Department for Business & Trade

The future of Smart Data: Developing governance models

January 2026

The following report was written by The Public Service Consultants (The PSC). The findings do not necessarily reflect the views of the Department for Business and Trade or the UK Government.

Authors: Josh Myers, Kirushne Suresan, Dr Fiona Jamieson, Katie Burns, Dr Antonio Weiss.

Executive Summary

Smart Data enables customers to make use of the data that companies hold about them – in combination with data about the company and its products as a whole – through the secure sharing of that data with Authorised Third-party Providers (ATPs) upon the customer's request. It has the potential to reshape how people and businesses in the UK access and use their data. By enabling consented data sharing within and between different sectors of the economy, Smart Data can deliver tangible benefits to consumers and businesses while turbocharging competition, innovation and economic growth. The Department for Business and Trade (DBT) is therefore looking to build the UK's Smart Data economy across a number of priority sectors.

To realise this vision, Smart Data schemes need more than good intentions and the right technology: they need effective governance. In this report, we identify 32 governance functions potentially required to successfully administer Smart Data schemes – including developing standards, accrediting Authorised Third-party Providers (ATPs), and enforcing compliance with data sharing mandates. Smart Data governance models concern which actors are responsible for undertaking these functions, how they work together, and how they are held to account. This research aims to inform the design of governance models to implement and manage future Smart Data schemes across the UK economy, with a focus on eight priority sectors: payment accounts (i.e. Open Banking), finance (beyond payment accounts), retail energy, telecommunications, property, transport, retail and agrifood.

As the only operational Smart Data scheme in the UK, Open Banking provides a useful starting point for developing Smart Data governance models in other sectors. Within Open Banking, implementation has been led by the independent Open Banking Limited (OBL), which is soon to become the Open Banking Future Entity, with regulatory oversight and enforcement provided by the Competition and Markets Authority (CMA). However, across our research, participants highlighted both significant strengths and weaknesses of the Open Banking model, suggesting this model should not be replicated exactly for new Smart Data schemes. Moreover, the Open Banking model does not provide insight into developing a more coordinated approach to governing Smart Data across different sectors, especially as cross-sector use cases start to emerge.

In the medium-term, our research findings suggest the UK should adopt a federated model for Smart Data governance (see Figure 1)**.** In this model:

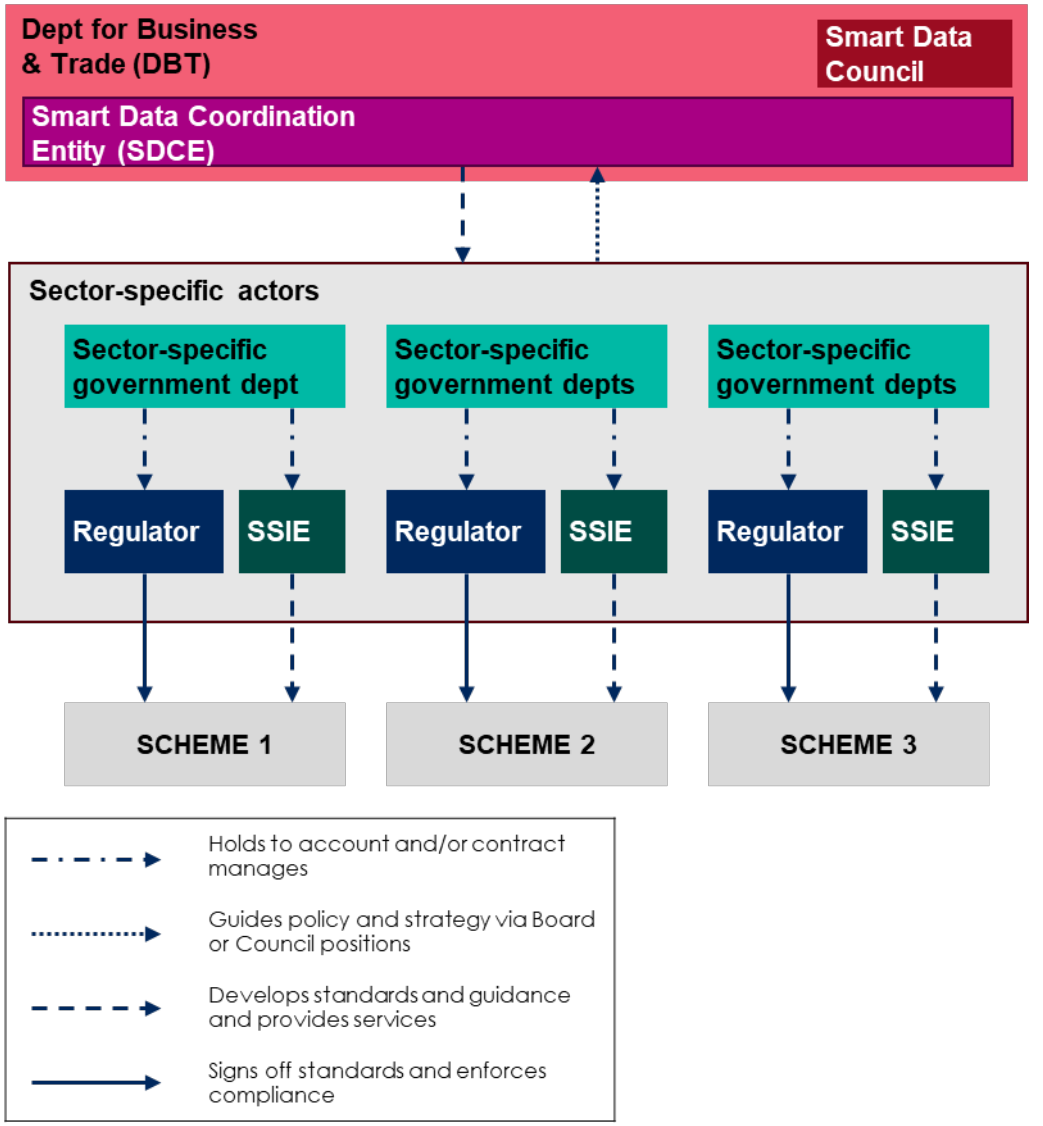
- **Formally appointed sector-specific bodies** (named Sector-specific Implementation Entities) lead the delivery of Smart Data schemes within their sector. Sector-specific Implementation Entities for each sector could be formally appointed through a competitive process held by the relevant government department (e.g. Department for Energy Security & Net Zero would appoint the Sector-specific Implementation Entity for a Smart Data scheme in retail energy) and then supervised by that government department for the duration of their contract (although the government department may delegate this responsibility to a regulator).[1] Among other responsibilities, they develop standards, develop data security classifications, handle customer complaints, monitor compliance and administer dispute resolution mechanisms within their scheme.

[1] Note that the recommendation to appoint Sector-specific Implementation Entities through a competitive process differs from the approach taken to establish Open Banking Limited (OBL) to implement the UK's Open Banking scheme. OBL was established through the Competition and Market Authority's Retail Banking Market Investigation Order 2017, which required the UK's nine largest banks and building societies (the CMA9) to collectively implement Open Banking, including by setting up and funding OBL. However, this approach is unlikely to be appropriate in other sectors where there is not a clear group of large market players who could be held responsible for establishing a Sector-specific Implementation Entity. See Explanation Box 3 in Section 5.3 for a full explanation as to why appointing Sector-specific Implementation Entities through a competitive process is preferred.

- **A central entity** (named a Smart Data Coordination Entity) provides centralised services and mandatory guidelines to ensure consistency and interoperability across different sectors. It is established as a new office within the Department for Business & Trade (DBT), held to account through existing governance structures and ministerial oversight in the department. The Smart Data Coordination Entity develops some common standards, manages central ATP accreditation, establishes a cross-sector service for authentication of customers and ATPs, and coordinates customer complaint and dispute resolution mechanisms across schemes.
- **Existing sector-specific regulators** (e.g. Ofgem for a Smart Data scheme in retail energy) would enforce compliance with data sharing mandates and standards in their sector, working closely with Sector-Specific Implementation Entities. Research participants expressed a clear preference for just one regulator to have responsibility for Smart Data in each sector.

This approach gives each sector the flexibility to move at its own pace, while still ensuring that the overall Smart Data economy remains coherent and supports easy data sharing between sectors. At this stage, a more centralised approach risks delaying early delivery of value in the most advanced sectors. The federated model therefore carves a pathway that makes the most of the promising progress already being driven by leading sectors.

Figure 1 - Summary of the recommended federated governance model in the medium-term.



To support this recommended governance model, we also identified who the key sector-specific actors might be across each Smart Data scheme – as outlined in Table 1. While it is typically straightforward to identify the lead government department for each sector, identifying appropriate regulators is more challenging in sectors with multiple regulators; in such cases, delivering an effective Smart Data scheme may require expanding or adapting the remit of an existing regulator (see rationale in Section 6.2). We have not named suggested actors to work as Sector-specific Implementation Entities here, as these roles would most likely be appointed via a competitive process. A detailed account of the relevant actors in each sector can be found in Appendix G.

Table 1 - Key sector-specific actors in the recommended federated governance model.

Sector	Government Department	Regulator	Sector-specific Implementation Entity
Payment accounts	HM Treasury	FCA	Open Banking Future Entity
Finance	HM Treasury	FCA	

Retail energy	DESNZ	Ofgem	Likely to be appointed through a competitive process, potentially drawing on existing industry bodies and initiatives (see Appendix G).
Telecoms	DSIT	Ofcom	
Property	MHCLG	HM Land Registry (tbc) – requires significant change to remit.	
Transport	DfT	Office for Rail and Road (tbc) – requires significant change to remit.	
Retail	DBT	CMA (tbc) – requires significant change to remit.	
Agrifood	Defra	Food Standards Agency (tbc) – requires significant change to remit.	

In the longer-term, we recommend that the government reviews whether to evolve towards a more Centrally-led model. As the Smart Data landscape matures through the establishment of schemes in an increasing number of sectors, a larger degree of centralisation could help ensure deeper interoperability, making cross-sector data sharing smoother, cheaper, and more reliable. Once a Smart Data Coordination Entity is established, gradually expanding its remit to take on more governance functions shouldn't slow progress in leading sectors but could instead reduce duplication and generate greater economies of scale. Table 2 notes which governance functions might be priorities for centralisation through this process of review and iteration (see a full account of a potential transition in Section 8.1).

Table 2 - Governance functions that may be centralised over time.

Governance functions	**From…** *(Recommended medium-term model)*	**To…** *(Potential long-term model)*
Standards development	The Smart Data Coordination Entity establishes a broad set of core 'common standards' across the Smart Data economy, including technical standards, security standards and customer experience standards. Sector-specific Implementation Entities build on these common standards to develop and maintain the full range of standards for their respective sectors.	The Smart Data Coordination Entity defines and maintains all standards for all schemes, with input from sector-specific advisory groups.
Customer protection and engagement	Sector-specific Implementation Entities manage complaints and define consent journeys based on central requirements; the Smart Data Coordination Entity coordinates across sectors to ensure consistency.	The Smart Data Coordination Entity delivers a unified customer redress platform and standardised consent solutions for all schemes.
Regulatory and compliance functions	Sector-specific Implementation Entities monitor compliance and manage sandbox testing, while enforcement remains with regulators; the Smart Data Coordination Entity coordinates across sectors to ensure consistency.	The Smart Data Coordination Entity monitors compliance, runs conformance testing, and issues enforcement referrals to regulators, taking a more active role across all regulatory and compliance functions.
Implementation functions	Sector-specific Implementation Entities develop delivery plans, lead stakeholder engagement, and resolve disputes	The Smart Data Coordination Entity leads implementation planning across all schemes and

Governance functions	From… *(Recommended medium-term model)*	To… *(Potential long-term model)*
	locally, based on guidance from the Smart Data Coordination Entity.	operates a unified cross-sector appeals and dispute resolution process.

To support this process, we also recommend that government commits to reviewing Smart Data governance models every five years to assess progress and make adjustments based on how the Smart Data landscape evolves, whilst remaining agile. This will potentially include increasing the degree of central coordination if needed. The five-year review cycle has been chosen to align with review periods for Smart Data schemes outlined in the Data (Use and Access) Act. At an extreme, this recurring review process could result in the conclusion that Sector-specific Implementation Entities are no longer necessary in certain sectors.

These recommendations are grounded in:

- A review of international and domestic literature to understand best practice for governance of Smart Data and wider data sharing schemes, and the use cases that are emerging;
- Over 100 stakeholder conversations, spanning industry, regulators, sector experts, and consumer representatives;
- 11 focus groups and a detailed, implementation focused workshop;
- Comparative and systematic assessment of three shortlisted governance models, drawn from a longlist of six potential governance models.

Table 3 summarises the perspectives of stakeholders on each of the three shortlisted governance models assessed, leading to our conclusion that Model 3 (Federated) is most appropriate in the medium-term, while Model 2 (Centrally-led) may be most appropriate in the longer term. Although there was a degree of variation between stakeholders of different types and from different sectors, the views summarised in table 3 were fairly consistently expressed by participants across our sample.

Table 3 - Stakeholder perspectives on three shortlisted Smart Data governance models.

Model description	Stakeholder perspectives
Model 2: Centrally-led. A large central entity leads delivery across all sectors, taking advice from sector-specific advisory groups and working with sector-specific regulators.	Stakeholders noted that the Centrally-led model could deliver the largest benefits for cross-sector data sharing in the longer-term, especially as more sectors are incorporated into the Smart Data economy; however, a more centralised approach risks delaying early delivery of value in the most advanced sectors.
Model 3: Federated. Sector-specific Implementation Entities lead delivery in their sector but are coordinated and supported by a moderately-sized central entity and work with sector-specific regulators.	Stakeholders consistently viewed the federated model as the most practical model to launch cross-sector Smart Data schemes in the short- to medium-term. It would enable progress at pace in leading sectors, while the Smart Data Coordination Entity still ensures that the overall Smart Data economy remains coherent and supports easy sharing of data between sectors.
Model 4: Regulator-led. Existing regulators establish new offices to deliver Smart Data schemes within their remits, coordinated and supported by a small central entity.	The regulator-led model was less favoured, as many raised doubts about whether regulators have the right mandate, capabilities or capacity to lead Smart Data delivery.

There are still several outstanding questions to resolve before the recommended governance model can be fully implemented. In particular, government still needs to determine:

1. **How to approach regulatory and compliance functions in sectors without a single sector-wide regulator.** In areas like property, transport, retail and agrifood, regulatory responsibilities are currently fragmented across multiple bodies. Based on stakeholder feedback, the preferred approach is to expand the remit of one trusted regulator in each sector to take on responsibility for Smart Data. However, expanding the remit of a regulator is a complex and likely challenging task: this approach therefore requires significant further testing, including with the relevant regulators who might assume these responsibilities.
2. **Where to host the Smart Data Coordination Entity.** Our leading hypothesis, based on stakeholder engagement, is that a Smart Data Coordination Entity would be best established as an office within the Department for Business & Trade; however, establishing a new Arm's Length Body was also considered.
3. **How to appoint Sector-specific Implementation Entities.** Our research suggests a competitive process run by the relevant sector-specific government department may be most appropriate for appointing Sector-specific Implementation Entities; however, there are alternative approaches which could be taken, including mandating large industry players to establish a Sector-specific Implementation Entity (as was the case in Open Banking).
4. **How to fund these governance models.** Although funding models were not within the scope of this research, they will be critical to the success of Smart Data governance. Indeed, stakeholders noted that sustainable, fair, and transparent funding arrangements will be an important consideration for future governance models. Further design of these governance models will therefore require careful consideration of initial public investment, long-term industry contributions, and fee structures that do not exclude smaller players.

Despite these outstanding questions, **the recommended federated model provides a credible, pragmatic foundation on which the Smart Data economy can be built** - helping the UK stay ahead of the curve and deliver meaningful value for people, businesses and the economy.

Contents

Tables

Glossary of terms

Term	Definition
Accreditation (of ATPs)	The process of assessing and formally approving ATPs for participation in Smart Data schemes, based on specified eligibility criteria.
Authentication	The process of verifying the identity of customers or ATPs prior to sharing data.
Authorised Third-party Provider (ATP)	An organisation that receives customer data through a Smart Data scheme, with the customer's explicit consent, to access and/or process it to provide a service.
Compliance	The act of meeting the obligations set out by a Smart Data scheme's rules and standards.
Customer consent	The explicit permission given by a customer for their data to be shared with an ATP.
Customer experience standards	Guidelines or requirements that govern how users interact with Smart Data services. These standards aim to ensure that user experiences are clear, consistent, and accessible.
Customer protection	Measures within Smart Data governance that aim to ensure customer rights are protected, including through clear consent processes, dispute resolution, security standards, and safeguards against misuse of data.
Data security classification	The process of categorising data types based on their level of sensitivity, to guide decisions around ATP accreditation levels.
Data security standards	Requirements that define how data must be protected during storage, transmission, and access. This may include encryption protocols, access controls, and monitoring practices.
Dispute resolution	A mechanism that enables customers or organisations to resolve disputes arising from data sharing. These may include complaint handling, appeals processes, and formal redress channels.
Governance	The structured coordination, oversight, and regulation of a Smart Data scheme to enable secure, efficient, and fair use of customer data.
Governance functions	The distinct activities required to successfully govern Smart Data schemes.
Implementation	The practical delivery and operation of a Smart Data scheme, including setting up governance structures, onboarding participants, deploying technical infrastructure, and ensuring scheme functionality.
Interoperability	The ability of two or more systems to exchange information and to use the information that has been exchanged. In this context, it is used to describe exchange of information between actors both *within* and *across* Smart Data schemes.
Regulators	Statutory bodies responsible for overseeing compliance with rules in specific sectors.
Smart Data	The secure sharing of customer data with Authorised Third-party Providers (ATPs), upon the customer's request.

Term	Definition
Smart Data scheme	The overarching regulatory and technical frameworks that enable secure, standardised sharing of customer data within specific sectors of the UK economy.
Smart Data use case	The specific, practical applications of data sharing enabled by Smart Data schemes. Each use case is designed to meet a defined user need and there may be numerous use cases enabled by each Smart Data scheme.
Standards	Agreed technical or procedural specifications that define how data should be shared, formatted, and secured within Smart Data schemes. These may include technical standards, security standards and customer experience standards.
Technical standards	Specific technical requirements that underpin Smart Data infrastructure, such as API protocols, encryption specifications, and data formatting conventions.
Trust framework	A set of principles, rules, and processes that define how participants in a data sharing scheme can interact safely and securely.

1. Introduction

1.1 Building the UK's Smart Data economy

The data economy is increasingly vital to driving economic growth. The UK Government is therefore investigating the introduction of new Smart Data schemes across a range of sectors, under the powers enabled by the Data (Use and Access) Act. The Smart Data powers can be used to mandate and enable "the secure sharing of customer data with Authorised Third-party Providers (ATPs) upon the customer's request to provide innovative services for the consumer or business user, such as automatic switching or better account management."[2] Often linked to sector-specific initiatives like Open Banking or Open Finance, it should not be confused with 'open data', which involves unrestricted access to non-sensitive data for public use, as promoted by the Open Data Institute.[3] However, Smart Data schemes may incorporate elements of open data: for example, under the Open Banking scheme banks are required to make the location of ATMs available via APIs. Smart Data schemes are the overarching regulatory and technical frameworks that enable secure, standardised sharing of customer data within specific sectors of the UK economy.

Key components of Smart Data schemes generally include:

1. **Customer consent**: Customer data is shared only when an authenticated customer requests it.
2. **Data sharing via Authorised Third-party Providers (ATPs):** Only third parties authorised through Smart Data accreditation processes can access customer data.
3. **Mandatory data sharing**: Data holders (e.g. banks) can be mandated to share customer data according to recognised standards if requested.
4. **Data sharing standards**: All participants in a scheme must work to agreed data sharing standards.

While these components are commonly associated with Smart Data schemes, their exact design can vary depending on the context. For example, not all Smart Data schemes are mandatory: some Smart Data schemes could be voluntary established without the support of any statutory instruments by commercial organisations through contractual law. Meanwhile, some sharing of customer data is permitted under existing laws like GDPR without explicit consent (such as contractual necessity), and the level of authorisation required for third parties to access data may depend on the sensitivity of the data involved and whether they seek 'read only' or 'write' access.

Smart Data in the UK was first introduced via Open Banking: a data sharing ecosystem established in 2017 when the Competition and Markets Authority mandated the nine largest banks and building societies in the UK to make payment account data available to Authorised Third-party Providers (ATPs) with customer consent. Open Banking services are now regularly used by over 13 million customers in the UK, with countries around the world replicating the UK's Open Banking approach.[4]

Expanding the UK's Smart Data economy beyond Open Banking has the potential to boost economic growth in the following ways: improving efficiency and productivity, creating new products and services, improving customer experiences, and encouraging market competition and innovation. Work is therefore ongoing to further understand the potential for Smart Data in sectors

[2] Department for Business & Trade, 2024. Regulatory Powers for Smart Data: Impact Assessment.
[3] Open Data Institute, 2016. What is open data?
[4] Open Banking, 2025, API Performance.

of the economy beyond payment accounts, including across other financial services,[5] retail energy,[6] telecommunications,[7] property, transport, retail and agrifood.

In each of these sectors, valuable data-sharing initiatives are already in progress (see Appendix G), which could be supported or expanded by the introduction of formal Smart Data schemes. Within payment accounts, this most obviously includes the existing Open Banking scheme. However, there is also a range of existing initiatives to consider in other priority sectors. For example:

- **In the finance sector**, the FCA are already leading thinking on the design of Open Finance, including through an Open Finance Sprint in Spring 2025.[8]
- **In the retail energy sector**, the Smart Energy Code[9] and Retail Energy Code[10] both provide rules for sharing data, several organisations operate existing data-sharing infrastructure, a proposed Smart Meter Data Repository programme aims to centralise smart meter data,[11] Ofgem has been establishing both a Data Sharing Infrastructure[12] and a consumer consent solution[13] for the entire sector, and the Department for Energy Security and Net Zero has already issued a Call for Evidence for developing a Smart Data scheme in the energy sector.[14]
- **In the telecommunications sector**, Ofcom's One Touch Switch (OTS) requirements enable data-sharing to support customers to switch providers easily without contacting their current provider.[15]
- **In the property sector,** the Open Property Data Association (OPDA) brings together stakeholders from across the property ecosystem to support property data standardisation, including through the Property Data Trust Framework,[16] while HM land Registry are digitising and centralising property data previously held by local authorities.[17]
- **In the transport sector**, the Bus Open Data Service (BODS) mandates open sharing of bus timetables, fares, and vehicle locations,[18] ITSO has developed a national standard for smart ticketing,[19] and the Open Transport Initiative has developed Open Standard APIs.[20]
- **In the retail sector**, GS1 is introducing new QR-enabled barcodes to offer expanded product-level data access[21] while the Institute for Grocery Distribution and University of Leeds provide a secure research data sharing model used by some major food retailers.[22]

---

[5] Financial Conduct Authority, 2021, Open finance: Feedback Statement.
[6] Department for Energy Security & Net Zero, 2025, Developing an energy smart data scheme.
[7] Ofcom, 2021, Open Communications – Enabling people to share data with innovative services.
[8] Financial Conduct Authority (FCA), 2025. FCA Open Finance Sprint 2025: Charting the course for open finance.
[9] Smart Energy Code Company, 2025. The Smart Energy Code.
[10] Retail Energy Code Company, 2019. Retail Energy Code.
[11] Department for Energy Security & Net Zero (DESNZ), 2023. Smart Meter Energy Data Repository Programme: Phase 1 projects.
[12] Ofgem, 2025. Governance of the Data Sharing Infrastructure.
[13] Ofgem, 2025. Consumer consent decision.
[14] Department for Energy Security & Net Zero, 2025. Developing an energy smart data scheme: call for evidence.
[15] Ofcom, 2024. Simpler and quicker broadband switching is here.
[16] Open Property Data Association, 2023. Property Data Trust Framework.
[17] HM Land Registry, 2023. Local Land Charges: preparing data for the new digital register.
[18] Department for Transport, 2020. Bus open data policy.
[19] ITSO, 2025. ITSO specification.
[20] Open Transport Association, 2025. Open Standard APIs.
[21] GS1, 2024. The next generation of barcodes: QR codes powered by GS1.
[22] Smart Data Research UK, 2024. Smart use of supermarket data.

- **In the agrifood sector**, the Food Data Transparency Partnership (FDTP) is aiming to standardise environmental impact and nutrition data[23] while the Agriculture and Horticulture Development Board is developing farm-level data sharing pilots.[24]

To establish successful Smart Data schemes, which support and build upon these existing initiatives, clear and effective governance will be required. Effective governance is particularly essential to support cross-sector use cases where services draw on data from multiple Smart Data schemes. Governance models therefore need to be established both *within* each Smart Data scheme and *across* the Smart Data economy as a whole.

1.2 Why is the governance of Smart Data important?

There is currently no single, widely accepted definition of 'governance' in the context of Smart Data. To address this, we reviewed relevant UK and international literature on Smart Data governance and developed a working definition that reflects the specific needs and characteristics of Smart Data schemes. Hence, in the context of Smart Data, we define 'governance' as:

The structured coordination, oversight, and regulation of a Smart Data scheme to enable secure, efficient, and fair use of customer data. It ensures accountability, compliance, and customer protection through defined roles and responsibilities and mechanisms for collaboration among stakeholders.

Put simply, Smart Data governance models therefore concern which actors do what, how they work together, and how they are held to account. Clear and effective governance models will be essential to the successful implementation of Smart Data schemes for a range of reasons.[25,26,27] For example, governance models are needed to:

1. **Ensure compliance with regulations**, establishing effective oversight and enforcement mechanisms which ensure participating organisations are held accountable.
2. **Set common standards**, developing common technical standards to enable successful data sharing between different parties.
3. **Protect and empower customers**, establishing clear routes to redress for customers if issues or malpractice arise, such as security breaches or data misuse.
4. **Engage relevant stakeholders,** incorporating the diverse perspectives of policymakers, regulators, data holders, ATPs and customers into the design of Smart Data schemes to ensure they are responsive to a broad range of needs.
5. **Ensure interoperability between schemes,** encouraging consistency between Smart Data schemes in different sectors to support cross-sector data sharing.

As the UK's Smart Data economy evolves, including incorporating new data types and sectors over time, data sharing across sectors is likely to offer increasingly significant value to customers and industry. Given uncertainties as to which sectors will see Smart Data schemes established, the Department for Business & Trade's task is therefore to design a pan-economy Smart Data governance model which is sufficiently robust and adaptable to support Smart Data schemes across all sectors of the economy.

[23] Defra, 2025. Food Data Transparency Partnership.
[24] Agriculture and Horticulture Development Board, 2024. Solutions for farm-level environmental data.
[25] Centre for Data Ethics & Innovation, 2023. Smart Data Implementation Guide.
[26] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[27] The Royal Society, 2020. The UK data governance landscape.

1.3 Research aims

This research aims to inform the design of such a pan-economy Smart Data governance model. The research therefore aims to:

1. Understand the existing stakeholder and data governance landscape in eight sectors: payments accounts (i.e. Open Banking), financial services (beyond payment accounts), retail energy, telecommunications, property, transport, retail and agrifood.
2. Identify the critical success factors for Smart Data governance.
3. Define interoperability in the Smart Data context, including understanding what a good experience looks like when different actors operate across multiple sectors.
4. Collate and test ideas for how Smart Data governance models could be designed, including to enable cross-sector interoperability.
5. Generate findings that recommend a path forward for the development and delivery of Smart Data governance models.

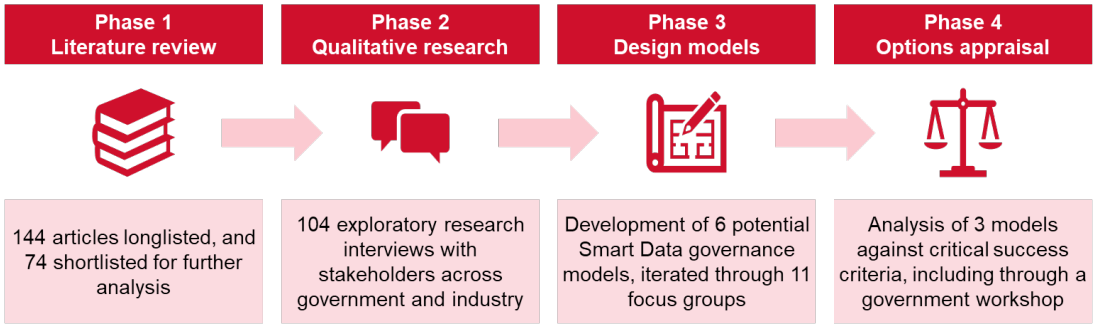
This report proceeds in seven further sections. *Section 2* summarises the methodology we used throughout this research, including a literature review, qualitative research and evaluation of several governance models. *Section 3* provides a summary of 32 governance functions required for a Smart Data scheme to function. *Section 4* provides further understanding of what interoperability means in the Smart Data context, and what it requires in practice. *Section 5* outlines the development of three shortlisted Smart Data governance models. *Section 6* identifies potential organisations which could assume responsibilities under these Smart Data governance models in each of the eight priority sectors. *Section 7* evaluates the three shortlisted models. And *Section 8* provides a recommended approach to developing Smart Data governance, including outlining eight next steps for delivery.

The research was undertaken by the Public Service Consultants (The PSC), on behalf of the Department for Business Trade between January 2025 and May 2025.

2. Methodology

The findings included in this report were generated through four phases of work. In the first phase, we undertook a literature review to understand existing governance models for Smart Data and other data sharing schemes in the UK and internationally. The literature review informed our second phase of work in which we conducted qualitative interviews with 104 government and industry stakeholders. In the third phase, we designed and iterated several potential governance models through a series of focus groups. In the fourth and final phase, we undertook an evaluation of options of those emerging governance models to reach a recommendation.

Figure 2 - Our four-phase research approach.



2.1 Phase 1: Literature review

The literature review aimed to (a) explore the key governance roles and functions required to successfully operate Smart Data schemes and (b) evaluate existing data-related governance models both within the UK and internationally.

To identify relevant literature, we developed a targeted sampling strategy informed by an initial scoping exercise. This involved identifying key words related to governance roles and functions, such as 'enforcement' and 'implementation', and agreeing on priority international case studies to investigate.[28] Agreed search terms were then applied across a range of databases and search engines, resulting in a longlist of 144 documents. 74 of these documents were then shortlisted for further analysis according to their relevance, recency and credibility of the source. As part of this early work, we also conducted a review of potential markets for Smart Data and identified both sector-specific and cross-sector use cases across the eight priority sectors.[29]

We conducted thematic analysis to:

1. Identify governance functions required to operate Smart Data schemes, such as accreditation of ATPs, monitoring and enforcing compliance, and providing routes for customer redress.
2. Identify the critical success factors for governance of Smart Data schemes or similar data sharing schemes.

The insights from this literature review, supplemented by early case study analysis of potential Smart Data markets, informed the key research questions, sampling approach and design of interview guides for the next phase of qualitative research.

[28] Australia, Singapore, European Union, United States, Brazil, Hong Kong, United Arab Emirates, India and Japan were selected as international case studies. Appendix B outlines key learnings from each country's approach to Smart Data governance.
[29] The 16 UK market case studies selected to inform our literature review were: retail banking, SME business lending, debt advice, mortgages, retail investment, pensions, retail energy, green finance, distributed energy resources (DER), home buying and selling, retail telecoms, public transport, automative and vehicle telematics, international shipping and trade, grocery shopping and carbon reporting.

2.2 Phase 2: Qualitative research

Following the literature review, we held semi-structured qualitative research interviews with 104 stakeholders. Our interview sample included representatives from industry (including large data holders, potential future ATPs and industry bodies), government departments, regulators, consumer advocacy groups and independent data experts. Participants in the sample spanned all eight sectors investigated through this research: payment accounts (i.e. Open Banking), financial services (beyond payment accounts), retail energy, telecommunications, property, transport, retail and agrifood. See Appendix D for more details on our qualitative research sample.

The qualitative research interviews intended to supplement the findings of our literature review to:

1. Validate, iterate and expand on an emerging list of governance functions.
2. Validate, iterate and expand on an emerging list of critical success factors.
3. Understand stakeholder preferences for the design Smart Data governance models.

2.3 Phase 3: Design models

Drawing on insights from the literature review and qualitative research, we designed six potential governance models for the Smart Data economy. For each of the governance models, we outlined the approach to executing the 32 identified governance functions. This included (a) identifying the appropriate actor(s) to execute that function and (b) outlining how that function would be executed by those actor(s). A key distinguishing feature between these different models is the extent to which the governance of Smart Data is centralised, and therefore whether a greater proportion of governance functions are undertaken by cross-sector or sector-specific entities.

To refine and iterate these models, we held a series of 11 focus groups with 61 relevant stakeholders, including a mix of those who participated in Phase 2 and new participants. The focus groups were held in three rounds:

Round 1 (2 focus groups): Initial input from expert cross-sector stakeholders.

Round 2 (7 focus groups): Sector-specific focus groups including government and industry representatives from each sector.

Round 3 (2 focus groups): Follow-up input from expert cross-sector stakeholders.

The potential governance models were iterated and improved between each round of focus groups to ensure participants had the chance to comment on the most advanced design for Smart Data governance models available at any given time.

We initially discounted three options – the most centralised option, the most decentralised option, and a market-driven option – due to negative feedback received during the first round of focus groups. This left us with three shortlisted Smart Data governance models to evaluate in Phase 4.

2.4 Phase 4: Evaluation of options

In Phase 4, we conducted an evaluation of three shortlisted Smart Data governance models to reach a recommended model for governing the Smart Data economy. We assessed each of the models against the ten critical success factors developed in Phase 1 and 2. To do so, we triangulated the following sources: (1) quantitative assessments of the model by attendees at a Smart Data workshop, (2) quantitative assessments of the model by a panel of synthetic sector representatives,[30] and (3) qualitative judgements from the research team, drawing on all the evidence gathered throughout the research. This enabled us to reach a recommendation for the future governance of the UK Smart Data economy.

[30] We used transcripts from our Phase 2 research interviews to develop AI-generated synthetic sector representatives. These synthetic sector representatives could efficiently synthesise the thoughts of all relevant research participants to appraise the governance models, avoiding the introduction of biases from researchers.

3. Governance functions within Smart Data

To design effective Smart Data governance models, we first needed to understand the full range of relevant governance functions – that is, the roles or services which need to be performed to successfully govern Smart Data schemes. The final governance models for UK Smart Data schemes should clearly outline who holds responsibility for executing each of these functions. We identified 32 Smart Data governance functions, primarily through a review of existing literature on Smart Data schemes in the UK (see Appendix A), international Smart Data schemes (see Appendix B) and other UK data-sharing initiatives (see Appendix C). This initial list of governance functions was then supplemented throughout our qualitative research.

The functions can be disaggregated into six high-level categories:

1. Policy and strategy
2. Standards development
3. Accreditation of Authorised Third-party Providers (ATPs)
4. Consumer protection and engagement
5. Regulatory and compliance
6. Implementation

The remainder of this section outlines the governance functions in each of these categories in more detail, including current approaches to executing those governance functions in the UK and design preferences shared by research participants. Further detail on the preferences of research participants can be found in Appendix F.

3.1 Policy and strategy

3.1.1 What are policy and strategy functions?

Policy and strategy functions define the overarching purpose, scope and operating principles of a Smart Data scheme. These functions establish the vision for how Smart Data can deliver value, guide which data should be shared and under what terms, and set the tone for how governance entities operate.

