Right, https://treasury.gov.au/policy-topics/economy/consumer-data-right
[11] Consumer Data Right - Rollout, https://www.cdr.gov.au/rollout
[12] Australia plans 'reset' of its Consumer Data Right regime, https://www.pinsentmasons.com/out-law/analysis/australia-plans-reset-consumer-data-right-regime
[13] Consumer Data Right, https://treasury.gov.au/policy-topics/economy/consumer-data-right

- **The Treasury:** Leads overall policy development, programme delivery, the creation of CDR Rules, and advises the government on sectoral designations.
- **Australian Competition and Consumer Commission (ACCC):** Acts as the primary regulator for accreditation and compliance across sectors. The ACCC is responsible for accrediting data recipients, managing the public CDR register of participants, ensuring compliance with the rules, and taking enforcement action where necessary.
- **Office of the Australian Information Commissioner (OAIC):** Regulates privacy and confidentiality under the CDR. It handles complaints and notifications of CDR data breaches.
- **Data Standards Body (DSB):** Responsible for developing and maintaining technical and consumer experience standards that all participants must adhere to.

- **Accreditation:** Third parties wishing to receive consumer data must undergo a rigorous accreditation process with the ACCC to become an **Accredited Data Recipient (ADR)**.[14]
- **Consent:** The framework operates on an explicit, opt-in consent model. Consumers must provide their express consent to an ADR to collect specific data for a clearly defined purpose and for a limited period.[15]
  - **Explicit and Informed Consent:** Before any data is shared, an ADR must obtain a consumer's express consent. The ADR is required to clearly present, via their website or app, exactly what data will be shared, how it will be used, who will have access to it, and the duration of the consent.[16]
    Granular Control: Consumers have the right to choose which specific types of data they wish to share.
  - **Time-Limited Consent:** Consent is not indefinite. Consumers must specify the period for which data can be shared, with a maximum duration of 12 months.
  - **Right to Withdraw:** Consumers must be informed that they can withdraw their consent at any time and be provided with clear instructions on how to do so.
  - **CDR Receipt:** After giving consent, the consumer must be provided with a "CDR receipt" that details the consent provided and the data holders from which data has been collected.
  - **Privacy Safeguards:** The consent process is protected by 13 specific legally binding privacy safeguards, which are regulated by the OAIC.[17]

[14] Consumer Data Right participants, https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-participants
[15] Your rights, Consumer Data Right, https://www.cdr.gov.au/your-rights; Consent - The basis for collecting and using CDR data, https://www.oaic.gov.au/__data/assets/pdf_file/0012/10245/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data-v2.0.pdf
[16] Legal obligations for data recipients, https://www.cdr.gov.au/for-providers/legal-obligations-data-recipients
[17] Consumer Data Right Privacy Safeguard Guidelines, https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines

3.1.1.3 Successes and Challenges

- **Successes:** The CDR established a secure, legally certain, and comprehensive framework for economy-wide data sharing. The clear roles of the regulators, binding standards, and robust privacy safeguards provide a high degree of trust and predictability for participants. The recent expansion to include *action initiation*, which allows a consumer to grant a service provider permission to perform actions on their behalf, positions the CDR as one of the leading data portability regimes globally.[18]
- **Challenges:** The implementation of the CDR has faced challenges, most notably *high compliance costs* for data holders. A 2023 independent review commissioned by the Treasury found that costs substantially exceeded initial estimates, driven by the complexity of the technical standards, the need for significant investment in legacy system upgrades, and the pace of regulatory change. Stakeholders commented on the lack of transparent cost-benefit analysis when introducing new rules. Furthermore, the ecosystem has struggled with *data quality* issues and *lower-than-expected consumer consent success rates*, which have acted as a barrier to the development of compelling and widely adopted consumer use cases.[19]

  A 2024 report by the Australian Banking Association (ABA) and Accenture, based on a strategic review of the first four years of the CDR, revealed several additional challenges. Uptake remains low, with only 0.31% of Australian customers reportedly using CDR products.[20] It also noted a lack of compelling or innovative use cases and low consumer awareness of CDR-enabled solutions.[21]

3.1.2 Brazil

3.1.2.1 Regulatory Framework

Brazil's Open Finance initiative is defined and directed by the country's primary financial regulators: the **Central Bank of Brazil (BCB)** and the **National Monetary Council (CMN)**. The framework is a regulatory mandate, and it operates in full compliance with Brazil's comprehensive **General Data Protection Law (LGPD)**, which provides the foundational privacy and data-sharing rights. This approach grants the central bank significant authority and agility in shaping the ecosystem.[22]

3.1.2.2 Implementation Model and Active Schemes

Brazil has pursued a regulator-led, mandatory, and phased implementation model that has allowed the ecosystem to scale quickly while expanding in scope.

---

[18] Statutory Review of the Consumer Data Right, https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf
[19] Consumer Data Right Compliance Costs Review Report, https://treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf
[20] Consumer Data Right Strategic Review, July 2024, https://www.ausbanking.org.au/wp-content/uploads/2024/07/CDR-Strategic-Review_July-2024.pdf
[21] Four Years in: Lessons for New Zealand from Australia's CDR Experience, https://www.russellmcveagh.com/insights-news/four-years-in-lessons-for-new-zealand-from-australias-cdr-experience/
[22] Open Finance - Banco Central do Brasil, https://www.bcb.gov.br/en/financialstability/open_finance

- **Active Schemes:** The initiative began as Open Banking and has officially transitioned to a broader **Open Finance** framework. The implementation was rolled out in four distinct phases between early 2021 and mid-2024.[23]
    - Phase 1 (Early 2021): Sharing of public data on financial products and services.
    - Phase 2 (Mid 2021): Sharing of customer-consented personal financial data.
    - Phase 3 (Late 2021–Early 2023): Initiation of payment transactions. This phase is integrated with Brazil's instant payment system, **Pix**.
    - Phase 4 (Early 2023–April 2024): Expansion to a full Open Finance scope, including data on insurance, pensions, and investments.
- **Role of Regulators:**
    - The **BCB**'s role is to foster a competitive financial system by setting the rules for Open Finance, performing supervisory and regulatory functions, and balancing the promotion of innovation with the need to ensure prudential soundness and data protection.[24]
    - **CMN:** The CMN co-regulates financial policies alongside BCB.
    - **National Data Protection Authority (ANPD):** While the BCB and CMN lead the Open Finance framework, the ANPD is responsible for enforcing Brazil's LGPD, which provides the foundational privacy and data-sharing rights that underpin the Open Finance framework.
- **Accreditation:** Participation is mandatory for Brazil's largest financial and payment institutions.[25] Other institutions licensed by the BCB can participate on a voluntary basis. This mandatory participation for major players was crucial for achieving mass adoption.

  Once an institution is part of the framework, most data and service sharing with other participants does not require formal bilateral agreements, as interactions are governed by the overarching rules set by the BCB and the CMN.[26] Foreign institutions wishing to participate must incorporate a local entity in Brazil and fulfill the same authorization requirements as any local institution.[27]

[23] An Open Banking (and Open Finance) Transformation in Brazil, https://luxhub.com/from-regulation-to-revolution-brazil-open-banking-finance-transformation/
[24] Open Finance - Banco Central do Brasil, https://www.bcb.gov.br/en/financialstability/open_finance
[25] Those in regulatory Segments 1 and 2.
[26] Regulation on Open Banking, Joint Resolution No. 1 of May 4th, 2020, https://www.bcb.gov.br/content/config/Documents/Open_Banking_CMN_BCB_Joint_Resolution_1_2020.pdf
[27] What are the requirements to obtain authorization in your jurisdiction? Global Financial Services Regulatory Guide, https://resourcehub.bakermckenzie.com/en/resources/global-financial-services-regulatory-guide/latin-america/brazil/topics/what-are-the-requirements-to-obtain-authorization-in-your-jurisdiction

- **Consent:** The consent process must be explicit, informed, and unequivocal. It follows a mandatory three-step journey for the customer: **Consent**, **Authentication**, and **Confirmation**. Customers can revoke their consent at any time.[28]

3.1.2.3 Successes and Challenges

- **Successes:** Brazil's Open Finance framework succeeded in scale and adoption. By 2024, the ecosystem had onboarded over 940 institutions, served 40 million customers, processed over 100 billion API calls, and managed over 60 million active consents.[29] A main driver of this success has been the clear, phased regulatory direction from the regulators and the strong synergy with the Pix instant payment system, which created immediate, tangible use cases for consumers and businesses.[30] The framework has also been credited with improving credit assessment for individuals in Brazil's large informal economy, thereby promoting financial inclusion.[31]

- **Challenges:** Primary challenges have been technical and operational. Traditional financial institutions have faced a significant burden in upgrading legacy IT systems to comply with the demanding Open Finance requirements. Ensuring API standardisation and interoperability across hundreds of diverse participants remains a complex task. As the ecosystem grows, ensuring robust data security and privacy, and managing the increased liquidity risks associated with faster deposit movements, are ongoing priorities for the BCB.[32]

  Notably, Brazil Open Finance encountered a significant issue in scheme governance.[33] It was noted that consumer consent forms were written by financial institutions in such a way that enables them to share and sell consumer data to firms outside the financial sector. This has had a severe impact on consumer trust and continued participation, as well as leading to significant cases of fraud. This observation demonstrates that Open Finance depends on **clear, meaningful consumer consent** and **strong scheme governance**. Poorly designed consent frameworks and unclear rules on data use can undermine trust, enable misuse and fraud, and ultimately threaten participation and the sustainability of the ecosystem.

---

[28] Open Finance - Banco Central do Brasil, https://www.bcb.gov.br/en/financialstability/open_finance
[29] Open Finance Brasil: A Case Study on Raidiam's Role in Secure Financial Data Sharing, https://www.raidiam.com/case-studies/open-finance-brasil
[30] An Open Banking (and Open Finance) Transformation in Brazil, https://luxhub.com/from-regulation-to-revolution-brazil-open-banking-finance-transformation/
[31] Success in Open Finance Requires Trust – Lessons from Brazil, https://www.cgap.org/blog/success-in-open-finance-requires-trust-lessons-brazil; Banking on Open Finance to Advance Financial Inclusion: Lessons from Brazil, https://www.cgap.org/research/podcast/banking-on-open-finance-to-advance-financial-inclusion-lessons-brazil
[32] Open Banking Evolution in Brazil: Transforming the Financial Landscape, https://docs.secureauth.com/ciam/en/open-banking-evolution-in-brazil–transforming-the-financial-landscape.html
[33] Risco de venda de dados do open finance preocupa bancos, https://valor.globo.com/financas/noticia/2025/10/06/risco-de-venda-de-dados-do-open-finance-preocupa-bancos.ghtml

3.1.3 European Union and Gaia-X

3.1.3.1 Regulatory Framework

The EU's framework for data sharing in finance is built on two key pieces of legislation: the **revised Payment Services Directive (PSD2)** and the **General Data Protection Regulation (GDPR)**. PSD2, which became applicable in January 2018, established the legal right for consumers to use **third-party providers (TPPs)** to access their payment account data and initiate payments.[34] GDPR, effective from May 2018, established a comprehensive data protection regime, including a right to data portability (Article 20), which gives data subjects the right to receive their personal data in a machine-readable format and transmit it to another provider.[35]

3.1.3.2 Implementation Model and Active Schemes

The EU model is regulator-mandated, creating a legal obligation for banks to provide access, but the implementation details vary across member states.