Table 4 – Governance functions in the 'Policy and strategy' category.

Governance functions in this category:
1a. Setting the vision and strategic direction: Identifying the key aims of the scheme in each sector, including by selecting priority use cases.
1b. Defining data sharing mandates: Determining the data types that industry organisations are required to share when requested by customers.
1c. Defining data sharing principles: Setting high-level principles which data sharing should comply with.
1d. Designing or adapting trust frameworks: Setting out how data is shared, used, and protected by participants in Smart Data schemes, including liability for errors or wrongdoing.
1e. Designing or adapting governance models: Deciding the design, composition and remit of formal Smart Data governance entities, including roles and decision-making powers.
1f. Aligning with other government policy: Aligning Smart Data schemes with broader digital and data strategies across government.
1g. Advising on policy and strategy: Feeding industry and consumer voices into all policy and strategy decisions.

Explanation box 1: Governance models vs. trust frameworks

While a trust framework outlines the rules for a Smart Data scheme, a governance model outlines which actors are responsible for ensuring the scheme operates according to those rules. If we applied this logic to a football match: while a trust framework would stipulate that players may not touch the ball with their hands, the governance model would stipulate that all match officials are responsible for flagging when this rule is broken, and the referee is responsible to administering punishments for said rule breaking.

Governance models and trust frameworks are intrinsically linked, with each inevitably informing and shaping the other. On the one hand, deciding who is most appropriate for ensuring a scheme operates according to certain rules (i.e. the governance model) depends on the nature of those rules (i.e. the trust framework). On the other, determining what the rules should be for a scheme (i.e. the trust framework) requires a knowledge of who the key actors are in a scheme (i.e. the governance model) in the first place.

3.1.2 The current state of policy and strategy functions

In the UK, policy and strategy functions for Smart Data are currently distributed across a combination of central government departments and regulators. DBT plays the lead role in shaping the cross-cutting Smart Data economy, including developing the legislative framework through the Data (Use and Access) Act. DBT's role involves setting overarching vision and direction, aligning Smart Data with broader data and digital policy, and supporting coherence across sector-specific initiatives. In the case of Open Banking, the CMA drove forwards policy and strategy through its Retail Banking Market Investigation Order 2017. However, in other cases it is expected that individual government departments will lead the development of Smart Data schemes within their respective domains: for instance, the Department for Energy Security and Net Zero (DESNZ) initiated policy development in the retail energy sector through its January 2025 Call for Evidence on Smart Data in Energy.[31]

Regulators such as the CMA, FCA and Ofcom have also played influential roles, particularly in shaping data sharing mandates and trust frameworks within their regulated industries. Their involvement helps ensure that strategic decisions are grounded in sectoral realities, regulatory standards, and consumer protection considerations.

3.1.3 What are the design preferences of participants for policy and strategy functions?

Research participants expressed the following preferences for the design and delivery of policy and strategy functions in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 1: Government should lead on setting public interest goals and strategic priorities.** Because these functions involve fundamental value judgements – such as which public outcomes to prioritise and what trade-offs are acceptable – several research participants argued they should be, in the main, executed by government departments, which are democratically accountable and mandated to act in the public interest.
- **Design preference 2: Governance should allow for flexibility to iterate data sharing mandates over time.** Participants recognised that the most impactful innovations often emerge unpredictably, as was the case in Open Banking. Governance models should therefore allow for iterative definition of data sharing mandates, including removing or retiring data sharing obligations that are no longer delivering value. This will require clear guidelines on when data sharing mandates should be reviewed and how.

[31] Department for Energy Security & Net Zero, 2025, Developing an energy smart data scheme.

3.2 Standards development

3.2.1 What is standards development?

Smart Data schemes are reliant on a range of standards which allow services and systems to connect securely and seamlessly: this includes technical standards for data formats and APIs, privacy and security standards, and customer experience standards. Without clear standards, Smart Data schemes may not support smooth data sharing between parties as intended and risk breaching data privacy and security legislation. While establishing a set of common standards across all Smart Data schemes could be one approach to enabling interoperability, some schemes may also be able to achieve interoperability through lighter-touch approaches, such as aligning formats for shared attributes only or adopting common identifiers.[32] Either way, establishing clear standards remains an important governance function to be executed within Smart Data schemes.

Table 5 - Governance functions in the 'Standards development' category.

Governance functions in this category:
2a. Defining and maintaining technical standards: Creating and updating the data and API specifications that underpin how data is shared between parties.
2b. Developing data security classifications: Defining levels of sensitivity for different types of data and adjusting security requirements accordingly.
2c. Developing privacy and security standards: Designing the controls, policies and procedures to ensure that data sharing protects user privacy and system security.
2d. Defining customer experience guidelines: Developing rules for customer data sharing journeys.
2e. Ensuring cross-sector interoperability of standards: Coordinating standards across sectors to ensure interoperability across industries.

3.2.2 The current state of standards development functions

In the UK's Open Banking scheme, Open Banking Limited (OBL) has led the way by developing and maintaining detailed API and data standards to supplement gaps in PSD2, enabling secure and interoperable data sharing between banks and ATPs.[33] In other sectors, standards are emerging through different mechanisms: for example, the Smart Energy Code outlines technical and security standards for energy data [34] and the Property Data Trust Framework has been developed by an industry coalition to standardise property-related data sharing.[35] These initiatives illustrate a growing recognition of the need for well-defined technical specifications, yet they remain siloed within their respective domains.

Beyond schemes within specific sectors, the British Standards Institution (BSI) plays an important role in developing formal standards that support interoperability, privacy, and data security across industries. However, there is currently no dedicated entity responsible for aligning Smart Data standards across sectors or ensuring consistency in areas like customer experience and data classification. This lack of coordination may hinder interoperability within and across Smart Data schemes. A more unified approach to standards development could therefore reduce duplication, lower compliance costs, and enable a smoother user experience across the wider Smart Data ecosystem.

[32] Department for Business & Trade, forthcoming. Mapping Data Standards: Evaluating how existing data standards can support future Smart Data schemes.
[33] OECD, 2021. Mapping data portability initiatives, opportunities and challenges.
[34] Smart Energy Code Company, accessed May 2025. The Smart Energy Code
[35] Home Buying and Selling Group, 2022. Property Data Trust Framework.

3.2.3 What are the design preferences of participants for standards development functions?

Research participants expressed the following preferences for the design and delivery of standards development functions in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 3: Technical standards should be developed by expert-led bodies with a mechanism for updates.** There was widespread recognition that government departments and regulators may not have the technical expertise required to develop and update technical standards in detail. Instead, participants advocated for standards to be developed by expert-led bodies, then signed off and implemented by regulators.
- **Design preference 4: Data sensitivity classifications should determine security and ATP accreditation requirements.** Participants broadly agreed that not all data is created equal when it comes to sensitivity and security, and that Smart Data governance should reflect this by adopting differentiated standards for data sharing and Authorised Third-party Provider (ATP) accreditation depending on data sensitivity classification and whether the ATP seeks 'read only' or 'write' access.
- **Design preference 5: Baseline privacy and security standards should be established centrally.** Participants expressed a preference for a central coordinating body to lead the development of baseline privacy and security standards that apply across all Smart Data schemes. Some participants noted that while not all data requires the same level of protection, consistent approaches to privacy and security help build trust in the system and reduce confusion for users.
- **Design preference 6: Standards should ensure customer journeys are simple and consistent, in line with mandatory guidelines.** Participants highlighted that clear customer experience guidelines are important to ensure user adoption of Smart Data-enabled services; simple, transparent and trustworthy data sharing journeys reduce user drop-off and build public confidence in Smart Data schemes.
- **Design preference 7: A core set of common standards with sector-specific extensions should be developed by a central body.** Many participants noted that different sectors often rely on common data 'touchpoints' (such as names, dates of birth, and addresses) to identify individuals, meaning that misalignment in how this core data is structured or authenticated can create friction and limit the feasibility of cross-sector services. There was strong support for the development of a core set of common technical standards that apply across all Smart Data schemes, with sector-specific extensions where necessary.
- **Design preference 8: Smart Data standards should build on existing sector standards, including those from Open Banking.** Participants widely supported the principle that technical standards for Smart Data schemes should not be developed from scratch where suitable standards already exist. Instead, Smart Data schemes should seek to build on and extend existing sector standards, particularly those developed under Open Banking.

3.3 Accreditation of Authorised Third-party Providers (ATPs)

3.3.1 What is accreditation of ATPs?

An Authorised Third-party Provider (ATP) is defined as any business or organisation that a customer gives permission to access and/or process their data for the provision of services.[36] It is generally agreed that ATPs should be authorised and held to appropriate standards with Smart

[36] Centre for Data Ethics & Innovation, 2023. Smart Data Implementation Guide.

Data schemes because they have access to protected consumer data.[37] By requiring ATPs to meet clear standards before they can operate, a robust accreditation process should ensure all data sharing meets relevant security and privacy standards, reducing the risk of customer data breaches.[38] Accreditation of ATPs will also need to be renewed periodically to ensure they are continuing to work to required standards. This function works in tandem with authentication of ATPs once a Smart Data scheme is established: authentication mechanisms ensure that ATPs are properly identified as accredited before they can access consumer data, providing another layer to consumer trust.

Explanation box 2: What is the difference between accreditation and authentication?

Accreditation determines whether an authorised third-party provider is permitted to access customer data through a Smart Data scheme. This accreditation provides certainty that a participant meets all the necessary criteria to operate securely within the scheme.

Authentication, on the other hand, is the process of verifying that a customer or Authorised Third-party Provider (ATP) is truly who they claim to be. For example, when a data holder receives an API call, it must authenticate that the requester is a legitimate ATP within the Smart Data scheme. Similarly, when a customer requests for their data to be shared, the ATP and/or data holder must authenticate that the person making the request is the legitimate owner of that data.

Table 6 - Governance functions in the 'Accreditation of Authorised Third-party Providers (ATPs)' category.

Governance functions in this category:
3a. Determining ATP accreditation requirements: Defining the eligibility criteria and conditions Authorised Third-party Providers must meet to be accredited.
3b. Delivering ATP accreditation process: Running the assessment and onboarding processes that grant or revoke ATP status for third parties.
3c. Maintaining an authorised list of ATPs: Keeping an up-to-date public list of accredited third parties that are authorised to access and use Smart Data, that allows data holders and users to confirm ATP credentials.
3d. Ensuring cross-sector recognition of ATP accreditation: Enabling ATPs accredited under one scheme or sector to be recognised in others without a duplicative process.

3.3.2 The current state of accreditation of ATPs

The Financial Conduct Authority's (FCA) Open Banking licensing process provides a strong example of an accreditation framework for ATPs. To become a regulated provider, firms must demonstrate compliance with a range of requirements, including holding professional indemnity insurance, implementing systems to safeguard data, and using a trust framework for identification when interacting with banks. Firms must also obtain explicit consumer consent to access their data and have clear processes for handling complaints, including escalation to independent bodies such as the Financial Ombudsman service.[39]

Open Banking Limited (OBL), the implementation entity for Open Banking, operates a Directory that relies on the FCA's register to check that ATPs are authorised to participate in the UK's Open Banking ecosystem. This Directory operates as a whitelisting system, enabling authorised

[37] Financial Conduct Authority, 2021. Open Finance Feedback Statement.
[38] Department of Business, Energy, & Industrial Strategy, 2020. Smart Data research - liability.
[39] Ibid.

providers to connect securely with consumers and offer Open Banking services.[40] Maintaining an up-to-date registry is vital to prevent unauthorised access while allowing accredited new joiners to seamlessly access the market. An entity to oversee such a registry, as OBL does for Open Banking, can help to prevent uncompetitive behaviour, and enact changes to the list of authorised providers as required. An example of such uncompetitive behaviour to be avoided can be found in the US's market-driven model Open Banking model: without a central directory of ATPs, dominant banks were able to control which ATPs could access data and complicated the process for consumers to switch ATPs, thereby reducing competition.[41]

3.3.3 What are the design preferences of participants for accreditation of ATPs?

Research participants expressed the following preferences for the design and delivery of accreditation of ATPs in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 9: ATP accreditation should be tiered and have consistent requirements across schemes.** Participants noted that accreditation requirements should be proportionate to the sensitivity of the data being accessed, building directly on established data security classifications (see function 2b). This would result in a tiered accreditation process, with potentially more stringent requirements for those ATPs accessing more sensitive data and those seeking 'write' access (as opposed to 'read only' access).
- **Design preference 10: Shared recognition of ATP accreditation across schemes should be enabled.** Participants largely supported the idea of a centralised ATP accreditation process, featuring one set of eligibility criteria, one authorised list of approved ATPs, and one accreditation journey. This model would allow accredited ATPs to access data across multiple sectors without undergoing duplicative approval processes and would enable data holders to use a consistent API call to authenticate ATP accreditation. If the ATP accreditation process was delivered as a centralised function, this would mark a departure from the approach taken in Open Banking, where the FCA accredited ATPs.

3.4 Customer protection and engagement

3.4.1 What are customer protection and engagement functions?

Customer protection and engagement functions are an important enabler of trust in and adoption of Smart Data schemes, and include handling customer complaints and redress, promoting public understanding of Smart Data, and defining consent and authentication requirements. Each of these functions plays a complementary role: redress mechanisms provide a safety net when things go wrong; consent and authentication requirements ensure customers retain control over who accesses their data and for what purpose; and educational efforts foster the confidence needed for individuals to participate fully in new data-driven services. Together, they ensure that customers are not only safeguarded from harm but are also active, informed participants in the data-sharing ecosystem.

Customer protection and engagement functions should also look to complement, rather than duplicate, existing data rights: for example, GDPR already sets out baseline protections for personal data sharing. However, Smart Data schemes may introduce more complex data flows that require clearly defined, tailored approaches to customer protection.

[40] Truelayer, accessed January 2025. Open banking regulation in the UK.
[41] European Journal of Law and Economics, 2023. Data portability and interoperability: An E.U.-U.S. comparison.

Table 7 - Governance functions in the 'Customer protection and engagement' category.

Governance functions in this category:
4a. Handling customer complaints and redress: Managing systems that allow customers to raise concerns and access remedies when issues arise.
4b. Promoting customer understanding: Promoting public understanding of Smart Data and encouraging safe and informed participation by consumers.
4c. Defining consent requirements: Ensuring informed customer consent is obtained before data is shared, through either setting clear consent requirements and/or offering shared or standardised customer consent solutions.
4d. Defining authentication requirements: Ensuring effective processes are in place to confirm the identity of customers providing consent for their data to be shared, through either setting clear authentication requirements and/or offering shared or standardised authentication solutions.

3.4.2 The current state of customer protection and engagement functions

Effective customer protection and engagement is a thorny challenge across all data sharing schemes in the UK. Several different organisations have responsibility for protecting customers and providing routes to redress. The Information Commissioner's Office (ICO) is the central authority for complaints related to data protection, including misuse or mishandling of personal data. Sector-specific regulators may also investigate data-related breaches within their remit, particularly where data issues intersect with broader regulatory responsibilities such as conduct or competition. In parallel, ombudsman services – such as the Financial Services Ombudsman or Energy Ombudsman – offer dispute resolution routes for consumers, though their focus is typically on service or product complaints rather than data rights specifically. However, this fragmented landscape means consumers are often left uncertain about where to turn, especially when data flows between sectors or is shared with non-regulated parties.

The UK government has previously encouraged the development of Alternative Dispute Resolution mechanisms (ADRs): that is, ways of resolving disputes between consumers and companies that don't involve going to court.[42] However, while frameworks such as GDPR, PSD2, and Open Banking provide access to ADRs, they often lack clarity and consistency, as ADR routes are not always obvious and operate inconsistently across different sectors, potentially leaving consumers vulnerable.[43] Debate remains as to whether Smart Data schemes should aim to address the aforementioned gaps in data-related customer redress across the economy through new governance models or whether they should simply make use of existing provisions.

In the case of the UK's Open Banking scheme, the CMA mandated the inclusion of customer redress mechanisms within the framework. In addition, ATPs must have a complaints procedure in place become authorised or registered by the FCA. Customers can escalate complaints to the independent Financial Ombudsman Service if their complaint is not resolved.[44] Where appropriate to protect consumers from harm, the FCA has a range of supervisory and enforcement tools it can use and ultimately financial sanctions may apply. However, consumers have faced uncertainty about which regulator to approach for redress or how liability will be apportioned among firms.[45] The Open Finance feedback statement underlines the importance of creating common complaint routes that are easy, accessible, timely, individual, and free.[46]

[42] Department for Business, Innovation & Skills, 2015. Alternative dispute resolution for consumers.
[43] Department of Business, Energy & Industrial Strategy, 2020. Smart Data research - liability.
[44] Ibid.
[45] Department for Business, Energy & Industrial Strategy, 2020. Smart Data research - liability.
[46] FCA, 2021. Open Finance Feedback Statement.

Meanwhile, current consent mechanisms, while mandated under frameworks like GDPR and Open Banking, remain often incomprehensible to consumers. Regulatory requirements necessitate multiple layers of Terms and Conditions and Privacy Notices, which can overwhelm consumers, meaning obtaining genuinely informed consent from customers is difficult.[47] The Open Finance Feedback Statement therefore has stated the requirement for a clear framework for customers to give and withdraw informed consent.[48] Ofgem's recent work on consumer consent reinforces this need, outlining proposals for a standardised, user-friendly consent framework in the energy sector.[49]

3.4.3 What are the design preferences of participants for customer protection and engagement functions?

Research participants expressed the following preferences for the design and delivery of customer protection and engagement functions in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 11: Redress processes should be coordinated across actors and sectors by a central body.** Many interviewees described the current landscape for data-related customer redress as fragmented and difficult to navigate. There was widespread support for a more coordinated and transparent redress process for Smart Data schemes, especially as data flows become increasingly cross-sectoral. While few believed a true 'single front door' for data-related complaints was realistic in the near term, many endorsed a model where 'all roads lead to the same destination': ensuring that complaints, regardless of where they are initially raised, are channelled into a common resolution process.
- **Design preference 12: A centralised, cross-sector consent management solution is preferred.** Participants widely supported the development of a centralised consent management system, such as a cross-sector consent dashboard, that would streamline how individuals authorise data sharing. Experiences from Open Banking highlighted that the development of separate consent processes by different banks both duplicated effort among banks and led to inconsistent consumer experiences. Ofgem's work to create a Consumer Consent Solution for the energy sector was highlighted as a foundation on which a broader cross-sector model could be built. It was also noted consent management solutions should consider how often customer consent needs to be reaffirmed for continued data-sharing.
- **Design preference 13: Authentication should be consistent, proportionate, and potentially shared across schemes.** Several participants endorsed developing a shared authentication solution that all schemes could rely on, potentially building upon emerging government digital identity services. Some participants noted that current models, like those used in Open Banking, offer useful technical precedents but would need to be adapted to accommodate a broader range of use cases and risk profiles.

3.5 Regulatory and compliance

3.5.1 What are regulatory and compliance functions?

Regulatory and compliance functions ensure all participants in a Smart Data scheme – including data holders and Authorised Third-party Providers (ATPs) – are acting in line with the scheme's rules, standards, and public interest objectives. Together, they uphold the credibility of the system, foster market confidence, and provide vital safeguards for customers by ensuring rules are not just written but followed. This applies whether the scheme is underpinned by statutory regulation or operates on a voluntary basis through contracts and existing law. As evidenced by the experience

[47] Department for Business, Energy & Industrial Strategy, 2020. Smart Data research - consent.
[48] FCA, 2021. Open Finance Feedback Statement.
[49] Ofgem, 2023. Data Sharing in a Digital Future: Consumer Consent.

of Open Banking in the UK, effective regulatory oversight over governance entities themselves is also required, ensuring that those charged with implementing Smart Data are held accountable.[50]

Internationally, Smart Data schemes use a range of mechanisms to ensure compliance with rules and protect consumers, including legal liability for participants and softer, incentive-based approaches. [51] In this context, *liability* refers to the legal responsibility of organisations for harms caused by breaches of scheme rules—for example, mishandling data, violating consent, or misrepresenting their status. This creates a strong compliance incentive, as organisations may face regulatory penalties, civil damages, or even criminal sanctions.

For example, Australia's Consumer Data Right (CDR), explicitly includes both civil and criminal liability provisions for non-compliance, such as making fraudulent data requests or falsely claiming accreditation. [52] The EU's General Data Protection Regulation (GDPR), while not specific to Smart Data, also includes liability provisions: organisations can be held accountable and fined by national data protection authorities, and individuals have a right to seek compensation. However, GDPR enforcement can vary between member states and often relies on regulatory investigations or individual complaints.[53]

Table 8 - Governance functions in the 'Regulatory and compliance' category.

Governance functions in this category:
5a. Monitoring compliance: Tracking whether organisations fulfil their obligations to comply with data sharing mandates and standards.
5b. Encouraging compliance: Providing guidance and support to help organisations comply with data sharing mandates and standards.
5c. Enforcing compliance: Investigating non-compliance and applying enforcement actions such as fines/penalties.
5d. Managing API conformance certification: Testing and authenticating whether APIs meet the required technical standards before they are deployed in live environments.
5e. Oversight of governance bodies: Holding governance bodies to account to ensure they act fairly, transparently and in the public interest.

3.5.2 The current state of regulatory and compliance functions

In the UK's Open Banking scheme, the current approach to regulatory and compliance functions is complex, with both the CMA and FCA taking on responsibilities.

The CMA can enforce scheme rules among the CMA9, as specified in its Retail Banking Market Investigation Order 2017, through directions or court proceedings. It is supported to so by Open Banking Limited (OBL) which monitors compliance, escalating issues to the CMA for enforcement as necessary.[54] To monitor compliance, OBL has established Management Information (MI) reporting requirements. For example, banks and ATPs must report their conversion rates – the proportion of end-users who successfully complete an Open Banking journey such as payment authorisation or linking bank accounts with ATPs – which OBL will flag to the CMA if they fall below an acceptable threshold.[55]

The CMA is supported in this endeavour by the Financial Conduct Authority (FCA), which regulates firms that provide Open Banking services, particularly ATPs (e.g., Account Information Service

[50] Competition and Markets Authority, 2022. Open Banking Lessons Learned Review.
[51] European Journal of Law and Economics, 2023. Data portability and interoperability: An E.U.-U.S. comparison.
[52] OECD, 2021. Mapping data portability initiatives, opportunities and challenges.
[53] GDPR Hub, accessed January 2025. Article 82 - Right to compensation and liability.
[54] CMA, 2022. The future oversight of the CMA's Open Banking remedies Response to consultation.
[55] Open Banking Limited, 2023. Trustee End Of Implementation Roadmap Report.

Providers, Payment Initiation Service Providers). Under the Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011, the FCA: receives reporting on certain aspects of Smart Data compliance (e.g. API availability), can approve or revoke authorisations for ATPs, can investigate misconduct or failure to meet regulatory standards, can impose substantial fines or sanctions, or can remove a provider from the Financial Services Register.[56]

Such mechanisms help ensure that Open Banking delivers its intended benefits, mitigating risks such as inconsistent API performance, which has historically hindered the effectiveness of Open Banking.[57]

However, the CMA's Open Banking Lessons Learned Review in 2022 noted that governance arrangements for OBL were "poorly defined", with it operating with a minimal board and no formal reporting lines. [58] This led to the formation of the Joint Regulatory Oversight Committee (JROC) in 2023 to provide oversight of OBL, ensuring it acts transparently and in the public interest. JROC comprises HM Treasury, the CMA, FCA, and PSR. The CMA and FCA are in turn held to account by their respective sponsoring government departments (HM Treasury for the FCA and DBT for the CMA) through statutory reporting requirements, regular performance reviews, and ministerial oversight.

3.5.3 What are the design preferences of participants for regulatory and compliance functions?

Research participants expressed the following preferences for the design and delivery of customer protection and engagement functions in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 14: Compliance monitoring should include light-touch reporting requirements.** Automated reporting requirements were seen as helpful to flag potential breaches without imposing excessive regulatory burden.
- **Design preference 15: Enforcement should be led by one regulator in each sector where possible.** Participants generally favoured having a single, clearly accountable regulator per sector, capable of investigating non-compliance and applying proportionate penalties or sanctions. This is straightforward in some sectors, but more complex in others (see Section 6.2).

3.6 Implementation

3.6.1 What are implementation functions?

Implementation functions are the practical engine of Smart Data schemes: they ensure that strategic decisions and regulatory frameworks are translated into real-world actions and outcomes. These functions focus on how Smart Data schemes are delivered, coordinated, and sustained over time. They encompass a broad set of operational responsibilities, including programme planning, stakeholder engagement, and financial management. Once the UK's Smart Data economy spans multiple sectors and regulatory domains, implementation functions will provide the connective tissue that holds these efforts together: aligning stakeholders, coordinating activities, resolving disagreements, and adapting plans in response to emerging challenges. They also play a key role in fostering collaboration – both within the UK and internationally – by promoting shared learning, consistent practice, and alignment with evolving global standards.

[56] Financial Conduct Authority, 2024. Payment Services and Electronic Money – Our Approach.
[57] Open Banking Limited, 2023. Trustee End Of Implementation Roadmap Report.
[58] Competition and Markets Authority, 2022. Open Banking Lessons Learned Review.

Table 9 - Governance functions in the 'Implementation' category.

Governance functions in this category:
6a. Developing implementation plans: Setting timelines, milestones and delivery plans for Smart Data rollout in each sector and across sectors.
6b. Stakeholder engagement and representation: Ensuring Smart Data governance reflects a range of perspectives, including but not limited to consumers, SMEs and industry.
6c. Facilitating knowledge sharing: Ensuring different actors and schemes are learning from one another.
6d. Setting up appeals and dispute resolution mechanisms: Providing clear and accessible routes to challenge decisions or resolve disagreements between parties (excluding customers).
6e. Managing funding models: Designing and implementing funding models for Smart Data governance bodies, including who pays and how.
6f. International engagement: Engaging with international governments and industry groups to align Smart Data schemes with global best practices and support cross-border data sharing.

3.6.2 The current state of implementation functions

In the UK's Open Banking scheme, many of the key implementation functions to date have been carried out by Open Banking Limited (OBL): a central implementation body established by the CMA. OBL was responsible for developing the implementation plan and delivering it in close consultation with stakeholders. This included coordinating input from banks, Authorised Third-party Providers (ATPs), consumer groups, and regulators, and establishing working groups and advisory panels to ensure diverse representation. OBL also developed a Dispute Management Service, enabling firms to resolve liability disputes in the event of consumer claims, and supported knowledge sharing across participants.[59]

3.6.3 What are the design preferences of participants for implementation functions?

Research participants expressed the following preferences for the design and delivery of implementation functions in future Smart Data governance models (see Appendix F for more detail):

- **Design preference 16: Stakeholder forums should represent a wide range of relevant actors, including SMEs, consumer advocates, and representatives from marginalised or underrepresented communities.** Participants across sectors emphasised the need for balanced and inclusive representation, ensuring that governance structures do not become dominated by large incumbents or disproportionately reflect the interests of a single stakeholder group.

[59] Open Banking Limited, 2023. Trustee End Of Implementation Roadmap Report.

4. Understanding interoperability in Smart Data

Throughout this report, we regularly refer to the concept of 'interoperability'. In the most general sense, interoperability refers to "the ability of two or more systems or components to exchange information and to use the information that has been exchanged."[60] In the context of the Smart Data economy, interoperability means ensuring that data can be seamlessly shared between actors both *within* and *across* Smart Data schemes. Effective interoperability is essential to unlocking the full value of Smart Data. As more services emerge that combine data from multiple sectors, governance systems should aim to ensure consistency and compatibility between schemes.

Within Smart Data schemes, interoperability is achieved when ATPs can smoothly access data from data holders in the same scheme to support delivery of the intended service. This is supported by a range of governance functions, including but not limited to:

- **2a. Defining and maintaining technical standards:** Data holders and ATPs working to common scheme-wide technical standards ensures data can be shared and interpreted easily.
- **3c. Maintaining an authorised list of ATPs:** Straightforward mechanisms for data holders to confirm ATPs are accredited enables and speeds up data sharing.
- **4c. Defining consent requirements:** Scheme-wide approaches to gathering and sharing customer consent facilitates smooth data sharing by enabling data holders to share customer data based on consent tokens gathered by ATPs.
- **4d. Defining authentication requirements:** Scheme-wide approaches to verifying the identity of both customers and ATPs facilitates smooth data sharing by enabling data holders to share customer data through (a) customer authentication gathered by ATPs and (b) a commonly agreed approach to authenticating the ATPs themselves.

Across Smart Data schemes, interoperability is achieved when ATPs can smoothly access data from data holders across multiple different schemes to support delivery of the intended service. This is also supported by a range of governance functions, including but not limited to:

- **2e. Ensuring cross-sector interoperability of standards:** Aligned standards across different schemes supports data sharing across schemes. This may include the development of a core set of shared data and API standards across sectors, particularly focusing on standardising unique identifiers like name, date of birth, and address. Without such interoperable standards, data is difficult to meaningfully exchange or interpreted between Smart Data schemes.
- **3d. Ensuring cross-sector recognition of ATP accreditation**: A centralised accreditation system – or alignment of several accreditation systems to enable passporting – is vital to enable ATPs to operate consistently across sectors without repeating approval processes.
- **4c. Defining consent requirements:** A standardised consent framework – potentially via a cross-sector consent dashboard – is key to enabling smooth experiences for customer and ensuring their permissions apply consistently across sectors.
- **4d. Defining authentication requirements:** Shared authentication standards, or even a cross-sector authentication solution, help reduce friction in cross-sector journeys and ensure consistent verification of customer and ATP identity regardless of which sector's data is being accessed.
- **5a. Monitoring compliance:** Ensuring a similar approach to monitoring compliance with data sharing mandates and standards is taken across sectors will be important to limit reporting burden for ATPs and ensure they can easily operate across sectors.

[60] Institute of Electrical and Electronics Engineers, 1990. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.

- **5c. Enforcing compliance:** A joined-up approach to investigating non-compliance and applying enforcement actions across different schemes will be critical to ensuring all participants in a Smart Data scheme operate according to agreed rules, and don't 'slip through the gaps' between different regulators when operating across sectors.

To further understand what interoperability means in the Smart Data context, and what it requires in practice, we tested it conceptually across a wide range of potential Smart Data use cases. Through these use cases, we examined where and how interoperability between Smart Data schemes could be challenged: for instance, in cross-sector services involving financial and property data, or in consumer switching journeys that touch on both telecoms and energy. This helped us explore the kinds of frictions that might arise, and the governance levers most relevant to resolving them.

To avoid duplication, we present just one detailed use case in this report. This example illustrates what full interoperability would look like for a use case supporting carbon reporting in food supply chains, from the perspective of four key actor types: (1) customers, (2) Authorised Third-party Providers (ATPs), (4) data holders, and (5) regulators. In doing so, it helps to illuminate how the governance functions outlined earlier in this section are necessary to deliver a seamless, interoperable experience across schemes.

Following the example use case, we also summarise several additional considerations that emerged during this exercise and our stakeholder engagement. These outline further interoperability and governance challenges that are not fully addressed in the use case outlined here, but which highlight the types of scenarios Smart Data governance may need to accommodate.

The role of government departments is not directly included in the example use case, because they are not directly involved in data sharing or operational delivery, and therefore are not direct beneficiaries of interoperability; their role focuses on setting policy and strategic direction. However, they have an obligation to consider interoperability when shaping policy and strategy, and should work in a joined-up way to ensure consistency and alignment across Smart Data schemes from the outset.

4.1 Example use case: Carbon reporting in food supply chains

Tracking the carbon emissions associated with food products is currently challenging. This example use case envisions an ATP providing a service that tracks and reports the carbon footprint of food products as they move through supply chains, focusing firstly on emissions from farms and transport providers. Using this service, supermarkets could provide product carbon footprint information through digital product labels. Meanwhile, businesses in the supply chain (i.e. farm operators or transport providers) may use the service for sustainability reporting, with the ATP having 'write' permissions to provide carbon intensity benchmarking and suggestions for reducing carbon emissions directly into farm and transport management systems. This involves sharing data from the following sectors:

- **Agrifood:** E.g. crop type, livestock emissions, fertiliser use, machinery fuel usage (to calculate farm-level emissions of the food product).
- **Transport:** E.g. distance travelled, vehicle type, fuel source, product batch tracking (to measure emissions associated with the distribution and movement of the food product).
- **Retail:** E.g. product identifiers such as Product SKU, shelf placement, packaging format (to link emissions to specific food products and present the carbon score at point of sale).

As before, rather than considering user experiences at every step of the journey for this use case, we focus on five key stages of the use case where interoperability is most essential:

1. An ATP applies for and receives accreditation to access relevant data.
2. Farms and transport providers give consent for sharing operational data and providing 'write access' to farm and transport management systems.
3. Technology platforms used by the farms and transport providers share data with the ATP.

4. The ATP converts operations data into carbon footprint estimates for each product item, and shares this with supermarkets.
5. The ATP provides carbon intensity benchmarking and suggestions for reducing carbon emissions directly into farm and transport management systems.

For this use case, we also explore the following two contingency scenarios: (1) a dispute arises between the ATP and a data holder about appropriate sharing of data, and (2) a customer makes a complaint that their data has been misused by the ATP. Please note that although in this example the use case customers are businesses, very similar user needs and interoperability considerations would apply in use cases where the customer is an individual consumer.

4.1.1 Stage 1: An ATP applies for and receives accreditation to access relevant data.

Table 10 - User needs and interoperability considerations in Stage 1 of an example use case.

Actor	User need	Interoperability considerations
Customer: N/A		
ATP: Agritech firm	**As an** agritech firm… **I need** to complete one simple accreditation process to access agrifood, transport and retail data… **So that** I can quickly and easily establish my carbon reporting service.	**Function 2b:** A clear schema of data security classifications across schemes enables the agritech firm to understand the security levels of each data type it aims to access, across agrifood, transport and retail schemes. **Function 3a:** A common approach to determining ATP eligibility criteria across schemes helps the agritech firm understand relevant accreditation requirements it needs to fulfil. **Function 3b or 3d:** A centralised cross-scheme accreditation process, and or a passporting system between schemes, means the agritech firm only applies for accreditation once.
Data holder: N/A		
Regulator: Agrifood regulator (tbc), Transport regulator (tbc), Retail regulator (tbc).	**As an** agrifood, transport or retail regulator… **I need** visibility of who has been accredited to share data within the scheme I regulate… **So that** I can uphold regulations and coordinate with other regulators if needed.	**Function 3a:** A common approach to determining ATP eligibility criteria across schemes helps regulators understand standards ATPs should work to, including if operating across multiple schemes. **Function 3c or 3d:** Access to a central authorised list of ATPs across all schemes – or access to standardised authorised lists from other sectors – means regulators can see which organisations are accredited to share data in their sector.

4.1.2 Stage 2: Farms and transport providers give consent for sharing operational data and providing 'write access' to farm and transport management systems.

Table 11 - User needs and interoperability considerations in Stage 2 of an example use case.

Actor	User need	Interoperability considerations
Customer: Farm operator or transport provider	**As a** farm operator or transport provider… **I need** to provide consent for data sharing and verify my identity just once at the beginning of the process… **So that** I don't have to repeat these steps multiple times.	**Function 4c:** Common consent requirements across schemes mean customers give consent for data sharing across the agrifood, transport, and retail sectors just once. **Function 4d:** Common authentication requirements across schemes mean customers verify their identity just once, and this supports data sharing by data holders across the agrifood, transport, and retail sectors.
ATP: Agritech firm	**As an** agritech firm… **I need** standard approaches to gathering customer consent and authenticating customers… **So that…** I can make data requests to data holders in different sectors at later stages of the process.	**Function 4c:** Common consent requirements across schemes mean ATPs can develop one simple interface for gathering customer consent, which it can then use to request data from across the agrifood, transport, and retail sectors. **Function 4d:** Common authentication requirements across schemes mean ATPs can develop a single customer authentication process to support data requests across the agrifood, transport, and retail sectors.
Data holder: N/A		
Regulator: N/A		

4.1.3 Stage 3: Technology platforms used by the farms and transport providers share data with the ATP.

Table 12 - User needs and interoperability considerations in Stage 3 of an example use case.

Actor	User need	Interoperability considerations
Customer: Farm operator or transport provider	**As a** farm operator or transport provider… **I need** to collect and submit my operational data in a single, standardised format… **So that** I can effectively contribute to the correct carbon footprint calculation of my product.	**Function 2a or 2e:** Common data standards across schemes mean farm operators provide agrifood details in a format which allows the food product to be reliably identified by all parties across the agrifood, transport and retail sectors.
ATP: Agritech firm	**As an** agritech firm… **I need** to receive data in standardised formats and via standardised APIs… **So that** I can easily access and use all relevant data from both farm and transport customers.	**Function 2a or 2e:** Common standards for data formats and APIs across schemes mean the ATPs can easily access data in a consistent format from both farm management systems and transport management systems.

Data holder: Farm management system or transport management system	**As a** farm management system or transport management system… **I need** to ensure the ATP requesting data is properly accredited and that there is consent from my farm or transport customer for data sharing… **So that** I am complying with all data sharing regulations when sharing farm or transport information.	**Function 3c or 3d:** Access to a central authorised list of ATPs across all schemes – or joined up authorised lists across sectors – means data holders can check ATPs are accredited to share data in their sector. **Function 4c:** Common consent requirements across sectors mean data holders are assured they have received appropriate customer consent to share data. **Function 4d:** Common authentication requirements across schemes mean data holders are assured the customer requesting data sharing has been appropriately authenticated.
Regulator: N/A		

4.1.4 Stage 4: The ATP converts operations data into carbon footprint estimates for each product item, and shares this with supermarkets.

Table 13 - User needs and interoperability considerations in Stage 4 of an example use case.

Actor	User need	Interoperability considerations
Customer: Supermarkets	**As a** supermarket… **I need** to receive product-level carbon data in a format that aligns with my existing product categorisation and labelling systems… **So that** I can easily integrate and display the information to shoppers.	**Function 2a or 2e:** Common product and emissions data standards across agrifood, transport and retail schemes mean supermarkets can integrate carbon data into their existing product catalogues with minimal customisation.
ATP: N/A		
Data holder: N/A		
Regulator: N/A		

4.1.5 Stage 5: The ATP provides carbon intensity benchmarking and suggestions for reducing carbon emissions directly into farm and transport management systems.

Table 14 - User needs and interoperability considerations in Stage 5 of an example use case.

Actor	User need	Interoperability considerations
Customer: N/A		
ATP: Agritech firm	**As an** agritech firm… **I need** to be able to 'write' permissions for farm and transport management systems… **So that** I can automatically suggest and implement emissions reductions actions on behalf of my clients.	**Function 3b:** A shared accreditation process across sectors ensures that once the ATP is approved to have 'write access' to data at a certain security classification, it can offer consistent services across agrifood, transport and retail without duplicative or inconsistent accreditation processes. **Function 4c:** A harmonised cross-sector consent framework ensures ATPs can easily gather consent from both farm operator and transport provider to both read data and initiate sustainability-related actions.

Data holder: Farm management system or transport management system	**As a** farm management system or transport management system… **I need** clarity on when and how an ATP can initiate changes through my platform… **So that** I can securely support the delivery of this additional service to my customers.	**Function 3c or 3d:** Access to a central authorised list of ATPs across all schemes – or joined up authorised lists across sectors – means data holders can check ATPs are accredited to not just read data but have 'write access' to data systems in their sector. **Function 4c:** Common consent requirements across sectors mean data holders are assured they have received appropriate customer consent to provide 'write access' to their systems. **Function 4d:** Common authentication requirements across schemes mean data holders are assured the customer enabling 'write access' to their system has been appropriately authenticated.
Regulator: N/A		

4.1.6 Contingency scenario 1: A dispute arises between the ATP and a data holder about appropriate sharing of data.

Table 15 - User needs and interoperability considerations in Contingency scenario 1 of an example use case.

Actor	User need	Interoperability considerations
Customer: N/A		
ATP: Agritech firm	**As an** agritech firm… **I need** a clear, consistent process for raising and resolving disputes with data holders across different sectors… **So that** I can address access issues efficiently and avoid delays to my service.	**Function 2a:** Common technical standards mean the ATP understands the conditions under which data must be shared and the grounds on which access may be denied. **Function 6d:** Aligned and joined-up dispute resolution mechanism(s) across schemes mean the ATP can appeal data access decisions using a standard process, regardless of which sector the data holder operates in.
Data holder: Farm management system or transport management system	**As a** farm management system or transport management system… **I need** a fair and transparent process for responding to disputes raised by ATP… **So that** I can comply with my obligations while protecting sensitive data and resolving issues efficiently.	**Function 2a:** Common technical standards mean the data holder – like the ATP – understands the conditions under which data must be shared and the grounds on which access may be denied. **Function 6d:** Aligned and joined-up dispute resolution mechanism(s) across schemes mean data holders can respond to challenges using a predictable and accessible process.
Regulator: Agrifood regulator (tbc), Transport regulator (tbc).	**As a** sector regulator… **I need** to be notified of escalated disputes between ATPs and data holders, and to coordinate with other regulators when cross-sector issues arise… **So that** I can ensure scheme data sharing requirements and standards and being adhered to.	**Function 5a:** Standard compliance monitoring approaches across schemes mean the regulator investigating has access to historical records of the ATP's actions related to both property and financial data. **Function 6d:** Aligned and joined-up dispute resolution mechanism(s) across schemes mean regulators are made aware of disputes relevant to them, and do not duplicate work.

4.1.7 Contingency scenario 2: A customer makes a complaint that their data has been misused by the ATP.

Table 16 - User needs and interoperability considerations in Contingency scenario 2 of an example use case.

Actor	User need	Interoperability considerations
Customer: Farm operator or transport provider	**As a** farm operator or transport provider**…** **I need** a clear route to raise a complaint or seek redress, regardless of whether the issue related to agrifood or transport data… **So that** I don't have to navigate multiple organisations or processes.	**Function 4a**: A joined up cross-sector approach to managing complaints across sectors means consumers can lodge complaints without needing to understand sector boundaries.
ATP: Agritech firm	**As an** agritech firm… **I need** a single route to respond to complaints or disputes related to the data I've shared… **So that** I can fairly represent my case.	**Function 4a:** A joined up cross-sector approach to managing complaints across sectors means only one organisation (e.g. ombudsman, regulator) will take responsibility for handling the complaint, giving the ATP a single route for response.
Data holder: N/A		
Regulator: Agrifood regulator (tbc), Transport regulator (tbc).	**As an** agrifood or transport regulator… **I need** to know which parts of the agrifood supply chain I am responsible for enforcing compliance over and have a clear record of ATP activities… **So I** can investigate and apply enforcement actions (e.g. fines/penalties) if needed.	**Function 4a:** A joined-up approach to managing complaints across sectors means regulators are made aware of complaints relevant to them, and do not duplicate work. **Function 5a:** Standard compliance monitoring approaches across schemes mean the regulator investigating has access to historical records of the ATP's actions related to both agrifood and transport data.

4.2 Additional interoperability considerations for Smart Data

Beyond the illustrative use case outlined within table 16, stakeholders also identified four additional challenges to interoperability between Smart Data schemes in different sectors. A summary of these considerations is included within this report to guide future testing and refinement of governance functions.

1. Risk from combined datasets across sectors

Stakeholders also noted that combining datasets from different Smart Data schemes, each of which may individually be low-risk, can create new risks when used together. For example, a service combining property, retail, and transport data could inadvertently create highly granular and personally identifiable behavioural profiles, with implications for both consent and data protection. These risks are often emergent and may not be visible when reviewing schemes in isolation. This implies that:

- ATP accreditation processes should consider not only the sensitivity of individual data types, but how they interact across schemes;

- Scheme governance bodies may need shared principles or assessment tools to evaluate compound risks from combining datasets;
- Consent mechanisms should support cross-scheme transparency, enabling consumers to understand and manage how their data is used in services operating across multiple schemes.

2. Complex liability chains

In more complex Smart Data use cases, multiple actors across several different sectors may be involved in a service's delivery. If data is inaccurate, misused, or misrepresented, it may be difficult to determine which actor is at fault. This kind of inter-scheme liability chain raises the need for:

- Alignment of liability models across schemes to reduce inconsistency: for example, avoiding situations where an ATP is held liable under one scheme for an issue that, under another scheme, would place responsibility on the data holder. Without such alignment, cross-sector ATPs may face conflicting or duplicative obligations.
- Cross-scheme approaches to complaint handling and enforcing compliance, to ensure that, when a service failure spans multiple schemes, it is clear who is responsible for investigating the issue and providing redress.

3. Interaction with GDPR and the ICO's role in Smart Data governance

In cross-sector Smart Data services involving personal data, it is likely that data protection obligations under UK GDPR will intersect with multiple sector-specific Smart Data rules. For example, an ATP operating across finance and energy may be fully compliant with both sectors' Smart Data standards, yet still fall short of broader data protection expectations: for instance, in how it processes combined datasets or responds to consumer consent withdrawal. In this scenario, it may be unclear whether the ICO or the relevant sector-specific regulator(s) should take the lead in investigation or enforcement. To support coherent cross-scheme oversight, governance models could consider:

- Formal memoranda of understanding (MoU) between the ICO and sector-specific regulators responsible for each scheme;
- Standardised consumer redress pathways and signposting mechanisms that work consistently across schemes;
- Inclusion of the ICO in the design and periodic review of Smart Data trust frameworks, particularly those affecting high-risk data combinations.

4. Data-sharing across international borders

Many Smart Data services may involve data flows across international borders. In such cases, data may originate in a UK Smart Data scheme (e.g. UK Open Finance) but be used in a Smart Data scheme in another country (or vice versa), creating interoperability pressures between schemes in different countries. Specific concerns include:

- Whether ATP accreditation, consent models, and liability safeguards in UK schemes across different sectors are recognised or enforceable for non-UK actors;
- Whether UK Smart Data rules across different sectors align with international technical and legal standards (e.g., ISO, W3C, EU Data Act);
- How disputes involving foreign data holders or ATPs will be resolved.

This suggests keeping international operability in mind when designing UK Smart Data schemes could be valuable, particularly if schemes are to scale and remain competitive globally.

5. Developing Smart Data governance models

Building on our understanding of the governance functions required to establish and operate Smart Data scheme, we developed a longlist of six potential governance models. These were shaped by insights from both our literature review and qualitative research and refined through an iterative process of stakeholder engagement. The design preferences expressed by research participants for each function (see Appendix F) greatly informed the design of the governance models, which were developed to reflect these preferences as fully and consistently as possible. A key point of differentiation between the models is the extent to which functions are carried out by a single cross-sector delivery body or by sector-specific delivery bodies within individual Smart Data schemes. The six models developed were as follows:

1. **Model 1: Unified delivery** - Features a central Smart Data Authority (SDA) that drives forward Smart Data schemes across all sectors, taking a single unified approach. Meanwhile, sector-specific regulators enforce compliance in their sector and provide feedback to the SDA.
2. **Model 2: Centrally-led** - Features a central Smart Data Implementation Entity (SDIE) that drives forward Smart Data schemes across all sectors. Unlike the Smart Data Authority (SDA) in Model 1, the SDIE receives input from Sector-specific Advisory Groups to tailor delivery and oversight of Smart Data initiatives to each sector's requirements. Sector-specific regulators enforce compliance in their sector and provide feedback to the SDIE.
3. **Model 3: Federated** - Features Sector-specific Implementation Entities driving Smart Data schemes within their respective sectors, supported by a central Smart Data Coordination Entity (SDCE). The SDCE provides some centralised services and mandatory guidelines to ensure consistency and interoperability. Sector-specific regulators enforce compliance in their sector, working closely with Sector-Specific Implementation Entities. Both Sector-specific Implementation Entities and sector-specific regulators provide feedback to the SDCE.
4. **Model 4: Regulator-led** - Features Smart Data Offices (SDOs) driving Smart Data schemes within their respective sectors. These SDOs are located within the relevant sector-specific regulators and are responsible for both implementation and compliance functions. They are supported by a central Smart Data Guidance Entity (SDGE) which provides both mandatory and advisory guidelines to ensure a degree of consistency across sectors.
5. **Model 5: Decentralised** - Features Sector-specific Implementation Entities that drive forward Smart Data schemes within their sector and are coordinated through an advisory Smart Data Forum (SDF). Sector-specific regulators enforce compliance in their sector. The Smart Data Forum is self-organised by Sector-specific Implementation Entities and regulators for each relevant sector, albeit with Secretariat support from DBT.
6. **Model 6: Market-driven** - An industry-led approach to Smart Data governance. An opt-in approach would be taken, where ATPs sign contracts with data holders when entering data sharing arrangements and compliance would be governed by contractual law. This model would rely on voluntary engagement, with market forces driving participation.

5.1 Shortlisting governance models

We held an initial round of focus groups to test high-level designs of these six governance models. Following these focus groups, we were able to discount three of the governance models.

- **Model 1 (Unified delivery) was discounted** because participants felt it was overly centralised, and therefore would be too cumbersome and slow to implement, potentially stifling progress and innovation. They also believed it would lack the necessary sector-

specific flexibility, struggle to gain industry buy-in, and could hold back Smart Data in sectors where progress is already being made.

- **Model 5 (Decentralised) was discounted** because participants felt that the lack of an empowered centralised entity would lead to inconsistency across sectors, hindering the development of cross-sector data sharing. They also expressed concerns that the forum would become a "talking shop," failing to make clear joint decisions and potentially resulting in deadlock. Additionally, it was seen as posing a high risk of duplication of effort.
- **Model 6 (Market-driven) was discounted** because, without mandated data sharing enforced by a regulator and an implementation entity to drive forward delivery, there is a risk that scheme participation would be limited. In particular, large incumbent data holders are unlikely to voluntarily take on the significant upfront costs required to establish necessary data sharing infrastructure. The lack of a consistent cross-sector governance approach, backed by appropriate regulation, could also result in inconsistent approaches across sectors, preventing cross-sector data sharing.

This left us with a shortlist of three remaining governance models to take forward into a more detailed design stage. Therefore, for each shortlisted governance model, the remainder of this section outlines: (a) which actor types would be best placed to carry out each governance function, and (b) how those functions would be delivered in practice. Section 6 then outlines which existing organisations might assume the responsibilities of each actor type in the eight priority sectors.

In reviewing these three shortlisted governance models, please note the following:

1. The shortlisted governance models have been developed drawing heavily on the design preferences expressed by participants throughout the research (see Section 3 and Appendix F). Where design preferences were expressed most forcefully and unanimously by research participants, we have endeavoured to reflect them appropriately across all three shortlisted models; meanwhile, where design preferences were less unanimously expressed, we have introduced some distinguishing features in how they are reflected across the different models.
2. The shortlisted governance models were developed, in part, to test contrasting approaches to delivery, with Model 2 (Centrally-led) representing the most centralised approach and Model 4 (Regulator-led) the most decentralised. As such, differences in how the 32 governance functions are allocated to different actors sometimes reflect a deliberate effort to distinguish the models and stimulate discussion, rather than to prescribe a single ‘correct’ approach; in several cases, these functions could reasonably be allocated to different actors depending on the final scheme design. Section 7 outlines the qualitative and quantitative assessment of the three shortlisted models by research participants: in providing a clear explanation of why some models were preferred over others, this also provides implicit insight as to the preferred distribution of governance responsibilities between actors among our research participants.
3. The shortlisted governance models all represent a potential ‘end state’ for governance of the Smart Data economy; therefore, we would reasonably expect lighter-touch approaches to delivering some governance functions to be taken in early stages of implementation. For example, the development of a cross-sector authentication solution or complaints platforms would be unlikely to materialise in the first year of Smart Data delivery.
4. The following sections specify which organisations would be responsible for delivering each governance function under each potential governance model; however, they do not specify whether it would be most appropriate for each governance function to be delivered in-house or through procurement. In particular, delivery of joint consent (function 4c) and authentication (function 4d) services might be appropriate for outsourcing.

5.2 Model 2: Centrally-led

Model 2 (Centrally-led) is the most centralised of the three shortlisted models, featuring a central Smart Data Implementation Entity (SDIE) that drives forward Smart Data schemes across all sectors. The SDIE receives input from Sector-specific Advisory Groups to (a) make sure cross-sector approaches work for all relevant sectors and (b) tailor Smart Data schemes to the specific needs and context of each sector where necessary. However, the model aims to ensure cross-sector consistency wherever possible. Sector-specific regulators enforce compliance in their sector and provide feedback to the SDIE to shape its approach to delivering Smart Data schemes.

Figure 3 - Summary of Model 2 (Centrally-led).

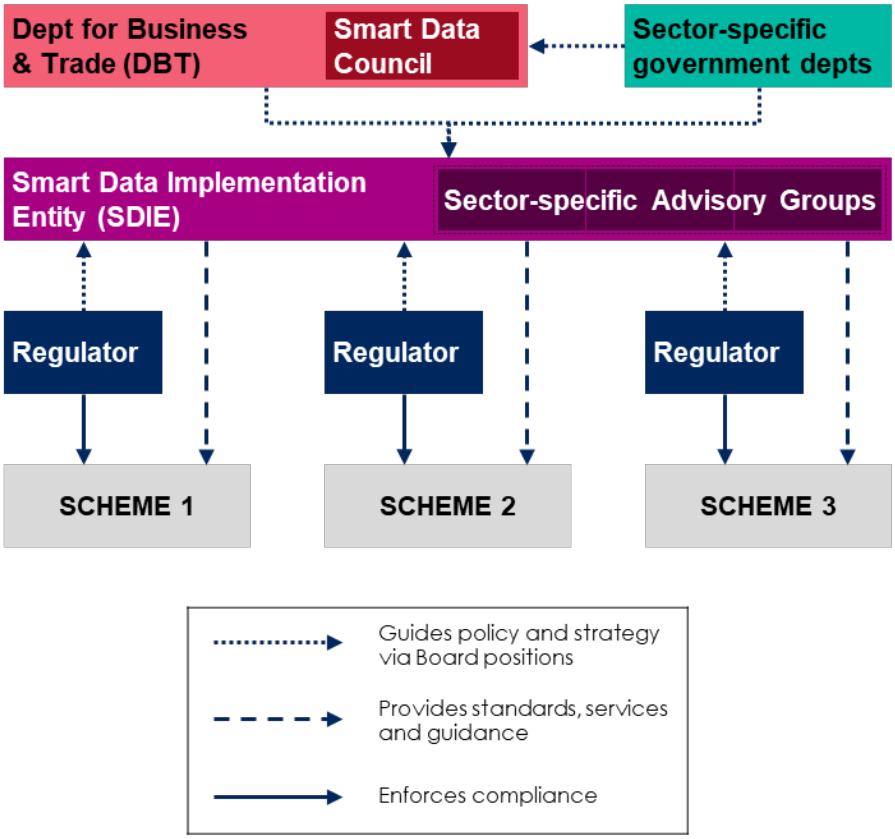


Table 17 provides a more detailed overview of how Model 2 (Centrally-led) would work, including a summary of the key actor types and a breakdown of responsibilities by governance function.

Table 17 - Detailed description of Model 2 (Centrally-led).

Model 2 (Centrally-led): The key actor types
Smart Data Implementation Entity (SDIE) In Model 2, the Smart Data Implementation Entity (SDIE) is the primary body responsible for driving Smart Data delivery across all participating sectors, aiming to promote cross-sector consistency wherever possible. Among numerous other responsibilities, it leads on developing common technical standards, accrediting ATPs, developing shared tools (e.g. consent dashboards, user authentication), and monitoring compliance across sectors. It convenes several Sector-specific Advisory Groups which advise the SDIE to ensure the delivery of Smart Data schemes is appropriate for all participating sectors. Given the extensive responsibilities and powers of the SDIE, it could be established as a new Arm's Length Body for the Department for Business & Trade (DBT). To ensure the needs of all sectors are accounted for, representatives from the relevant government department and

regulator for each participating sector could sit on the Board of the SDIE. For example, if a new Smart Data scheme was introduced in the retail energy sector, the Department for Energy Security and Net Zero (DESNZ) and Ofgem would each take a seat on the SDIE Board.

Sector-specific Advisory Groups
Sector-specific Advisory Groups provide input to the SDIE from industry, government departments, regulators, and customer representatives. The groups are convened by the SDIE (who would perform any secretariat duties) but each is co-chaired by one government and one industry representative from the relevant sector. Sector-specific Advisory Groups advise the SDIE on all aspects of Smart Data scheme delivery, with the recommendations of Sector-specific Advisory Groups shared with the SDIE Board for discussion and/or approval. However, they are purely advisory and do not have decision-making power.

Regulators
Sector-specific regulators (e.g. Ofgem for retail energy) primarily enforce compliance within their relevant sector, ensuring adherence to Smart Data mandates and standards. They investigate reported violations and apply penalties as necessary; however, responsibilities for monitoring compliance sit with the SDIE. Sector-specific regulators would also sign off the technical standards developed by the SDIE for implementation in the relevant sector. Sector-specific regulators contribute to shaping the work of the SDIE through Board positions at the SDIE and contributions to Sector-specific Advisory Groups. The Information Commissioner's Office (ICO) remains responsible for enforcing related data sharing regulation (e.g. GDPR).

DBT & other government departments
DBT collaborates with sector-specific government departments (e.g. DESNZ for retail energy) and regulators (e.g. Ofgem for retail energy) to set economy-wide Smart Data policy and ensure alignment with national goals. In doing so, DBT draws on expertise from different sectors through the Smart Data Council, which includes relevant government departments, regulators and industry experts; in this model, it also includes representation from the SDIE, while avoiding full duplication of membership with the SDIE Board. DBT could be responsible for establishing and overseeing the SDIE as a new Arm's Length Body.

However, sector-specific government departments define Smart Data mandates within their respective sectors, collaborating with DBT to ensure consistency. Sector-specific government departments, like sector-specific regulators, also contribute to shaping the work of the SDIE through Board positions at the SDIE and contributions to Sector-specific Advisory Groups.

Model 2 (Centrally-led): Responsibility for each governance function	
1. Policy and strategy	
1a. Setting the vision and strategic direction: Identifying the key aims of the scheme in each sector, including by selecting priority use cases.	DBT leads on setting the vision for Smart Data across sectors. This includes developing a plan for new sectors to be introduced to the Smart Data economy and establishing priority goals for the SDIE. When a new scheme is being established, sector-specific government departments define the priority aims and use cases for the sector, with support from DBT. In doing so, they consult with a wide range of stakeholders across the relevant sector, including the relevant regulator: this supports the convening of a group of engaged stakeholders to form a Sector-specific Advisory Group within the SDIE once the scheme is established.

1b. Defining data sharing mandates: Determining the data types industry organisations are required to share when requested by customers.	Sector-specific government departments define data sharing mandates for their respective sectors, deciding on the data types that data holders are required to share with ATPs at the customer's request. Sector-specific government departments are supported to do so by DBT and consult with a wide range of stakeholders across the relevant sector, laying the foundations for developing Sector-specific Advisory Groups.
1c. Defining data sharing principles: Setting high-level principles which data sharing should comply with.	DBT sets high-level cross-sector data sharing principles to underpin data sharing practices across all sectors. This provides guidelines for developing or adapting Smart Data trust frameworks and standards.
1d. Designing or adapting trust frameworks: Setting out how data is shared, used, and protected by participants in Smart Data schemes, including liability for errors or wrongdoing.	DBT designs an economy-wide Smart Data Trust Framework, informed by the established data sharing principles and drawing on expertise from across sectors through the Smart Data Council. The trust framework is signed off and published by DBT and informs delivery of a wide range of other governance functions included in this table. Once established, DBT is responsible for reviewing the Smart Data Trust Framework periodically, potentially through the Smart Data Council, to reflect technological advancements, changes in legislation, and the introduction of new sectors to the Smart Data economy. DBT is responsible for signing off any updates to the Smart Data Trust Framework.
1e. Designing or adapting governance models: Deciding the design, composition and remit of formal Smart Data governance entities, including roles and decision-making powers.	DBT designs a cross-sector Smart Data governance model, working with sector-specific government departments to formalise powers for relevant governance bodies in each sector through secondary legislation where necessary. DBT leads reviews of Smart Data governance models every five years, and implements changes as required.
1f. Aligning with other government policy: Aligning Smart Data schemes with broader digital and data strategies across government.	DBT scans for relevant interdependencies across government departments and actively aligns Smart Data approaches (including through instruction to the SDIE). Sector-specific government departments and regulators bring new developments across government to DBT's attention via their role on the Smart Data Council.
1g. Advising on policy and strategy: Feeding industry and consumer voices into all policy and strategy decisions, thereby shaping the work in 1a, 1b, 1c, 1d and 1e.	The Smart Data Council, including relevant government departments, regulators, industry experts and the SDIE, feeds expertise from across sectors into policy and strategy decisions made by DBT and sector-specific government departments. Where sector-specific challenges arise, DBT and sector-specific government departments may also draw on the advice of Sector-specific Advisory Groups within the SDIE.

2. Standards development	
2a. Defining and maintaining technical standards: Creating and updating the data and API specifications that underpin how data is shared between parties.	A Central Standards Working Group, convened within the SDIE and comprising technical experts from Sector-specific Advisory Groups, defines and periodically updates standards across all Smart Data schemes. Technical standards are uniform across sectors as far as possible, although with some scope for sector-specific standards. Where Sector-specific Advisory Groups identify a change is required to either economy-wide or sector-specific standards, they make a recommendation to the Central Standards Working Group which retains decision-making power. Sector-specific regulators then sign off standards for their sector.
2b. Developing data security classifications: Defining levels of sensitivity for different types of data and adjusting security requirements accordingly.	A Central Data Classification Working Group, convened within the SDIE and comprising technical experts from Sector-specific Advisory Groups, sets data security classifications across all Smart Data schemes, taking into account the risks associated with both 'read only' and 'write' access. Sector-specific Advisory Groups make recommendations when they identify a change is required, but do not have decision-making power.
2c. Developing privacy and security standards: Designing the controls, policies and procedures to ensure that data sharing protects user privacy and system security.	The SDIE develops privacy and security standards for all Smart Data schemes, taking into account different data security classifications and differences in risk between 'read only' and 'write' access for ATPs. These include consent mechanisms, identity authentication, breach protocols, and data minimisation principles. The SDIE works closely with the ICO to ensure consistency with national data protection laws. Sector-specific Advisory Groups make recommendations when they identify a change is required, but do not have decision-making power.
2d. Defining customer experience guidelines: Outlining rules for customer data sharing journeys.	The SDIE sets minimum customer experience requirements across all schemes, including testing potential user journeys with consumers. Sector-specific Advisory Groups make recommendations when they identify a change is required, but do not have decision-making power.
2e. Ensuring cross-sector interoperability of standards: Coordinate standards across sectors to ensure interoperability across industries.	The SDIE ensures that all technical standards, data security classifications, privacy and security standards and customer experience guidelines are sufficiently aligned across sectors to enable interoperability.
3. Accreditation of Authorised Third-party Providers (ATPs)	
3a. Determining ATP accreditation requirements: Defining the eligibility criteria and conditions Authorised Third-party Providers must meet to be accredited.	The SDIE defines common ATP eligibility criteria across sectors (e.g. insurance, data protection standards), building on established standards and tiering requirements in line with the security classification of the data being accessed. Where Sector-specific Advisory Groups identify a change is required to these eligibility criteria, they make a recommendation to the SDIE which retains decision-making power.

3b. Delivering ATP accreditation process: Running the assessment and onboarding processes that grant or revoke ATP status for third parties.	The SDIE operates a central ATP accreditation service, including onboarding, document checks, background screening, and periodic review and renewal of accreditation once granted. ATP accreditation provided by the SDIE is valid for data at permitted security classifications across all sectors, ensuring ATPs need to be accredited just once to share data across sectors.
3c. Maintaining an authorised list of ATPs: Keeping an up-to-date public list of accredited third parties that are authorised to access and use Smart Data, that allows data holders and users to confirm ATP credentials.	The SDIE maintains a dynamic, publicly searchable authorised list of accredited ATPs, noting the data security classifications they are permitted to access. This is accessible via an API and regularly updated to reflect additions, revocations and updates to the permissions of ATPs.
3d. Ensuring cross-sector recognition of ATP accreditation: Enabling ATPs accredited under one scheme or sector to be recognised in others without a duplicative process.	The SDIE facilitates cross-sector recognition of ATP accreditation across sectors by ensuring consistent eligibility criteria, running a single accreditation process and maintaining a central authorised list of ATPs recognised across all sectors.
4. Customer protection and engagement	
4a. Handling customer complaints and redress: Managing systems that allow customers to raise concerns and access remedies when issues arise.	The SDIE operates a single platform for handling customer complaints, providing a 'single front door' for Smart Data-related customer redress where the initial complaint cannot be resolved directly with the data holder. This may include developing a complaints contact address, responding to complaints which do not meet thresholds for action, investigating less serious complaints and liaising with scheme participants to reach a resolution, and/or signposting more serious complaints to the ICO, relevant regulator or Ombudsman as needed.
4b. Promoting consumer understanding: Promoting public understanding of Smart Data and encouraging safe, informed participation by consumers.	The SDIE runs national communications and education campaigns to raise awareness of Smart Data, educating customers about their privacy rights and how Smart Data could benefit them. The SDIE collaborates with consumer groups to ensure messages reach diverse audiences.
4c. Defining consent requirements: Outlining rules for how informed customer consent is obtained, including offering shared or standardised customer consent solutions.	The SDIE leads on developing unified, cross-sector customer consent requirements, consent journeys and consent dashboards, likely drawing on Ofgem's existing work to develop a customer consent solution. It ensures consent mechanisms are simple, clear, and comply with GDPR and other data protection regulations. Where necessary, Sector-specific Advisory Groups input into the design of sector-specific consent journeys.

4d. Authenticating customers and ATPs: Establishing processes to confirm the identity of customers and ATPs in Smart Data schemes, potentially leveraging digital identity frameworks.	The SDIE sets customer and ATP authentication standards, ensuring consistency across sectors and taking into account different data security classifications. The SDIE collaborates with trusted digital identity providers to establish an interoperable cross-sector authentication service which meets those standards. Sector-specific Advisory Groups may advise on different user types and tiering of authentication requirements in each sector.
5. Regulatory and compliance	
5a. Monitoring compliance: Tracking whether organisations fulfil their obligations to comply with data sharing mandates and standards.	The SDIE continuously monitors compliance with data sharing mandates and standards across all Smart Data schemes, potentially including establishing reporting requirements for some data holders. The SDIE issues pre-enforcement notices where low-level instances of non-compliance are first identified. Serious or ongoing instances of non-compliance are escalated to the relevant regulator with recommended next steps.
5b. Encouraging compliance: Providing guidance and support to help organisations comply with data sharing mandates and standards.	The SDIE works with Sector-specific Advisory Groups to co-develop guidance and best practice toolkits to support data holders and ATPs to comply with data sharing mandates and standards, including when operating across sectors. These are customised by sector and published openly.
5c. Enforcing compliance: Investigating non-compliance and applying enforcement actions such as fines/penalties.	Regulators retain full enforcement responsibility, investigating reported instances of non-compliance and applying penalties as necessary among data holders and ATPs. The SDIE supports coordination between regulators when instances of non-compliance straddle the boundaries of two or more schemes.
5d. Managing API conformance certification: Testing whether APIs meet required technical standards before they are deployed.	The SDIE, with input from Sector-specific Advisory Groups, provides a centralised conformance certification process for APIs, offering sandbox environments to ensure APIs meet published standards before live deployment.
5e. Oversight of governance bodies: Holding governance bodies to account to ensure they act fairly, transparently and in the public interest.	DBT are responsible for overseeing the SDIE, ensuring it operates transparently and in the public interest. Oversight includes regular performance reviews and public reports to ensure the SDIE meets its objectives and remains accountable to the public.
6. Implementation	
6a. Developing implementation plans: Setting timelines, milestones and delivery plans for Smart Data rollout in each sector and across sectors.	The SDIE develops a detailed cross-sector Smart Data implementation plan, drawing on the advice of the Sector-specific Advisory Groups. This plan is reviewed and signed off by DBT, drawing on expertise from across sectors through the Smart Data Council. Progress is tracked through quarterly reviews to ensure Smart Data rollout remains on track.

6b. Stakeholder engagement and representation: Ensuring Smart Data governance reflects a range of perspectives, including but not limited to consumers, SMEs, and industry.	The SDIE runs stakeholder engagement programmes centrally when consulting on changes to Smart Data delivery. It ensures that engagement is inclusive and that diverse perspectives (e.g. SMEs, rural businesses, marginalised consumer groups) shape Smart Data delivery.
6c. Facilitating knowledge sharing: Ensuring different actors and schemes are learning from one another.	The SDIE maintains a broad Smart Data community of practice to share insights and lessons across schemes. Sector-specific Advisory Groups feed in case studies, pilots and pain points to share.
6d. Setting up appeals and dispute resolution mechanisms: Providing clear and accessible routes to challenge decisions or resolve disagreements between parties (excluding customers).	The SDIE manages a centralised dispute resolution process to resolve disagreements between parties (excluding customers) in all Smart Data schemes, ensuring consistent processes and access to appeals across sectors.
6e. Managing funding models: Designing and implementing funding models for Smart Data governance bodies, including who pays and how.	DBT designs and administers a cross-sector funding model for Smart Data schemes, taking the advice of sector-specific government departments and regulators. This could include drawing on: government investment for initial set-up costs, regulatory levies, ATP accreditation fees, and/or commission taken on any other payments made within schemes (depending on the chosen commercial model).
6f. International engagement: Engaging with international governments and industry groups to align Smart Data schemes with global best practices and support cross-border data sharing.	DBT leads the UK's international Smart Data engagement. The SDIE supports this by engaging in international forums and bilateral relationships with Smart Data schemes in other countries. This includes ensuring alignment with global data exchange frameworks (e.g. ISO, W3C).

5.3 Model 3: Federated

Model 3 (Federated) takes a less centralised approach to Smart Data governance than Model 2 (Centrally-led). In Model 3, Sector-specific Implementation Entities drive Smart Data schemes within their respective sectors, supported by a central Smart Data Coordination Entity (SDCE). The SDCE could be established within the Department for Business & Trade and provide centralised services and mandatory guidelines to ensure consistency and interoperability across different sectors; however, it has a significantly smaller scope than the Smart Data Implementation Entity (SDIE) in Model 2. Sector-specific regulators enforce compliance in their sector, working closely with Sector-Specific Implementation Entities. Both Sector-specific Implementation Entities and sector-specific regulators would shape the work of the SDCE, potentially via positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators. This model aims to balance sector-specific needs and nuance with the benefits of central coordination in areas like developing standards and accrediting ATPs.