- **Active Schemes:** The primary active scheme is **Open Banking**, as mandated by PSD2. This covers **Account Information Services (AIS)** and **Payment Initiation Services (PIS)** for any payment account accessible online.[36] The European Commission is now exploring a broader **Open Finance** framework that would extend these principles to other financial products like insurance, pensions, and investments.[37]
- **Role of Regulators:**
    - The **European Banking Authority (EBA)** is responsible for developing the **Regulatory Technical Standards (RTS)** that supplement PSD2, most notably the RTS on Strong Customer Authentication (SCA) and Common and Secure Communication, which define the technical and security requirements for data access across the EU.
    - **National Competent Authorities (NCAs)** in each member state are responsible for overseeing and enforcing PSD2 compliance within its jurisdiction.[38]
- **Accreditation:**

---

[34] Payment Services Directive 2 and Open Banking, Policy and Guidance, UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/guidance/payment-services-directive-2-and-open-banking
[35] Art. 20 GDPR – Right to data portability - General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-20-gdpr/
[36] Payment Services Directive 2 and Open Banking, Policy and Guidance, UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/guidance/payment-services-directive-2-and-open-banking
[37] From Open Banking to Open Finance: FiDA, https://www.nortonrosefulbright.com/en-419/knowledge/publications/b029b764/from-open-banking-to-open-finance-fida
[38] PSD2, https://www.solix.com/kb/psd2; Payment Services Directive (PSD2): the European Banking Authority adopts an opinion on strong customer authentication for implementation from 14 September, https://finance.ec.europa.eu/system/files/2019-06/190621-eba-opinion-strong-customer-authentication-statement_en.pdf

- **Authorisation Body:** TPPs must be authorised by the **NCA**, such as the national central bank or financial regulator, in their home member state.
- **Authorized Entities:** Authorized entities are licensed as either an **Account Information Service Provider (AISP)** or a **Payment Initiation Service Provider (PISP)**.[39]
- **Passporting:** A key feature of the EU model is "passporting". Once a TPP is authorised by the NCA in one member state, that license can be passported across the entire European Economic Area (EEA), allowing the firm to operate in all member states without needing to seek separate authorisation in each one.[40]

- **Consent:** The interaction between PSD2 and GDPR creates a complex consent environment. TPPs must obtain explicit consent from the user to provide their service. This consent is different from explicit consent under the GDPR. It is an additional requirement of a contractual nature, but it must be understood in coherence with the GDPR and in a way that preserves its useful effect.[41,42]
  - **GDPR Standard:** To be valid under the GDPR, consent must be freely given, specific, informed, and an unambiguous indication of the individual's wishes.[43] Pre-ticked boxes or inactivity do not constitute valid consent.[44] Explicit consent must also meet this criteria, but must also be affirmed in a clear statement (whether oral or written).

3.1.3.3 Successes and Challenges

- **Successes:** PSD2 successfully created a harmonised legal framework for Open Banking across the EEA, establishing a competitive market for TPPs and driving significant innovation in financial services. It has spurred the development of new services for debt management, credit assessment, and personal financial management. The directive has successfully shifted the industry towards more secure, API-based data access.[45]
- **Challenges:** A major challenge has been the **inconsistent quality and performance of bank APIs**, which often create obstacles for TPPs and lead to poor user experience. The implementation of

[39] Understanding AIS and PIS — and how they can boost your business, https://www.mastercard.com/europe/en/news-and-trends/Insights/2022/understanding-ais-and-pis-and-how-they-can-boost-your-business.html
[40] What is 'passporting' and why does it matter? https://www.ukfinance.org.uk/sites/default/files/uploads/pdf/BQB3-What-is-passporting-and-why-does-it-matter-UKF.pdf
[41] Preparing for PSD2 and GDPR – how to develop a compliant strategy, https://www.sas.com/en_gb/insights/articles/data-management/preparing-for-psd2-and-gdpr.html
[42] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf
[43] Process personal data lawfully, https://www.edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en
[44] What are the GDPR consent requirements? https://gdpr.eu/gdpr-consent-requirements/
[45] PSD2: Taking advantage of open-banking disruption, https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption

Strong Customer Authentication (SCA) has been particularly challenging, with onerous and frequent re-authentication requirements causing high rates of customer drop-off. There is also inconsistent adoption and enforcement of the rules across member states, and TPPs face ongoing burdens like conflicting regulatory requirements between PSD2 and GDPR.[46]

3.1.3.4 The EU Data Act

The entry into full application of Regulation (EU) 2023/2854, known as the Data Act, on September 12, 2025, marks a significant milestone in the digital governance of the European Single Market. By mandating that users, both consumers and enterprises, have a legally enforceable right to access and transfer the data generated by their connected products and related services, the Regulation forces a structural redesign of data architectures across the EU.

The Data Act represents a functional expansion of the data portability right established in Article 20 of the GDPR. The GDPR's portability right was limited in three significant ways: it applied only to personal data, it required a legal basis of consent or contract, and it was technically limited to what was "technically feasible". The Data Act supplements these limiters for the IoT context. It extends rights to "users", defined broadly to include legal persons (businesses) as well as individuals.[47] This means a factory owner (a legal person) has the same statutory right to port data from their connected industrial robots as a consumer has to port data from their smart thermostat. This shift effectively turns every connected device in the EU into a potential API endpoint, accessible not just by the manufacturer, but by the user and their designated service providers. As envisaged in the UK's Smart Data approach, the EU Data Act is poised to unlock new opportunities for innovation and competition, particularly in aftermarket services.

3.1.3.5 Gaia-X and the UK's Engagement with Gaia-X

Closely related to data portability schemes, Gaia-X is a European project that establishes a federated and secure data infrastructure standard, allowing data to be shared while preserving user control over access rights and data usage. More specifically, while regulations such as the Payment Services Directive 2 (PSD2) and the EU Data Act provide the legal mandate for data sharing, Gaia-X provides the technical infrastructure and the trust framework to operationalise these mandates without compromising the security or autonomy of the participants.

At its core, Gaia-X is a political and strategic project designed to reduce Europe's dependency on non-EU technology "hyperscalers".[48] It is not a single "European cloud" but a federated system built on common standards, rules, and open-source tools. Its key principles are data sovereignty (giving users full control

[46] PSD2 in review, https://plaid.com/blog/psd2-in-review/
[47] A Game-Changer in Data Regulation: The EU Data Act unpacked, https://technologyquotient.freshfields.com/post/102j0a8/a-game-changer-in-data-regulation-the-eu-data-act-unpacked
[48] Gaia-X: the bid for a sovereign European cloud, https://www.polytechnique-insights.com/en/columns/digital/gaia-x-the-bid-for-a-sovereign-european-cloud/

over their data), transparency, and interoperability, aligned with European values.[49] Its main product is a "Trust Framework" for verifiable, machine-readable governance and compliance.[50]

Against this backdrop, the following considerations outline how the UK's Smart Data schemes could engage with Gaia-X:

- **Securing Future Data Adequacy** Although the EU's data adequacy decision for the UK was recently renewed until 2031, any future failure to maintain this status would impose "costly compliance complications" and "economic barriers" on UK firms.[51] Proactively aligning UK Smart Data technical standards with the Gaia-X Framework provides verifiable proof of the UK's commitment to European data protection values, de-risking future political decisions.

- **Economic Integration** The EU is building its future digital single market and cross-sector "data spaces" (e.g., Catena-X in automotive) on Gaia-X principles.[52] Without an interoperability bridge, UK businesses risk being locked out, facing technical and regulatory friction that will damage their competitiveness.[53]

- **Maintaining Influence** The standards and rules for Europe's future digital economy are being developed within Gaia-X working groups. Active UK engagement in these processes would help ensure that emerging standards reflect UK interests and facilitate future interoperability.[54]

In summary, strategic alignment with international standards such as Gaia-X appears important for the UK to enable seamless digital trade and maintain influence in global markets. Embedding interoperability as a core technical requirement in Smart Data schemes will safeguard market access, reduce compliance burdens for internationally active businesses, and may bring an opportunity to transform regulatory alignment into a competitive advantage for the UK economy.

[49] Gaia-X explained, https://gaia-x-hub.de/en/gaia-x-explained/; The importance of Gaia-X and the relevance of industry adopters such as T-Systems (a joint blog post with T-Systems), https://gaia-x.eu/the-importance-of-gaia-x-and-the-relevance-of-industry-adopters-such-as-t-systems-a-joint-blog-post-with-t-systems/
[50] Gaia-X Trust Framework, https://gaia-x.eu/wp-content/uploads/2024/05/An-Introduction-to-the-Gaia-X-Trust-Framework_2024-V4.pdf
[51] The European Commission renewed the UK's data adequacy decisions in December 2025, ensuring free personal data flows until December 2031. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_3059
[52] Gaia-X: the bid for a sovereign European cloud, https://www.polytechnique-insights.com/en/columns/digital/gaia-x-the-bid-for-a-sovereign-european-cloud/
[53] How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/
[54] Why join? Gaia-X: A Federated Secure Data Infrastructure, https://gaia-x.eu/join-gaia-x/why-join/

3.2 Market-Facilitated

The following jurisdictions operate data sharing schemes which primarily have evolved through industry partnerships, rather than being mandated by the government.

3.2.1 United States

3.2.1.1 Regulatory Evolution

To date, the United States has taken a market-facilitated approach to Open Banking rather than one mandated by regulators. However, at the time of writing, this approach is evolving, with the U.S. attempting to shift from reliance on private sector bilateral agreements towards a more structured, regulatory-led framework.

- **The Historical Foundation** Unlike the European Union or the UK, which implemented concrete regulatory mandates (like PSD2) early on, the U.S. has traditionally favoured a market-driven approach.
    - **Voluntary Data Sharing** Financial institutions and fintechs established their own standards for data sharing.
    - **Screen Scraping** In the absence of standardised APIs, many services relied on "screen scraping," where consumers shared their login credentials with third parties to pull data.
- **Section 1033** The legal bedrock for consumer data rights is Section 1033 of the Dodd-Frank Act (2010). This section provides that a covered entity (like a bank) must make a consumer's financial product and service information available to them upon request, subject to rules prescribed by the Consumer Financial Protection Bureau (CFPB).[55]
- **Personal Financial Data Rights (The 2024 Final Rule)** In October 2024 the Consumer Financial Protection Bureau (CFPB) released a Final Rule implementing Section 1033 of the Dodd-Frank Act, also known as the "Personal Financial Data Rights" rule.[56] It mandates the use of consumer interfaces (such as online portals), explicitly defines authorised third parties and aggregators, and promotes the use of APIs while explicitly discouraging screen scraping. It sets a phased compliance schedule based on the size of the financial entity. These dates originally ran from April 1, 2026, through April 1, 2030.
- **Regulatory Uncertainty** However, following significant legal challenges, on August 22, 2025, the CFPB issued an Advanced Notice of Proposed Rulemaking (ANPR) which signaled a

[55] The term "consumer" means an individual or an agent, trustee, or representative acting on behalf of an individual (U.S. Code § 5533 - Consumer rights to access information). https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=12-USC-567770122-149880695&term_occur=999&term_src=title:12:chapter:53:subchapter:V:part:C:section:5533

[56] Required Rulemaking on Personal Financial Data Rights - CFPB, https://www.consumerfinance.gov/personal-financial-data-rights/

"reconsideration" of the 2024 final rule.[57] The CFPB views this reconsideration as necessary to align with the "policy preferences of new leadership" and to correct "defects" in the previous regulation.[58]

- **Economic Fairness and Cost Recovery** The Bureau suggests the 2024 rule may have created an imbalance by prohibiting financial institutions ("data providers") from charging fees to cover the costs of sharing data.
- **Security and Malign Actors** The Bureau argues that the transition to digital finance has introduced "tens of thousands of malign actors" seeking to compromise data.
- **Consumer Privacy and Unwitting Disclosure** The Bureau indicates that the 2024 rule may not have sufficiently protected consumers from unwittingly licensing or selling their data.
- **Timeline** The compliance dates in the 2024 final rule have been stayed (paused) until the CFPB completes its current reconsideration process.[59] Currently, the CFPB is reviewing nearly 14,000 comments received during the comment period for the ANPR.[60]

3.2.1.2 Implementation Model and Active Schemes

The US model so far has been market-led, with data sharing occurring primarily through commercial agreements between banks and data aggregators. Historically, this has often relied on less secure methods such as "Screen Scraping", in which consumers grant consent by sharing their login credentials.

Screen Scraping is a method of data access in which a third party uses a consumer's login credentials (such as usernames and passwords) to log into the consumer's account interface, such as an online banking website, and retrieve data by accessing the information displayed on the screen as if it were the consumer.[61]

- **Active Schemes:** There is no single, government-mandated "scheme". The ecosystem consists of data aggregators (like Plaid and Finicity) that have built connections to thousands of financial institutions. If the 2024 final rule were to come into force, then data providers would have to make covered data available to consumers and authorised third parties via secure APIs, free of

[57] Personal Financial Data Rights Reconsideration, https://www.consumerfinance.gov/rules-policy/rules-under-development/personal-financial-data-rights-reconsideration/
[58] Personal Financial Data Rights Reconsideration - CFPB, https://public-inspection.federalregister.gov/2025-16139.pdf
[59] US judge blocks consumer agency's 'open banking' rules for now, https://www.reuters.com/sustainability/boards-policy-regulation/us-judge-blocks-consumer-agencys-open-banking-rules-now-2025-10-29/
[60] Personal Financial Data Rights Reconsideration, https://www.regulations.gov/document/CFPB-2025-0037-0001/comment
[61] Screen Scraping: Outdated Technology, Open Banking Is Here, https://noda.live/articles/screen-scraping-vs-open-banking

charge, and would phase out screen scraping.[62] However, as above, this rule is now being reconsidered.

- **Role of Regulators:** The CFPB is the key federal regulator responsible for implementing **Section 1033 of the Dodd-Frank Act**. The CFPB's role is to write and enforce the "Personal Financial Data Rights" rule which sets out the requirements for data providers and authorised third parties. The CFPB is also responsible for formally recognising industry standard-setting bodies to promote the development of standardised data formats.[63]
- **Authorization Model:** At present, there is no authorisation model. If the 2024 final rule comes into force, it **does not establish a government-run accreditation or licensing body** for third parties. Instead, the rule sets out criteria that a third party must satisfy to be considered an **"authorised third party"**. This involves the third party certifying that it will adhere to specific obligations regarding the secure collection, limited use, and retention of consumer data.[64]
- **Consent (under the 2024 final rule):** The 2024 final rule requires third parties to obtain express, informed consent from the consumer. This authorisation is valid for one year, after which it must be re-obtained. Consumers have the right to revoke access at any time.[65]
    - **Express and Informed Consent:** Third parties must obtain express and informed authorisation from a consumer before accessing their data. This includes providing clear disclosures about the third party, the data to be collected, and the purpose of the collection.
    - **Purpose Limitation:** Third parties are prohibited from using the data for purposes beyond what the consumer expressly authorised, such as for targeted advertising or cross-selling, without separate consent.
    - **Time-Limited Authorisation:** A consumer's authorisation is valid for a maximum of one year, after which it must be re-obtained.
    - **Right to Revoke:** Consumers have the right to revoke a third party's access at any time. The third party must make this process easy and must cease data collection and delete retained data upon revocation.
- **Consent (before the 2024 final rule):** Before the Personal Financial Data Rights rule (the 2024 final rule) takes effect (and while Screen Scraping is not fully outlawed), consumer consent was

[62] Required Rulemaking on Personal Financial Data Rights, https://www.federalregister.gov/documents/2024/11/18/2024-25079/required-rulemaking-on-personal-financial-data-rights

[63] Required Rulemaking on Personal Financial Data Rights, https://www.consumerfinance.gov/personal-financial-data-rights/

[64] Required Rulemaking on Personal Financial Data Rights, https://www.consumerfinance.gov/personal-financial-data-rights/

[65] US: CFPB Finalizes Open Banking Rule Under Section 1033: Key Takeaways for Accessing Consumer Financial Data, https://privacymatters.dlapiper.com/2024/11/cfpb-finalizes-open-banking-rule-under-section-1033-key-takeaways-for-accessing-consumer-financial-data/

managed in a legally fragile and technically invasive manner, often relying on implied rather than explicit consent. The mechanics of consent were governed by private contractual arrangements rather than public regulation. In particular, under Screen Scraping, the primary way a consumer "consented" to data sharing was by providing their bank username and password to a third-party application (such as a budgeting tool) or a data aggregator (such as Plaid).

- **Implied Permission**: By providing these credentials, the consumer gave the third party the power to "impersonate" them. The third party's software would log into the bank's website just as the user would, "scraping" the data off the screen.
- **The "All-or-Nothing" Problem**: Unlike modern APIs, screen scraping usually couldn't be "permissioned" for specific data. If you gave an app your password to see your balance, the scraper could often see everything because it had full access to the customer's online banking portal.

3.2.1.3 Successes and Challenges

- **Successes:** The market-led approach in the US so far has fostered a highly innovative and dynamic fintech sector, with data aggregators enabling a vast array of popular consumer finance applications. In addition, the market-led approach is said to offer data portability services at much lower costs than the UK's Open Banking scheme.[66]

- **Challenges:** The implementation of the Section 1033 of the Dodd-Frank Act is facing significant challenges and uncertainty. As above, the 2024 final rule was met with legal challenges from banking associations.

  Pay for access Notably, in November 2025, reports indicated that JPMorgan Chase had reached agreements with major data aggregators requiring fintechs to pay for access to customer bank data, a move that could accelerate the commercialisation of Open Banking in the U.S.

  As the 2024 final rule is reconsidered, key issues, such as whether banks may charge for secure data access and how fees should be structured, are increasingly being decided through private contracts. CFPB recently sought industry input on allowing "reasonable" fees, signalling a shift from an earlier no-fee regulatory stance.

  This approach gives large banks significant influence over the commercial terms of Open Banking. Critics warn it may entrench incumbent power and weaken the principle of consumer control over financial data.[67]

[66] DRCF interviews with industry experts.
[67] JPMorgan Chase to charge fintechs for customer data access, https://paymentexpert.com/2025/11/17/jpmorgan-chase-to-charge-fintechs-for-customer-data-access/

3.2.2 Hong Kong SAR

3.2.2.1 Regulatory Framework

Hong Kong's approach to Open Banking is guided by the **Hong Kong Monetary Authority (HKMA)**. In July 2018, the HKMA published its **Open API Framework for the Hong Kong Banking Sector**, a set of policy objectives and guidelines that encourages banks to adopt open APIs in a collaborative and phased manner.[68] It is one of the HKMA's seven "Smart Banking" initiatives.[69]

3.2.2.2 Implementation Model and Active Schemes

Hong Kong's implementation model is voluntary, bank-led, and phased, with the regulator acting as a facilitator and standard-setter rather than an enforcer.

- **Banking and Finance:** The Open API Framework has been implemented in four phases[70]:
    - Phase I (Jan 2019): Product Information (e.g., deposit rates, credit card offerings).
    - Phase II (Oct 2019): Customer Acquisition (e.g., applications for new products).
    - Phase III (from Dec 2021): Account Information (e.g., accessing account balances and transaction data).
    - Phase IV (from Dec 2021): Transactions (e.g., initiating payments and transfers).
- **Role of Regulators:** The HKMA sets the policy direction and expectations, but has adopted a decentralized approach to supervision. Banks themselves are responsible for vetting, onboarding, and monitoring the **Third-Party Service Providers (TSPs)** they partner with. The **Hong Kong Association of Banks (HKAB)**, facilitated by the HKMA and funded and formed in agreement by banks, develops key industry standards, including the **Common Baseline** for TSP onboarding and the technical standards for Phases III and IV.[71]
- **Accreditation:** Hong Kong has a decentralized, bank-led model for managing third-party access, with **no central accreditation body**. The **HKMA** sets the overall policy direction but delegates the responsibility for vetting third parties to the banks themselves.[72]
    - **Bilateral Agreements:** Third-Party Service Providers (TSPs) do not need to be authorised by the HKMA. Instead, they must enter into **bilateral commercial agreements** with each bank they wish to partner with.