Figure 4 - Summary of Model 3 (Federated).

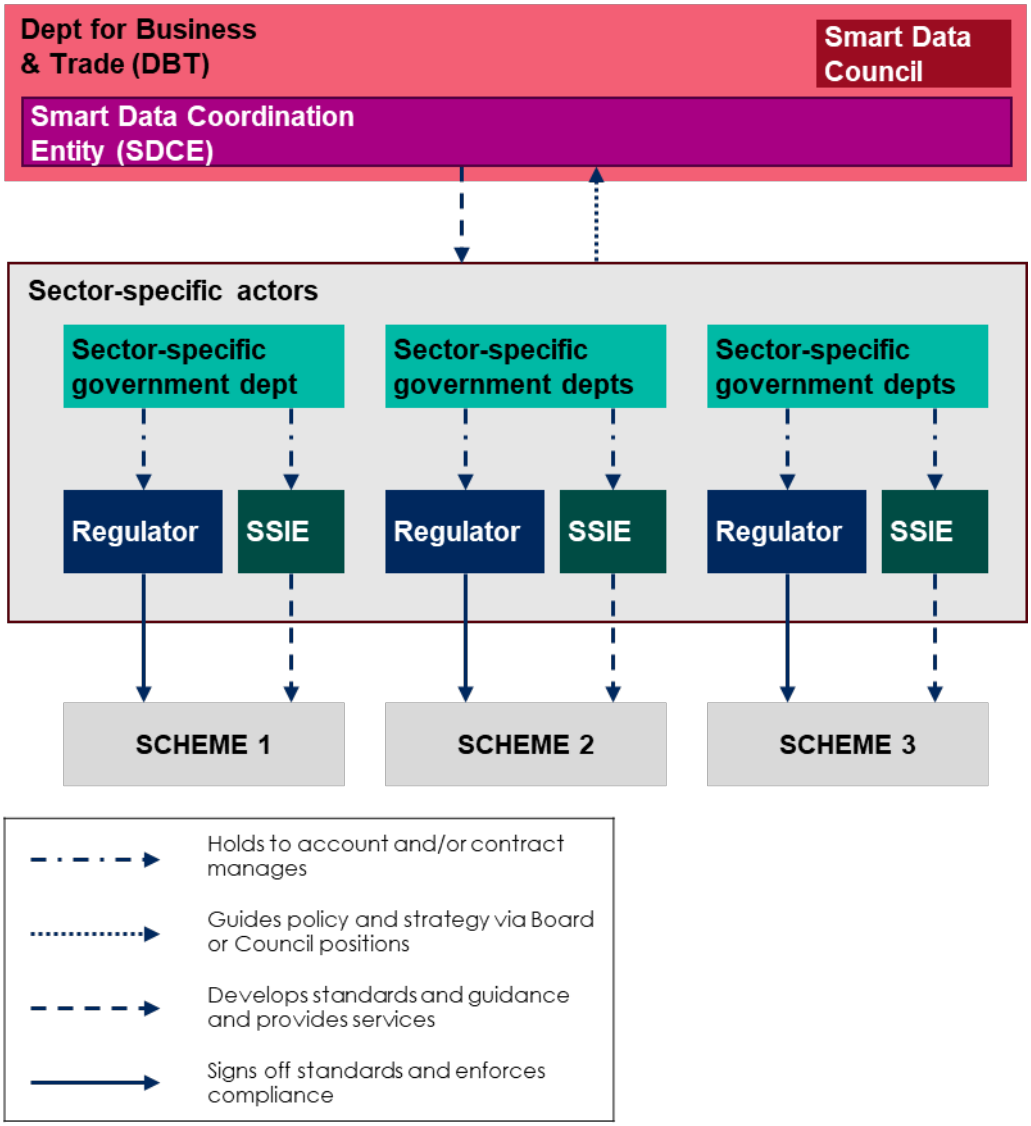


Table 18 provides a more detailed overview of how Model 3 (Federated) would work, including a summary of the key actor types and a breakdown of responsibilities by governance function.

Table 18 - Detailed description of Model 3 (Federated).

Model 3 (Federated): The key actor types
Sector-specific Implementation Entities In Model 3, Sector-specific Implementation Entities drive forward Smart Data delivery within each sector. Among other things, they develop standards, develop data security classifications, handle customer complaints, monitor compliance and administer dispute resolution mechanisms within their scheme. However, in completing many of these governance functions, they work within guidelines established by the Smart Data Coordination Entity (SDCE). They are not responsible for either accreditation of ATPs or authentication of customers and ATPs: both of these functions remain with the SDCE. Sector-Specific Implementation Entities also work closely with the relevant sector-specific regulator and shape the work of the SDCE through the Smart Data Council. We anticipate there would only be one Sector-specific Implementation Entity per Smart Data scheme, although note that in some sectors it could be explored whether multiple Sector-specific Implementation Entities are needed (e.g. in finance

where a Smart Data scheme could cover markets as diverse as pensions, investments, mortgages and insurance).

The Open Banking Future Entity (as the successor to Open Banking Limited) would remain as the Sector-specific Implementation Entity for the Open Banking scheme. For schemes in other sectors, Sector-specific Implementation Entities could be appointed under 5 year contracts through a competitive process held by the relevant sector-specific government department (e.g. DESNZ would run the formal appointment process for a Sector-specific Implementation Entity in the retail energy sector).[61] Sector-specific Implementation Entities would then be supervised by that government department for the duration of their contract; however, government departments may also delegate responsibility for appointing and managing Sector-specific Implementation Entities to a relevant sector-specific regulator if they choose. Recognising Sector-specific Implementation Entities may be appointed through a competitive process, we do not name potential candidates for taking on these roles in this report. However, it should be noted that there are existing industry bodies which would be well placed to take on this role in some sectors (e.g. finance, retail energy, property) but not others (e.g. retail, agrifood).[62]

Smart Data Coordination Entity (SDCE)

The Smart Data Coordination Entity (SDCE) coordinates schemes across the Smart Data economy, providing core services and mandatory guidelines across sectors to ensure consistency and interoperability; however, it has a significantly smaller scope than the Smart Data Implementation Entity (SDIE) in Model 2. It develops some common standards, manages central ATP accreditation, manages a central approach to authenticating customers and ATPs, and coordinates customer complaint and dispute resolution mechanisms across schemes. Over time, it may also provide a common customer consent solution.

As the SDCE has more limited responsibilities than the SDIE in Model 2, it could be established as a new office within the Department for Business & Trade (DBT), held to account through existing governance structures and ministerial oversight in the department. As part of DBT, the SDCE would draw on expertise from across sectors via the Smart Data Council.

Regulators

As in Model 2, sector-specific regulators (e.g. Ofgem for retail energy) primarily enforce compliance within their relevant sector, ensuring adherence to Smart Data mandates and standards. They investigate reported violations and apply penalties as necessary; however, responsibilities for monitoring compliance sit with the Sector-specific Implementation Entities. Sector-specific regulators would also sign off the technical standards developed by the SDCE and Sector-specific Implementation Entities for implementation in the relevant sector. Sector-specific regulators work closely with Sector-specific Implementation Entities and contribute to shaping the work of the SDCE, via either positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators. In some instances, the relevant government department may also choose to delegate responsibility for appointing and managing Sector-specific Implementation Entities to a relevant sector-specific regulator if they choose. The Information Commissioner's Office (ICO) remains responsible for enforcing related data sharing regulation (e.g. GDPR)

[61] See Explanation box 3 for the rationale as to why Sector-specific Implementation Entities should be appointed through a competitive process.

[62] See Appendix G for an account of existing industry bodies which could perform the role of a Sector-specific Implementation Entity in each sector.

DBT & other government departments
As in Model 2, DBT collaborates with sector-specific government departments and regulators to set economy-wide Smart Data policy and ensure alignment with national goals. In doing so, DBT draws on expertise from across sectors through the Smart Data Council, which includes relevant government departments, regulators and industry experts. DBT is also responsible for establishing the SDCE as a new office within the department.

However, sector-specific government departments define Smart Data mandates within their respective sectors, collaborating with DBT to ensure consistency. Sector-specific government departments would also be responsible for appointing and managing Sector-specific Implementation Entities in most cases, although they may choose to delegate this to the relevant sector-specific regulator. Sector-specific government departments, like sector-specific regulators, would also contribute to shaping the work of the SDCE, via either positions on the Smart Data Council or a separate forum of relevant government departments and regulators.

Model 3 (Federated): Responsibility for each governance function	
1. Policy and strategy	
1a. Setting the vision and strategic direction: Identifying the key aims of the scheme in each sector, including by selecting priority use cases.	DBT leads on setting the vision for Smart Data across sectors. This includes developing a plan for new sectors to be introduced to the Smart Data economy and establishing priority goals for the SDCE. When a new scheme is being established, sector-specific government departments define the priority aims and use cases for the sector, with support from DBT. In doing so, they consult with a wide range of stakeholders across the relevant sector, including the relevant regulator and potential candidate organisations for the role of Sector-specific Implementation Entity.
1b. Defining data sharing mandates: Determining the data types industry organisations are required to share when requested by customers.	Sector-specific government departments define data sharing mandates for their respective sectors, deciding on the data types that data holders are required to share with ATPs at the customer's request. Sector-specific government departments are supported to do so by DBT and consult with a wide range of stakeholders across the relevant sector, including potential candidate organisations for the role of Sector-specific Implementation Entity.
1c. Defining data sharing principles: Setting high-level principles which data sharing should comply with.	DBT sets high-level cross-sector data sharing principles to underpin data sharing practices across all sectors. This provides guidelines for developing or adapting Smart Data trust frameworks and standards.
1d. Designing or adapting trust frameworks: Setting out how data is shared, used, and protected by participants in Smart Data schemes, including liability for errors or wrongdoing.	DBT designs an economy-wide Smart Data Trust Framework, informed by the established data sharing principles and drawing on expertise from across sectors through the Smart Data Council. The trust framework is signed off and published by DBT, and informs delivery of a wide range of other governance functions included in this table. Once established, DBT is responsible for reviewing the Smart Data Trust Framework periodically, potentially through the Smart Data Council, to reflect technological advancements, changes in legislation, and the introduction of new sectors to the Smart Data economy. DBT is responsible for signing off any updates to the Smart Data Trust Framework.

1e. Designing or adapting governance models: Deciding the design, composition and remit of formal Smart Data governance entities, including roles and decision-making powers.	DBT designs a cross-sector Smart Data governance model, working with sector-specific government departments to formalise powers for relevant governance bodies in each sector through secondary legislation where necessary. DBT leads reviews of Smart Data governance models every five years, and implements changes as required.
1f. Aligning with other government policy: Aligning Smart Data schemes with broader digital and data strategies across government.	DBT scans for relevant interdependencies across government departments and actively aligns Smart Data approaches through the SDCE. Sector-specific government departments and regulators bring new developments across government to DBT's attention via their role on the Smart Data Council.
1g. Advising on policy and strategy: Feeding industry and consumer voices into all policy and strategy decisions, thereby shaping the work in 1a, 1b, 1c, 1d and 1e.	The Smart Data Council, including relevant government departments, regulators, industry experts and the SDIE, feeds expertise from across sectors into policy and strategy decisions made by DBT and sector-specific government departments. Where sector-specific challenges arise, DBT and sector-specific government departments may also draw on the advice of Sector-specific Implementation Entities.
2. Standards development	
2a. Defining and maintaining technical standards: Creating and updating the data and API specifications that underpin how data is shared between parties.	The SDCE convenes a Central Standards Working Group (which could be developed from the existing Smart Data Council), comprising a range of independent experts from across relevant sectors. The Central Standards Working Group defines and periodically updates a broad set of core 'common standards' across the Smart Data economy, with a focus on standardising common attributes across different datasets (e.g. unique identifiers). Sector-specific Implementation Entities build on these common standards to develop and maintain the full range of standards for their sector. Where Sector-specific Implementation Entities identify a change is required to 'common standards', they make a recommendation to the Central Standards Working Group which retains decision-making power. This provides an appropriate balance between ensuring technical standards promote interoperability across sectors while enabling sector-specific standards to be shaped by sector-specific expertise where needed. Sector-specific regulators then sign off standards for their sector.
2b. Developing data security classifications: Defining levels of sensitivity for different types of data and adjusting security requirements accordingly.	The SDCE sets guidelines for data security classification levels across all Smart Data schemes. Sector-specific Data Classification Working Groups, convened by Sector-specific Implementation Entities, work within these guidelines to develop and maintain full data security classifications for their sector, drawing on expert knowledge of data types in their sector. This takes into account the risks associated with both 'read only' and 'write' access. They submit these data security classifications to the SDCE on an annual basis to inform the accreditation of ATPs.

2c. Developing privacy and security standards: Designing the controls, policies and procedures to ensure that data sharing protects user privacy and system security.	The SDCE develops privacy and security standards for all Smart Data schemes, taking into account different data security classifications and differences in risk between 'read only' and 'write' access for ATPs. These include consent mechanisms, identity authentication, breach protocols, and data minimisation principles. The SDCE works closely with the ICO to ensure consistency with national data protection laws. Sector-specific Implementation Entities make recommendations when they identify a change is required, but do not have decision-making power. This function is centralised to ensure all Smart Data schemes operate under a consistent minimum baseline of privacy and security protections, which is essential for building customer trust and ensuring compliance with data protection law.
2d. Defining customer experience guidelines: Outlining rules for customer data sharing journeys.	The SDCE defines high-level customer experience principles. In line with those principles, Sector-specific Implementation Entities then set specific customer experience requirements for their sector, including testing potential user journeys with consumers, recognising the fact that customers in different sectors may have different needs.
2e. Ensuring cross-sector interoperability of standards: Coordinate standards across sectors to ensure interoperability across industries.	The SDCE leads efforts to align standards across sectors, including through mandating a broad set of common cross-sector technical standards, setting guidelines for data security classifications, defining uniform privacy and security standards across schemes, and defining high-level customer experience principles.
3. Accreditation of Authorised Third-party Providers (ATPs)	
3a. Determining ATP accreditation requirements: Defining the eligibility criteria and conditions Authorised Third-party Providers must meet to be accredited.	The SDCE defines common ATP eligibility criteria across sectors (e.g. insurance, data protection standards), building on established standards and tiering requirements in line with the security classification of the data being accessed. Where Sector-specific Implementation Entities identify a change is required to these eligibility criteria, they make a recommendation to the SDCE which retains decision-making power.
3b. Delivering ATP accreditation process: Running the assessment and onboarding processes that grant or revoke ATP status for third parties.	The SDCE operates a central ATP accreditation service, including onboarding, document checks, background screening, and periodic review and renewal of accreditation once granted. ATP accreditation provided by the SDCE is valid for data at permitted security classifications across all sectors, ensuring ATPs need to be accredited just once to share data across sectors.
3c. Maintaining an authorised list of ATPs: Keeping an up-to-date public list of accredited third parties that are authorised to access and use Smart Data, that allows data holders and users to confirm ATP credentials.	The SDCE maintains a dynamic, publicly searchable authorised list of accredited ATPs, noting the data security classifications they are permitted to access. This is accessible via an API and regularly updated to reflect additions, revocations and updates to the permissions of ATPs. Maintaining a centralised authorised list of ATPs enables ATPs to easily access data across sectors.

3d. Ensuring cross-sector recognition of ATP accreditation: Enabling ATPs accredited under one scheme or sector to be recognised in others without a duplicative process.	The SDCE facilitates cross-sector recognition of ATP accreditation across sectors by ensuring consistent eligibility criteria, running a single accreditation process and maintaining a central authorised list of ATPs recognised across all sectors.
4. Customer protection and engagement	
4a. Handling customer complaints and redress: Managing systems that allow customers to raise concerns and access remedies when issues arise.	Each Sector-specific Implementation Entity handles customer complaints in its sector as a first port of call where the initial complaint cannot be resolved directly with the data holder. In doing so, Sector-specific Implementation Entities work in line with cross-sector guidance on customer redress created by the SDCE. This may include developing a complaints contact address, responding to complaints which do not meet thresholds for action, investigating less serious complaints and liaising with scheme participants to reach a resolution, and/or signposting more serious complaints to the ICO, relevant regulator or Ombudsman as needed. Where complaints relate to data sharing across multiple sectors, the SDCE determines which Sector-specific Implementation Entity should lead on responding, based on pre-agreed criteria developed by the SDCE.
4b. Promoting consumer understanding: Promoting public understanding of Smart Data and encouraging safe, informed participation by consumers.	The SDCE runs national communications and education campaigns to raise awareness of Smart Data, educating customers about their privacy rights and how Smart Data could benefit them. The SDCE and Sector-specific Implementation Entities collaborate with consumer groups to ensure messages reach diverse audiences.
4c. Defining consent requirements: Outlining rules for how informed customer consent is obtained, including offering shared or standardised customer consent solutions.	The SDCE develops cross-sector customer consent requirements. Sector-specific Implementation Entities then develop consent journeys for their sector in line with these requirements, ensuring consent mechanisms are simple, clear, and comply with GDPR and other data protection regulations. Over time, the SDCE supersedes the work of Sector-specific Implementation Entities by developing unified, cross-sector consent journeys and consent dashboards, likely drawing on Ofgem's existing work to develop a customer consent solution. However, development of this cross-sector consent solution does not delay the implementation of early Smart Data schemes.
4d. Authenticating customers and ATPs: Establishing processes to confirm the identity of customers and ATPs in Smart Data schemes, potentially leveraging digital identity frameworks.	The SDCE sets customer and ATP authentication standards, ensuring consistency across sectors and taking into account different data security classifications. The SDCE collaborates with trusted digital identity providers to establish an interoperable cross-sector authentication service which meets those standards. Sector-specific Implementation Entities may advise on different user types and tiering of authentication requirements in each sector.

5. Regulatory and compliance	
5a. Monitoring compliance: Tracking whether organisations fulfil their obligations to comply with data sharing mandates and standards.	Sector-specific Implementation Entities continuously monitor compliance with data sharing mandates and standards within the relevant Smart Data scheme, in line with guidance set by the SDCE. Sector-specific Implementation Entities issue pre-enforcement notices where low-level instances of non-compliance are first identified. Serious or ongoing instances of non-compliance are escalated to the relevant regulator with recommended next steps.
5b. Encouraging compliance: Providing guidance and support to help organisations comply with data sharing mandates and standards.	The SDCE works with Sector-specific Implementation Entities to co-develop guidance and best practice toolkits to support data holders and ATPs to comply with data sharing mandates and standards, including when operating across sectors. These are customised by sector and published openly.
5c. Enforcing compliance: Investigating non-compliance and applying enforcement actions such as fines/penalties.	Regulators retain full enforcement responsibility, investigating reported instances of non-compliance and applying penalties as necessary among data holders and ATPs. The SDCE supports coordination between regulators when instances of non-compliance straddle the boundaries of two or more schemes.
5d. Managing API conformance certification : Testing whether APIs meet required technical standards before they are deployed.	The SDCE provides a centralised infrastructure for API conformance testing, offering standard sandbox environments to ensure APIs meet published standards before live deployment. Within this common infrastructure, Sector-specific Implementation Entities create tailored tests and sandbox environments to ensure APIs meet specific standards in their sector.
5e. Oversight of governance bodies: Holding governance bodies to account to ensure they act fairly, transparently and in the public interest.	As a new office within DBT, the SDCE is held to account through existing governance structures and ministerial oversight in the department. Oversight includes regular performance reviews and public reports to ensure the SDCE meets its objectives and remains accountable to the public. Sector-specific Implementation Entities are held to account by the sector-specific government departments which hold their contracts. This includes through quarterly progress reviews and annual contract reviews.

6. Implementation	
6a. Developing implementation plans: Setting timelines, milestones and delivery plans for Smart Data rollout in each sector and across sectors.	The SDCE develops a high-level cross-sector Smart Data implementation plan, drawing on expertise from across sectors through the Smart Data Council. Sector-specific Implementation Entities use that plan to define their own detailed delivery plans, which are signed off by the relevant sector-specific government department and the SDCE. Progress against these delivery plans is tracked through quarterly progress reviews and annual contract reviews for Sector-specific Implementation Entities.
6b. Stakeholder engagement and representation: Ensuring Smart Data governance reflects a range of perspectives, including but not limited to consumers, SMEs, and industry.	The SDCE runs stakeholder engagement programmes when consulting on cross-sector changes to Smart Data delivery. Sector-specific Implementation Entities do the same when consulting on sector-specific changes to Smart Data delivery. Both actors ensure engagement is inclusive and that diverse perspectives (e.g. SMEs, rural businesses, marginalised consumer groups) shape Smart Data delivery. The SDCE draws on expertise from across sectors through the Smart Data Council, which includes consumer, SME and industry representatives.
6c. Facilitating knowledge sharing: Ensuring different actors and schemes are learning from one another.	The SDCE maintains a broad Smart Data community of practice to share insights and lessons across schemes. Sector-Specific Implementation Entities feed in case studies, pilots and pain points to share.
6d. Setting up appeals and dispute resolution mechanisms: Providing clear and accessible routes to challenge decisions or resolve disagreements between parties (excluding customers).	The SDCE develops a generic dispute resolution model to resolve disagreements between parties (excluding customers) in a Smart Data scheme. Sector-specific Implementation Entities adopt this model and implement it within their scheme. The SDCE supports coordination between Sector-specific Implementation Entities when disputes straddle the boundaries of two or more schemes.
6e. Managing funding models: Designing and implementing funding models for Smart Data governance bodies, including who pays and how.	DBT designs and administers a cross-sector funding model for Smart Data schemes, taking the advice of sector-specific government departments and regulators. This could include drawing on: government investment for initial set-up costs, regulatory levies, ATP accreditation fees, and/or commission taken on any other payments made within schemes (depending on the chosen commercial model).
6f. International engagement: Engaging with international governments and industry groups to align Smart Data schemes with global best practices and support cross-border data sharing.	DBT (and the SDCE within it) leads the UK's international Smart Data engagement, by engaging in international forums and bilateral relationships with Smart Data schemes in other countries. This includes ensuring alignment with global data exchange frameworks (e.g. ISO, W3C).

Explanation box 3: A competitive process for appointing Sector-specific Implementation Entities

The recommendation within Model 3 (Federated) to appoint Sector-specific Implementation Entities through a competitive process differs from the approach taken to establish Open Banking Limited (OBL) to implement the UK's Open Banking scheme. OBL was established through the Competition and Market Authority's Retail Banking Market Investigation Order 2017, which required the UK's nine largest banks and building societies (the CMA9) to collectively implement Open Banking, including by setting up and funding OBL.

Appointing Sector-specific Implementation Entities through a competitive process is likely preferable to this approach within Model 3 (Federated) for five reasons:

1. **More fragmented markets in sectors beyond banking**: There is not a clear group of large market players who could be held responsible for establishing a Sector-specific Implementation Entity in all sectors where Smart Data could be introduced.
2. **Independence of Sector-specific Implementation Entities:** The Open Banking experience suggests that Sector-specific Implementation Entities should not be solely funded or controlled by large data holders, who in some instances may wish to limit data sharing to prevent rising costs.
3. **Limiting burden on large data holders:** The Open Banking experience suggests the burden placed on large data holders to establish an implementation body alongside their own data-sharing infrastructure was disproportionately large given data holders were not significant beneficiaries from Smart Data schemes.
4. **Promoting innovation:** Several research participants noted a competitive appointment process may incentivise Sector-specific Implementation Entities to innovate and keep costs low
5. **Building on existing industry initiatives:** In some sectors, existing industry bodies are already well-positioned to take on the role of Sector-specific Implementation Entity, meaning mandating industry to establish a new body may be duplicative.

However, there are alternative approaches to establishing Sector-specific Implementation Entities which could be further explored.

5.4 Model 4: Regulator-led

Model 4 (Regulator-led) also takes a more decentralised approach to Smart Data governance than Model 2. However, rather than relying on separate Sector-specific Implementation Entities (like Model 3), it gives more power and delivery responsibilities to sector-specific regulators. In Model 4, Smart Data Offices are established within each sector-specific regulator, and are tasked with both implementing and regulating Smart Data in the relevant sector. They are supported by a central Smart Data Guidance Entity (SDGE). The SDGE provides a limited number of mandatory guidelines to regulator-led Smart Data Offices to ensure a degree of consistency and interoperability across sectors; however, most guidelines it provides are advisory, meaning its power and remit is smaller than both the SDIE in Model 2 and the SDCE in Model 3. The positioning of Smart Data Offices within regulators enables there to be just one responsible body for Smart Data within each sector.

Figure 5 - Summary of Model 4 (Regulator-led).

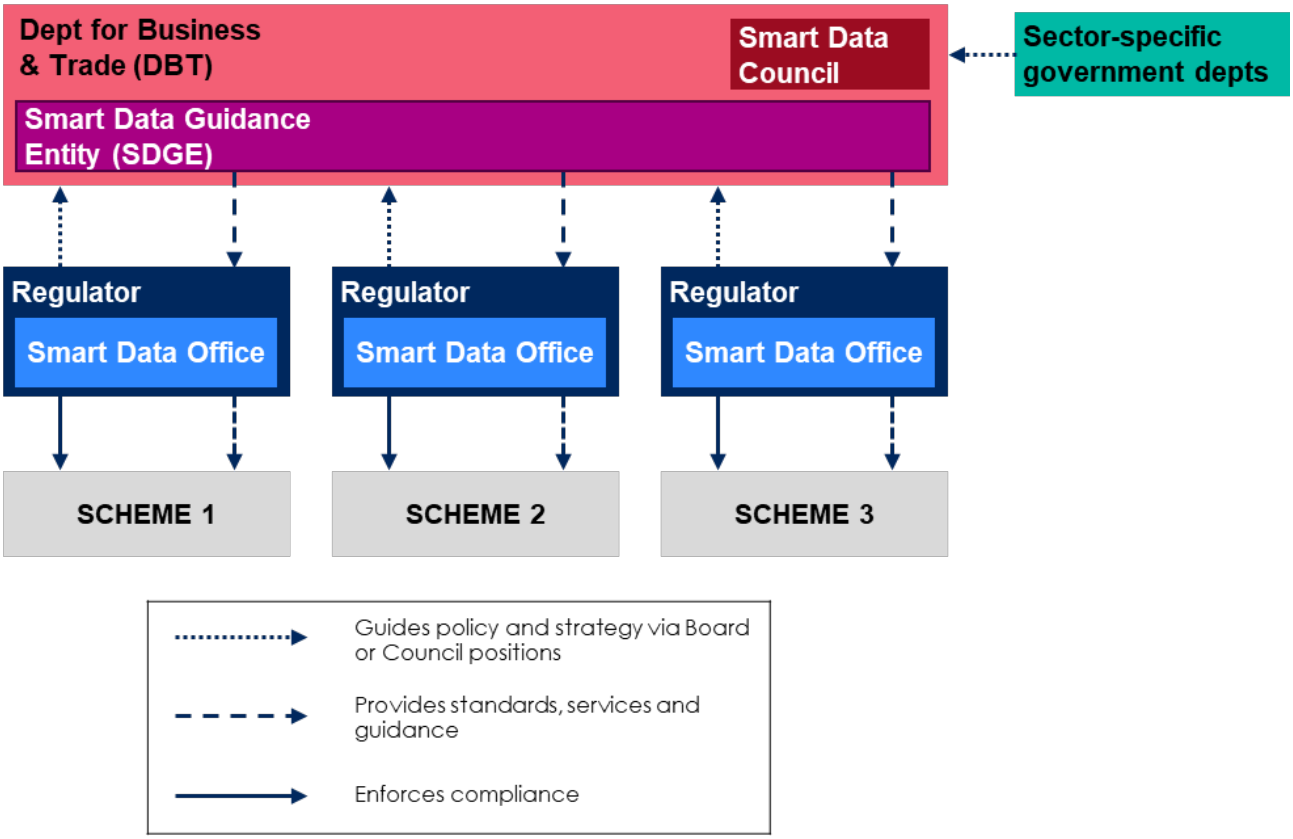


Table 19 provides a more detailed overview of how Model 4 (Regulator-led) would work, including a summary of the key actor types and a breakdown of responsibilities by governance function.

Table 19 - Detailed description of Model 4 (Regulator-led).

Model 4 (Regulator-led): The key actor types
Regulators (including Smart Data Offices) In Model 4, regulators in each sector are responsible for both delivery and regulation of Smart Data in their sector. Each regulator establishes a Smart Data Office to achieve these aims, which is responsible for undertaking the majority of Smart Data governance functions in that sector. Indeed, each Smart Data Office has a wide remit: among other things, they develop standards, set data security classifications, accredit ATPs, handle customer complaints, establish authentication systems for customers and ATPs, monitor and enforce compliance, and administer dispute resolution mechanisms within their scheme. However, in completing many of these governance functions, they work within guidelines established by the Smart Data Guidance Entity (SDGE). The Information Commissioner's Office (ICO) remains responsible for enforcing related data sharing regulation (e.g. GDPR). In some sectors, it is evident where Smart Data Offices could be established: for example, in the FCA for finance, Ofgem for retail energy, and Ofcom for telecommunications. However, in other sectors, it is less clear which regulator would lead on Smart Data, and therefore where a Smart Data Office could be established (see Section 6.2 for further discussion of this challenge).
Smart Data Guidance Entity (SDGE) The Smart Data Guidance Entity (SDGE) is responsible for providing a limited number of mandatory guidelines to regulator-led Smart Data Offices to ensure a degree of consistency

and interoperability across sectors. Its power and remit is smaller than both the SDIE in Model 2 and the SDCE in Model 3. While it still sets some common standards and a range of mandatory guidelines, it sets does not develop shared tools or services, such as central ATP accreditation, authenticating customers and ATPs, or complaint and dispute resolution mechanisms across schemes. However, it does run a programme for passporting of ATP accreditation across sectors.

Like the SDCE in Model 3 (Federated), the SDGE could be established as a new office within the Department for Business & Trade (DBT), held to account through existing governance structures and ministerial oversight in the department. As part of DBT, the SDGE would draw on expertise from across sectors through the Smart Data Council. However, given the more limited power and remit of the SDGE than the SDCE in Model 3, it could also potentially be established by expanding the Open Banking Future Entity (as the successor to Open Banking Limited). This would build on the expertise and infrastructure developed to date but require the development of new statutory powers for the Open Banking Future Entity, new funding models, rebranding, the onboarding of expertise from sectors outside finance, and transfer of formal sponsorship and oversight of the Open Banking Future Entity to DBT.

DBT & other government departments
As in Models 2 and 3, DBT collaborates with sector-specific government departments and regulators to set economy-wide Smart Data policy and ensure alignment with national goals. In doing so, DBT draws on expertise from across sectors via the Smart Data Council, which includes relevant government departments, regulators and industry experts. DBT is also responsible for establishing the SDGE as a new office within the department or transitioning OBL into a cross-sector SDGE.

However, sector-specific government departments define Smart Data mandates within their respective sectors, collaborating with DBT to ensure consistency. Sector-specific government departments, like sector-specific regulators, would also contribute to shaping the work of the SDGE, via either positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators.

Model 4 (Regulator-led): Responsibility for each governance function	
1. Policy and strategy	
1a. Setting the vision and strategic direction: Identifying the key aims of the scheme in each sector, including by selecting priority use cases.	DBT leads on setting the vision for Smart Data across sectors. This includes developing a plan for new sectors to be introduced to the Smart Data economy and establishing priority goals for the SDGE. When a new scheme is being established, sector-specific government departments define the priority aims and use cases for the sector, with support from DBT. In doing so, they consult with a wide range of stakeholders across the relevant sector, prioritising the relevant regulator.
1b. Defining data sharing mandates: Determining the data types industry organisations are required to share when requested by customers.	Sector-specific government departments define data sharing mandates for their respective sectors, deciding on the data types that data holders are required to share with ATPs at the customer's request. Sector-specific government departments are supported to do so by DBT and consult with a wide range of stakeholders across the relevant sector, prioritising the relevant regulator.

1c. Defining data sharing principles: Setting high-level principles which data sharing should comply with.	DBT designs an economy-wide Smart Data Trust Framework, informed by the established data sharing principles, and working closely with relevant regulator-led Smart Data Offices in leading sectors. The trust framework is signed off and published by DBT and informs delivery of a wide range of other governance functions included in this table. Once established, the Smart Data Council is responsible for reviewing the Smart Data Trust Framework periodically to reflect technological advancements, changes in legislation, and the introduction of new sectors to the Smart Data economy. DBT is responsible for signing off any updates to the Smart Data Trust Framework.
1d. Designing or adapting trust frameworks: Setting out how data is shared, used, and protected by participants in Smart Data schemes, including liability for errors or wrongdoing.	SDGE develops a common Smart Data trust framework, informed by the data sharing principles set by DBT, which is adapted by each Smart Data Office; signed off and published by DBT and sector-specific government departments. The common trust framework will outline key approaches to maintaining trust, such as data security standards, breach protocols, and responsibility for data stewardship. The common and adapted frameworks will be updated periodically to reflect technological advancements and changes in legislation.
1e. Designing or adapting governance models: Deciding the design, composition and remit of formal Smart Data governance entities, including roles and decision-making powers.	DBT designs a cross-sector Smart Data governance model, working with sector-specific government departments to formalise powers for relevant governance bodies in each sector through secondary legislation where necessary. DBT leads reviews of Smart Data governance models every five years, working closely with regulator-led Smart Data Offices, and implements changes as required.
1f. Aligning with other government policy: Aligning Smart Data schemes with broader digital and data strategies across government.	DBT scans for relevant interdependencies across government departments and actively aligns Smart Data approaches through the SDGE. Sector-specific government departments and regulator-led Smart Data Offices bring new developments across government to DBT's attention via their role on the Smart Data Council.
1g. Advising on policy and strategy: Feeding industry and consumer voices into all policy and strategy decisions, thereby shaping the work in 1a, 1b, 1c, 1d and 1e.	The Smart Data Council, including relevant government departments, regulators, industry experts and the SDIE, feeds expertise from across sectors into policy and strategy decisions made by DBT and sector-specific government departments. Where sector-specific challenges arise, DBT and sector-specific government departments work closely with regulator-led Smart Data Offices.

2. Standards development	
2a. Defining and maintaining technical standards: Creating and updating the data and API specifications that underpin how data is shared between parties.	A Central Standards Working Group, convened by the SDGE, defines and periodically updates a narrow set of core 'common standards' across all Smart Data schemes, focusing only on standardising common attributes across different datasets (e.g. unique identifiers). Smart Data Offices build on these common standards to develop and maintain the full range of standards for the scheme in their sector. Where Smart Data Offices identify a change is required to 'common standards', they make a recommendation to the Central Standards Working Group which retains decision-making power.
2b. Developing data security classifications: Defining levels of sensitivity for different types of data and adjusting security requirements accordingly.	Smart Data Offices develop and maintain full data security classifications for the scheme in their sector, taking into account the risks associated with both 'read only' and 'write' access. Smart Data Offices use these classifications to inform their ATP accreditation processes. The SDGE sets mandatory guidelines for data security classification levels across all Smart Data schemes to guide this work.
2c. Developing privacy and security standards: Designing the controls, policies and procedures to ensure that data sharing protects user privacy and system security.	Smart Data Offices develop privacy and security standards for the scheme in their sector, taking into account different data security classifications and differences in risk between 'read only' and 'write' access for ATPs. These include consent mechanisms, identity authentication, breach protocols, and data minimisation principles. The SDGE establishes some mandatory privacy and security guidelines across all Smart Data schemes to guide this work. The SDGE and Smart Data Offices work closely with the ICO to ensure consistency with national data protection laws.
2d. Defining customer experience guidelines: Outlining rules for customer data sharing journeys.	Smart Data Offices set specific customer experience requirements for the scheme in their sector, including testing potential user journeys with consumers. The SDGE defines advisory high-level customer experience principles across all Smart Data schemes.
2e. Ensuring cross-sector interoperability of standards: Coordinate standards across sectors to ensure interoperability across industries.	The SDGE leads efforts to align standards across all Smart Data schemes, including through mandating a narrow set of common cross-sector standards and setting advisory guidelines for data security classifications, privacy and security standards, and customer experience standards.
3. Accreditation of Authorised Third-party Providers (ATPs)	
3a. Determining ATP accreditation requirements: Defining the eligibility criteria and conditions Authorised Third-party Providers must meet to be accredited.	Smart Data Offices define specific ATP eligibility criteria (e.g. insurance, data protection standards) for the scheme in their sector, building on established standards and tiering requirements in line with the security classification of the data being accessed. The SDGE develops some mandatory minimum requirements eligibility criteria for ATPs across all Smart Data schemes to guide this work.