---

[68] Open API Framework for the Hong Kong Banking Sector Common Baseline, https://www.hkab.org.hk/files/record/fintech/1/HKAB_-_Common_Baseline-1675853755.pdf
[69] The Next Phase of the Banking Open API Journey, https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf
[70] Open Banking in Hong Kong - DSGPay, https://www.dsgpay.com/blog/open-banking-in-hong-kong/
[71] Open API Framework for the Hong Kong Banking Sector, https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf; Open API Framework for the Hong Kong Banking Sector Common Baseline, https://www.hkab.org.hk/files/record/fintech/1/HKAB_-_Common_Baseline-1675853755.pdf
[72] Hong Kong: HKMA publishes Open API Framework, https://www.regulationtomorrow.com/asia/hong-kong-hkma-publishes-open-api-framework/

- **Bank-Led Vetting:** Each bank is responsible for conducting its own due diligence, onboarding, and ongoing monitoring of its TSP partners.[73]
- **The Common Baseline:** To streamline this process, the **HKAB** as a central entity has developed a "Common Baseline". This document provides a set of business and risk management considerations that banks use as a guide when assessing TSPs, ensuring a degree of consistency in the decentralized vetting process.

- **Consent:** Consent management is handled within the bilateral relationship between the bank, the TSP, and the customer, guided by the standards developed by the HKAB.[74]
  - **Consent Refresh:** The standards refer to a 90-day period for consent refresh as an international reference point, but banks and TSPs are encouraged to adopt a risk-based approach and adjust the period based on specific use cases.[75]
- **Other schemes:** "iAM Smart" Platform[76]

  Launched in December 2020, "iAM Smart" is a foundational piece of digital infrastructure that provides a single, digital identity for all Hong Kong Identity Card holders aged 11 and over.[77] This appears developed independently of Hong Kong's Open Banking initiative but has potential to complement and enhance it by providing a secure, user-friendly authentication mechanism for accessing financial services.
  - **Authentication:** Allows users to access different government, public, and private online services with a single identity, using biometric or PIN authentication.
  - **Digital Signing:** The "iAM Smart+" version provides a digital signing function with legal backing under the Electronic Transactions Ordinance, allowing users to handle statutory documents and procedures online.
  - **Personalised Notifications:** Users can receive personalised reminders and updates from various government services.

[73] The HKMA Open API Framework defines TSPs broadly as "partners" of banks, which can include other banks or technology firms. It does not explicitly state that a TSP must be a Hong Kong-incorporated entity.(Open API Framework for the Hong Kong Banking Sector, https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf)
[74] Consultation Conclusions on Phase III Banking Open API Standards, https://www.hkab.org.hk/files/record/fintech/2/Consultation_Conclusions_on_Phase_III_Banking_Open_API_Standards-1675854026.pdf
[75] Consultation Conclusions on Phase III Banking Open API Standards, https://www.hkab.org.hk/files/record/fintech/2/Consultation_Conclusions_on_Phase_III_Banking_Open_API_Standards-1675854026.pdf
[76] iAM Smart, https://www.iamsmart.gov.hk/en/
[77] Government launches "iAM Smart", https://www.info.gov.hk/gia/general/202012/29/P2020122900647.htm

3.2.2.3 Successes and Challenges

- **Successes:** The voluntary, phased approach has been successful in driving the initial adoption of open APIs. By 2020, over 20 participating banks had launched more than 800 open APIs for Phases I and II. The HKMA reports a high adoption rate of these Phase I and II use cases and notes over 900 registrations by third-party service providers to access these APIs, indicating strong interest from TSPs and growing use in services such as foreign-exchange, deposit-rate, and loan product comparison. Phase II APIs are intended to process applications for banking products and services and thus enable more streamlined digital onboarding, although the authority cautions that it may take time for new applications to emerge. Compared with more prescriptive open-banking regimes, the HKMA's industry-driven, phased approach is often viewed as less onerous, but publicly available evidence on relative compliance cost levels remains limited.[78]

- **Challenges:** In Hong Kong's decentralised, bank-led Open API model, each bank conducts its own onboarding and monitoring of TSPs and negotiates commercial agreements on a bilateral basis. This structure can make participation more complex and time-consuming for both TSPs and banks and makes negotiations more challenging, particularly in agreeing liability limits for data breaches and misuse. Because assessments and contracts are bank-specific, implementations and liability terms may vary across institutions, complicating the establishment of uniform, ecosystem-wide liability arrangements. While the rollout of lower-risk Phases I and II has been relatively rapid, HKMA acknowledges that moving to more complex and sensitive data-sharing in later phases will require more detailed standard-setting, interoperability work and strengthened risk management and consumer protection measures.[79]

3.2.3 Japan

3.2.3.1 Regulatory Framework

Japan's Open Banking initiative is primarily shaped by the **Revision of the Banking Act**, which came into effect in June 2018.[80] It *requires* banks to develop **open API systems** and to publicise their policies on cooperation with third parties. The **Financial Services Agency (FSA)** oversees the regime, promoting a market-driven or "organic" approach based on required development of open API systems. In this sense,

---

[78] The Next Phase of the Banking Open API Journey, https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf

[79] Hong Kong: HKMA releases plans for Phases III and IV of Open API Framework, https://www.regulationtomorrow.com/asia/hong-kong-hkma-releases-plans-for-phases-iii-and-iv-of-open-api-framework/; The Next Phase of the Banking Open API Journey, https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf; Consumer Protection Measures of Authorized Institutions in respect of Open Application Programming Interface Framework, https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20191029-1-EN/20191029-1-EN.pdf

[80] Open Banking Trends in Japan, https://www.jetro.go.jp/ext_images/australia/banners/OpenBanking_Factsheet_f.pdf

the Japanese model can also be seen as a hybrid framework: it combines a regulatory mandate for technical infrastructure with a market facilitated approach for commercial execution.

3.2.3.2 Implementation Model and Active Schemes

Building on the Revision of the Banking Act, the **commercial execution** of Japanese Open Banking is market-facilitated, with regulatory encouragement rather than a strict mandate. It relies on banks and TSPs to form partnerships and drive innovation.[81]

- **Active Schemes:** Japan does not operate a single, centrally branded open-banking scheme; instead, individual banks are developing and opening APIs to partner with fintech firms.[82] Early use cases have centred on account-information services for personal finance management and cloud-based corporate accounting, with increasing attention to payment-related use cases such as peer-to-peer payment platforms.[83]
- **Role of Regulators:**
    - **FSA:** The Financial Services Agency is the primary regulator overseeing Japan's open-banking framework. Under the Revisions of the Banking Act, banks are required to develop systems for the introduction of open APIs within a specified period, and only FSA-registered electronic payment service providers may access those APIs, although banks retain discretion over which registered providers they contract with.[84] The FSA's key functions are:
        - **Supervision:** Encouraging banks to develop open API systems and requiring them to publicise their policies on cooperation with third-party providers.[85]
        - **Registration of TPPs:** The FSA established a registration system for TPPs (known as Electronic Payment Service Providers), setting requirements for their financial soundness, system security, and data management practices.[86]

[81] "In Japan, the FSA has established an authorisation process for TPPs, introduced an obligation for banks to publish their Open APIs policies, and encouraged banks to contract with at least one TPP by 2020. The majority of Japanese banks are taking this regulatory encouragement very seriously and are on track to fulfil the 2020 deadline." Open Banking around the world, https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html
[82] The State of Opening Banking In Japan, https://www.forrester.com/apac/the-state-of-open-banking-in-japan-en/
[83] The Slow Introduction of Open Banking and APIs in Japan, https://www.frbsf.org/podcasts/pacific-exchanges/open-banking-apis-japan/
[84] Open Banking Trends in Japan, https://www.jetro.go.jp/ext_images/australia/banners/OpenBanking_Factsheet_f.pdf
[85] The State of Opening Banking In Japan, https://www.forrester.com/apac/the-state-of-open-banking-in-japan-en/
[86] Japan Open Banking Framework, https://ozoneapi.com/the-open-finance-tracker/library/japan-open-banking-framework/

    - **Promoting Transparency:** The FSA promotes transparency in banks' initiatives to enable customers to make informed choices.[87]
- **Accreditation:** As above, the **FSA** has established a registration system for third parties.[88]
    - **Registration Body:** TPPs must **register with the FSA** to operate.
    - **Registration Requirements:** To be registered, an applicant must meet several criteria, including:
        - Demonstrating a sufficient financial basis to operate the business properly.
        - Having the necessary system preparations and security measures in place.
        - Establishing a legal representative in Japan.
        - Having a clean regulatory compliance history.
- **Consent:** TPPs are required to enter into contracts with banks, which must include provisions for sharing liability and implementing security measures for user information.[89]

3.2.3.3 Successes and Challenges

- **Successes:** Japan's market-driven approach has helped cultivate a collaborative relationship between traditional banks and fintech startups, contrasting with the more 'disruptor'-oriented model often seen in the United States.[90] The FSA's encouragement and registration system have provided a degree of regulatory clarity while still allowing for flexibility and innovation. A significant number of banks have successfully opened APIs and formed partnerships.

- **Challenges:** A major challenge is the lack of a clear legal right to data portability, similar to the EU's GDPR, which means implementation remains largely voluntary and dependent on banks' willingness to cooperate. The financial system is complex and fragmented, and Japan has a high cultural preference for cash, which can slow the adoption of digital financial services. The existence of multiple, vendor-driven API standards also creates challenges for interoperability.[91]

[87] Open Banking Trends in Japan, https://www.jetro.go.jp/ext_images/australia/banners/OpenBanking_Factsheet_f.pdf
[88] Open Banking Trends in Japan, https://www.jetro.go.jp/ext_images/australia/banners/OpenBanking_Factsheet_f.pdf
[89] Open Banking in the Context of Fast Payments, https://fastpayments.worldbank.org/sites/default/files/2023-09/Open%20Banking%20and%20FPS_Final_August%2028.pdf
[90] A systemic success of the Japanese approach is the collaborative relationship between traditional banks and fintech startups, which contrasts with the "disruptor" model often seen in the United States. https://www.frbsf.org/podcasts/pacific-exchanges/open-banking-apis-japan/
[91] "This multiplicity is evident even in Japan by itself, where a handful of system vendors have created multiple standards around API infrastructure", https://www.frbsf.org/podcasts/pacific-exchanges/open-banking-apis-japan/

3.3 Public Infrastructure-Led

The following jurisdictions fall primarily into the public infrastructure led model of implementation.

3.3.1 Estonia

3.3.1.1 Regulatory Framework

Estonia's model for data sharing is not based on sector-specific 'open banking' legislation but on X-Road, a national data exchange layer.[92] Launched in 2001, X-Road is an open-source, decentralised and secure platform that underpins data exchange between public-sector and private-sector organisations.[93] The X-Road legal framework[94] enables this interoperability, mandating public sector bodies to use the platform[95] and establishing the principles for data exchange, such as the "once only" principle, where citizens only need to provide information to the state once.[96]

3.3.1.2 Implementation Model and Active Schemes

Estonia's model is public infrastructure led: the government provides the core data exchange layer as a public good, which any authorized entity may use to offer services.

- **Active Schemes:** X-Road is not a standalone 'scheme' but the enabling data-exchange infrastructure for thousands of e-services across Estonian society, underpinning services from e-tax and e-health to population, business and land registries as well as private-sector services such as banking and insurance.[97] Today it connects hundreds of public- and private-sector institutions and enterprises and supports more than 3,000 digital services.[98]

[92] X-Road® — Data Exchange, https://x-road.global/data-exchange
[93] X-Road Technology: A digital backbone of Estonia's Cyber security and DPI, https://futureshiftlabs.com/x-road-technology-a-digital-backbone-of-estonias-cyber-security-and-dpi/
[94] "Legislatively, the first version of X-Road was consulted in lockstep with Estonia's data protection authority. In parallel at the time, crucial legislation in the early 2000s made e-Identification obligatory for Estonian citizens and established digital signatures as equivalent to hand-written ones. These two legislative developments enabled X-Road's signing and logging scheme" (Jackson Dreyling and Pappel, 2022). This is further supported by other laws like the Personal Data Protection Act and the Public Information Act, which govern data possession, usage, and access rights.
[95] Estonia's data exchange lets you pay your taxes in five minutes, https://apolitical.co/solution-articles/en/data-exchange-platform-making-estonia-leader-digital-governance
[96] Case Study: Estonia's Digital Transformation Journey, https://journal.govcx.org/case-study-estonias-digital-transformation-journey/
[97] e-Estonia, https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf; X-road – Interoperability services, https://e-estonia.com/solutions/interoperability-services/x-road/
[98] X-Road Technology: A digital backbone of Estonia's Cyber security and DPI, https://futureshiftlabs.com/x-road-technology-a-digital-backbone-of-estonias-cyber-security-and-dpi/

- **Role of Regulators and Governance:** Estonia's model is unique in that it is not regulated by a specific "Smart Data" authority but is instead governed as a piece of core national digital infrastructure.
    - **Information System Authority (RIA):** The RIA at the Ministry of Economy and Communications is the government agency responsible for the development and management of the X-Road data exchange layer. The RIA acts as the X-Road operator, defining regulations, accepting new members, and operating the central components of the software.[99]
    - **Nordic Institute for Interoperability Solutions (NIIS):** In a significant evolution of governance, Estonia and Finland jointly founded NIIS in 2017. NIIS is now responsible for the central management, development, verification, and auditing of X-Road's open-source code. This collaborative, cross-border governance model ensures the sustainable and interoperable development of the core technology for all participating nations.[100]
- **Accreditation:** Estonia's X-Road does not use a separate accreditation authority; instead, participation is based on a membership model governed by the national X-Road operator (in Estonia's case, RIA), which sets rules and accepts new members.[101] To participate, an organisation (either public or private) must become a **member** of the X-Road ecosystem. The process involves:
    - **Applying for Membership:** The organisation applies to the RIA, which is responsible for accepting new members and defining the regulations of the ecosystem.
    - **Registering a Security Server:** Once approved, the member must register its "Security Server", the certified gateway that connects its internal information systems to the X-Road network. The Central Server, also operated by the RIA, maintains the definitive registry of all members and their security policies, ensuring a secure and trusted environment.[102]
- **Consent and Security:** X-Road is a data exchange layer that ensures the confidentiality and integrity of data transferred between organisations, but it does not manage end-user consent. The responsibility for managing user consent lies with the individual data sources and service consumers, which must implement their own systems or use third-party solutions to handle consent management in compliance with relevant EU and Estonian data protection laws.

---

[99] X-Road® — Implementation Models, https://x-road.global/implementation-models
[100] X-Road - Wikipedia, https://en.wikipedia.org/wiki/X-Road
[101] X-Road® — Implementation Models, https://x-road.global/implementation-models
[102] The Central Server and trust services do not have an active role in the data exchange process. Instead, the Security Server uses their services asynchronously in the background. Thanks to this, an X-Road ecosystem can remain operational for a long period of time (from hours to days depending on the configuration) without the Central Server and trust services being available. https://x-road.global/data-exchange

X-Road has a decentralised architecture in which data are exchanged directly between service consumers and providers over mutually authenticated, encrypted (mTLS) channels, without any central message broker or data store.[103] All messages are digitally signed, time-stamped and logged by Security Servers, creating an auditable and legally robust record of each data exchange.[104]

3.3.1.3 Successes and Challenges

- **Successes:** The X-Road model has been greatly successful, forming the bedrock of one of the world's most advanced digital societies.[105] By automating processes, it saves Estonians an estimated 820+ years of working time annually from just 5% of its queries, with further unmeasured efficiency gains from machine-to-machine exchange.[106] The system has proven secure and resilient, with no publicly reported major breaches despite persistent cyber threats.[107] X-Road's transparent, auditable logs have fostered trust between citizens and the state, and it has enabled cross-border data exchange, most notably with Finland.

- **Challenges:** The primary challenge of the Estonian model is its replicability. Its success is rooted in a long-term political commitment to digitalization that began in the 1990s,[108] a relatively small population, and the willingness to build foundational digital public infrastructure from the ground up. For larger economies with entrenched legacy systems and more fragmented governance structures, adopting such a comprehensive, top-down infrastructure-led approach would be a significant and long-term undertaking.

3.3.2 Singapore

3.3.2.1 Regulatory Framework

Singapore's Open Finance approach exemplifies a public-infrastructure-led model, driven by the **Monetary Authority of Singapore (MAS)** and the **Smart Nation and Digital Government Group (SNDGG)**. The framework is not based on a single prescriptive law but on a series of government initiatives that leverage a foundational national digital identity system.[109]

---

[103] X-Road® Data Exchange, https://x-road.global/data-exchange
[104] X-Road Technology Overview, https://x-road.global/x-road-technology-overview
[105] Estonia: How the X-Road paved the way to a digital society, https://www.publictechnology.net/2023/12/20/society-and-welfare/estonia-how-the-x-road-paved-the-way-to-a-digital-society
[106] How do Estonians save annually 820 years of work without much effort? https://e-estonia.com/how-save-annually-820-years-of-work/
[107] X-Road Technology: A digital backbone of Estonia's Cyber security and DPI, https://futureshiftlabs.com/x-road-technology-a-digital-backbone-of-estonias-cyber-security-and-dpi/
[108] How it all began? From Tiger Leap to digital society, https://www.educationestonia.org/tiger-leap/
[109] Singapore Financial Data Exchange (SGFinDex), https://www.mas.gov.sg/development/fintech/sgfindex

3.3.2.2 Implementation Model and Active Schemes

Singapore's Open Finance model is a joint public-private effort: the government builds and operates the core digital infrastructure while financial institutions (both public and private) connect to it as data providers and offer financial planning services that leverage the consolidated data.

- **Active Schemes:** The flagship initiative is the **Singapore Financial Data Exchange (SGFinDex)**, launched in December 2020. SGFinDex is the world's first public digital infrastructure that uses a national digital identity and centrally managed online consent system to enable individuals to consolidate their financial information.[110] It allows users to pull data from participating banks, insurers, and government agencies into a single view within their preferred financial planning application.[111]

  More broadly, the architecture of data sharing in Singapore rests on the foundation of its National Digital Identity (NDI) framework.[112] This framework consists of several key, interoperable components:

  - **Singpass**: Singapore's universal digital identity, used by approximately 97% of eligible residents (Citizens and PRs aged 15+) for secure authentication to over 2,700 services across 800+ government agencies and businesses.[113]
  - **MyInfo**: Built on Singpass, MyInfo is a consent-driven data-sharing service that allows users, after authenticating, to grant explicit consent for verified personal data from government databases to be shared via modern APIs with service providers to pre-fill application forms.[114] It functions as a national consent and data-sharing platform.[115]

- **Role of Regulators and Governance:** SGFinDex is a joint initiative led by **MAS** (the financial regulator) and **SNDGG**, with the **Government Technology Agency (GovTech)** developing the

[110] Singapore Financial Data Exchange (SGFinDex), https://www.mas.gov.sg/development/fintech/sgfindex
[111] SGFinDex, https://www.sgfindex.gov.sg/about-us
[112] National Digital Identity and Government Data Sharing in Singapore, https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report%20(abridged%20version).pdf
[113] The trusted digital identity for all Singapore residents - Singpas, https://www.developer.tech.gov.sg/assets/files/singpass-factsheet-121022.pdf; Singpass: Our trusted digital identity for secure and convenient access to services, https://www.tech.gov.sg/products-and-services/for-citizens/digital-services/singpass/
[114] National Digital Identity and Government Data Sharing in Singapore, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099300010212228518/p171592079b3e50d70a1630d5663205bf94
[115] How Singapore's national digital identity and government digital data sharing platform fosters inclusion and resilience, https://blogs.worldbank.org/en/digital-development/how-singapores-national-digital-identity-and-government-digital-data-sharing

technical infrastructure. The government owns and operates the central infrastructure, ensuring security and neutrality, while MAS regulates the participating financial institutions.[116]

- **Participation:** Participation is based on financial institutions and government agencies connecting to the central SGFinDex infrastructure. The list of participants includes major banks, insurers, and government bodies like the Central Provident Fund Board (CPF), Housing & Development Board (HDB), and the Inland Revenue Authority of Singapore (IRAS).[117] Since institutions are already regulated by MAS, no separate accreditation layer for SGFinDex participation is needed.[118]
- **Consent and Authentication:** SGFinDex is built on Singpass. Users authenticate via trusted Singpass login and provide explicit consent for each data retrieval, providing a unified, secure method across all participants.[119]
    - **Authentication via Singpass:** Singpass verifies users before connecting accounts and retrieving data, used consistently for every request to simplify the experience.
    - **User Control:** Users retain full control over their data and can revoke consent at any time.
    - **Data-Blind Infrastructure:** SGFinDex is data-blind, transmitting only encrypted data without storing any personal financial information, maximising privacy and security.

3.3.2.3 Successes and Challenges

- **Successes:** SGFinDex has been highly successful in terms of user adoption and impact. The number of users grew from 120,000 in 2021 to over 400,000 by the end of 2024.[120] The platform provides tangible benefits to consumers, allowing them to get a holistic view of their finances for better planning, from budgeting and loan management to retirement and insurance planning.[121] Singpass' trusted authentication has been crucial, enabling a seamless user experience that largely overcomes consent friction seen in other markets.[122]
- **Challenges:** Like Estonia's X-Road, Singapore's SGFinDex success relies on the prior existence and widespread adoption of public digital infrastructure, including trusted national digital

[116] Singapore Financial Data Exchange (SGFinDex), https://www.mas.gov.sg/development/fintech/sgfindex
[117] SGFinDex, https://www.sgfindex.gov.sg/about-us
[118] MAS: Behind Singapore's Smart Financial System, https://www.lseg.com/en/risk-intelligence/glossary/regulatory-compliance/mas
[119] SGFinDex, Government Technology Agency (GovTech), https://www.tech.gov.sg/products-and-services/for-citizens/digital-services/sgfindex
[120] Banks, insurers see more customers using SGFinDex for financial planning, https://www.straitstimes.com/business/banks-insurers-increasingly-see-customers-using-sgfindex-for-financial-planning
[121] Connect all your finances in one place with SGFinDex, https://www.prudential.com.sg/sgfindex
[122] SGFinDex, https://www.sgfindex.gov.sg/about-us

identity (Singpass) and data-sharing platforms (MyInfo). These represent significant long-term investments and political commitment that would be challenging to replicate quickly elsewhere.