3b. Delivering ATP accreditation process: Running the assessment and onboarding processes that grant or revoke ATP status for third parties.	Smart Data Offices operate an ATP accreditation service for their sector, including onboarding, document checks, background screening, and periodic review and renewal of accreditation once granted. The SDGE develops some mandatory minimum requirements for the ATP accreditation process across all Smart Data schemes in order to ensure interoperability through an ATP passporting system (see function 3d).
3c. Maintaining an authorised list of ATPs: Keeping an up-to-date public list of accredited third parties that are authorised to access and use Smart Data, that allows data holders and users to confirm ATP credentials.	Smart Data Offices maintain dynamic, publicly searchable authorised lists of accredited ATPs in their sector, noting the data security classifications they are permitted to access. This is accessible via an API and regularly updated to reflect additions, revocations and updates to the permissions of ATPs. The SDGE develops some mandatory minimum requirements for ATP authorised lists across all Smart Data schemes in order to ensure interoperability through an ATP passporting system (see function 3d).
3d. Ensuring cross-sector recognition of ATP accreditation: Enabling ATPs accredited under one scheme or sector to be recognised in others without a duplicative process.	The SDGE supports Smart Data Offices in establishing mutual recognition of ATPs: it hosts an accreditation passporting framework, reducing the risk of duplicative accreditation. The SDGE also maintains a record of equivalencies and facilitates dispute resolution in cross-sector access cases.
4. Customer protection and engagement	
4a. Handling customer complaints and redress: Managing systems that allow customers to raise concerns and access remedies when issues arise.	Each Smart Data Office handles customer complaints in its sector as a first port of call, where the initial complaint cannot be resolved directly with the data holder. In doing so, Smart Data Offices work in line with cross-sector guidance on customer redress created by the SDGE. This may include developing a complaints contact address, responding to complaints which do not meet thresholds for action, investigating complaints and liaising with scheme participants to reach a resolution, and/or signposting complaints to the ICO or relevant Ombudsman as needed. Where complaints relate to data sharing across multiple sectors, the SDGE determines which Smart Data Office should lead on responding, based on pre-agreed criteria developed by the SDGE.
4b. Promoting consumer understanding: Promoting public understanding of Smart Data and encouraging safe, informed participation by consumers.	The SDGE runs national communications and education campaigns to raise awareness of Smart Data, educating customers about their privacy rights and how Smart Data could benefit them. The SDGE and Smart Data Offices collaborate with consumer groups to ensure messages reach diverse audiences.

4c. Defining consent requirements: Outlining rules for how informed customer consent is obtained, including offering shared or standardised customer consent solutions.	Smart Data Offices develop consent requirements and consent journeys for their sector, ensuring consent mechanisms are simple, clear, and comply with GDPR and other data protection regulations. The SDGE establishes advisory consent guidelines across all Smart Data schemes, and convenes Smart Data Offices to support voluntary sharing of common customer consent solutions (e.g. drawing on Ofgem's existing work to develop a customer consent solution).
4d. Authenticating customers and ATPs: Establishing processes to confirm the identity of customers and ATPs in Smart Data schemes, potentially leveraging digital identity frameworks.	Smart Data Offices set customer and ATP authentication standards for the Smart Data scheme in their sector, taking into account different data security classifications. Smart Data Offices also collaborate with trusted digital identity providers to establish authentication services for the Smart Data scheme in their sector. The SDGE establishes advisory authentication guidelines across all Smart Data schemes, and convenes Smart Data Offices to support voluntary sharing of common authentication solutions.
5. Regulatory and compliance	
5a. Monitoring compliance: Tracking whether organisations fulfil their obligations to comply with data sharing mandates and standards.	Smart Data Offices continuously monitor compliance with data sharing mandates and standards within the relevant Smart Data scheme. Smart Data Offices issue pre-enforcement notices where low-level instances of non-compliance are first identified.
5b. Encouraging compliance: Providing guidance and support to help organisations comply with data sharing mandates and standards.	Smart Data Offices develop guidance and best practice toolkits to support compliance with data sharing mandates and standards in the Smart Data scheme in their sector.
5c. Enforcing compliance: Investigating non-compliance and applying enforcement actions such as fines/penalties.	Smart Data Offices, which sit within existing regulators, retain full enforcement responsibility, investigating serious or ongoing instances of non-compliance and applying penalties as necessary among data holders and ATPs. The SDGE supports coordination between Smart Data Offices when instances of non-compliance straddle the boundaries of two or more schemes.
5d. Managing API conformance certification: Testing whether APIs meet required technical standards before they are deployed.	Smart Data Offices create infrastructure for API conformance testing for the Smart Data scheme in their sector, offering standard sandbox environments to ensure APIs meet published standards before live deployment. The SDGE provides advisory guidelines for API conformance testing across all Smart Data schemes.

5e. Oversight of governance bodies: Holding governance bodies to account to ensure they act fairly, transparently and in the public interest.	As Smart Data Offices are established within existing regulators, they held to account through existing governance structures and ultimately ministerial oversight through their sponsoring department. If established as a new office within DBT, the SDGE is also held to account through existing governance structures and ministerial oversight in the department. Oversight includes regular performance reviews and public reports to ensure the SDGE meets its objectives and remains accountable to the public. However, if established by expanding the Open Banking Future Entity, formal sponsorship and oversight of the Open Banking Future Entity would need to be handed to DBT from the FCA.
6. Implementation	
6a. Developing implementation plans: Setting timelines, milestones and delivery plans for Smart Data rollout in each sector and across sectors.	The SDGE develops a high-level cross-sector Smart Data implementation plan, drawing on expertise from across sectors through the Smart Data Council. Smart Data Offices use that plan to define their own detailed delivery plans, which are signed off by the Board of the relevant regulator and the relevant sector-specific government department.
6b. Stakeholder engagement and representation: Ensuring Smart Data governance reflects a range of perspectives, including but not limited to consumers, SMEs, and industry.	The SDGE runs stakeholder engagement programmes when consulting on cross-sector changes to Smart Data delivery. Smart Data Offices do the same when consulting on sector-specific changes to Smart Data delivery. Both actors ensure engagement is inclusive and that diverse perspectives (e.g. SMEs, rural businesses, marginalised consumer groups) shape Smart Data delivery. The SDGE draws on expertise from across sectors through the Smart Data Council, which includes consumer, SME and industry representatives.
6c. Facilitating knowledge sharing: Ensuring different actors and schemes are learning from one another.	The SDGE maintains a broad Smart Data community of practice to share insights and lessons across schemes. Smart Data Offices feed in case studies, pilots and pain points to share.
6d. Setting up appeals and dispute resolution mechanisms: Providing clear and accessible routes to challenge decisions or resolve disagreements between parties (excluding customers).	Smart Data Offices develop dispute resolution mechanisms to resolve disagreements between parties (excluding customers) in the Smart Data scheme in their sector. The SDGE supports coordination between Smart Data Offices where disputes straddle the boundaries of two or more schemes.
6e. Managing funding models: Designing and implementing funding models for Smart Data governance bodies, including who pays and how.	DBT develops guidelines for the funding model for Smart Data schemes, taking the advice of sector-specific government departments and Smart Data Offices. Sector-specific government departments establish specific funding models for the Smart Data scheme in their sector, which are in turn implemented by Smart Data Offices. This could include drawing on: government investment for initial set-up costs, regulatory levies, ATP accreditation fees, and/or commission taken on any other payments made within schemes (depending on the chosen commercial model).

6f. International engagement: Engaging with international governments and industry groups to align Smart Data schemes with global best practices and support cross-border data sharing.	DBT and the SDGE lead the UK's international Smart Data engagement, by engaging in international forums and bilateral relationships with Smart Data schemes in other countries. This includes ensuring alignment with global data exchange frameworks (e.g. ISO, W3C).

6. Identifying relevant actors

Building on the development of three Smart Data governance models in the previous section, this section explores which existing organisations could adopt the roles of different actor types within future Smart Data governance models for each of our eight priority sectors: payment accounts (i.e. Open Banking), financial services (beyond payment accounts), retail energy, telecommunications, property, transport, retail and agrifood. These findings are based on the perspectives of our research participants: they have not been fully tested with all of the named organisations. They are therefore intended to support discussion and should be further tested and refined by government as part of future policy development.

The following tables lay out recommended options for each of the three shortlisted governance models, covering (1) government departments, (2) regulators, (3) cross-sector bodies and (4) sector-specific bodies. This work was supported by the full mapping of the Smart Data stakeholder landscape in Appendix G.

6.1 Government departments

Across all three shortlisted governance models, responsibility for Smart Data is shared between the Department for Business and Trade (DBT) and sector-specific government departments. DBT is positioned as the central owner of the cross-sector Smart Data economy, responsible for overarching coordination, cross-cutting infrastructure, and enabling interoperability. Sector-specific departments retain policy responsibility for individual Smart Data schemes in their relevant sector. It is typically straightforward to identify which government department should hold responsibility for Smart Data schemes in each sector, with little disagreement between research participants on this matter.

In all options, DBT would have responsibilities to coordinate and facilitate Smart Data in and between all sectors, as seen in Table 20.

Table 20 - Responsibilities for DBT across all shortlisted governance models.

	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
Responsible for:	Policy and strategy (1a, 1c, 1d, 1e, 1f, 1g), Regulatory and compliance (5e), Implementation (6a, 6e, 6f)	Policy and strategy (1a, 1c, 1d, 1e, 1f, 1g), Regulatory and compliance (5e), Implementation (6e, 6f)	Policy and strategy (1a, 1c, 1d, 1e, 1f, 1g), Regulatory and compliance (5e), Implementation (6e, 6f)
Supports on:	Policy and strategy (1b)	Policy and strategy (1b), Implementation (6a)	Policy and strategy (1b), Implementation (6a)

Other departments would also have responsibilities relating to Smart Data schemes in their sectors. Table 21 lists the expected lead government department for each of the eight sectors investigated in this research.

Table 21 - Relevant government departments per sector, and their responsibilities in each shortlisted governance model.

	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
Responsible for:	Policy and strategy (1a, 1b, 1g)	Policy and strategy (1a, 1b), Regulatory and compliance (5e), Implementation (6a)	Policy and strategy (1a, 1b, 1d, 1g), Implementation (6a, 6e)
Supports on:	Policy and strategy (1e, 1f), Implementation (6e)	Policy and strategy (1e, 1f, 1g), Implementation (6e)	Policy and strategy (1e, 1f), Implementation (6e)
Agrifood	Department for Environment, Food & Rural Affairs (Defra)		
Payment accounts	HM Treasury (HMT)		
Finance	HM Treasury (HMT)		
Property	Ministry for Housing, Communities & Local Government (MHCLG)		
Retail	Department for Business & Trade (DBT)		
Retail energy	Department for Energy Security & Net Zero (DESNZ)		
Telecoms	Department for Science, Innovation & Technology (DSIT)		
Transport	Department for Transport (DfT)		

As new sectors are incorporated into the Smart Data economy, beyond the eight priority sectors listed in table 21, prospectives schemes may arise for which it is less obvious which government department should take responsibility. As the lead department for Smart Data, we suggest DBT takes on responsibility for scoping and delivering these schemes in full.

6.2 Regulators

Variation in the regulatory landscape across different sectors poses a key challenge in the design of Smart Data governance models. Some sectors benefit from well-established, centralised regulatory bodies. For example, the Financial Conduct Authority (FCA) regulates the conduct of payment accounts and other financial services, Ofgem regulates retail energy, and Ofcom regulates telecommunications. These regulators have clear statutory mandates and could, fairly straightforwardly, take on Smart Data responsibilities within their sectors, regardless of which of the three shortlisted governance models outlined in this report are adopted.

Other sectors, however, do not have a single lead regulator. For example:

- **In the property sector**, different actors are overseen by a patchwork of regulators. Estate agents face regulation from the National Trading Standards Estate and Letting Agency Teams, alongside voluntary codes from bodies like Propertymark; conveyancers face regulation from multiple bodies including the SRA, CLC, CILEX and the Law Society; property search providers are regulated through the Property Codes Compliance Board (PCCB); mortgage providers and brokers fall under the oversight of the Financial Conduct Authority (FCA); surveyors are regulated by the Royal Institute of Chartered Surveyors (RICS); and HM Land Registry enforces strict licence terms for organisations accessing its data, despite not being a regulator *per se*.

- **In the transport sector**, regulatory responsibilities are distributed between several organisations including: the Office for Rail and Road (ORR) for most land travel, the Civil Aviation Authority (CAA) for air travel, the Maritime and Coastguard Agency (MCA) for maritime safety, and specialist bodies such as the Office of the Traffic Commissioner and DVSA, which have limited capacity to enforce compliance in local transport schemes.
- **In the retail sector,** there is limited oversight by regulators, although the Office for Product Safety and Standards (OPSS) oversees general product safety, the Food Standards Agency (FSA) regulates food safety and hygiene within grocery retail, and the Competition and Markets Authority (CMA) enforces fair competition across retail markets.
- **In the agrifood sector,** a wide array of statutory, quasi-regulatory, and voluntary bodies regulate the different parts of the supply chain, from farm to fork. The Food Standards Agency (FSA) oversees food safety and hygiene across the UK; the Environment Agency (EA) regulates environmental protection; the Animal and Plant Health Agency (APHA) is responsible for biosecurity, animal disease data, and import controls; and the Grocery Code Adjudicator (GCA) enforces fair trading between retailers and suppliers.

For sectors with such a fragmented regulatory landscape, identifying which organisations should be responsible for enforcing compliance with data sharing mandates and standards within a Smart Data scheme is challenging.[63] As one participant put it:

> *"Establishing regulatory remits in all sectors is a thorny problem, and probably something that will have to evolve over time as more sectors come onboard."*
>
> **Regulator**

However, we have identified four potential options for assigning regulatory responsibility for Smart Data schemes in these sectors without a single unified regulator:

1. **Regulator Option 1: An existing cross-sector regulator**. An existing cross-sector regulator (e.g. the ICO) is responsible for regulating Smart Data in all sectors without a single unified regulator.
2. **Regulator Option 2: Expanding the powers of one regulator per sector**. In each sector without a single unified regulator, the scope and powers of one existing regulator or government body are expanded to regulate the entirety of the relevant Smart Data scheme.
3. **Regulator Option 3: Coalitions of regulators**. Where necessary, coalitions of existing regulators are empowered to regulate Smart Data together. For example, in the transport sector, the ORR, CAA and MCA would all work together to regulate Smart Data. However, this approach is especially challenging in governance Model 4 (Regulator-led) where one regulator in each sector would also be expected to house a Smart Data Office.
4. **Regulator Option 4: A new cross-sector regulator**. Government appoints or creates a new cross-sector regulator for Smart Data.

Among the four proposed options for assigning regulatory responsibility in sectors without a single unified regulator, **Regulator Option 2, expanding the powers of one regulator per sector, emerged as the most viable and widely supported approach.**

Firstly, Regulator Option 1 – assigning Smart Data responsibilities to an existing cross-sector regulator – was ruled out as a short-term option. The ICO and Regulatory Innovation Office (RIO)

[63] It should be noted that while the evidence gathered through this research suggests Smart Data schemes will be most effective if delivered with support from a regulator with clear responsibility for that scheme, it is theoretically possible for Smart Data schemes to be delivered with no such regulatory oversight, with data sharing governed by existing contractual law and civil proceedings.

were both touted by some as potential candidates for this role. While the ICO has expressed support for Smart Data,[64] its existing remit is largely focused on data protection and information rights, and that Smart Data powers go beyond this remit. Indeed, Smart Data powers, where they are exercised, are intended to provide enhanced data portability rights beyond the right to data portability in Article 20 of the UK GDPR, which the ICO is responsible for enforcing within its current remit. Meanwhile, RIO is still being established and is tightly focused on four other priority policy areas. The ICO noted that any future involvement of the ICO in delivering Smart Data beyond their existing remit would need to consider whether the necessary legal framework, capability, funding, and operational designs are in place. These would ultimately be decisions for parliament.

Secondly, stakeholders expressed significant concerns about Regulator Option 3, which proposes the use of coalitions of regulators within each sector. Participants from across sectors were clear that Smart Data schemes would benefit from having a single responsible regulator within each sector. A coalition model risks a lack of clarity for data holders and Authorised Third-party Providers (ATPs), duplication of effort, and cases of non-compliance 'falling through the gaps'. Stakeholders also emphasised that distributing responsibilities for regulation of Smart Data between several regulators in each scheme would make it less likely that regulators develop the domain-specific knowledge necessary for effective Smart Data oversight.

Thirdly, Regulator Option 4 – creating a new cross-sector regulator – was widely seen as politically unfeasible. Stakeholders across government highlighted that there is little appetite within government for establishing new arms-length bodies, particularly in the context of fiscal constraints and civil service reform.

In contrast, Regulator Option 2 strikes a pragmatic balance between building on the existing regulatory landscape and providing a centralised approach to regulating each Smart Data scheme. Expanding the remit of an existing, trusted regulator within each sector would minimise institutional disruption, allow for the development of deep domain expertise, and provide clear lines of accountability. It also aligns with the cross-sector preference for a single regulator per Smart Data scheme. Further stakeholder conversations beyond the scope of this project will be needed to determine the most appropriate choice as a Smart Data regulator in each sector. However, our leading hypothesis for the most appropriate regulator in each of the four sectors without a clear regulator is as follows:

- **In the property sector**, **HM Land Registry (HMLR**) has emerged as the most suitable candidate to serve as the Smart Data regulator, despite the significant evolution this would represent from its current statutory remit. Existing regulators in the sector cover only specific professions, and therefore risk prioritising the interests of some groups over others and lacking the expertise or authority to cover the entire sector. In contrast, HMLR is already at the heart of data infrastructure in the property sector, maintaining authoritative title records and setting licensing conditions for access to its datasets. HMLR is also currently investing substantially in further data transformation programmes. In this quasi-regulatory role, HMLR has therefore developed expertise in managing data access, security, and commercial usage rights, which Smart Data schemes would heavily rely on. However, there remain three substantial challenges to this proposal: (1) vesting full regulatory powers in HMLR would require a significant departure from its current quasi-regulatory remit; (2) HMLR would also be a key data holder in a property Smart Data scheme, and so would also require means to hold itself to account; and (3) HMLR does not currently handle land or property registration in Scotland or Northern Ireland, while its role in a property Smart Data scheme would cover all four devolved nations. These potential

[64] ICO, 2025. Information Commissioner's response to the Data (Use and Access) (DUA) Bill.

challenges will require significant further discussion before a firm decision is taken on who adopts the role of regulator for a property Smart Data scheme.

- **In the transport sector, the Office of Rail and Road (ORR)** is likely the most appropriate organisation to lead regulation of Smart Data. Among the various transport modes, early Smart Data use cases are most likely to be concentrated in public transport and road transport, where initiatives like the Bus Open Data Service and Rail Data Marketplace have already demonstrated tangible value. This positions ORR as the most natural Smart Data regulator for transport, given its existing oversight of rail and elements of road transport.
- **In the retail sector,** the Competition and Markets Authority (CMA) may be best placed to regulate a Smart Data scheme; however, no clear consensus on a single most appropriate regulator for Smart Data in the retail sector emerged from the research, and therefore this recommendation should be treated with even greater caution than others. The CMA's broad remit across consumer protection and digital market fairness positions it as a relatively neutral and cross-cutting body. This contrasts with more narrowly focused regulators like the Office for Product Safety and Standards (OPSS) or the Food Standards Agency (FSA), both of which only cover specific product types such as general goods or groceries.
- **In the agrifood sector, the Food Standards Agency (FSA)** appears to be the most appropriate candidate to regulate a Smart Data scheme. The FSA is already deeply embedded in food system governance and has a track record of enforcing data-based schemes such as the Food Hygiene Rating System. However, this would still represent a major expansion of the FSA's current role, particularly into areas like environmental data, upstream farm data, and commercial data flows that fall beyond its existing statutory remit. It's also important to note the FSA currently does not have a remit in Scotland, where food safety, standards, and related matters are the responsibility of Food Standards Scotland.

Given these findings, Table 22 lists the expected lead regulator for each of the eight sectors investigated through this research.

Table 22 - Relevant regulators per sector, and their responsibilities in each shortlisted governance model.

	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led *Not including Smart Data Offices*
Responsible for:	Customer protection and engagement (4a),[65] Regulatory and compliance (5c)	Customer protection and engagement (4a),[66] Regulatory and compliance f (5c)	Regulatory and compliance (5e), Implementation (6a)
Supports on:	Policy and strategy (1f, 1g), Implementation (6e)	Policy and strategy (1f, 1g), Implementation (6e)	Policy and strategy (1b)
Agrifood	**Food Standards Agency** – assuming adopting Regulator Option 2. Other relevant regulators include the Environment Agency (EA), the Animal and Plant Health Agency (APHA), and the Grocery Code Adjudicator (GCA).		
Payment accounts	**Financial Conduct Authority**		
Financial services	**Financial Conduct Authority**		
Property	**HM Land Registry** – assuming adopting Regulator Option 2. Other relevant regulators include the Council for Licensed Conveyancers (CLC), the Law Society, the National Trading Standards Estate Agency Team, the Royal Institute of Chartered Surveyors (RICS), the Solicitors Regulation Authority (SRA), the Chartered Institute of Legal Executives (CILEX), the Property Codes Compliance Board (PCCB), and the Financial Conduct Authority (FCA).		
Retail	**Competition and Markets Authority** – assuming adopting Regulator Option 2. Other relevant regulators include the Office for Product Safety and Standards (OPSS), and the Food Standards Agency (FSA).		
Retail energy	**Ofgem**		
Telecoms	**Ofcom**		
Transport	**Office for Rail and Road** – assuming adopting Regulator Option 2. Other relevant regulators include the Civil Aviation Authority (CAA), the Maritime and Coastguard Agency (MCA), the Office of the Traffic Commissioner, and DVSA.		

In addition to the responsibilities outlined in table 22, the ICO would retain responsibility for enforcing national data protection laws (e.g. GDPR) in all shortlisted governance models.

6.3 Cross-sector bodies

Each of the three shortlisted governance models also envisage a key role for a new cross-sector body, which performs a centralised role across all eight sectors. The type of organisation proposed varies for each shortlisted governance model depending on the nature and scope of the function that cross-sector body would perform, with the Smart Data Implementation Entity (SDIE) in Model 2 having the broadest scope and the Smart Data Guidance Entity (SDGE) in Model 4 having the narrowest scope. Justifications for these differing approaches are provided throughout Section 5. Table 23 reiterates the organisations expected to take on these cross-sector roles in each shortlisted governance model.

[65] This may be responsibility of the ICO, a different regulator and/or an Ombudsman, depending on customer complaint jurisdiction, and Regulator Option selected (see Section 6.2).
[66] This may be responsibility of the ICO, a different regulator and/or an Ombudsman, depending on customer complaint jurisdiction, and Regulator Option selected (see Section 6.2).

Table 23 - Recommended actors to adopt Smart Data governance functions as a 'cross-sector body', and their responsibilities in each shortlisted governance model.

	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
Role	Smart Data Implementation Entity (SDIE)	Smart Data Coordination Entity (SDCE)	Smart Data Guidance Entity (SDGE)
Responsible for:	Standards development (2a, 2b, 2c, 2d, 2e), Accreditation of ATPs (3a, 3b, 3c, 3d), Customer protection and engagement (4a, 4b, 4c, 4d), Regulatory and compliance (5a, 5b, 5d), Implementation (6a, 6b, 6c, 6d)	Standards development (2a, 2b, 2c, 2d, 2e), Accreditation of ATPs (3a, 3b, 3c, 3d), Customer protection and engagement (4a 4b, 4c, 4d), Regulatory and compliance (5a, 5b, 5d), Implementation (6a, 6b, 6c, 6d, 6f)	Policy and strategy (1d), Standards development (2a, 2b, 2c, 2d, 2e), Accreditation of ATPs (3d), Customer protection and engagement (4b), Regulatory and compliance (5b, 5d), Implementation (6a, 6b, 6c, 6f)
Supports on:	Policy and strategy (1g), Regulatory and compliance (5c), Implementation (6f)	Regulatory and compliance (5c)	Accreditation of ATPs (3a, 3b, 3c), Customer protection and engagement (4a, 4c, 4d), Regulatory and compliance (5c), Implementation (6d)
Agrifood	**New Arm's Length Body** – established by the Department for Business & Trade (DBT), with the relevant government department and regulator for each participating sector sitting on the Board.	**New government office** – established within the Department for Business & Trade (DBT).	**New government office** – established within the Department for Business & Trade (DBT).
Payment accounts			
Financial services			
Property			
Retail			
Retail energy			
Telecoms			
Transport			

6.4 Sector-specific bodies

In each shortlisted governance model, the role of a central body is supplemented by the work of several sector-specific bodies. Unlike the cross-sector body, these sector-specifics bodies tailor delivery to the needs of individual sectors. The appropriate sector-specific body for each sector differs depending on the governance model adopted. While in Model 2 (Centrally-led) new Sector-specific Advisory Groups would be established, Model 3 (Federated) would see Sector-specific Implementation Entities formally appointed through a competitive process, and Model 4 (Regulator-led) would see Smart Data Offices established within the lead regulator for each sector. Table 24 outlines how this might work in each sector.

Table 24 - Recommended actors to adopt Smart Data governance functions as a 'sector-specific body', and their responsibilities in each shortlisted governance model.

	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
Role	Sector-specific Advisory Groups	Sector-specific Implementation Entities	Smart Data Offices within regulators
Responsible for:	N/A	Standards development (2a, 2b, 2d), Customer protection and engagement (4a, 4b, 4c), Regulatory and compliance (5a, 5b, 5d), Implementation (6a, 6b, 6d)	Policy and strategy (1d), Standards development (2a, 2b, 2c, 2d), Accreditation of ATPs (3a, 3b, 3c, 3d), Customer protection and engagement (4a, 4b, 4c, 4d), Regulatory and compliance (5a, 5b, 5c, 5d), Implementation (6a, 6b, 6d)
Supports on:	Policy and strategy (1g), Standards development (2a, 2b, 2c, 2d), Accreditation of ATPs (3a), Customer protection and engagement (4c, 4d), Regulatory and compliance (5b, 5d), Implementation (6a, 6c)	Policy and strategy (1g), Standards development (2a, 2b, 2c, 2d), Accreditation of ATPs (3a), Customer protection and engagement (4d), Implementation (6c)	Policy and strategy (1c, 1f, 1g), Standards development (2a), Implementation (6c, 6e)
Agrifood	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within the **Food Standards Agency** - assuming adopting Regulator Option 2.
Payment accounts	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within the **Financial Conduct Authority.**
Financial services	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	
Property	Newly formed group, including relevant regulators, government	Appointed through a competitive process, potentially drawing on existing industry	New office within **HM Land Registry -** assuming adopting Regulator Option 2.

	departments, and industry representatives (see Appendix G).	initiatives (see Appendix G).	
Retail	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within the **Competition and Markets Authority** - assuming adopting Regulator Option 2.
Retail energy	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within **Ofgem.**
Telecoms	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within **Ofcom.**
Transport	Newly formed group, including relevant regulators, government departments, and industry representatives (see Appendix G).	Appointed through a competitive process, potentially drawing on existing industry initiatives (see Appendix G).	New office within the **Office of Rail and Road** - assuming adopting Regulator Option 2.

7. Evaluating Smart Data governance models

Following the design of the three shortlisted governance models, we conducted an evaluation to assess the relative strengths and weaknesses of each model and identify a preferred option. The evaluation drew on two main components:

(1) **Qualitative analysis** by the research team, informed by evidence gathered throughout the project.

(2) **Quantitative analysis** of the models against ten critical success factors. Scores were provided by participants in a cross-sector Smart Data workshop and by a panel of synthetic sector representatives.

Together, these inputs allowed us to compare models from multiple perspectives and reach a final recommendation. The rest of this section outlines our evaluation of options in further detail.

7.1 Qualitative analysis

We synthesised findings from the qualitative research phase – including focus group discussions and stakeholder interviews – to understand perceived strengths and weaknesses of the three shortlisted governance models. While views varied across sectors and stakeholder types, a clear pattern emerged: Model 2 (Centrally-led) was considered desirable in the long-term but risky to deliver, Model 3 (Federated) was consistently seen as the most workable option in the short-term, and Model 4 (Regulator-led) was viewed less favourably overall.

7.1.1 Model 2: Centrally-led

Stakeholders valued Model 2's emphasis on central oversight, which was often seen as critical to driving cross-sector consistency and interoperability. However, significant questions were raised about how feasible such a model would be to deliver in the short term. Views diverged in particular between stakeholders who saw centralisation as necessary to drive momentum, and those who felt it risked representing a bottleneck and holding progress back in leading sectors.

Table 25 - Participant perspectives on the strengths and weaknesses of Model 2 (Centrally-led).

Strengths
1. Clear authority: A repeatedly heard strength of Model 2 was the clarity it offered in having one body with the authority and responsibility to drive progress across all sectors. *"This model is attractive because there is a central body that can just get on and make decisions."* **Cross-sector expert** *"You need someone to set the tone and coordinate across sectors. Without that, you risk divergence and confusion."* **Transport stakeholder**
2. Strong coordination across sectors: Interviewees highlighted the value of the Smart Data Implementation Entity (SDIE) in maintaining cross-sector interoperability, especially for functions like accreditation and standards. *"Having a single entity in charge makes it easier to make sure everything is working together."* **Finance stakeholder** *"The central SDIE is a natural home for coordination."* **Cross-sector expert**

Weaknesses

1. Barrier to short-term delivery: Despite its conceptual appeal, Model 2 prompted consistent concern about its practical deliverability. Participants often questioned whether a central implementation entity with such a wide range of responsibilities could realistically be stood up and resourced in a timely way.

> *"There is no clear home for this kind of body in government. Even if you create one, it'll take years to get it functioning."*
>
> **Cross-sector expert**

> *I worry [this model] is unworkable from a social and political perspective. It could fail and waste a lot of time and money.*
>
> **Cross-sector expert**

2. Limited sector-specific flexibility: In sectors with lower Smart Data maturity, participants worried that a single central implementation body might take a one-size-fits-all approach that fails to account for the specific needs and constraints of individual markets. Although the Sector-specific Advisory Groups' function in Model 2 is to mitigate this risk, participants questioned how much influence these groups would hold as decision-making power ultimately remains with the Smart Data Implementation Entity.

> *"It might look neat on paper, but if it slows things down or doesn't get the detail right for our sector, it'll cause more harm than good."*
>
> **Property stakeholder**

3. Risk of disengagement: Some interviewees also flagged potential risks around industry buy-in, noting that too much central control could deter active participation.

> *"If it feels too much like central government imposing a model, it risks people switching off."*
>
> **Agrifood stakeholder**

> *"You need to have the sector involved to get them to adopt it – they won't just follow rules passed down from above."*
>
> **Telecoms stakeholder**

7.1.2 Model 3: Federated

Model 3 attracted consistent support from all sectors across interviews and focus groups. Stakeholders valued its balance of clear coordination and sector-specific delivery, seeing it as both workable and adaptable. The model was often viewed as the most realistic to implement in the short term, as it builds on existing sector capabilities and avoids the complexities of establishing a wholly centralised entity. Crucially, participants appreciated that Model 3 allows more advanced sectors to begin implementation at pace, while enabling less mature sectors to progress on a timeline that suits their readiness and needs. While some concerns were raised about variable capacity across sectors to appoint a Sector-specific Implementation Entity, Model 3 was generally seen as a strong foundation for Smart Data governance.

Table 26 - Participant perspectives on the strengths and weaknesses of Model 3 (Federated).

Strengths

1. Sector-specific flexibility: Participants frequently highlighted the sector-led delivery model as one of the core strengths of Model 3. Stakeholders appreciated the autonomy it gives sectors to tailor implementation to their own context, while still ensuring cross-sector interoperability through the Smart Data Coordination Entity (SDCE).

> *"Agrifood has its own very specific challenges, so having a model where we can shape things ourselves is far more likely to work."*
>
> **Agrifood stakeholder**
>
> *"[This model] gives you a system where those who are ready can get going, and the others don't get left behind - they can catch up when they're ready."*
>
> **Energy stakeholder**

2. Industry engagement and trust: Model 3's ability to garner engagement trust from industry was also consistently noted, particularly as it would likely build on existing industry partnerships in most sectors through the appointment of Sector-specific Implementation Entities.

> *"You must let each sector shape the rules if you want us to be engaged. Model 3 gives us skin in the game."*
>
> *Telecoms stakeholder*

Weaknesses

1. Risk of inconsistencies: Several participants acknowledged the potential challenge of ensuring consistency of approach across different sectors under this model, posing a potential threat to cross-sector interoperability.

> *"There's a risk that everyone does a good job in their own lane, but it doesn't join up."*
>
> **Energy stakeholder**

2. Uneven sector delivery: Some also expressed concern that sectors with less organisational maturity may struggle to establish or operate effective Sector-specific Implementation Bodies. While many participants felt this was manageable through targeted support and oversight, it was seen as a potential drag on overall delivery pace.

> *"The real risk is you get great schemes in finance and none in retail. You'll need a very clear framework to keep everyone on track."*
>
> **Cross-sector expert**
>
> *"Some sectors just aren't there yet. You'll need a way to help them catch up without holding the others back."*
>
> **Cross-sector expert**

7.1.3 Model 4: Regulator-led

Model 4 received more negative feedback across interviews and focus groups. While participants appreciated its use of existing institutions, many raised doubts about whether regulators have the right mandate, capabilities or capacity to lead Smart Data delivery. Concerns centred on the risk of slow decision-making, inconsistent engagement with stakeholders, and limited focus on innovation. Although some participants saw this model as a lower-cost and familiar option, it was generally not viewed as a long-term solution.

Table 27 - Participant perspectives on the strengths and weaknesses of Model 4 (Regulator-led).

Strengths

1. Leverages existing infrastructure: The most cited strength of Model 4 was its use of existing institutions, which many participants saw as potentially enabling faster setup and lower overheads. This was especially noted in sectors like finance and retail energy, where regulators already play a substantial role.