3.4 Hybrid and Transitioning

The following jurisdictions' data sharing schemes feature a combination of the described models, rather than pursuing one explicitly.

3.4.1 India

3.4.1.1 Regulatory Framework

India has developed a unique and sophisticated public-private framework for data sharing known as the **Data Empowerment and Protection Architecture (DEPA)**.[123] DEPA is a policy framework that aims to give individuals and businesses control over their data through a consent-based sharing mechanism.[124] It is designed to be a layer of the "India Stack", a set of open APIs and digital public goods.

India Stack is a collection of open Application Programming Interfaces (APIs) and digital public goods designed to unlock the economic fundamentals of identity, data, and payments at a population scale. Often described as the "national plumbing for the Internet Age", it enables presence-less, paperless, and cashless services via a unified platform for governments and businesses.[125]

The infrastructure consists of four distinct technology layers:

- **Presenceless Layer:** Utilises Aadhaar, a biometric digital ID system, to authenticate citizens remotely and instantly.
- **Paperless Layer:** Replaces physical documents with digital records through tools like eKYC (electronic Know Your Customer), eSign, and DigiLocker.
- **Cashless Layer:** Facilitates interoperable, real-time payments between banks, fintech firms, and digital wallets, primarily through the Unified Payments Interface (UPI).
- **Consent Layer:** Manages the flow of personal data through "Account Aggregators", ensuring users maintain control and can give permission for their data to be processed.

This infrastructure has revolutionised financial inclusion in India, allowing millions of people in the informal economy to open bank accounts and settle transactions digitally.[126]

[123] Data - India Stack, https://indiastack.org/data.html
[124] Consent management puts users at the core, https://law.asia/consent-management-solutions/
[125] India Stack, https://indiastack.org/
[126] Stacking Up Financial Inclusion Gains in India, https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm

3.4.1.2 Implementation Model and Active Schemes

India's model is a hybrid, combining regulatory oversight with a decentralised, interoperable network of private entities acting as consent managers. The extensive use of India Stack further imparts features commonly associated with public infrastructure-led models.

- **Active Schemes:** The primary implementation of DEPA is the **Account Aggregator (AA) framework**, which went live in September 2021.[127] Account Aggregators are **Reserve Bank of India (RBI)** regulated entities that act as neutral "Consent Managers", facilitating the secure flow of a user's financial data between Financial Information Providers (e.g., banks, insurance companies, pension funds) and Financial Information Users (e.g., lenders, wealth managers).[128]
- **Role of Regulators:** The **RBI** is the primary regulator for the financial sector implementation of DEPA. It licenses and regulates the Account Aggregators as a special class of Non-Banking Financial Company (NBFC-AA).[129] Other sectoral regulators, like those for insurance and pensions, also participate in the ecosystem. To address operational challenges, the RBI has recently introduced a framework for Self-Regulatory Organisations (SROs) to enhance coordination and dispute resolution within the ecosystem.[130]
- **Accreditation:**
    - **Licensing Body:** The **RBI** is the sole authority for licensing participants. An authorised entity is known as an **Account Aggregator (AA)**.
    - **Licensing Process:** To operate as an AA, an entity must obtain a specific **NBFC-AA (Non-Banking Financial Company - Account Aggregator) license** from the RBI. This makes the AA a regulated entity under the direct supervision of the central bank, subject to its master directions on security, governance, and consumer protection.
- **Consent:** The Digital Personal Data Protection (DPDP) Act 2023 embeds the concept of a **consent manager** as integral to deploying the new data protection regime in the country.[131]
    - **Consent Manager Model:** The AA framework introduces a new entity called a Consent Manager (the *Account Aggregator itself*). AAs are neutral, RBI-regulated intermediaries

[127] Convenience Drives Rapid Adoption of Account Aggregators in India, https://www.cgap.org/blog/convenience-drives-rapid-adoption-of-account-aggregators-in-india
[128] Data - India Stack, https://indiastack.org/data.html
[129] A Deep Dive into RBI's Account Aggregator Framework, https://hyperverge.co/blog/account-aggregator-framework-rbi/
[130] RBI's New Account Aggregator Framework Means For Consumers, https://www.outlookmoney.com/banking/rbis-new-account-aggregator-framework-what-consumers-stand-to-gain
[131] Reconciling the Account Aggregator and Consent Manager Frameworks, https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/

that facilitate the flow of data but are "data-blind": they cannot see, store, or sell the data they handle.[132]

- **Electronic Consent Artefact:** Technically, the entire system is built on a standardised, programmable digital template for capturing user consent. This "consent artefact" is granular, allowing users to specify exactly what data to share, with whom, and for how long.[133]
- **Centralised User Control:** Consumers can approve, manage, and revoke all their consent agreements, giving them complete and ongoing control over their data.

3.4.1.3 Successes and Challenges

- **Successes:** The Account Aggregator framework has achieved phenomenal scale and user adoption. By August 2024, the framework had crossed 100 million successful consents, with an estimated 80-90 million users (8% of the adult population).[134] The number of linked accounts grew from 39 million in December 2023 to 120 million by December 2024.[135] The ecosystem includes over 155 FIPs (Financial Information Providers) and 475 FIUs (Financial Information Users).[136] This success is driven by the convenience it offers for use cases like loan applications and personal finance management, and it has significant potential to enhance **financial inclusion** for those with thin credit files.
- **Challenges:** Despite its rapid growth in user numbers, the AA ecosystem faces challenges in **consent conversion**.[137] Businesses (Financial Information Users) report low conversion rates and significant customer drop-offs during the consent process. This is often attributed to a complex user journey, technical failures in data fetching from multiple Financial Information Providers, and a lack of user understanding. While millions of consents are given, the final step of successfully retrieving and using the data for a service can often fail, directly impacting business outcomes and the user experience. This highlights a crucial gap between high-level user willingness and practical, operational success.

---

[132] Data Empowerment and Protection Architecture (DEPA), https://corpotechlegal.com/data-empowerment-and-protection-architecture-niti-aayog/; Data - India Stack, https://indiastack.org/data.html
[133] Electronic Consent Framework, https://www.dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf
[134] India's Account Aggregator Framework Crosses 100 million Consents in Three Years, https://sahamati.org.in/media-article/indias-account-aggregator-framework-crosses-100-million-consents-in-three-years/
[135] Convenience Drives Rapid Adoption of Account Aggregators in India, https://www.cgap.org/blog/convenience-drives-rapid-adoption-of-account-aggregators-in-india
[136] India's Account Aggregator Framework Crosses 100 million Consents in Three Years, https://sahamati.org.in/media-article/indias-account-aggregator-framework-crosses-100-million-consents-in-three-years/
[137] The Account Aggregator Consent Conversion Crisis, https://blog.setu.co/articles/account-aggregator-consent-conversion-crisis

For businesses looking to leverage the AA framework, key considerations include:[138]

- Technical integration: Existing systems may not support standard AA data formats or consent protocols.
- Regulatory compliance: AA-related compliance guidelines evolve alongside data protection laws like the DPDP Act.

3.4.2 United Arab Emirates

3.4.2.1 Regulatory Framework

The UAE has a unique dual regulatory landscape. "Onshore UAE" is regulated by the **Central Bank of the UAE (CBUAE)**, while two financial free zones, the **Dubai International Financial Centre (DIFC)** and the **Abu Dhabi Global Market (ADGM)**, have their own independent regulators and legal systems based on English common law.[139] While Open Banking has been market-led in both onshore UAE and the two free zones, in 2024, the CBUAE issued a comprehensive, mandatory **Open Finance Regulation** for the *onshore jurisdiction*, creating a formal, centralised framework.[140]

3.4.2.2 Implementation Model and Active Schemes

The UAE is transitioning from a fragmented, market-led approach to a centralised, regulator-mandated model for its onshore financial sector while continuing to allow a more flexible approach within the free zones.

- **Active Schemes:** Prior to the 2024 regulation, several large banks had launched their own API portals, and infrastructure providers were building a market-led ecosystem.[141] The new **Open Finance Regulation** now mandates participation for all CBUAE licensees in a phased rollout, starting with banks and insurance companies.[142] The framework covers a broad Open Finance scope, including banking and insurance products, and includes both data sharing and payment initiation.[143]
- **Role of Regulators:** The **CBUAE** is the central regulator for the onshore Open Finance Framework. It has established a new subsidiary, **Nebras Open Finance LLC**, to oversee the

[138] A Deep Dive into RBI's Account Aggregator Framework, https://hyperverge.co/blog/account-aggregator-framework-rbi/
[139] Dubai International Financial Centre - Wikipedia, https://en.wikipedia.org/wiki/Dubai_International_Financial_Centre
[140] CBUAE issues the Open Finance Regulation to ensure the soundness and efficiency of services and promote innovation and competitiveness, https://www.centralbank.ae/media/rxfeelkt/cbuaei-2.pdf, Open Finance Regulation, CBUAE Rulebook, https://rulebook.centralbank.ae/en/rulebook/open-finance-regulation-0
[141] Open Finance in the UAE: Policies and Players Powering the Shift, https://whitesight.net/open-finance-in-the-uae-policies-and-players-powering-the-shift/
[142] Open Finance Regulation, CBUAE Rulebook, https://rulebook.centralbank.ae/en/rulebook/open-finance-regulation
[143] UAE Central Bank Implements Open Finance Framework, https://www.twobirds.com/en/insights/2024/uae/uae-central-bank-implements-open-finance-framework

implementation and management of the central infrastructure.[144] This infrastructure consists of a **Trust Framework**, an **API Hub**, and **Common Infrastructural Services**.

- **Accreditation:** The UAE has a dual regulatory system, with a newly centralised framework for the "onshore" jurisdiction and separate regimes for its two international financial free zones.
    - **Onshore UAE:** The Open Finance Regulation establishes a formal licensing process.[145]
        - **Licensing Body:** CBUAE
        - **Process:** New entrants must apply for this specific license. Existing CBUAE-licensed entities, such as banks and insurers, are "deemed licensed" but must still notify the CBUAE and obtain its approval before offering Open Finance services.[146]
- **Consent:** The Open Finance Regulation establishes a centralised framework where explicit user consent is a core feature.[147]

  Such user consent must be[148]:
    - specific to the purpose for which it is provided;
    - given using a clear, objective and affirmative statement or action;
    - clear as to the duration of the consent; and
    - capable of being withdrawn.

3.4.2.3 Successes and Challenges

- **Successes:** The UAE's market-led beginnings allowed for early experimentation and the development of real-world use cases. The new CBUAE regulation provides a clear, comprehensive, and centralised framework that addresses the fragmentation of the earlier approach. By establishing a central API Hub and Trust Framework, the CBUAE is creating a regulator-led consolidated trust framework, which should accelerate secure and standardised adoption.

---

[144] UAE's Open Finance Evolution and the Rise of Embedded Finance, https://blog.brankas.com/UAE-Open-Finance-Evolution-and-the-Rise-of-Embedded-Finance%20
[145] UAE Central Bank Implements Open Finance Framework, https://www.twobirds.com/en/insights/2024/uae/uae-central-bank-implements-open-finance-framework
[146] Open Finance Providers and their Licensing, https://rulebook.centralbank.ae/en/rulebook/open-finance-providers-and-their-licensing
[147] Open Finance Regulation, CBUAE Rulebook, https://rulebook.centralbank.ae/en/rulebook/open-finance-regulation-0
[148] UAE OPEN FINANCE REGULATION - Q&AS, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2024/05/uae-open-finance-regulation.pdf

- **Challenges:** A key challenge will be the implementation of this new, ambitious framework. Onboarding all licensees, ensuring the central infrastructure is robust and scalable, and managing the transition from a market-led to a mandatory system will be a complex undertaking. Harmonizing the onshore framework with the separate regulatory environments of the DIFC and ADGM remains important.

4. Analysis

The review of individual jurisdictions reveals distinct patterns and recurring themes in the global development of Smart Data. This section summarises these findings to analyse the different models of governance, the role of standards, the critical nature of the consent experience, and economic and social impacts observed worldwide.

4.1 Models of Governance and Regulation

While the global landscape of data portability reveals a clear evolution from single-sector Open Banking towards economy-wide Smart Data frameworks, the pathways taken by different jurisdictions vary significantly. Three distinctive types of governance and regulation have emerged, each presenting a different balance of trade-offs between speed, cost, innovation, and legal certainty.

The **Regulator-Mandated (Top-Down)** model, exemplified by Australia's Consumer Data Right (CDR) and Brazil's Open Finance framework, provides the highest degree of legal certainty and can mandate participation from incumbent data holders. This approach is effective at overcoming market inertia and establishing a secure, standardised ecosystem quickly. Brazil's success in achieving substantial scale within a few years demonstrates the effectiveness of a clear, phased mandate from a strong central regulator. However, this model carries significant risks. The Australian experience serves as a cautionary tale, where a highly prescriptive, multi-regulator framework has led to high and ongoing compliance costs for industry, with participants questioning whether the benefits have justified the expense.[149] The rigidity of a top-down model can also slow down adaptation to new technologies and use cases if the rule-making process is not agile.

In contrast, the **Market-Facilitated (Bottom-Up)** model, seen in the US and Japan, prioritises innovation and flexibility. By allowing the market to develop solutions organically through commercial partnerships, this approach can foster an dynamic and innovative financial sector. However, it often suffers from a lack of standardisation, leading to a fragmented ecosystem where TPPs must build and maintain multiple bespoke integrations. This fragmentation also complicates data security, as the reliance on diverse, non-standardised connection methods like screen scraping in the US can leave personal information more vulnerable to unauthorised access compared to centralised, encrypted APIs.[150] This model also creates significant regulatory uncertainty, particularly around liability for data breaches and fraud, which can deter investment and participation from more risk-averse institutions. The ongoing legal and political challenges to the CFPB's Section 1033 Personal Financial Data Rights rule in the US

[149] "… it was evident that many participants question the cost-benefit justification of ongoing changes to CDR rules and CDR data standards, based on the very low level of usage that they observe among their customer base." Consumer Data Right Compliance Costs Review Report, https://treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf

[150] While Japan's Open Banking framework is mostly market-led, the 2018 Revision of the Banking Act obliges banks to develop open API systems, mandating secure connection methods.

highlight the instability of a framework that lacks a firm, unambiguous legislative consensus from the outset.

The third type is the **Public Infrastructure-Led** model, pioneered by relatively smaller economies, such as Estonia and Singapore. This approach reframes the challenge: instead of building a new data-sharing infrastructure for each sector, it leverages a pre-existing, trusted national Digital Public Infrastructure. The existence of Estonia's X-Road data exchange layer and Singapore's Singpass national digital identity provides a universal, secure, and interoperable foundation for data-sharing applications, whether in finance, health, or government services. This model inherently solves many of the problems other models struggle with. It creates trust by design, simplifies the user consent journey to a single, familiar mechanism, and ensures interoperability from the ground up. However, this model typically demands significant upfront investment, sustained political commitment, and strong governance arrangements.

Within this context, a robust Digital Verification Services (DVS) trust framework, as envisioned in the DUAA, could play an important role in supporting Smart Data initiatives. **Integrating DVS with Smart Data schemes** may help enable a more unified and secure user experience, similar to that seen in leading public infrastructure-led models.

4.2 The Role of Standards and Interoperability

The success of Smart Data ecosystems hinges on the quality and adoption of common technical standards. Without them, the system fragments into a collection of proprietary, costly, and inefficient point-to-point integrations. The international review shows different approaches to developing these standards. The UK's Open Banking created a dedicated, industry-funded implementation entity (the OBIE) to develop standards collaboratively. Australia established a Data Standards Body (DSB) within a government department, while Brazil's Central Bank has taken a more direct role in guiding the standard-setting process.[151]

A consistent lesson across all governance models is the critical importance of adopting internationally recognised technical and security standards. Aligning with established standards not only reduces development and compliance costs for participants but also facilitates cross-border interoperability and market access. The transition to a multi-sector Smart Data framework in the UK under the DUAA presents a particular consideration: different government departments may oversee different schemes, increasing the risk of divergent standards and fragmented implementation. Without strong central coordination, this might recreate data silos that Smart Data aims to eliminate, undermining cross-sector innovation and imposing unnecessary burdens on businesses operating in multiple sectors.

[151] "The Central Bank has determined the market standards and the technical specifications for the implementation of APIs by the participating institutions. More recently, the authority edited Normative Instruction No 130, of 22 July 2021, to publish version 3.0 of the Open Banking API manual. With this, the Central Bank seeks to ensure that data sharing between institutions takes place in an efficient and secure manner.", How Brazil regulates Open Banking, https://www.ibanet.org/how-brazil-regulates-open-banking

Beyond cross sectoral consistency, there is also a strong case for international alignment. As data portability matures globally, the ability for UK-based businesses to interoperate with international Smart Data ecosystems will become increasingly important. This is especially pertinent for firms integrated into global supply chains with cross-border operations. The UK could benefit from adopting or aligning with widely used international standards. Such alignment would not only reduce costs but also position the UK as a leader in global Smart Data interoperability.

4.3 Consumer Awareness and Consent Journey

4.3.1 Consumer Awareness and Promotion

The effectiveness of any Smart Data ecosystem is ultimately contingent upon its adoption by consumers and small businesses. While robust governance and technical interoperability provide the necessary foundation, these frameworks remain dormant unless users are both aware of their existence and understand the tangible benefits they offer. Even the most elegantly designed scheme, incorporating state-of-the-art security and seamless API integration, will fail to achieve its policy objectives if the value proposition is not clearly communicated to the public. International experience highlights this necessity; for instance, Australia's Consumer Data Right (CDR) initially faced significant challenges with consumer uptake, underscoring the importance of **active promotion and clear communication** of the benefits of consumer-driven data sharing.[152]

For individuals and SMEs, the decision to share data involves a calculation of trust and utility; therefore, fostering a high level of **data literacy** and **understanding**, and demonstrating real-world improvements in service competition or financial inclusion are essential for driving the participation required to realise the system's full potential.[153]

4.3.2 Consent and the User Experience

At the heart of each Smart Data scheme is the principle of user consent. The global experience reveals that the design and implementation of the consent journey are as important as the legal principle. For example, India's Account Aggregator (AA) framework is a notable success, achieving a scale of over 100 million consents and engaging a significant portion of the Indian population. Its design, which uses neutral "Consent Managers" that are data-blind, is a powerful model for empowering users and building trust. However, some industry practitioners noted that businesses using the framework face significant commercial challenges, including low consent conversion rates and high customer drop-off during

[152] Release of Strategic Review into roll-out of the Consumer Data Right, https://www.ausbanking.org.au/release-of-strategic-review-into-roll-out-of-the-consumer-data-right/

[153] Research demonstrates that possessing information, often described as awareness, does not automatically translate into understanding. See for example, Gu et al. (2025), Park life: the difference between having financial information and understanding it on park home owners' quality of life, *Town Planning Review*.

onboarding, pointing to potential implementation issues such as fragmentation in user consent journeys.[154]

Beyond technical friction, the integrity of the consent itself is paramount. Brazil's Open Finance experience serves as a cautionary tale regarding the misuse of consent language. In some instances, financial institutions drafted consent forms so broadly that they enabled the sharing and selling of consumer data to firms outside the financial sector. This lack of transparency led to significant cases of fraud and a severe erosion of consumer trust. More broadly, a lack of trust in the integrity of the consent can ultimately hinder adoption and undermine the overall success of a data portability scheme.

Furthermore, in the absence of robust regulatory frameworks, markets may default to practices such as Screen Scraping, in which consent is governed by private contracts rather than public standards. Under this model, a user "consents" by providing their bank username and password to a third party. This creates a dangerous "all-or-nothing" problem: because the third party is essentially impersonating the user, they often gain full access to the customer's entire online banking portal rather than just the specific data points required.

These observations highlight an important lesson: a legally compliant consent mechanism alone is insufficient. If the experience of granting consent is confusing, lengthy, or perceived as insecure, users may disengage from the process even when they are willing in principle to share their data. In such cases, the consent journey itself can become a bottleneck to adoption and overall scheme success.

The UK's experience with Open Banking may offer a blueprint for the user journey. By mandating standardised APIs and developing rigorous Customer Experience Guidelines (CEG), the UK vastly improved the user experience of granting consent.[155] This optimised journey allows users to authorise data sharing via their trusted mobile banking app using biometrics in seconds, eliminating the need for password sharing and ensuring that consent is both granular and frictionless.[156]

Singapore's SGFinDex offers another model, where the consent process is seamlessly integrated with the trusted and familiar Singpass national digital identity system, resulting in a simple, secure, and highly effective user journey. For other jurisdictions developing their Smart Data schemes, this means that the design of the consent management system and the user journey for each Smart Data scheme must be a primary focus, prioritising clarity, simplicity, security and trusworthiness to ensure that the potential economic benefits are not lost at the final hurdle of user interaction.