> *"If you've already got a regulator that understands the space, it makes sense to build on what's there."*
>
> **Energy stakeholder**

Weaknesses

1. Limited capacity or capability to deliver: Concerns about the capabilities and capacity of regulators to delivery Smart Data schemes were widespread. Many stakeholders questioned whether traditional regulators, often set up for compliance and oversight, would be able to drive forward Smart Data schemes effectively, especially where innovation and technical implementation are needed.

> *"Regulators are built to enforce the rules, not rewrite them, and that's what Smart Data needs."*
>
> **Telecoms stakeholder**

2. Limits to engagement: Some stakeholders also felt that regulators and industry were unlikely to engage proactively and productively with each other in the way required for successful Smart Data delivery.

> *"You'll get stakeholder engagement, sure – but it'll be the same roundtables and consultations, not co-design."*
>
> **Cross-sector expert**

3. Risk of inconsistencies: As with Model 3, several participants acknowledged the potential challenge of ensuring consistency of approach across different sectors under this model, posing a potential threat to cross-sector interoperability.

> *"It's harder to create a consistent user experience when every sector is doing their own thing."*
>
> **Cross-sector expert**

4. Gaps in regulatory coverage: In sectors without a strong or relevant regulator, the model was seen as especially weak. Participants worried it would leave major gaps in leadership or require substantial changes to regulators' mandates to be viable.

> *"There is no overarching statutory regulator for estate agents in the UK – we have limited governance in the first place, so I don't see how this works for us."*
>
> **Property stakeholder**

7.2 Quantitative analysis

A quantitative element to the evaluation was introduced to verify our qualitative assessment of the shortlisted governance models and provide a clearer basis for identifying a final recommendation.

Each of the three shortlisted governance models were scored against ten critical success factors (see Appendix E), derived from a combination of the literature review, analysis of international data portability initiatives, and engagement with stakeholders. These criteria reflect the outcomes that a successful Smart Data governance model should deliver and therefore offer a strong and relevant framework for consistently evaluating the design of each governance model.

The scoring was conducted using a five-point scale where 1 indicated the model did not meet the criterion and 5 indicated it met it fully. For nine of the ten critical success factors, scores were gathered from two sources: (1) participants in a cross-sector Smart Data workshop for government departments (provided anonymously) and (2) a panel of synthetic sector representatives (see Appendix H.1). The last critical success factor (Minimised cost) was not assessed this way, as research participants consistently struggled to offer views on this. Instead, this critical success has been assessed using an indicative costings analysis (see Appendix H.2).

To analyse the scores, we aggregated and averaged the results across the two sources. Further detail on the numerical results, and how we tested the robustness of those results, can be found in Appendix H.

7.3 Evaluation outcome

Drawing on the qualitative analysis, quantitative analysis and indicative costings, we have developed a final evaluation of each shortlisted governance models against the ten critical success factors. Unlike in the quantitative analysis, we use the categories of High, Medium, Low (rather than numerical scores) to assess the overall strength of each model. This simplified scale appropriately reflects how we have folded qualitative insights into the quantitative analysis. It also enables a clearer visual comparison across the three models. The rating of Medium for all three models under 'minimised cost' reflects the limited differences in likely costs between the models (see Appendix H.2).

Table 28 - Assessment of the three shortlisted governance models against ten critical success factors.

Critical success factors	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
1. Accountability: Ensuring all scheme participants are playing by the rules through effective compliance monitoring and enforcement.	**High**	**Medium**	**Medium**
2. Consumer trust: Building and sustaining consumer trust through clear communications, consent mechanisms, and redress systems.	**Medium**	**Medium**	**Medium**
3. Industry trust: Building and sustaining industry trust through clear rules and transparent decision-making.	**Low**	**High**	**Medium**
4. Inclusive engagement: Actively engaging all relevant stakeholders, including SMEs, consumers, and marginalised or underrepresented groups.	**Medium**	**High**	**Medium**
5. Tailoring to sectors: Reflecting the specific needs and levels of readiness in each sector.	**Medium**	**High**	**Medium**

Critical success factors	Model 2: Centrally-led	Model 3: Federated	Model 4: Regulator-led
6. Cross-sector coordination: Effectively coordinating across sectors to ensure interoperability and a consistent consumer experience.	**High**	**Medium**	**Low**
7. Adaptability: Supporting the development of new schemes and use cases over time and responding flexibly to feedback.	**Medium**	**High**	**Low**
8. Competition and innovation: Leaving space for competitive markets to thrive and promote innovation wherever possible.	**Low**	**High**	**Low**
9. Timely delivery: Enabling implementation at pace and delivering real-world impact quickly	**Medium**	**High**	**Low**
10. Minimised cost: Keeping the costs of Smart Data schemes as low as possible, especially for smaller actors.	**Medium**	**Medium**	**Medium**

As shown in Table 28, Model 3 (Federated) received the greatest number of High ratings, followed by Model 2 (Centrally-led), with Model 4 (Regulator-led) consistently receiving only Medium or Low scores. We provide further analysis of the six critical success factors where Model 3 received a 'High' rating in our evaluation. For each factor, we compare the performance of Model 3 against Model 2, explaining why the federated model performed more strongly in the eyes of stakeholders. These insights reflect both the quantitative scoring exercise, and the qualitative feedback gathered during interviews and focus groups.

Industry trust: Building and sustaining industry trust through clear rules and transparent decision-making.

Model 3: High | Model 2: Low

Model 3 was seen as significantly more likely to earn the trust of industry participants. Participants emphasised that trust is best built through co-design with industry and familiarity with sector-specific challenges: this is supported in Model 3 by the delivery of Smart Data schemes by Sector-specific Implementation Entities which thoroughly understand the relevant sector. In contrast, many participants thought a new central government body, like the Smart Data Implementation Entity, would struggle to inspire trust among participants, as it is likely to be seen as too distant from sector realities. We heard this perspective expressed especially vocally among those in the agrifood sector, where participants were clear that – in a sector with low trust in government and some pre-existing resistance to data sharing requirements – data sharing mandates from a central government body, which was not led by those with experience in the agrifood sector, would be highly unlikely to generate industry buy-in.

Inclusive engagement: Actively engaging all relevant stakeholders, including SMEs, consumers, and marginalised or underrepresented groups.

Model 3: High | Model 2: Medium

Stakeholders felt that Model 3 was better placed to embed inclusive engagement into decision-making by placing engagement responsibilities with the Sector-specific Implementation Entities. These bodies were thought to create clearer and more trusted channels for participation due to existing relationships or community structures within sectors. While Model 2 convenes Sector-

specific Advisory Groups, their purely advisory role and distance from decision-making were seen as limiting.

Tailoring to sectors: Reflecting the specific needs and levels of readiness in each sector.

Model 3: High | Model 2: Medium

Participants consistently highlighted a preference for tailoring governance to the specific dynamics, risks, and readiness levels of different sectors. Model 3's federated structure was seen as enabling this by allowing Sector-specific Implementation Entities to adapt rules, standards, and implementation timelines based on sector-specific needs. Although the Sector-specific Advisory Groups within Model 2 feed in sector-specific nuance to the central Smart Data Implementation Entity (SDIE), this input is advisory only and a step removed from delivery and decision-making.

Adaptability: Supporting the development of new schemes and use cases over time and responding flexibly to feedback.

Model 3: High | Model 2: Medium

Model 3 was seen as more adaptable to evolving markets as it allows for sector-specific components to evolve at their own pace without requiring changes across the entire governance structure. Stakeholders noted that this model also makes it easier to bring new schemes on board over time by appointing a new Sector-specific Implementation Entity. In contrast, Model 2's centralised design could limit responsiveness, as updates and expansion would need to be managed through the central body.

Competition and innovation: Leaving space for competitive markets to thrive and promote innovation wherever possible.

Model 3: High | Model 2: Low

Model 3 was perceived to better support competition and innovation. Because Sector-specific Implementation Entities are formally appointed on time-bound contracts, they are arguably more incentivised encourage innovation. These entities also understand the commercial dynamics of their sector and are well positioned to foster new use cases. This contrasts with Model 2, where the stronger central authority of the Smart Data Implementation Entity (SDIE) was seen by some as a potential barrier to innovation.

Timely delivery: Enabling implementation at pace and delivering real-world impact quickly.

Model 3: High | Model 2: Medium

Model 3's federated approach was seen as more capable of delivering progress quickly in sectors that are 'Smart Data ready', such as finance and retail energy, while still enabling other sectors to join when prepared. Model 3 additionally allows for new Smart Data schemes to be folded in over time by appointing Sector-specific Implementation Entities as needed for sectors with emerging schemes. In contract, stakeholders thought Model 2 could potentially cause delay to early delivery, since its centralised structure requires more extensive setup and agreement before any sector can begin implementation.

8. Recommendation

8.1 Overall recommendation

In the medium-term, we recommend proceeding with Model 3 (Federated) as the most appropriate governance approach for implementing Smart Data schemes across the UK economy. Under this model, Sector-specific Implementation Entities would lead delivery within their respective sectors, coordinated by a central Smart Data Coordination Entity (SDCE). The SDCE could be established within the Department for Business & Trade (DBT) and provide centralised services and mandatory guidelines to ensure consistency and interoperability across different sectors. Sector-specific regulators would enforce compliance in their sector, working closely with Sector-specific Implementation Entities. Sector-specific Implementation Entities, sector-specific regulators and sector-specific government departments would shape the work of the SDCE, via either positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators. To support long-term flexibility and accountability, we recommend that Sector-specific Implementation Entities are formally appointed on 5-year contracts, through a competitive process held by the relevant government department and with built-in review points. For a full description of Model 3 (Federated), see Section 5.3.

In leading sectors such as finance and retail energy – where potential Smart Data governance infrastructure and stakeholder readiness are already high – this model would enable progress at pace. The model also allows for other sectors to be phased in over time as they become ready to design and deliver their own Smart Data schemes. However, the SDCE can ensure that the overall Smart Data economy remains coherent and interoperable, supporting easy sharing of data between sectors. At this stage, a more centralised approach risks delaying early delivery of value in the most advanced sectors.

In the longer-term, it may be beneficial to expand the role and remit of the SDCE to provide greater cross-sector consistency and oversight, thereby shifting towards elements of Model 2 (Centrally-led). This transition would see the SDCE take on a wider range of centralised governance functions similar to those proposed for the Smart Data Implementation Entity in Model 2 (Centrally-led). The rationale for this potential transition is threefold. Firstly, as the Smart Data landscape matures and schemes are established in more sectors, a larger degree of centralisation could help ensure deeper interoperability, making cross-sector data sharing smoother, cheaper, and more reliable. Secondly, as more schemes are established, the relative value of reducing duplication and generating economies of scale through centralisation increases. And thirdly, in comparison to moving straight to Model 2 (Centrally-led), gradually expanding the remit of a central coordinating entity reduces delivery risks and the likelihood of hindering progress in leading sectors. For a full description of Model 2 (Centrally-led), see Section 5.2.

To inform this transition, we recommend undertaking a Smart Data governance review every five years, at intervals which align with review periods for the Data (Use and Access) Actand the contract end dates for Sector-specific Implementation Entities. The review process serves to allow government to assess whether the federated approach continues to meet delivery goals, whether more sectors are ready to be phased in, and whether any further governance functions should be centralised. At an extreme, this could result in the conclusion that Sector-specific Implementation Entities are no longer necessary in certain sectors, and implementing Model 2 (Centrally-led) in full.

Table 29 illustrates how specific governance functions could evolve from a federated to a more centralised approach over time. 14 of the 32 governance functions might expect to see changes in delivery through this transition, with the remaining 18 governance functions seeing no change or very limited change over time. In particular, no change over time is expected in the delivery of policy and strategy functions or the accreditation of ATPs.

Table 29 - Summary of potential centralisation of governance functions over time, from a starting point of Model 3 (Federated).

Governance function	Recommended starting point (Model 3: Federated)	Recommendations for the future
1. Policy and strategy: No change or very limited change over time for all governance functions in this category.		
2. Standards development		
2a. Defining and maintaining technical standards	The SDCE convenes a Central Standards Working Group, comprising a range of independent experts from across relevant sectors. The Central Standards Working Group defines and periodically updates a broad set of core 'common standards' across the Smart Data economy, with a focus on standardising common attributes across different datasets (e.g. unique identifiers). Sector-specific Implementation Entities build on these common standards to develop and maintain the full range of standards for their sector. Where Sector-specific Implementation Entities identify a change is required to 'common standards', they make a recommendation to the Central Standards Working Group which retains decision-making power. Sector-specific regulators then sign off standards for their sector.	The Central Standards Working Group, convened by the SDCE, defined and periodically updates technical standards across all Smart Data schemes. Sector-specific Implementation Entities advise the Central Standards Working Group on sector-specific issues (e.g. the most common or appropriate data formats for data points only found in that sector). If Sector-specific Implementation Entities are disbanded over time, the SDCE established Sector-specific Advisory Groups to provide sector-specific advice.
2b. Developing data security classifications	The SDCE sets guidelines for data security classification levels across all Smart Data schemes. Sector-specific Data Classification Working Groups, convened by Sector-specific Implementation Entities, work within these guidelines to develop and maintain full data security classifications for their sector. This takes into account the risks associated with both 'read only' and 'write' access. They submit these data security classifications to the SDCE on an annual basis to inform the accreditation of ATPs.	The SDCE takes on responsibility for developing data security classifications across all Smart Data schemes. Sector-specific Implementation Entities advise the SDCE on sector-specific issues (e.g. the appropriate classification of data points only found in that sector). If Sector-specific Implementation Entities are disbanded over time, the SDCE established Sector-specific Advisory Groups to provide sector-specific advice.
2c. Developing privacy and security standards: No change or very limited change over time.		
2d. Defining customer experience guidelines	The SDCE defines high-level customer experience principles. In line with those principles, Sector-specific Implementation Entities then set specific customer experience requirements for their sector, including testing potential user journeys with consumers.	The SDCE sets specific customer experience requirements across all schemes. Sector-specific Implementation Entities advise the SDCE on sector-specific issues. If Sector-specific Implementation Entities are disbanded over time, the SDCE establishes Sector-specific Advisory Groups to provide sector-specific advice.

Governance function	Recommended starting point (Model 3: Federated)	Recommendations for the future
2e. Ensuring cross-sector interoperability of standards	The SDCE leads efforts to align standards across sectors, including through mandating a broad set of common cross-sector technical standards, setting guidelines for data security classifications, defining uniform privacy and security standards across schemes, and defining high-level customer experience principles.	The SDCE remains responsible for aligning standards across sectors, but has more power to do so as it now sets technical standards, data security classifications and customer experience guidelines across all schemes.
3. Accreditation of Authorised Third-party Providers (ATPs): No change or very limited change over time for all governance functions in this category.		
4. Customer protection and engagement		
4a. Handling customer complaints and redress	Each Sector-specific Implementation Entity handles customer complaints in its sector as a first port of call where the initial complaint cannot be resolved directly with the data holder. In doing so, Sector-specific Implementation Entities work in line with cross-sector guidance on customer redress created by the SDCE. This may include developing a complaints contact address, responding to complaints which do not meet thresholds for action, investigating less serious complaints and liaising with scheme participants to reach a resolution, and/or signposting more serious complaints to the ICO, relevant regulator or Ombudsman as needed. Where complaints relate to data sharing across multiple sectors, the SDCE determines which Sector-specific Implementation Entity should lead on responding, based on pre-agreed criteria developed by the SDCE.	The SDCE develops a single platform for handling customer complaints, providing a 'single front door' for Smart Data-related customer redress. This may include developing a complaints contact address, responding to complaints which do not meet thresholds for action, investigating less serious complaints and liaising with scheme participants to reach a resolution, and/or signposting more serious complaints to the ICO, relevant regulator or Ombudsman as needed.
4b. Promoting consumer understanding: No change or very limited change over time.		
4c. Defining consent requirements	The SDCE develops cross-sector customer consent requirements. Sector-specific Implementation Entities then develop consent journeys for their sector in line with these requirements, ensuring consent mechanisms are simple, clear, and comply with GDPR and other data protection regulations.	Over time, the SDCE supersedes the work of Sector-specific Implementation Entities by developing unified, cross-sector consent journeys and consent dashboards. Sector-specific Implementation Entities advise the SDCE on sector-specific issues. If Sector-specific Implementation Entities are disbanded over time, the SDCE establishes Sector-specific Advisory Groups to provide sector-specific advice.
4d. Authenticating customers and ATPs: No change or very limited change over time.		

Governance function	Recommended starting point (Model 3: Federated)	Recommendations for the future
5. Regulatory and compliance		
5a. Monitoring compliance	Sector-specific Implementation Entities continuously monitor compliance with data sharing mandates and standards within the relevant Smart Data scheme, in line with guidance set by the SDCE. Sector-specific Implementation Entities issue pre-enforcement notices where low-level instances of non-compliance are first identified. Serious or ongoing breaches are escalated to the relevant regulator with recommended next steps.	The SDCE continuously monitors compliance with data sharing mandates and standards across all Smart Data schemes, potentially including establishing reporting requirements for some data holders. The SDCE issues pre-enforcement notices where low-level instances of non-compliance are first identified, and escalates serious or ongoing breaches to the relevant regulator.
5b. Encouraging compliance: No change or very limited change over time.		
5c. Enforcing compliance: No change or very limited change over time.		
5d. Managing API conformance certification	The SDCE provides a centralised infrastructure for API conformance testing, offering standard sandbox environments to ensure APIs meet published standards before live deployment. Within this common infrastructure, Sector-specific Implementation Entities create tailored tests and sandbox environments to ensure APIs meet specific standards in their sector.	If Sector-specific Implementation Entities are disbanded, the SDCE builds on its centralised infrastructure for API conformance testing to offer scheme-specific sandbox environments.
5e. Oversight of governance bodies	As a new office within DBT, the SDCE is held to account through existing governance structures and ministerial oversight in the department. Oversight includes regular performance reviews and public reports to ensure the SDCE meets its objectives and remains accountable to the public. Sector-specific Implementation Entities are held to account by the sector-specific government departments which hold their contracts. This includes through quarterly progress reviews and annual contract reviews.	If Sector-specific Implementation Entities are disbanded, sector-specific government departments are brought onto the Board of the SDCE to ensure they can continue to appropriately shape Smart Data schemes in their sector.
6. Implementation		
6a. Developing implementation plans	The SDCE develops a high-level cross-sector Smart Data implementation plan, drawing on expertise from across sectors through the Smart Data Council. Sector-specific Implementation Entities use that plan to define their own detailed delivery plans, which are signed off by the relevant sector-specific government department and the SDCE. Progress against these delivery plans is tracked through quarterly progress reviews and annual contract reviews for Sector-specific Implementation Entities.	The SDCE develops a detailed Smart Data implementation plan for all sectors. Sector-specific Implementation Entities advise the SDCE on sector-specific issues. If Sector-specific Implementation Entities are disbanded over time, the SDCE established Sector-specific Advisory Groups to provide sector-specific advice.

Governance function	Recommended starting point (Model 3: Federated)	Recommendations for the future
6b. Stakeholder engagement and representation	The SDCE runs stakeholder engagement programmes when consulting on cross-sector changes to Smart Data delivery. Sector-specific Implementation Entities do the same when consulting on sector-specific changes to Smart Data delivery. Both actors ensure engagement is inclusive and that diverse perspectives (e.g. SMEs, rural businesses, marginalised consumer groups) shape Smart Data delivery. The SDCE draws on expertise from across sectors through the Smart Data Council, which includes consumer, SME and industry representatives.	The SDCE takes on responsibility for sector-specific stakeholder engagement, alongside engagement on cross-sector changes to Smart Data delivery.
6c. Facilitating knowledge sharing: No change or very limited change over time.		
6d. Setting up appeals and dispute resolution mechanisms	The SDCE develops a generic dispute resolution model to resolve disagreements between parties (excluding customers) in a Smart Data scheme. Sector-specific Implementation Entities adopt this model and implement it within their scheme. The SDCE supports coordination between Sector-specific Implementation Entities when disputes straddle the boundaries of two or more schemes.	The SDCE develops a centralised dispute resolution process to resolve disagreements between parties (excluding customers) in all Smart Data schemes, superseding the need for Sector-specific Implementation Entities to run sector-specific dispute resolution processes.
6e. Managing funding models: No change or very limited change over time.		
6f. International engagement: No change or very limited change over time.		

This recommendation reflects the findings of our evaluation of options, which assessed each shortlisted model against ten critical success factors developed during earlier phases of research.

- **Model 2 (Centrally-led) performed well in the evaluation of options**, particularly on criteria such as accountability and cross-sector coordination. Stakeholders recognised that its stronger central body could help drive consistency, enforce standards, and avoid duplication of effort. Its centralised structure was considered well-suited to supporting interoperability between schemes, helping to ensure a consistent experience for customers and more efficient data sharing across sectors. However, this model was also considered more difficult to deliver in the short term, likely to slow progress for sectors ready to advance with Smart Data schemes, and potentially unable to adapt to the varying needs of different sectors.
- **Model 3 (Federated) emerged as the strongest performer overall.** It received the most 'High' ratings in the results of the quantitative analysis, maintaining its lead across all weighted and unweighted scoring scenarios (see Appendix H.1). It was valued for its flexibility and deliverability, especially in enabling the most advanced sectors to begin delivering value sooner. The qualitative analysis reinforced these findings, with Model 3 receiving consistent positive feedback in interviews and focus groups across sectors. It was seen as the most pragmatic approach to launching cross-sector Smart Data governance models without being held back by the complexity of standing up an all-encompassing centralised delivery body from the outset.
- **Model 4 (Regulator-led) was less favoured**, as many raised doubts about whether regulators have the right mandate, capabilities or capacity to lead Smart Data delivery.

The recommended Model 3 (Federated) therefore provides the UK with a Smart Data governance model that is deliverable now and can adapt to the needs of different sectors. However, through the use of 5-yearly review cycles, it is also adaptable over time, leaving the door open to a more centralised approach in future which offers the greatest benefits for avoiding duplication enabling cross-sector data-sharing.

Explanation box 4: Funding models for Smart Data governance

Establishing funding models is out of scope for this project. This report focuses on designing governance models for Smart Data, not on determining how they will be funded. While we identify governance functions and the roles required to deliver them, the specific financial models for supporting these roles – whether through public investment, industry contributions, or other means – will require separate policy work to be specified in secondary legislation.

However, stakeholders consistently told us that funding models are critical to success. Across interviews and focus groups, stakeholders highlighted the importance of ensuring that governance entities are sustainably and fairly funded, in order to incentivise all actors with a Smart Data scheme to develop effective Smart Data propositions.

What we heard from stakeholders included:

- **Governance costs should not fall solely on data holders**. In the UK's Open Banking scheme, the nine large banks were required to fund not only their own data sharing infrastructure to remain compliant with Open Banking rules, but also the operational costs of Open Banking Limited. Many stakeholders described this as inequitable, noting that it fostered a 'compliance-only' mindset among some data holders. Data holders often will bear the brunt of upfront investments in Smart Data schemes, while deriving relatively little direct commercial benefit from data sharing itself. In contrast, Authorised Third-party Providers (ATPs) are frequently better positioned to monetise Smart Data but contribute far less to initial set-up and governance. To avoid repeating this dynamic, future schemes could pursue more equitable funding approaches.
- **Short-term public funding may be required.** Particularly for new or less developed sectors, many felt that government investment would be necessary to initiate governance activities, given the time required for schemes to become self-sustaining.
- **In the longer term, a 'user pays' model was generally seen as appropriate**. There was support for exploring sustainable models in which those who benefit most from Smart Data schemes, such as Authorised Third-party Providers (ATPs), contribute to its ongoing cost, potentially via regulatory levies, ATP accreditation fees, or charges per API call.
- **Governance funding models are dependent on commercial models**. Participants stressed that the ideal model for funding Smart Data governance can only be determined once commercial models for Smart Data schemes as a whole are established. Only then will it be clear how value flows to different actors through the Smart Data scheme, and therefore what an appropriate model for funding governance bodies would be.

> *"Funding of Smart Data should make sure that data providers and users benefit financially rather than seeing Smart Data as a compliance burden and money sink."*
>
> **Cross-sector expert**
>
> *"The government might need to support initial costs to get a scheme off the ground – otherwise it won't get the breadth of participation."*
>
> **Agrifood stakeholder**
>
> *"Who pays is a huge question. You can't ask start-ups to fund everything upfront – we won't participate."*
>
> **Property stakeholder**

8.2 Next steps for delivery

We have identified eight early delivery actions to begin implementing the recommended medium-term governance model: a federated Smart Data approach coordinated by a central Smart Data Coordination Entity (SDCE). These represent the immediate next steps required to put the preferred model into practice, including promoting cross-sector interoperability from the outset. However, a larger piece of work will be required to develop a robust and comprehensive delivery plan with clear timelines over the longer term. Importantly, the recommended governance model should be viewed as an end state to work towards over time, recognising that many of its components will need to be developed and implemented incrementally rather than established all at once.

The eight early delivery actions are:

1. **Confirm high-level model architecture**: Formally adopt Model 3 (Federated) as the UK's starting governance model for Smart Data, by publishing an official decision statement or ministerial announcement.
2. **Identify priority sectors:** Confirm which sectors are highest priority to progress with establishment of Smart Data schemes in the short term (likely to be finance and retail energy).
3. **Bring together regulators**: Regulators should be brought together as soon as possible to begin supporting the development of consistent Smart Data regulation approaches across sectors: the Digital Regulation Cooperation Forum (DRCF) could offer a useful forum for this collaboration. A first step here might be to further stress test and if needed refine the recommendations in this report. This will also support the identification of appropriate Smart Data regulators in sectors without a single sector-wide regulator: potentially the most difficult outstanding question for the development of Smart Data governance models. The experience of the Joint Regulatory Oversight Committee (JROC) in Open Banking suggests coordinating a joint approach among different regulators may prove challenging, and so starting work early to align regulators around a unified purpose and approach will be important.
4. **Publish a Smart Data implementation plan**: Outline potential timelines for the establishment of a cross-sector Smart Data governance model, to guide stakeholders and coordinate governance activity across sectors. Gather input from industry, regulators and other government departments to inform this.
5. **Establish the Smart Data Coordination Entity (SDCE):** Decide on and initiate the preferred route for establishing the SDCE. Stand up the SDCE, defining clear responsibilities and lines of accountability (e.g. to a minister or Steering Group). The SDCE should be established early in order to set a common basis for Sector-specific Implementation Entities to build upon once appointed. In particular, the SDCE should prioritise establishing a set of core common technical standards and a cross-sector ATP accreditation process: these are the highest priority governance functions for promoting cross-sector interoperability.
6. **Set contractual terms for Sector-specific Implementation Entities**: Develop standardised example specifications and contracts for Sector-specific Implementation Entities to define expectations in detail. Support other government departments to tailor specifications and contracts for Sector-specific Implementation Entities to their sector's needs if required. Their responsibilities should not be defined only as delivery of a successful Smart Data scheme in their relevant sector. They should also have responsibilities for engaging effectively with the SDCE and actively supporting interoperability across schemes: this should be a core contractual requirement, not an optional add-on.

7. **Appoint initial Sector-specific Implementation Entities in leading sectors:** If appointing Sector-specific Implementation Entities via a competitive process, publish standard eligibility and selection criteria for Sector-specific Implementation Entities after consultation with relevant regulators and government departments. Support other government departments to deliver a competitive formal appointment process in their sector. Sector-specific Implementation Entities should be appointed after the SDCE is established, so that they have common standards and a central ATP accreditation process to build upon.
8. **Provide oversight of initial Smart Data scheme delivery in leading sectors:** Provide active oversight and coordination during initial delivery stages in leading sectors, ensuring the SDCE and early Sector-specific Implementation Entities remain aligned on timelines and delivery targets. Support cross-government communication to ensure relevant departments (e.g. HM Treasury, DESNZ) are aligned and resourced to support scheme launch. To ensure cross-sector interoperability, DBT should play a proactive role in prompting government departments, regulators and Sector-specific Implementation Entities in leading sectors such as finance and retail energy to consider whether emerging Smart Data approaches could be scaled or adapted across other sectors, including testing with government departments and regulators in sectors not yet implementing Smart Data schemes. This early engagement will allow departments and regulators to shape cross-sector design decisions, ensuring that the Smart Data governance model works not only for current schemes but also for those planned in the future.

Appendix A – Learning from current UK Smart Data schemes

The UK has been a global leader in implementing and exploring Smart Data schemes, with significant progress made in introducing Open Banking and growing interest across other industries. Indeed, efforts are underway to understand what Smart Data schemes in the wider finance, retail energy and telecommunications sectors might look like. This sector-specific thinking undertaken to date should be considered and built upon for designing governance models for the Smart Data economy at large. This section outlines the progress made in each of the sectors and identifies key learnings for the design of Smart Data governance models.

Key learnings for Smart Data governance

- **A central implementation entity can drive adoption and compliance,** as the role of Open Banking Limited (OBL) has demonstrated in Open Banking. While OBL faced governance challenges, its existence helped prevent market fragmentation and ensured a level playing field for ATPs. Notably, OBL was established and funded by the UK's nine largest banks and building societies under a CMA order – a structure that may have influenced both its legitimacy and its ability to secure cooperation.
- **Well-defined reporting structures** are important for Smart Data governance. Indeed, the transition to a Future Entity for Open Banking governance is a direct response to OBL's lack of independent oversight, inadequate reporting lines, and concentration of power in the Implementation Trustee.
- **Balanced stakeholder representation** supports successful Smart Data schemes. The Future Entity in Open Banking also aims to correct current shortcomings here by introducing a more balanced governance board with varied stakeholder representation and independent scrutiny.
- **Sector-specific governance models require tailored approaches.** Consultations on new Smart Data initiatives highlight the importance of governance models that reflect the specific needs and challenges of different sectors. This suggests that while overarching governance principles (e.g., accreditation, enforcement) could be consistent and built with interoperability in mind, sector-specific frameworks should be flexible enough to accommodate industry differences.

A.1 Open Banking

The UK's Open Banking ecosystem currently comprises over 300 Authorised Third-party Providers, and 13 million small businesses and consumers use the scheme regularly.[67] It offers significant opportunities for consumers, financial services and the UK economy.[68] The governance model for Open Banking in the UK changed in 2023, most notably with the establishment of the Joint Regulatory Oversight Commission. This section outlines UK's Open Banking governance model both before and after this change in more detail.

A.1.1 Open Banking 1.0 (2017-2023)

From its inception in 2017 to 2023, Open Banking relied on 3 key governance bodies:

[67] Department for Energy Security & Net Zero, 2025, Developing an energy smart data scheme.
[68] Financial Conduct Authority, 2021. Open Finance Feedback Statement.

1. **Open Banking Limited (OBL),** formerly known as the Open Banking Implementation Entity (OBIE), to set standards (including data standards, API specifications and trust frameworks), maintain a directory of ATPs, monitor compliance and provide routes for industry redress.
2. **The Competition and Markets Authority (CMA)** to set policy objectives and enforce compliance among the large banks in the CMA9.
3. **The Financial Conduct Authority (FCA)** to accredit new ATPs joining the Directory maintained by OBL.

OBL was created in 2017 through the CMA's Retail Banking Market Investigation Order 2017 (henceforth *the Order*). OBL is a not-for-profit implementation entity that lies at the heart of the UK's Open Banking ecosystem.[69] It is funded by (but fully independent of) the nine largest banking and building society institutions in the UK and Northern Ireland, known as the CMA9.[70] OBL has played four primary roles in Open Banking to date:

1. **Standards development,** including developing and maintaining the Open Banking data standards, API specifications and a trust framework.
2. **Maintaining the directory of ATPs**.[71] However, accreditation of ATPs itself is conducted by the FCA.
3. **Regulatory and compliance,** including maintaining a trust framework and ensuring. This includes collecting management information from the CMA9, monitoring whether security and counter-fraud measures are upheld, and providing a Conformance Certification Service.[72] However, enforcement of compliance is conducted by the CMA.
4. **Customer protection and engagement,** by providing routes for industry redress via a Dispute Management System which facilitates resolution of complaints between banks and Authorised Third-party Providers.

OBL is a vehicle utilised by the CMA to enable compliance with the Order. Without an implementation entity like OBL, the burden of coordination and standardisation within Open Banking would likely have fallen on individual stakeholders, resulting in fragmentation, inefficiencies, and heightened consumer risk. However, it is important to note that OBL is not, and has never been, a regulator within Open Banking. Therefore, while it has been central to setting standards and monitoring compliance with those standards, it does not have the power to enforce compliance. [73]

The CMA's *Order* empowered an 'Implementation Trustee' to lead the OBL and ultimately take responsibility for implementing Open Banking. An advisory group called the Implementation Entity Steering Group (IESG) was also convened to support the Implementation Trustee and engage relevant stakeholders.[74] The IESG brought together a wide variety of stakeholders including: the CMA9, the CMA, Pay.UK, the Payment Systems Regulator (PSR), industry representatives, the Information Commissioner's Office (ICO), HM Treasury, the FCA, and independent representatives for both consumers and small businesses.[75,76] The IESG is not a decision-making body for OBL but a forum for the provision of advice to the trustee on the delivery of the roadmap set out in the CMA's *Order*.[77]

---

[69] Open Banking Implementation Entity, 2020. Open Banking Annual Report 2020.
[70] OECD, 2024. The impact of data portability on user empowerment, innovation, and competition.
[71] Department for Energy Security & Net Zero, 2025, Developing an energy smart data scheme.
[72] Open Banking Implementation Entity, 2020. Open Banking Annual Report 2020.
[73] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[74] Open Banking Implementation Entity, 2020. Open Banking Annual Report 2020.
[75] Competition and Markets Authority, 2022. The future oversight of the CMA's Open Banking remedies Response to consultation.
[76] Open Banking Implementation Entity, 2020. Open Banking: Annual Report 2020.
[77] Competition Markets Authority, 2022. Retail Banking Market Investigation Agreed Arrangements.

In 2021, an independent report from Alison White highlighted the significant governance failures faced by OBL and prompted the 2022 Open Banking Lessons Learned Review, written by the CMA.[78] The report concluded that OBL had not ensured proper management of the UK's Open Banking scheme in accordance with the *Order*, attributing the failure to both OBL and primary stakeholders, including the CMA.

The CMA's review identified that "too much power was vested in one individual" (the Chair and Implementation Trustee of OBL). The review noted that the Trustee's role as Chair, requiring them to act as a director in accordance with the Companies Act, could potentially conflict with their role as Trustee under the *Order*.[79] It also found that governance arrangements for OBL were "poorly defined", with it operating with a minimal board and no formal reporting lines to the CMA, which left oversight fragmented and ineffective. Indeed, it said that OBL's governance processes "fell down the cracks between the CMA and CMA9," leading to insufficient checks and balances and a lack of independent scrutiny.[80] These issues were exacerbated by the CMA's underestimation of Open Banking's complexity, viewing it as a short-term initiative with minimal governance needs which led to inadequate resourcing and strategic oversight. Several missed opportunities to reassess governance models in 2017 and 2018, coupled with a lack of engagement at senior levels, further entrenched these issues, undermining the effectiveness of the OBL.

A.1.2 Open Banking 2.0 (2023-present)

OBL's suggested governance failures underlined the need for a more cohesive and forward-looking governance model, leading to the formation of the Joint Regulatory Oversight Committee (JROC) in 2023. Comprising HM Treasury, CMA, FCA, and PSR, JROC oversees Open Banking's evolution while employing a "regulatory sandbox" model to test and adapt governance models.[81]

The recommendations for the next phase of Open Banking, published by JROC in 2023, outline a staged transition for the scheme with increasing responsibility for a yet-to-be-established Future Entity.[82] Recommendations were shaped by taking stakeholder views, namely those of industry participants, consumers, and business stakeholders, into account. Those engaged expressed a strong preference for the Future Entity to evolve into a central standard-setting body, capable of adapting to future Smart Data initiatives, such as Open Finance.