---

[154] The Account Aggregator Consent Conversion Crisis, https://blog.setu.co/articles/account-aggregator-consent-conversion-crisis; Workshop on Design Guidelines for Informed Consent in Account Aggregators (AAs), https://sahamati.org.in/design-guidelines-for-informed-consent-in-aa/

[155] Customer Experience Guidelines - Open Banking Standards, https://standards.openbanking.org.uk/customer-experience-guidelines/latest/

[156] Improving Customer Journeys - Open Banking, https://www.openbanking.org.uk/insights/improving-customer-journeys/

4.4 Economic and Social Impact

The evidence from mature Smart Data ecosystems demonstrates tangible economic and social benefits. In Brazil and India, Open Finance is a powerful tool for **financial inclusion**, allowing lenders to use real transaction data to assess creditworthiness for individuals and SMEs who lack a formal credit history. In Estonia, the efficiency gains from the X-Road platform are measured in the millions of working hours saved annually, representing a significant productivity boost for the entire economy. In the EU and UK, Open Banking has spurred a wave of **innovation**, creating new tools for personal financial management[157], debt advice, and streamlined lending.[158]

However, these benefits are consistently hindered by a set of recurring challenges. High **compliance costs** and the burden of keeping pace with rapid regulatory changes, as seen in Australia, can strain industry resources and deter participation. Poor **API quality**, a persistent complaint in the early years of the EU's PSD2, can render innovative services unusable and erode consumer trust.[159] **Resistance from incumbent data holders**, a key issue in market-led systems, can stifle competition and slow the pace of adoption. For them cost is also a significant consideration, as they must fund substantial compute capacity and cybersecurity infrastructure to handle large volumes of external API calls on top of aging legacy core systems.

[157] The development of tools such as personal financial management services, helps consumers gain clearer insight into their finances and enhances their ability to find more competitive market offerings in increasingly complex markets (see, e.g., Gu and Wenzel, 2014, Strategic obfuscation and consumer protection policy, *Journal of Industrial Economics*; Chioveanu et al., 2026, Firm Prominence and Price Framing, *Journal of Economic Behavior and Organization*.)

[158] Open Banking Case studies Insights, https://www.openbanking.org.uk/news/insight-type/case-studies/; For recent empirical evidence from academic research, see Babina et al., 2025, Customer Data Access and Fintech Entry: Early Evidence from Open Banking, *Journal of Financial Economics*.

[159] PSD2 in review, Plaid, https://plaid.com/blog/psd2-in-review/

5. Considerations for Smart Data in the UK

The Data (Use and Access) Act 2025 provides a flexible legislative tool, but the success of the initiative will depend on the strategic choices made in secondary legislation. This international review offers a preliminary evidence base from which to draw clear, actionable considerations. The following insights may help navigate the trade-offs between innovation, security, cost, and competition to build a leading interoperable Smart Data ecosystem.

5.1 Designing a Fit-for-Purpose Governance Body

A recurring theme from the international analysis is the critical importance of a clear and effective governance structure. The UK could establish a central **Smart Data governance body** to provide strategic oversight and ensure consistency across all schemes developed under the DUAA. This body could serve as the primary authority for:

- Setting a clear *national strategic direction* for Smart Data, with a strong focus on *cross-sector* and potentially *international* interoperability.
- Mandating a *common* set of baseline technical, security, and consumer experience *standards* to which all sectoral schemes should adhere.
- Acting as a *central* point of *coordination* between government departments, regulators, and industry to prevent the development of data silos.
- Overseeing the development and maintenance of *shared infrastructure*, such as a central directory of participants, in coordination with the DVS framework.

5.2 A Framework for Prioritisation, Phasing and Customisation

The ambition to create an economy-wide Smart Data framework is substantial. However, attempting a rollout across multiple complex sectors can lead to excessively high costs and implementation fatigue. An effective approach might be a phased rollout that builds momentum and allows for iterative learning.

A phased, use-case-driven approach to sectoral expansion through a clear public roadmap for designation could benefit the UK's approach, prioritising sectors where:

- There is a clear and compelling consumer benefit (e.g., simplified switching, better financial management).
- There is strong alignment with existing government policy objectives (e.g., using energy data to support Net Zero, or transport data to improve public services).
- The industry has a degree of technical readiness and willingness to participate.

For example, starting with the already-identified priority of the energy sector would allow the government and industry to build expertise and refine the implementation model before tackling more complex sectors.

Similarly, given the inherent strengths and weaknesses of different implementation models, the UK may consider allowing different sectors to adopt different approaches, ranging from market-led, industry-driven initiatives to more prescriptive, regulator-led frameworks, or hybrid models, depending on each sector's digital maturity, market structure, and regulatory context. For example, sectors where the market is particularly innovative and competitive may be better suited to a more market orientated approach, at least in commercial execution of a smart data scheme, whereas sectors that require greater regulatory oversight may benefit from a more prescriptive model.

This does not mean that sectors should be developed in isolation. Rather, the goal is to leverage the UK's legislative flexibility while maintaining a strong, unified strategic vision. This approach allows sectors to progress at different speeds and through different mechanisms, while still adhering to common interoperability standards and an overarching strategic framework, avoiding the rigidity of a purely economy-wide, regulatory- or market-led model.

5.3 Fostering Interoperability and a Unified Framework

The ultimate value of a Smart Data economy lies in the ability for data to flow seamlessly and securely across sectoral boundaries, enabling novel services. This may be impossible without interoperability by design. The most advanced models in this respect, seen in Estonia and Singapore, achieve this through a unified, underlying digital public infrastructure.

The UK could consider use of a common set of core technical and security standards across all future Smart Data schemes. These standards could be based on proven, international best practices. The development of Smart Data schemes may also be integrated with the **Digital Verification Services trust framework**. By leveraging the DVS for identity verification, authentication, and potentially as a backbone for the consent management system, one may build the trust and seamless user experience that has been critical to Singapore's success with Singpass.

Furthermore, as seen in the EU and Gaia-X initiatives, prioritising alignment with international standards is essential to ensure that the UK's framework remains compatible with global data ecosystems. This approach avoids the risk of technical isolation and ensures that UK businesses can compete and collaborate effectively on an international scale.

5.4 Mitigating Key Risks: Liability, Costs, Incentives, Security, and Potential Unintended Consequences

For businesses to invest and participate with confidence, the regulatory framework should be predictable, incentive compatible, and the risks manageable. The international review highlights four

key areas of concern for industry: an unclear liability framework, lack of participation incentives for data holders, unmanaged compliance costs, and the threat of data breaches.

Considerations for the UK:

- **Establish a Clear Liability Framework** The secondary legislation for each scheme may consider establishing a clear, tiered liability framework that fairly and predictably apportions responsibility for data breaches, fraud, and unauthorised transactions between data holders and authorised third parties.
- **Ensure Sustained Participation** To encourage data holders to participate and share data, the framework may consider regulatory mandates requiring participation from incumbent data holders. However, where mandatory participation alone proves insufficient to drive meaningful engagement, the framework could research and consider complementary positive incentives, including recognition schemes for compliant participants, requirements for reciprocal data access, or opportunities for new revenue streams through data sharing, to ensure sustained and voluntary commitment to the ecosystem.
- **Implement Transparent Cost-Benefit Analysis** To avoid industry friction and cost overruns, a transparent process of cost-benefit analysis for all new rules and standards may be considered. This process may actively solicit industry input on implementation costs and publicly document how this feedback has been considered in final decisions. Mechanisms to reduce compliance burden on smaller participants, such as tiered implementation timelines or support for shared infrastructure, could be considered.
- **Strengthen Security Standards and Breach Protocols** To mitigate the threat of data breaches and build consumer trust, the framework may consider establishing mandatory, high-grade security standards for all participants. This could include robust technical specifications for encryption and authentication, alongside a unified, cross-sectoral protocol for the rapid notification and coordinated management of security incidents to ensure a swift and effective response.

Finally, while there have not been significant reports of anti-competitive behaviour in existing Smart Data ecosystems, the design of these schemes must be mindful of **potential unintended consequences**. For example, if the framework allows for easy monitoring of competitors' pricing or other key variables, it could inadvertently facilitate **tacit collusion**. Therefore, safeguards could be built into the design to monitor and mitigate such adverse market outcomes, ensuring that the primary goal of enhancing competition is not undermined. [160]

[160] Smart data and price transparency schemes: discussion paper, https://assets.publishing.service.gov.uk/media/689c9f499a65499b446361f6/smart_data_and_price_transparency_schemes_discussion_paper.pdf

6. Conclusion

The international evolution of Smart Data frameworks highlights a variety of approaches, successes, and challenges. With the Data (Use and Access) Act 2025, the UK is uniquely positioned to build a leading data sharing ecosystem by combining the most effective elements from international models.

A successful rollout will depend on several strategic pillars. First, the establishment of a **central governance body** is essential to provide a unified vision and ensure cross-sectoral interoperability, preventing the emergence of disconnected sectoral silos. Second, a **phased, use-case-driven rollout**, supported by **tailored implementation models** that adapt to the specific digital maturity and regulatory needs of each sector, will allow for iterative learning and demonstrate immediate value. Third, fostering **interoperability by design** and integrating with the UK's **Digital ID and Trust Framework** can create a secure, seamless user journey. Crucially, this must be underpinned by initiatives to enhance **consumer awareness and understanding**, ensuring that the public understands and trusts the benefits of data sharing.

Furthermore, building industrial confidence requires **mitigating key risks** through clear secondary legislation that defines **liability frameworks**, mandates **high-grade security standards**, and employs **transparent cost-benefit analyses**. Relatedly, where mandated participation proves insufficient for data holders, frameworks may research **positive measures** such as recognition schemes, requirements for reciprocal data access, or opportunities for revenue sharing. On the other hand, Smart Data schemes may also include **robust monitoring and enforcement mechanisms** from design to detect and prevent **anti-competitive conduct**, such as information exchange arrangements that could facilitate collusion or the abuse of market power by dominant platforms to disadvantage smaller competitors.

Finally, **strategic alignment with international standards**, such as the EU's Gaia-X, will be critical for maintaining the UK's global influence and ensuring that domestic businesses remain competitive in an increasingly integrated global digital economy.

By leveraging these international insights, the UK may be better positioned to develop a secure, efficient, and innovative data-sharing framework that delivers meaningful benefits to both consumers and businesses. In doing so, it can help unlock the full potential of Smart Data to drive economic growth, enhance consumer choice, and foster a more inclusive digital economy.