The Future Entity is envisioned in UK Finance and Baringa's 'Open Banking Futures, Blueprint and Transition Plan' as a not-for-profit company limited by guarantee.[83] This company would be headed by a Board comprising nine voting members, including independent directors, a consumer organisation representative, and participant representatives. This structure ensures balanced representation while avoiding undue influence from any single group. The Future Entity will also implement high standards of corporate governance, following the UK Corporate Governance Code, with dedicated committees for audit, risk, and remuneration, and a clear separation of responsibilities between the Chair and CEO.

The Future Entity's role will extend beyond governance in Open Banking to support initiatives like Open Finance. It will maintain transparent reporting to JROC, which will oversee its composition and ensure alignment with regulatory objectives. By adopting proven tools like the Consumer Evaluation Framework and engaging stakeholders effectively, the Future Entity will foster trust and continuity while driving innovation in Open Banking and beyond.[84]

---

[78] White, A., 2021. Investigation of Open Banking Limited.
[79] Competition and Markets Authority, 2022. Open Banking Lessons Learned Review.
[80] White, A., 2021. Investigation of Open Banking Limited.
[81] Ju, Y, Liu, H. & Zhang, X., 2024. Personal Financial Data Sharing Mechanisms within the Open Banking Framework. *International Journal of Education and Humanities.*
[82] Joint Regulatory Oversight Committee, 2023. Recommendations for the next phase of open banking in the UK.
[83] UK Finance & Baringa, 2021. Open Banking Futures: March 2021 Blueprint And Transition Plan.
[84] Competition and Markets Authority, 2022. The future oversight of the CMA's Open Banking remedies Response to consultation.

The CMA is considering whether an Implementation Trustee will remain necessary under the Future Entity or if it should be replaced by a monitoring trustee to oversee compliance and reporting on the CMA9's obligations.[85] The Future Entity's funding will initially continue under the current OBL funding model, with CMA9 as primary contributors, until the Board of the Future Entity and JROC agree on a sustainable long-term funding mechanism.[86]

The governance model of Open Banking strongly indicates the importance of formal regulatory powers and a central implementation entity. The CMA's authority to compel the CMA9 to establish and fund OBL, combined with OBL's technical expertise, was instrumental in ensuring successful implementation and outcomes compared to other jurisdictions.[87] It also led to the successful achievement of the CMA's initial reasoning for Open Banking: driving competition in retail banking. However, JROC's roadmap for the Future Entity reflects lessons from OBL's governance challenges, emphasising the need for stronger oversight and balanced stakeholder representation. Within a long-term regulatory framework, the Future Entity aims to continue refining and expanding Open Banking whilst avoiding past pitfalls.[88]

A.2 Open Finance

Building on the principles of Open Banking, Open Finance aims to broaden Smart Data's reach across the financial sector, encompassing additional markets and data types such as mortgages, pensions, insurance, and investments. Open Finance envisions giving customers greater control over their financial data, enabling them to access tailored advice, switch providers, and optimise their financial decisions. The FCA and other regulators are working to define the framework, drawing lessons from Open Banking's governance model. Respondents to consultations have emphasised the need for clear liability models, robust accreditation systems, and effective cross-sector coordination.[89] Although still in development, Open Finance underlines the importance of scalability and adaptability in governance models to support the diverse needs of financial services.

The governance model for Open Finance will require a coordinated and flexible framework to replicate and expand upon the successes of Open Banking. In 2019, the FCA published a Call For Input (CFI) to inform their regulatory strategy towards Open Finance. Respondents to this consultation emphasised the importance of key governance elements including:

1. **Functional roles:** standards development, customer protection and engagement, ATP authentication, conformance testing (i.e. allowing firms to check and prove they have met the standards), and maintaining an accredited directory of firms.
2. **Supervisory roles:** the regulatory and compliance functions of monitoring, enforcement, and reporting.

Each of these elements were vital to the success of Open Banking.[90] The Open Finance Feedback Statement notes that governance of Open Finance will likely require a central implementation entity like OBL to manage these functions and ensure coordination across the ecosystem.[91]

Lessons from Open Banking suggest that strong regulatory oversight and legislative compulsion will be necessary to drive full participation and compliance in Open Finance. The CFI respondents noted that a future entity for Open Finance could sit within a central governing body alongside other sector-specific entities to promote cross-sector alignment. The Centre for Finance, Innovation and Technology (CFIT) has commented that having an accountable body focused on managing

[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Financial Conduct Authority, 2021, Open finance: Feedback Statement.
[90] Financial Conduct Authority, 2021, Open finance: Feedback Statement.
[91] Ibid.

the implementation of Open Banking has been a key factor in the UK's success, especially when compared to less coordinated approaches in other jurisdictions.[92] CFIT has expressed their readiness to steward the development and implementation of UK Open Finance.

A.3 Smart Data in the energy sector

A potential future Smart Data scheme in the retail energy sector is also under consideration in the UK. It seeks to empower customers by enabling access to data about tariffs, energy usage, and renewable energy options, while also addressing pressing challenges such as decarbonisation and energy efficiency. The UK's Department for Energy Security and Net Zero (DESNZ) published a call for evidence in January to understand the potential for introducing a Smart Data scheme in the energy sector, and the accompanying governance models. DESNZ notes that roles and responsibilities within the scheme would include both:

1. **Functional roles:** data classification, role definitions for access and use, access rights, accreditation requirements, validation requirements.
2. **Supervisory roles:** the regulatory and compliance functions of monitoring, enforcement, and reporting.

In addition, DESNZ notes that a Smart Data energy scheme would likely include both an Authority and Ecosystem Controller. The Authority would be "the regulator who has the power to determine the rules of the scheme and assign roles and permissions" while the Ecosystem Controller would "administer the scheme on [the Authority's] behalf, ensuring compliance with the scheme rules." This is very much in the image of Open Banking, where the Competition and Markets Authority represents the Authority and Open Banking Limited the Ecosystem Controller. DESNZ also highlight the potential to standardise and centralise certain functions or responsibilities across sectors to enable cross-sector use cases: this might include accreditation of ATPs, performance monitoring, and/or enforcement processes.[93] However, as this initiative is only just entering its consultation phase, these initial ideas for the design of Smart Data governance models in the energy sector will likely still evolve substantially based on stakeholder feedback.

A.4 Open Communications

A future Open Communications Smart Data scheme could focus on enabling customers to share data on their telecommunications usage, including broadband and mobile services, to increase competition, improve service quality, and reduce costs for customers. The CMA recommended in 2018 that Ofcom should investigate a Smart Data scheme as a means of increasing consumer engagement and overcoming the 'loyalty penalty' in communications markets. However, much like Smart Data in the energy sector, the development of an Open Communications scheme remains in the consultation phase.

Ofcom launched an initial call for evidence on Open Communications in 2020.[94] This demonstrated that, if the creation of an Open Communications scheme is mandated in legislation, Ofcom anticipate receiving specific powers to implement it.[95] In terms of governance, Ofcom outlined the likely need for:

1. **Robust and compulsory ATP accreditation schemes**, potentially building upon Ofcom's existing voluntary accreditation scheme for digital comparison tools.
2. **An approach to determining liability and offering redress**, noting that third parties in communications sector currently sit outside the jurisdiction of any Alternative Dispute

[92] Centre for Finance, Innovation and Technology, 2024. Embracing the UK's Open Finance Opportunity.
[93] Department for Energy Security & Net Zero, 2025, Developing an energy smart data scheme.
[94] Ofcom, 2020. Open Communications: Enabling people to share data with innovative services.
[95] Ofcom, 2020. Open Communications: Enabling people to share data with innovative services.

Resolution (ADR) scheme, such as the Ombudsman Services or the Communication and Internet Services Adjudication Scheme (CISAS).

3. **A continuing role for the Information Commissioner's Office ICO** to develop and enforce data protection rules for communications providers and ATPs that reflect the specifics of Open Communications.
4. **Dedicated regulatory oversight of Open Communications ATPs**, above and beyond Ofcom and the CMA's current approach to enforcing consumer and competition law.

Respondents to Ofcom's consultation were generally supportive of these principles. However, opinions differed as to whether an accreditation scheme for ATPs should be (a) cross-sector to support cross-sector interoperability or (b) sector-specific to ensure it adequately addresses communications-specific concerns. In general, regulators and consumer advocacy groups favoured a cross-sector approach, while telecommunications providers favoured a sector-specific approach. Several respondents also suggested a cross-industry working group is developed to support approaches to data standardisation.[96]

A.5 Cross-sector Smart Data Initiatives

Respondents to the FCA's 2021 Open Finance Call for Input largely supported the idea of a centralised entity playing a key role in coordination and oversight.[97] They emphasised its potential to ensure consistency of standards and approaches to support the delivery of Smart Data initiatives across multiple industries. Specifically, respondents suggested that the Smart Data Function could:

1. Establish an appropriate and proportionate ATP accreditation/certification system that works across sectors and monitor their performance.
2. Serve as a delivery arm with different industry implementation entities under it (e.g. OBL).
3. Define cross-sector standards for data and APIs which enable interoperability across sectors.
4. Be responsible for the centralised oversight of the wider data system.
5. Coordinate timelines across markets.

A cross-sector approach to accreditation was identified as a key need as ATPs that hope to operate across markets would face duplicative requirements if different accreditation processes were introduced for each Smart Data initiative. The introduction of a simplified cross-sectoral accreditation process was proposed to ensure that ATPs could be vetted once and then access customer data across different Smart Data initiatives to offer maximum value.[98] However, security and accreditation needs may vary significantly between sectors. For example, adopting the FCA's authorisation standard as a universal baseline could prove overly burdensome for sectors with lower risk profiles or different regulatory contexts. Any cross-sector process would therefore need to balance efficiency with proportionality, ensuring high standards without deterring ATP participation.

Despite these proposals, the establishment of the Smart Data Function as initially outlined by BEIS has not been explicitly detailed in recent publications. However, ongoing discussions around Smart Data governance suggest that the principles of cross-sector coordination, standardisation and accreditation remain central to the evolving Smart Data landscape.

---

[96] Ofcom, 2021. Update on Open Communications: Enabling people to share data with innovative services.
[97] Financial Conduct Authority, 2021. Open Finance: Feedback Statement.
[98] Department for Business, Energy & Industrial Strategy, 2019. Smart data: Putting consumers in control of their data and enabling innovation.

Appendix B – Learning from international Smart Data schemes

Countries worldwide are adopting diverse approaches to Smart Data governance, reflecting their unique regulatory priorities, market conditions, and resources. While some jurisdictions (e.g. Australia, Brazil) follow regulation-led models with mandated and standardised data sharing frameworks, others (e.g. US, Japan) favour market-driven approaches where participation is voluntary. This section explores these varying governance models across jurisdictions, offering insights into different governance models, implementation challenges, and emerging best practices.

Assessing the effectiveness of Smart Data governance models internationally remains challenging due to the limited availability of evaluations and comparative studies, particularly in English. However, while direct assessments of governance successes are scarce, the case studies shared within this report can still provide inspiration and a range of lessons for designing governance models.

Notably, the term 'Smart Data' is rarely used internationally. However, Smart Data is fundamentally a form of 'data portability' – defined as "the ability of users to easily transfer their personal data from one service provider to another" – and the term 'data portability' is commonly used internationally. In the following section, we continue to use the term Smart Data when referring to international data portability initiatives for consistency, although note that specific legislation or frameworks may use the term data portability instead.

Key learnings for Smart Data governance

1. **Open Banking has been delivered in tandem with aspects of wider Open Finance schemes** in many other countries, clearly evidencing the practicality of joint Smart Data governance models across banking and finance.
2. **Cross-sector Smart Data governance across banking and energy** has also been developed in Australia, with cross-sector accreditation processes, redress mechanisms and data standards bodies.
3. **Central banks have been assigned as the lead authority** for governance of Open Banking and/or Open Finance schemes in many jurisdictions (e.g. Brazil, India, EU Member States, UAE) due to their regulatory stability and enforcement power. There may be a correlation between central banks acting as the lead authority and the speed of Open Banking and/or Open Finance implementation, with Brazil, India, and the EU achieving live status within 2–3 years, and the UAE in just one year - though market readiness likely greatly influences these timelines.
4. **Smart Data governance models should be able to scale and adapt.** Much like in Open Banking in the UK, the governance models in many international Smart Data schemes (e.g. in Japan, US and Australia) have evolved over time to meet changing technological and regulatory needs.

B.1 Australia

In Australia, Smart Data schemes are governed by the Consumer Data Right (CDR) framework, introduced in 2019, which allows consumers to share their data with accredited third parties to obtain better deals on products and services. The CDR is currently active in the banking and

energy sectors.[99] Designed to empower consumers by giving them greater ownership over their data, the CDR follows a compulsory regulatory model, mandating data holders to share consumer data with accredited ATPs upon the customer's request by stipulating the technical standards to be used for data sharing.[100]

The governance model of the CDR is built on collaboration between multiple government bodies:

1. **The Australian Competition and Consumer Commission (ACCC)** leads the accreditation process, manages the CDR register of accredited data recipients (ADRs), and enforces compliance.
2. **The Office of the Australian Information Commissioner (OIAC)** oversees privacy and confidentiality aspects, including data breach notifications and consumer complaints.
3. **The Data Standards Body (DSB)**, within the Treasury, develops and maintains technical and consumer experience standards through consultation with multistakeholder advisory groups.

Together, these bodies form a coordinated system to support secure and transparent data sharing across sectors.[101]

The CDR was initially planned to expand from banking into energy and telecommunications in 2021. However, in 2023, the CDR was paused for the superannuation (pensions in Australia), insurance, and telecommunications sectors.[102] The Australian Government redirected focus toward maturing existing implementations after an independent 2023 report highlighted that compliance costs significantly exceeded initial estimates.[103] In 2024, the Assistant Treasurer described the CDR as a "good idea, badly executed," acknowledging the need for a strategic reset to address the key concerns with the current CDR. These concerns include: [104]

1. **High regulatory burden** and disproportionately high compliance costs for mid-tier banks due to frequent rework of the standards
2. **Lack of incentive** for businesses to use CDR data
3. **Low CDR take-up** amongst consumers

Following this, a CDR 'reset' was announced, with consultations aimed at simplifying customer consent and reducing participation barriers to enhance adoption and drive greater competition.

Open Banking in Australia introduced the principle of data reciprocity, requiring third-party providers to share relevant consumer data with banks. This feature addressed criticisms of earlier Open Banking models elsewhere, such as those in the UK, which created a one-sided data sharing relationship.[105] In the energy sector, CDR implementation focuses on customer account details, billing data, and meter usage, with write-access capabilities for ATPs being legislated for to enhance functionality.[106] The sector-by-sector rollout demonstrates the flexibility and scalability of Australia's approach, though challenges remain in aligning cross-sector standards and governance.

B.2 Singapore

Singapore has adopted a guided market-led approach to Smart Data governance. The 2021 amendment to Singapore's Personal Data Protection Act (PDPA) introduced a 'Data Portability

[99] Australian Government, accessed January 2025. What is CDR?
[100] OECD, 2024. The impact of data portability on user empowerment, innovation, and competition.
[101] Ibid.
[102] Dentons, accessed February 2025. Australia's data portability rights: An update on what's happening on the Consumer Data Right.
[103] Better Regulation Advisory, 2023. Consumer Data Right Compliance Costs Review.
[104] Ashurst.COM, accessed February 2025. A reset for the Consumer Data Right.
[105] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[106] Department for Energy Security & Net Zero, 2025. Developing an energy smart data scheme: call for evidence.

Obligation', requiring organisations to provide consumers with their data in a machine-readable format upon request.[107] However, unlike compulsory models, Open Banking and data sharing initiatives in Singapore are supported through non-binding guidance issued by the Monetary Authority of Singapore (MAS) rather than strict regulations. MAS has partnered with the Association of Banks in Singapore to release open API-based system architecture standards, facilitating voluntary adoption by financial institutions and third parties.[108]

At the core of Singapore's Smart Data governance is the Singapore Financial Data Exchange (SGFinDex, 2020): the world's first state-controlled digital infrastructure integrating a national digital identity system (SingPass) for secure data sharing. SGFinDex connects financial data from government agencies, banks, and other financial institutions, enabling users to access their financial information via a centralised platform.[109] SingPass serves as the user authentication mechanism for customers, ensuring security while streamlining data sharing processes. This centralised model offers cost-efficiency for participating institutions but has limitations, such as the single points of vulnerability represented by SGFinDex and SingPass.[110] SGFinDex was developed by the public sector in collaboration with The Association of Banks in Singapore and seven participating banks, including Citi and HSBC.[111]

Singapore's Smart Data governance demonstrates the effectiveness of collaboration between regulators, financial institutions, and industry stakeholders. SGFinDex is a joint initiative by MAS and the Smart Nation and Digital Government Group (SNDGG), with the support of the Ministry of Manpower (MOM).[112] In Open Banking, MAS supports innovation through initiatives like the Financial Industry API Register, which lists APIs developed by financial institutions, and the ASEAN Fintech Innovation Network, which encourages interoperability and develops a vibrant Smart Data ecosystem.[113] The Personal Data Protection Commission facilitates complaints between customers and providers for SGFinDex.[114]

SGFinDex is expanding as part of Singapore's Smart Nation initiative, with plans to include insurers and the Singaporean Exchange (SGX) Central Depository (CDP), integrating new sectors into the Singaporean Smart Data ecosystem.[115] This demonstrates the adaptability of Singapore's governance model for cross-sector use.

B.3 European Union

The European Union (EU) adopted a mandated but not standardised data sharing approach to Smart Data governance, underpinned by frameworks like the General Data Protection Regulation (GDPR) and the Second Payment Services Directive (PSD2).

GDPR establishes a foundational right to data portability, allowing individuals to request the transfer of their personal data to third parties, thereby shifting market dynamics toward consumer control over data.[116]

PSD2, implemented by the European Commission in 2018, extends the principle of data sharing specifically within the financial sector by mandating banks to grant ATPs secure access to customer account data through standardised APIs.[117] While PSD2 requires banks to facilitate data portability, it does not impose specific technical implementation standards. Instead, individual EU

[107] OECD, 2024. The impact of data portability on user empowerment, innovation, and competition.
[108] National University of Singapore, 2020. Open Banking: The Changing Nature of Regulating Banking Data - A case study of Australia and Singapore.
[109] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[110] Ibid.
[111] Ozone API, accessed January 2025. Singapore Financial Data Exchange – SGFinDex.
[112] Smart Nation, accessed February 2025. Singapore Financial Data Exchange (SGFinDex).
[113] Singapore Management University, 2022. Open Finance: Regulatory Challenges.
[114] Consultative Group to Assist the Poor, 2020. Open Banking: How To Design For Financial Inclusion.
[115] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[116] European Journal of Law and Technology, 2024. The right to data portability: A holistic analysis of GDPR, DMA & the Data Act.
[117] Centre on Regulation in Europe, 2021. Making Data portability more effective for the digital economy.

member states were responsible for incorporating the directive into their national laws and regulations. For Open Banking, 16 EU jurisdictions are led by central banks, 10 by financial services authorities, and one by a securities commission (Greece).[118]

The European Banking Authority (EBA) plays a key role in overseeing Open Banking by developing technical standards and guidelines, ensuring compliance with PSD2 requirements.[119] However, enforcement is decentralised, with National Competent Authorities (NCAs) in each member state responsible for monitoring compliance and addressing violations. PSD2 implementation and governance models also vary across EU member states.

In Germany, the Berlin Group, a coalition of banks and financial service providers, leads NextGenPSD2, a standard adopted by over 3,600 European banks.[120] This represents ~80% of European market coverage in implemented PSD2 Open Banking standards.[121] This de facto technical standard ensures interoperability and secure API access for ATPs, harmonising compliance efforts across the Eurozone. Governance is industry-led, with a Plenary overseeing various taskforces responsible for security, authorisation, and implementation. In Germany, the Federal Financial Supervisory Authority (BaFin) mandatorily enforces PSD2, protecting consumers and encouraging institutions to adopt fintech solutions.[122]

In Czechia, the Czech Banking Association (CBA) established the Czech Open Banking Standard (COBS) as a voluntary standard for PSD2 compliance.[123] While PSD2 mandates open banking, Czech banks retain flexibility in implementation, allowing deviation where necessary to align with proprietary payment service provider systems. COBS is governed by a working group that reviews changes annually, integrating regulatory updates and industry feedback.

In Poland, the banking sector responded to PSD2 by developing Polish API, a voluntary framework defining API access for TPPs.[124] Unlike in Germany, participation is not mandatory, and entities may opt for alternative PSD2-compliant solutions. Governance is maintained through a central registry and a certificate-based trust framework, ensuring API security.

In France and Belgium, an API provider formed by a group of major French banks called STET developed a national API standard compliant with PSD2.[125] While STET's corporate board manages overall strategy and development, a separate Clearing and Settlement Mechanism (CSM), governed by its participants, controls the routing and processing of payments.[126]

In Sweden, PSD2 is enforced through *Finansinspektionen*: Sweden's financial supervisory authority.[127]

Despite progress, the EU faces challenges in achieving consistent implementation. Uneven competition enforcement and regulatory frameworks among member states have made uniform practices difficult to achieve.[128] In 2022, Following the increase in Open Banking adoption rates, the EU initiated discussions over PSD3 with the aim of expanding Open Banking into Open Finance and standardising data sharing.[129]

Beyond financial services, the EU has adopted sector-specific regulations imposing data sharing obligations. For instance, the Motor Vehicle Regulation requires vehicle manufacturers to share certain vehicle data, while the Electricity Directive of 2019 mandates consumer data sharing

---

[118] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[119] Stripe, accessed February 2025. Open banking regulation explained: A guide.
[120] Ozone API, accessed February 2025. NextGenPSD2.
[121] Berlin Group, accessed February 2025. Press Release 2023.
[122] Macro Global, accessed February 2025. State of Open Banking in Europe.
[123] Ozone API, accessed February 2025. Czech Standard for Open Banking – COBS.
[124] Ozone API, accessed February 2025. Polish API.
[125] Ozone API, accessed February 2025. STET PSD2 API.
[126] Ibid.
[127] Macro Global, accessed February 2025. State of Open Banking in Europe.
[128] European Journal of Law and Economics, 2023. Data portability and interoperability: An E.U.-U.S. comparison.
[129] Macro Global, accessed February 2025. State of Open Banking in Europe.

among electricity suppliers to encourage competition and innovation.[130] The EU does, however, lack a unified governance model for cross-sector Smart Data portability.

B.4 United States[131]

Historically, the United States has taken a market-driven approach to Open Banking, relying on financial institutions to develop their own data sharing frameworks. Unlike the UK and EU, where Open Banking is mandated through regulatory directives, the US has allowed banks to self-regulate data sharing agreements.[132]

Without a standardised API strategy, many ATPs continue to rely on screen scraping: an outdated and insecure method of accessing consumer financial data.[133] This approach is costly and inefficient for ATPs, as they must negotiate separate agreements with individual banks or resort to accessing accounts through customer credentials. For banks, this introduces liability concerns, as they remain solely responsible for customer protection even when data is accessed by ATPs without their explicit knowledge.[134] Additionally, screen scraping often grants ATPs access to more consumer data than necessary, increasing security risks for both customers and financial institutions. The absence of a clear regulatory framework has therefore led to fragmented implementation, limiting consumer choice and inhibiting the widespread adoption of secure, interoperable data sharing solutions.

Growing pressure from policymakers has led to regulatory intervention, particularly following a 2022 Executive Order on competition, which explicitly encouraged the Consumer Financial Protection Bureau (CFPB) to strengthen data portability rights.[135] The CFPB is a key regulatory player in the US which oversees financial data sharing and influences the regulatory landscape through its reports and proposals.[136] Following the Executive Order, the CFPB proposed new rules in 2023 under a previously dormant provision in Section 1033 of the Dodd-Frank Act, aiming to provide consumers with greater control over their financial data and enable secure data sharing with third-party providers.[137] This new rule is called the 'Personal Financial Data Rights' rule.

Despite these new advances, the US financial services market remains highly fragmented, with multiple regulators overseeing different aspects of financial data portability. One example is the Office of the Comptroller of the Currency (OCC), which supervises and regulates national banks and federal savings associations and monitors their roles in Open Banking.[138] The Securities and Exchange Commission, which regulates the securities market in the US, has not issued any specific guidance on Open Banking but has developed APIs that provide public access to financial filings and market data submitted by listed companies.[139]

The Financial Data Exchange (FDX), an industry-led body, plays a central role in attempting to unify API standards across financial institutions and promoting interoperability.[140] FDX has applied to the CPFB for formal recognition as a standards-setting entity, helping financial institutions develop common API-based data sharing protocols.[141] The FDX API standard is currently widely

[130] Centre on Regulation in Europe, 2021. Making Data portability more effective for the digital economy.
[131] Please note that this section captures the state of play in the United States prior to the advent of the Trump administration in January 2025. The significant reshaping of the US federal government in the intervening period may have changed the nature of regulatory intervention in Smart Data.
[132] University of Edinburgh, 2023. Secure Hardware Adoption in the Open Data Context.
[133] Accenture, 2025. Consumer Data Right Strategic Review.
[134] Deloitte, accessed February 2025. Open Banking around the world.
[135] Brookings, 2023. Data portability and interoperability.
[136] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[137] Ibid
[138] Office of the Comptroller of the Currency (OCC), 2023. Remarks at FDX Global Summit "Open Banking and the OCC".
[139] U.S. Securities and Exchange Commission, accessed February 2025. EDGAR Application Programming Interfaces.
[140] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[141] Open Banking Expo, accessed January 2025. FDX applies to be recognised as standards-setting body by CFPB.

adopted in the US. The FDX, combined with the Personal Financial Data Rights Rule, hence plays a key role in pushing the US market towards more secure, regulated data sharing practices.

B.5 Brazil

Brazil has emerged as one of the fastest adopters of Open Finance, implementing Smart Data regulations across both retail banking and insurance in 2021, with both initiatives going live by 2022.[142] The country has taken a regulation-led approach with mandated and standardised data sharing. The Central Bank of Brazil (Banco Do Brasil, BCB) serves as the lead authority, overseeing governance, compliance, and enforcement. Unlike in other jurisdictions where Open Banking and Open Finance are treated separately, Brazil has integrated all financial institutions (i.e. including retail banks) into the same Open Finance scheme, defining the data holders as 'All Financial Institutions'.[143] The unified regulatory structure enables high interoperability.

Governance of Brazil's Open Finance ecosystem is managed through a three-tiered system, consisting of:

1. **The Deliberative Council**, which defines internal regulations, structural guidelines, and approves norms and specifications.
2. **The Secretariat**, responsible for operational coordination
3. **Technical Groups**, which conduct studies and develop technical proposals in alignment with the directives set by the Deliberative Council and the Central Bank.[144]

The National Monetary Council (NMC) also plays a central role in defining participation criteria for Open Finance institutions.[145] These regulatory bodies work together to ensure the effective implementation and evolution of Open Finance in Brazil.

Brazil's governance model has supported one of the fastest Open Finance adoptions globally, with its four-stage phased implementation strategy playing a key role in ensuring a structured and efficient rollout.[146] This strategic rollout has resulted in one of the fastest Open Finance adoptions globally, reaching five million connected accounts within a year, significantly outpacing the UK's Open Banking trajectory. Moreover, Brazil's governance model benefits from national ID integration, which streamlines accreditation and security processes for financial institutions.[147] Unlike the UK, which requires additional regulatory accreditation, Brazilian institutions can rely on pre-existing national ID verification for onboarding.

Despite Brazil's successes, challenges remain in cross-sector governance operations. While Open Banking has thrived under BCB's leadership and extensive legal prowess, Open Insurance has struggled due to being regulated by a separate authority with a more limited remit.[148] This regulatory fragmentation perhaps highlights the importance of strong, centralised oversight for successful cross-sector data portability initiatives. Ensuring cross-sector coordination will be essential for the future evolution of Brazil's Open Finance landscape.

B.6 Hong Kong

Hong Kong has adopted a guided approach to Smart Data governance, primarily relying on voluntary participation rather than regulatory mandates. In 2018, the Hong Kong Monetary Authority (HKMA) published the Open API Framework, which provides guidelines for financial

[142] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[143] Ibid.
[144] Inter-American Development Bank, 2023. Open Finance in Latin America and the Caribbean.
[145] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[146] Inter-American Development Bank, 2023. Open Finance in Latin America and the Caribbean.
[147] Department for Business, Energy and Industrial Strategy, 2021. Smart Data Research: Third Party Accreditation.
[148] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.

institutions but does not require them to participate.[149] Unlike the UK's Open Banking model, where accreditation of ATPS through the OBL is mandatory, Hong Kong does not impose an accreditation requirement for participants.[150] Hong Kong does not have a planned law or legislation addressing customer liability. Instead, contracts with third parties must include customer protection terms, ensuring consumers are not liable for unauthorised transactions unless they act fraudulently or with gross negligence.[151] As accreditation and customer liability mechanisms are critical for consumer protection and building public trust in the Smart Data ecosystem, this could pose a barrier to Hong Kong's trust framework.

Hong Kong's Open Banking framework is among the most developed in the Asia-Pacific (APAC) region, facilitating Payments, General Insurance, Savings & Investments, Customer Lending, and Mortgages data, with Pensions data being the only missing component.[152] Hong Kong also drives innovation in its Smart Data landscape, as shown by the HKMA's launch of the Commercial Data Interchange (CDI) in 2022 to provide an interoperable platform for data sharing between banks, developers, and third-party providers such as telecommunications companies.[153] This next-generation financial data infrastructure furthered Hong Kong's Open Banking and Open Finance ecosystem.[154] A set of CDI governance documents, standardised agreements and templates were issued by the HKMA to assign different parties' responsibilities and liabilities in CDI.[155] However, participation in CDI remains voluntary, allowing financial institutions to choose whether to integrate and leverage commercial data for improved financial products.

Banks are expected to establish a formal Third-Party Service Provider (TSP) governance process, covering due diligence, onboarding, monitoring, security, and consumer protection.[156] A consultation concluded that a common baseline for TSP governance should be agreed upon by banks, allowing for consistent onboarding while permitting institution-specific requirements. Contract terms between banks and TSPs must have a clear set of policies and processes defining areas of consumer protection in accordance with the codes of practice issued by the Privacy Commissioner of Personal Data (PCPD).

While this market-led approach encourages flexibility and innovation, it can create challenges in standardisation and security. Recognising these issues, the HKMA has announced plans to take a more active role in setting security and data sharing standards for the later phases of API implementation.[157] This reflects a broader trend in market-driven jurisdictions where regulators intervene to address interoperability and consumer protection challenges as Smart Data ecosystems mature.[158]

B.7 United Arab Emirates

The United Arab Emirates (UAE) has rapidly implemented a regulation-led Open Finance framework, achieving live status in 2024 after passing their Open Finance regulation in 2023.[159] The Central Bank of the UAE (CBUAE) is the lead authority, mandating all financial institutions under its supervision to participate in Open Finance, and standardising the rollout. Other key regulators include the Dubai Financial Services Authority (DFSA) and the Abu Dhabi Global Market (ADGM) Financial Services Regulatory Authority, both of which support the initiative's development.

---

[149] Hong Kong Monetary Authority, accessed January 2025. Open Application Programming Interface (API) for the Banking Sector.
[150] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[151] Bank for International Standards, 2019. Report on open banking and application programming interfaces (APIs).
[152] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.
[153] Hong Kong Monetary Authority, accessed January 2025. Commercial Data Interchange (CDI).
[154] Singapore Management University, 2022. Open Finance: Regulatory Challenges.
[155] Ozone API, accessed January 2025. Open API Framework for Hong Kong.
[156] Ibid.
[157] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[158] Ibid.
[159] Ibid.

UAE's Open Finance framework mandates customer-consented data sharing across banking, insurance, payments, and financial services, offering a wide array of services to consumers.[160] A key feature of the UAE's model is its centralised API Hub, ensuring interoperability and security in financial data sharing. The API Hub enforces a Testing and Certification Process to ensure all Licensed Financial Institutions (LFIs), and ATPs, adhere to regulatory standards before offering Open Finance services.[161] Unlike many jurisdictions, the UAE's Open Finance Framework integrates Open Banking and Open Insurance under a single regulation.[162] UAE hence offers one of the most comprehensive cross-sector date portability implementations globally.

The governance model of Open Finance in the UAE is highly centralised, ensuring strong oversight, compliance, and consumer protection with the CBUAE setting regulations.[163] Notably, the UAE is the first regulator globally to implement a consolidated Trust Framework and centralised API within its Open Finance Framework, enabling a single secure connection for cross-sectoral data sharing and transaction initiation with user consent.[164] The Trust Framework houses a Participant Directory for identity verification, digital certificates for secure communication, and a regulatory sandbox for testing and compliance validation.[165] Additionally, strict liability and enforcement mechanisms ensure consumer protection, with financial penalties for non-compliance and compensation requirements in case of disputes.[166] Combined, the UAE's fast-tracked approach, centralised regulatory oversight, and cross-sector integration set a benchmark for efficient and secure Open Finance governance.

B.8 India

India has adopted a somewhat atypical approach to Open Banking and Open Finance, built on India Stack: a Digital Public Infrastructure (DPI) integrating identity, data, and payments.[167] DPI is defined as shared digital systems that are secure, interoperable and can support the delivery of and access to public and private services across society.[168] India has standardised, but not mandated, data sharing.

India Stack was developed to address financial exclusion in a previously predominantly cash-based economy by reducing barriers to digital transactions. The expansion of digital payments enabled by India Stack has played a large role in driving economic development, stabilising rural incomes, and increasing sales for firms in the informal sector.[169] India Stack is managed collaboratively, with key components such as Aadhaar (biometric digital ID), the Unified Payments Interface, DigiLocker (electronic document storage), and the Account Aggregator (AA) framework owned and maintained by different regulatory bodies.[170]

The Account Aggregator Framework, introduced in 2019 by the Reserve Bank of India (RBI), is central to India's data sharing governance.[171] It enables individuals to securely share their financial data, such as bank statements, insurance, pensions, and investment records, between regulated entities via standardised APIs. through standardised APIs.[172] Unlike most Open Banking models, which narrowly focus on bank account and payment data, as in the UK's Open Banking scheme, India's AA Framework enables access to a much broader range of financial information. This includes insurance policies, mutual fund holdings, pension contributions, and tax records. This

[160] Ozone API, accessed January 2025. CBUAE.
[161] Open Finance UAE, accessed January 2025. Testing and certification Framework.
[162] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[163] Ozone API, accessed January 2025. CBUAE.
[164] Two Birds, accessed January 2025. UAE Central Bank Implements Open Finance Framework.
[165] Central Bank of the UAE, 2023. CBUAE Open Finance Regulation.
[166] Open Finance UAE, accessed January 2025. Limitation of the liability model.
[167] IndiaStack, accessed January 2025. IndiaStack.
[168] OECD, 2024. Digital Public Infrastructure For Digital Governments.
[169] International Monetary Fund, accessed February 2025. Stacking Up Financial Inclusion Gains in India.
[170] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[171] Ozone API, accessed January 2025. India Stack.
[172] Department of Financial Services, accessed May 2025. Account Aggregator Framework.

wider scope makes it close to a full-fledged Open Finance system rather than traditional Open Banking.

The Account Aggregator ecosystem is run by Sahamati, a self-organised, non-profit organisation that also maintains the AA central registry.[173] Sahamati was tasked with growing the account aggregator ecosystem and running an "umbrella" entity for account aggregators.[174] It also operates a framework for smooth grievance redressal of all customer complaints. This includes referring customers to the relevant Ombudsman.[175] Sahamati undertook part of the regime's governance, including developing certification guidelines on software and issuing technical standards.[176]

The National Payments Corporation of India (NPCI) also plays a critical role by running the Unified Payments Interface (UPI).[177] The UPI integrates digital payment service providers with the banking system. The NPCI is responsible for approving banks and third-party application providers for participation in this system. Both the Account Aggregator and the UPI are regulated by The Reserve Bank of India.[178]

Despite its broad regulatory coverage, customer lending and mortgage data is not yet live in India's Open Banking and Open Finance ecosystem. India initially relied on sector-specific regulations, such as the vertical data protection regulation for Open Finance: The Digital Personal Data Protection (DPDP) Act (2023).[179] India's approach highlights the benefits of a state-led digital infrastructure but also underlines the need for a unified regulatory framework to balance interoperability and financial inclusion.

B.9 Japan

Japan has adopted a market-driven yet coordinated approach to Smart Data governance, balancing industry-led innovation with regulatory oversight. The Financial Services Agency regulates electronic payment service providers, including account aggregators and ATPs. The legislation for 'Electronic Payment Intermediate Service Providers' (2018) requires registering with the Financial Services Agency, establishing an authorisation process, and requiring banks to publish their Open API policies.[180]

Unlike the prescriptive regulatory models of the EU or UK, Japan's framework is voluntary but highly structured, reflecting a broader trend in Asia where governments provide high-level guidance while allowing markets to dictate adoption.[181] For example, while there is no formal or compulsory Open Banking framework, the Japanese government has encouraged financial institutions to contract with at least one ATP by 2020.[182] This effectively drives adoption through regulatory encouragement rather than direct mandates. The Association for Electronic Payment Services, a private body, has also been designated to handle customer complaints, ensuring a consumer protection mechanism within the voluntary framework.[183]

At an international level, Japan has led efforts to shape cross-border data governance through its Data Free Flow with Trust (DFFT) initiative, introduced by former Prime Minister Shinzo Abe in 2019.[184] Data Free Flow with Trust (DFFT), introduced in 2019, aims to promote the free flow of

[173] Kniru, accessed January 2025. Account Aggregator System: India's Open Banking Revolution.
[174] Sahamati, accessed January 2025. Empowering Indians with their Data for a Better Financial Future.
[175] Sahamati, accessed January 2025. Sahamati's Approach to Dispute Resolution.
[176] Consultative Group to Assist the Poorest, 2020. Open Banking: How To Design For Financial Inclusion.
[177] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[178] Ozone API, accessed January 2025. India Stack.
[179] Cambridge Centre for Alternative Finance, 2024. The Global State of Open Banking and Open Finance.
[180] Ozone API, accessed January 2025. Japan Open Banking Framework.
[181] Consultative Group to Assist the Poorest, 2020. Open Banking: How To Design For Financial Inclusion.
[182] Open Banking around the world, accessed January 2025. Open Banking around the world.
[183] Ibid.
[184] Economic Research Institute for ASEAN and East Asia, 2024. Future of Data Governance in Asia and Operationalisation of 'Data Free Flow with Trust' Policy Brief.

data while ensuring trust in privacy, security, and intellectual property rights.[185] Japan's leadership in the G20 and G7 has driven the mobilisation of DFFT, culminating in the establishment of an Institutional Arrangement for Partnership to promote interoperable global data governance.[186] As part of the initiative, Japan proposed creating an international database of policies and regulations on cross-border data flows, aiming to provide clarity, especially for SMEs navigating complex regulatory landscapes. However, challenges remain in ensuring alignment across regulatory frameworks and balancing industry flexibility with consumer protections.

Overall, Japan's model highlights the potential of voluntary frameworks to drive Open Banking adoption while demonstrating the importance of international regulatory collaboration in an increasingly interconnected Smart Data economy.

[185] OECD, accessed January 2025. Data free flow with trust.
[186] Economic Research Institute for ASEAN and East Asia, 2024. Future of Data Governance in Asia and Operationalisation of 'Data Free Flow with Trust' Policy Brief.

Appendix C – Learning from other UK data sharing schemes

The development of Smart Data governance models will also benefit from learnings from other data sharing schemes within the UK. This section examines governance models for two of these data sharing schemes, highlighting their potential relevance for Smart Data governance models.

Key learnings for Smart Data governance

1. **Leveraging established regulators**, rather than creating entirely new governance bodies, may be effective for Smart Data schemes.
2. **Industry forums which continuously improve data standards** may be needed in some sectors; however, others could proceed with existing cross-sector data standards.
3. **Safeguards to give ATPs equal footing**, such as fair access to data, transparent accreditation, and measures to prevent dominance, should be built into governance models.

C.1 Commercial Credit Data Sharing

The Commercial Credit Data Sharing (CCDS) scheme was introduced by HM Treasury in 2015 under the Small and Medium-Sized Business (Credit Information) Regulations to enhance competition in SME lending by lowering barriers for new entrants. Before CCDS, major banks held exclusive access to SME financial data, limiting challenger banks' ability to effectively assess credit risk and provide credit options to SMEs. CCDS requires **Designated Banks**, a group of nine major institutions, to share SME credit data with **Designated Credit Reference Agencies (CRAs)**, which collect, process, and distribute this data to eligible lenders with SME consent. This allows newer lenders to make better-informed lending decisions, particularly benefiting small and newer businesses with limited credit histories.[187]

The governance of the Commercial Credit Data Sharing (CCDS) scheme involves multiple key entities, each with distinct roles and responsibilities. **HM Treasury** oversees policy implementation, conducts statutory reviews, consults stakeholders to ensure CCDS meets its objectives, and accredits Designated Credit Reference Agencies (CRAs). Meanwhile, the **Financial Conduct Authority (FCA)** monitors compliance, conducts market studies, and enforces CCDS regulations.[188] Noting that governance arrangements in the credit market are "too slow to respond to changes in the market to allow for it to adapt in a nimble manner and lack the appropriate representation", the FCA are now developing a new **Credit Reporting Governance Body (CRGB)**.[189]

The CCDS scheme has successfully increased competition in SME lending by lowering entry barriers for challenger banks and alternative lenders.[190] In turn, the policy is estimated to have boosted the probability of SMEs establishing new borrowing relationships by 25%.[191] Strong oversight by HM Treasury and regulatory enforcement by the FCA have therefore been effective in ensuring compliance.

However, there are also drawbacks to the CCDS governance design to learn from:[192]

[187] HM Treasury, 2024. CCDS Post-Implementation Review.
[188] Ibid.
[189] FCA, 2023. Credit Information Market Study.
[190] CFIT, 2024. SME Finance Taskforce – Smart Data: improving SME lending to drive economic growth.
[191] Bank of England, 2024. Customer data access and fintech entry: early evidence from open banking.
[192] HM Treasury, 2024. CCDS Post-Implementation Review.

Lack of flexibility in changing Designated Banks: As UK businesses have been increasingly turning to challenger and specialist banks, the market share of the Designated Banks in the CCDS scheme has fallen substantially since 2015. This trend is reducing the proportion of the market that finance providers are certain to receive data on from the designated CRAs and raising issues of fairness.

Inconsistent data quality: In the early stages of CCDS, inconsistent data quality prompted HM Treasury to set up forums to work closely with credit providers and CRAs to agree on and continuously improve data templates.

Lack of competition among CRAs: Under the CCDS scheme, non-designated finance providers did not need to provide data to all designated CRAs, but instead could provide data to one or more of the designated CRAs as they prefer. This resulted in one CRA becoming dominant and limiting competition.

C.2 Mobility-as-a-Service

Mobility-as-a-Service (MaaS) platforms integrate data from multiple transport services into a single, accessible platform, allowing users to easily plan, book, and pay for journeys across different modes of transport.[193]

In terms of governance, the **Department for Transport (DfT)** is responsible for developing and publishing the MaaS Code of Practice: a voluntary framework that guides the development of MaaS platforms.[194] Meanwhile, the **Competition and Markets Authority (CMA)** plays a role in monitoring anti-competitive behaviours, such as exclusivity agreements between MaaS platforms and transport providers that could limit consumer choice, by virtue of its existing remit.[195] The Code of Practice also acknowledges that, as the MaaS market grows in the UK, there may be a need for DfT to also monitor the market to ensure it is operating in a fair way.

The MaaS Code of Practice places significant emphasis on data standardisation and interoperability. However, rather than bringing stakeholders together to create MaaS-specific standards, the UK government encourages transport operators and MaaS providers to align with national and international data standards, such as those established by the British Standards Institute (BSI) and the **Information Commissioner's Office's (ICO)** Data Sharing Code of Practice).[196] These standards ensure consistent, accurate data quality.

TNO conducted research into the various governance models for MaaS across the Netherlands, Austria, Finland, France, the US and Singapore. The research notes that in some countries public authorities play a major role and set up their own MaaS platform, while in other countries government plays a much more limited or reactive roles, mainly in setting framework conditions or playing a facilitating role in building an ecosystem. TNO notes the benefits of these different approaches remain unclear. However, across all countries, TNO note that public-private collaboration is key, saying: "organising cooperation between all relevant stakeholders is key when it comes to the development and deployment of MaaS. It is crucial that a representative selection of different categories of stakeholders be included, with specific attention to end-users and consumer groups.[197]

MaaS governance models offer lessons for Smart Data schemes by demonstrating how industry-led innovation can be balanced with regulatory safeguards by utilising existing bodies like the ICO for data privacy guidance and the CMA for competition oversight.

---

[193] MaaS Alliance, accessed January 2025. Mobility as a Service?
[194] Department for Transport, accessed January 2025. Mobility as a Service: code of practice
[195] Ibid.
[196] Ibid.
[197] TNO, 2021. Policy options to steer Mobility as a Service: international case studies

Appendix D – Overview of qualitative research sample

This section provides a summary of our qualitative research samples across (1) qualitative research interviews, (2) focus groups, and (3) a cross-sector workshop with government stakeholders.

D.1 Qualitative research interviews

In total, 104 stakeholders were interviewed on a one-to-one basis. These interviews were conducted with representatives from across the Smart Data ecosystem, including:

- **Current and potential Authorised Third-party Providers (ATPs),** such as fintech firms and data-enabled service providers operating in sectors like banking, property, and transport.
- **Data Holders**, including major utilities, banks, retailers, and telecom providers that hold consumer datasets potentially in scope for Smart Data access.
- **Sector Experts**, such as legal, academic, and industry consultants with specialist knowledge of data sharing, governance models, and digital infrastructure.
- **Regulators**, drawn from a mix of economic, sector-specific, and data-focused regulatory bodies across all priority sectors.
- **Relevant Government Departments**, including teams responsible for sector policy, digital regulation, or consumer data rights in the UK.

Table 30 provides a summary of the total samples by stakeholder type and sector.

Table 30 - Summary of our qualitative research sample.

Industry	ATP	Data Holder	Sector Expert	Regulator	Relevant Gov't Dept	Total
Finance	7	10	13	7	2	**39**
Energy	1	3	3	1	2	**10**
Property	3	7	4	4	4	**22**
Retail	1	2	4	0	0	**7**
Transport	1	0	6	0	1	**8**
Telecoms	0	5	0	1	3	**9**
Agrifood	0	0	4	1	1	**6**
Several/all	0	0	2	0	1	**3**
Total	**13**	**27**	**36**	**14**	**14**	**104**

Stakeholder engagement was particularly strong in the finance sector, which accounted for 39 interviewees. This reflects the sector's maturity in data sharing practices and prior experience with Open Banking. Similarly, high levels of engagement were achieved in property where we conducted 22 interviews, reflecting a strong appetite for improved data sharing in this traditionally analogue sector. In contrast, the remaining sectors yielded fewer participants, suggesting lower levels of readiness or interest in cross-sector Smart Data governance discussions at this stage.

D.2 Focus groups

A series of eleven focus groups were conducted to explore cross-sector perspectives and test the emerging governance model options. These sessions formed a key part of the stakeholder engagement strategy, complementing one-to-one interviews by enabling richer, interactive discussion and sector-specific deep dives.

Focus groups brought together a mix of data holders, Authorised Third-party Providers, regulators, and sector experts from across the Smart Data ecosystem. Sessions were held both on a sector-specific basis – targeting stakeholders within individual priority sectors – and in cross-sector formats, designed to extract comparative reflections and highlight cross-sector governance challenges and opportunities.

In total, 61 stakeholders participated in focus groups. Engagement levels varied across sectors, reflecting differences in stakeholder readiness, maturity of data sharing discussions, and appetite to engage in governance design. Finance, property, and cross-sector groups attracted the highest participation, while other areas such as retail had more limited attendance. This variation aligns with observed patterns in the one-to-one interviews and highlights the need for tailored engagement strategies across sectors in future phases. The breakdown of focus group participation is summarised in Table 31.

Table 31 - Summary of attendance at focus groups.

Focus group	Total attendees
Cross-sector Round 1	8
Finance & Banking	9
Retail	2
Telecommunications	5
Transport	7
Agrifood	7
Retail energy	5
Property	9
Cross-sector Round 2	9

D.3 Government workshop

A dedicated workshop with UK government officials was held toward the end of the research period to sense-check emerging findings, test the feasibility of proposed governance models, and explore practical implementation considerations. Participants included policy leads from relevant departments (e.g. DBT, DSIT, HMT), Smart Data policy owners, digital regulation specialists, and representatives from teams involved in Open Banking and Smart Data legislation. This session helped to refine assumptions in the evaluation of options, particularly relating to cost modelling, institutional feasibility, and legislative pathways.

Appendix E - Critical Success Factors for Smart Data governance

To ensure that Smart Data schemes achieve their intended outcomes and operate effectively over time, it is essential to identify the key conditions that underpin successful governance. These Critical Success Factors represent the foundational enablers that should be in place for Smart Data to deliver value for consumers, industry, and government alike. The Critical Success Factors outlined in Table 32 were developed through a combination of rigorous literature review, analysis of international Smart Data and data portability initiatives, and extensive engagement with UK stakeholders across sectors. We have identified ten factors that serve as a guide for designing and implementing robust Smart Data governance models in the UK. We have also used these Critical Success Factors as key criteria for evaluating the likely success of different governance model designs (see Section 7.2).

Table 32 - Ten critical success factors we used to assess potential Smart Data governance models.

Trust and inclusion	**1. Accountability:** Ensuring all scheme participants are playing by the rules through effective compliance monitoring and enforcement.
	2. Consumer trust: Building and sustaining consumer trust through clear communications, consent mechanisms, and redress systems.
	3. Industry trust: Building and sustaining industry trust through clear rules and transparent decision-making.
	4. Inclusive engagement: Actively engaging all relevant stakeholders, including SMEs, consumers, and marginalised or underrepresented groups.
Balancing sector needs	**5. Tailoring to sectors:** Reflecting the specific needs and levels of readiness in each sector.
	6. Cross-sector coordination: Effectively coordinating across sectors to ensure interoperability and a consistent consumer experience.
Future readiness	**7. Adaptability:** Supporting the development of new schemes and use cases over time and responding flexibly to feedback.
	8. Competition and innovation: Leaving space for competitive markets to thrive and promote innovation wherever possible.
Deliverability	**9. Timely delivery:** Enabling implementation at pace and delivering real-world impact quickly
	10. Minimised cost: Keeping the costs of Smart Data schemes as low as possible, especially for smaller actors.

The remainder of this section explores each Critical Success Factor in turn.

E.1 Accountability

Holding scheme participants to account is perhaps the most essential success factor for Smart Data governance models. Smart Data schemes are complex data sharing ecosystems which require all scheme participants – data holders, ATPs and customers – to have confidence that all

other parties are playing by the agreed rules of the scheme.[198] This requires clear and effective accountability mechanisms. Accountability mechanisms are also important for protecting consumers from harm, ensuring that scheme participants are both adequately protecting consumer data and refraining from misuse of customer data, such as unwelcome selling-on of data.[199]

The importance of governance models holding scheme participants to account has been clearly demonstrated in the UK's Open Banking scheme. In 2020, Open Banking Limited (OBL) developed a Customer Evaluation Framework to evaluate live products and services enabled by Open Banking: this included a detailed, evidence-based review of the performance of large retail banking providers across six primary outcome areas. The positive impact was notable, with OBL reporting "a significant uplift in conformance, availability, and performance" in this period.[200] The importance of governance models holding scheme participants to account was further reinforced by responses to the Competition & Markets Authority's consultation on Open Banking in 2022[201] and the Financial Conduct Authority's Call for Input on Open Finance in 2021.[202]

Internationally, central banks have been responsible for enforcing regulations and standards in many jurisdictions (e.g. Brazil, India, EU Member States, UAE), building on their existing regulatory power. Although we cannot prove causation, several jurisdictions which have taken this approach have implemented Smart Data schemes faster than the UK.

> *"There must be strong accountability. Otherwise, people start bending the rules and the whole thing just falls apart."*
>
> **Finance stakeholder**
>
> *"You need clear accountability – no one is going to take part if they think someone else is getting a free ride."*
>
> **Property stakeholder**

E.2 Consumer trust

Many consumers are instinctively sceptical or mistrustful of Smart Data schemes: a 2022 poll of 2,000 UK residents suggested only 25% and 28% of the public think the benefits of Open Finance and Open Communications respectively outweigh the potential risks. Older people are especially likely to be mistrustful or sceptical of Smart Data schemes.[203] This is a finding replicated internationally: for example, 81% of Americans believe the potential risks of data collection by companies outweigh the benefits.[204] By increasing the transfer of personal data between organisations, Smart Data schemes may therefore risk heightening the public's fears and confusions around personal data sharing.[205]

However, as Open Banking adoption grows, Smart Data schemes have a foundation of trust to build upon. Participation in Open Banking has continued to rise, with 14% of digitally active banking customers using it as of January 2024.[206] It is crucial that new Smart Data schemes do not undermine this growing trust.[207]

Successful governance models should therefore look to build and sustain consumer trust in Smart Data schemes. To achieve this, in addition to holding scheme participants to account (see 5.1),

---

[198] Department for Business, Energy & Industrial Strategy, 2020. Smart Data Research Report: Authentication and Trust.
[199] Department for Business & Trade, 2024. Regulatory Powers for Smart Data: Impact Assessment.
[200] Open Banking Implementation Entity, 2020. Open Banking: Annual Report 2020.
[201] Competition & Markets Authority, 2022. The future oversight of the CMA's Open Banking remedies: Response to consultation.
[202] Financial Conduct Authority, 2021. Open Finance: Feedback Statement.
[203] Department for Science, Innovation & Technology, 2022. Part one: Examining public attitudes towards Smart Data schemes.
[204] Auxier, B. et al., 2019. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Pew Research Center.
[205] OECD, 2021. Mapping data portability initiatives, opportunities and challenges.
[206] Open Banking Limited, 2025. Open Banking Impact Report 2024.
[207] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.

governance models should also: enable clear communication with consumers, provide transparency in decision-making processes, and be simple and understandable for the average consumer.

> *"While wider data sharing can fuel innovation and economic growth, it must not compromise individuals' rights... consumer autonomy and privacy should not be overshadowed by market-driven goals."*
>
> **Cross-sector expert**
>
> *"Getting the APIs right is important, but so is user consent. If people don't trust the process, they won't share anything."*
>
> **Transport stakeholder**

E.3 Industry trust

Interview participants consistently emphasised that – alongside trust from customers – trust from industry is also a precondition for widespread participation in Smart Data schemes. Many stakeholders, especially from sectors where data sharing is not yet mandated, expressed concern that without clear and consistently applied rules, businesses may hesitate to invest in new data sharing infrastructure or service development. Several interviewees stressed that perceived favouritism, inconsistent rule enforcement, or opaque governance processes could undermine confidence and deter both data holders and potential Authorised Third-party Provider (ATP) providers from participating.

> *"Too often the data gets stuck because people are scared of letting it go. The rules need to give them confidence… There's nervousness about liability. If something goes wrong, they want to know someone's got their back."*
>
> **Property stakeholder**
>
> *"Customer trust and industry trust are two sides of the same coin—if either breaks, the whole system wobbles."*
>
> **Agrifood stakeholder**

Across multiple interviews, stakeholders warned that without sufficient transparency and inclusive decision-making built into the governance framework, Smart Data could be perceived by large data holders merely as a regulatory compliance exercise. This mindset risks encouraging minimal adherence to standards rather than proactive engagement or innovation in ways which deliver maximum value to customers. Participants stressed that this was evident in Open Banking, where some banks initially focused on doing the bare minimum rather than investing in service quality or new product development.

> *"You want industry to lean in, not just tick the boxes. That means governance has to feel fair and transparent."*
>
> **Finance stakeholder**

E.4 Inclusive engagement

When identifying the features of ethical and trustworthy Smart Data Schemes, the Department for Business & Trade previously noted that: "a multistakeholder, inclusive conversation that is ongoing is needed for the long-term success of Smart Data."[208] There are several reasons for this, including: to successfully draw on the technical expertise and experience of industry players; to effectively and fairly balance the interests of different parties including data holders, ATPs and

[208] Department for Business & Trade, 2023. Smart Data: Identifying the features of ethical and trustworthy Smart Data Schemes.

consumers; and to establish buy-in, cooperation and trust among stakeholders across the Smart Data ecosystem.[209] Recent developments in Open Banking governance have increasingly reflected this principle, with efforts to diversify participation and formalise inclusive stakeholder input. The importance of broad stakeholder engagement within a governance framework has been reiterated for not just Smart Data schemes, but all data sharing schemes: for example, when establishing the Common Information Model (CIM) in the energy sector, Ofgem noted that data users, vendors and network licensees should all have equal opportunities to input into governance processes.[210]

> *"There's a role for central government to set some rules, but we also need bottom-up input. It has to work in the real world."*
>
> **Transport stakeholder**

E.5 Tailoring to sectors

As the UK Government considers introducing Smart Data schemes across new sectors,[211] 'copying and pasting' governance models from Open Banking may not be appropriate. Different sectors include varying ecosystems of actors, who may already work together in specific ways, and face different challenges to data sharing.

For example, Open Banking mandates liability rules for banks and ATPs, but insurance and telecoms rely heavily on contractual terms between parties to govern liability.[212] The enactment of governance functions for each Smart Data scheme will likely therefore benefit from significant sector-specific expertise and tailoring. Both BT and Which? made this point forcefully in their response to Ofcom's consultation on Open Communications,[213] with the latter saying: "while we support the idea of the UK having a clear and coordinated approach to the regulation and oversight of Smart Data initiatives, it is important that the specific issues of each sector are taken into account and that they are not sacrificed over cross-platform solutions."[214]

In particular, global experience shows that industry-specific standard-setting bodies (e.g., Singapore's Financial Data Exchange, the Berlin Group in the EU) often improve technical innovation and adoption. As a recent review of data portability approaches across the EU and US therefore concluded, industry-specific standards-setting organisations may be more appropriate than cross-sector equivalents due to differing levels of "competence in evaluating the standards that will work best in each market setting."[215]

> *"A central entity could help make sure things don't diverge too much. But we'd want to retain sector expertise – energy has very specific risks."*
>
> **Energy stakeholder**

E.6 Cross-sector coordination

Smart Data governance should aim to strike a balance between sector-specific tailoring and cross-sector coordination. While governance models should be adapted to the unique requirements and liability structures of individual sectors, increasing cross-sector use cases necessitate alignment in enforcement, accreditation, and data standards to avoid fragmentation and inefficiencies.

The winners and finalists of the Department for Business & Trade's Smart Data Discovery Challenge demonstrate how future Smart Data use cases will be increasingly cross-sector: for

---

[209] Rubinfield, D., 2023. Data portability and interoperability: An E.U.-U.S. comparison.
[210] Ofgem, 2022. The Common Information Model (CIM) regulatory approach and the Long Term Development Statement.
[211] Department for Business & Trade, 2024. The Smart Data Roadmap: action the government is taking in 2024 to 2025.
[212] Navigant Insurance, accessed January 2025. Comprehensive Guide to Contractual Liability Insurance.
[213] Ofcom, 2021. Update on Open Communications: Enabling people to share data with innovative services.
[214] Which?, 2023. Which? response to Ofcom's Consultation on Open Communications.
[215] Rubinfield, D., 2023. Data portability and interoperability: An E.U.-U.S. comparison.

example, the use case proposed by Smartlayer.ai would combine Open Banking data *and* Smart Energy data to improve consumer choice in home finance, energy consumption and CO2 emissions reduction.[216] Future Smart Data governance models will therefore need to support cross-sector use cases. This includes ensuring cross-sector alignment and coordination in terms of, among other things, enforcement action by regulators, data standards, ATP accreditation approaches, and implementation timelines.[217] This point has been raised by a range of players across relevant industries, including in responses to calls for evidence on Open Finance[218] and Open Communications.[219]

Cross-sector coordination across Open Banking and Open Finance is clearly feasible, and these schemes have been delivered jointly in many other countries. Meanwhile, cross-sector Smart Data governance models across banking and energy have been developed in Australia, with cross-sector accreditation processes, redress mechanisms and data standards bodies. However, Australia's Smart Data schemes have faced several challenges and delays, meaning there are currently no shining examples of effective cross-sector Smart Data governance models internationally.

> *"We've got to have the freedom for propositions and for schemes to be cross-sector. That's where the value really comes."*
>
> **Finance stakeholder**
>
> *"Interoperability matters. We can't design energy Smart Data in a vacuum – people's financial and housing data also affect their energy needs."*
>
> **Energy stakeholder**
>
> *"We should be aligning with what's happening in other sectors – energy, finance, property. A joined-up approach would make a real difference."*
>
> **Transport stakeholder**

E.7 Adaptability

Smart Data governance models should be adaptable to evolving market needs. Indeed, following a 2022 consultation, the Competition and Markets Authority noted that Open Banking governance models must be "sustainable and adaptable to the future needs of the ecosystem."[220] The Joint Regulatory Oversight Committee's recommendations for the next phase of Open Banking in 2023 took this a step further by suggesting Open Banking governance models should not just be adaptable to the future of banking but to Smart Data developments beyond banking, most notably in other areas of finance.[221] Ofgem has also noted within the energy sector that data sharing governance models should "allow for agile updates".[222] This finding is corroborated by both: (a) international evidence, with both Australia and Brazil struggling to adapt their governance models when expanding Smart Data schemes beyond financial services; and (b) the experience of the UK's Commercial Credit Data Sharing scheme, where it became clear the list of providers mandated to contribute data to the schemes needed to adapt to changing market dynamics.

> *"We favour regulatory structures that can evolve. Smart Data is going to have to adapt to AI, machine learning, and any other learnings along the way."*
>
> **Cross-sector expert**

---

[216] Department for Business & Trade, 2024. Smart Data Discovery Challenge winners pave the way for new £750,000 prize launch this summer.
[217] OECD, 2021. Mapping data portability initiatives, opportunities and challenges.
[218] Financial Conduct Authority, 2021. Open Finance Feedback Statement.
[219] Ofcom, 2021. Update on Open Communications: Enabling people to share data with innovative services.
[220] Competition & Markets Authority, 2022. The future oversight of the CMA's Open Banking remedies: Response to consultation.
[221] Joint Regulatory Oversight Committee, 2023. Recommendations for the next phase of open banking in the UK.
[222] Ofgem, 2022. The Common Information Model (CIM) regulatory approach and the Long Term Development Statement.

E.8 Competition and innovation

Participants highlighted that Smart Data governance models should avoid becoming over-prescriptive or overly centralised, as doing so could stifle the competitive dynamics that drive innovation. A range of interviewees, from fintech firms to energy innovators, stated that governance models should provide baseline rules and standards but leave space for differentiation in service design, customer experience, and value propositions. Well-designed governance models were seen as critical to supporting the design of schemes that encourage competition, in order to create a dynamic ecosystem of services and providers who can compete on experience, cost, and outcomes. Participants also noted the importance of building competition into governance itself through inclusive structures and participation, to ensure decision-making does not become concentrated in the hands of a few.

> *"We really need to see competition at every level of the stack… ecosystems stagnate when a whole bunch of people feel hard done by."*
>
> **Finance stakeholder**

E.9 Timely delivery

Across interviews, there was a strong desire for momentum and urgency in the rollout of Smart Data schemes. Delays were seen as contributing to stakeholder fatigue and limiting real-world benefits for both consumers and industry. Some participants referenced previous experiences, such as the UK's Open Banking scheme and several international examples, where protracted timelines created uncertainty and delayed investment decisions. Others noted that without early, visible wins, Smart Data could lose political and commercial backing. To this end, interviewees argued that clear delivery plans, realistic timelines, simple governance structures and strong programme management are essential features of Smart Data governance models that aim to deliver impact at pace. There was also a strong preference for iterative implementation, using "test and learn" approaches that build functionality gradually rather than waiting for a fully developed end-state. This would allow benefits to emerge sooner, while still learning and adapting along the way.

> *"We need to move much faster… We've spent a long, long, long time in the small pond of Open Banking."*
>
> **Authorised Third-party Provider**

E.10 Minimised cost

To boost the overall net economic benefit of Smart Data schemes, governance models should aim to reduce the costs and administrative burden of participating in schemes for all actors. This point was raised by several contributors to the FCA's call for evidence on Open Finance.[223] The experience of Australia is also instructive here: the Consumer Data Right in Australia imposed sufficiently significant compliance burdens on mid-tier banks, which led to reduced adoption rates and ultimately delayed the whole scheme. Smart Data schemes should therefore strive for simple governance models, reducing duplication of activity across sectors and schemes, and minimising compliance requirements among scheme participants (e.g. for regular reporting), especially for smaller firms.[224] For example, OBL has flagged that reusing assets and infrastructure from Open

[223] Financial Conduct Authority, 2021. Open Finance Feedback Statement.
[224] Brookings Institute, 2023. Data portability and interoperability: A primer on two policy tools for regulation of digitized industries.

Banking for schemes like Open Communications will reduce implementation costs and avoid unnecessary duplication.[225]

> *"Excessive regulatory burden and cost can really hinder adoption. We saw that in Australia, where costs can really get out of hand."*
>
> **Finance stakeholder**

[225] Open Banking Implementation Entity, 2021. Open Banking Implementation Entity Response to Ofcom's Consultation on Open Communications.

Appendix F - Design preferences for Smart Data governance

This section outlines stakeholder preferences on how specific aspects of Smart Data governance models should be designed, drawing directly from the views shared by research participants. It focuses on the practical choices that need to be made within each governance function, such as who should lead, how decisions should be made, and what trade-offs are acceptable. These insights build on the critical success factors explored earlier and provide a foundation for designing robust, credible governance models. By understanding what stakeholders believe will work in practice, we can develop proposals that are not only theoretically sound but also politically and commercially viable.

This section describes some key design preferences from research participants in line with the governance functions outlined in Section 3. While some of the 32 governance functions prompted strong reactions and preferences from participants, others did not. We therefore only include reflections on 16 out of 32 governance functions.

F.1 Policy and strategy

Design preference 1: Government should lead on setting public interest goals and strategic priorities.

1a. Setting the vision and strategic direction: Identifying the key aims of the scheme in each sector, including by selecting priority use cases.

Participants agreed that setting the vision and strategic direction of Smart Data schemes is not a neutral or purely technical exercise: it is inherently political. By mandating data sharing and determining who bears the cost, these schemes reshape markets in ways that prioritise certain outcomes, such as consumer empowerment or decarbonisation, over others. There was consensus that government departments should therefore lead on articulating the public interest goals of Smart Data, setting strategic priorities, and deciding where trade-offs should lie, as part of a governance framework.

> *"[Smart Data requires] politicians to make a political choice because ultimately, no, not everyone wins. And someone has to pay for this. You are introducing a new cost into the economy. And that cost is worthwhile if you think the smart data is worth it. But the decision should be made by government, not outsourced to regulators or industry."*
>
> **Cross-sector technology expert**

Design preference 2: Governance should allow for flexibility to iterate data sharing mandates over time.

1b. Defining data sharing mandates: Determining the data types industry organisations are required to share when requested by customers.

Participants emphasised the importance of grounding all policy – and especially the development of data sharing mandates – in mission-led use cases that are specific, tangible, and relevant to sectoral challenges. Clear use cases were seen as essential to motivate investment, reduce ambiguity, and establish early momentum. Our market case studies provide a starting point for sector-specific and cross-sector use case examples across the 8 priority sectors.

> *"You need use cases that people can see the value in to get them involved: abstract data sharing won't move the dial."*
>
> **Agrifood stakeholder**

> *"We need a clear idea of the use cases as opposed to thinking 'build it all and they will come.' There were parts of Open Banking that have been about once a year."*
>
> **Finance stakeholder**

At the same time, participants recognised that schemes need to remain flexible: the most impactful innovations often emerge unpredictably as was the case in Open Banking. Governance models should therefore allow for iterative definition of data sharing mandates. To enable this, policymakers will need to remain in close, ongoing dialogue with industry to understand which use cases are emerging and which data types are critical to unlocking them. Participants argued that government should have the authority and the willingness to extend data sharing mandates where needed to enable valuable new services. Equally, there was strong support for a clear review process to remove or retire data sharing obligations that are no longer delivering value, with finance stakeholders noting some requirements within Open Banking mandates are almost entirely unused. Smart Data schemes should therefore avoid accumulating technical debt by ensuring data sharing mandates remain proportionate, purposeful, and aligned to demonstrable user demand.

> *"The things we thought would happen [in Open Banking] at the start didn't, and the things that did happen and added the most value, we didn't see coming."*
>
> **Finance stakeholder**

However, governance models should also provide data holders with sufficient lead time and certainty by taking a systematic, periodic approach to updating data sharing mandates. Stakeholder warned stability in data sharing mandates over time is crucial, citing the cost of adapting systems and governance each time requirements shift.

> *"We can't be in a world where what's required changes every few months - that kills confidence and investment."*
>
> **Finance stakeholder**
>
> *"Regulation shouldn't change as quickly as the market. It should always be retrospective. Otherwise, it is going to throttle that market."*
>
> **Telecoms stakeholder**

Note that, due to limited relevant contributions from participants, the following governance functions were not addressed in this section:

- 1c. Defining data sharing principles: Setting high-level principles which data sharing should comply with.
- 1d. Designing or adapting trust frameworks: Setting out how data is shared, used, and protected by participants in Smart Data schemes, including liability for errors or wrongdoing.
- 1e. Designing or adapting governance models: Deciding the design, composition and remit of formal Smart Data governance entities, including roles and decision-making powers.
- 1f. Aligning with other government policy: Aligning Smart Data schemes with broader digital and data strategies across government.
- 1g. Advising on policy and strategy: Feeding industry and consumer voices into all policy and strategy decisions.

F.2 Standards development

Design preference 3: Technical standards should be developed by expert-led bodies with a mechanism for updates.

2a. Defining and maintaining technical standards: Creating and updating the data and API specifications that underpin how data is shared between parties.

Participants strongly agreed that clear, well-maintained technical standards, particularly for APIs and data formats, are foundational to effective Smart Data schemes. However, there was widespread recognition that government departments and regulators may not have the technical expertise required to develop and update these standards in detail. Instead, interviewees advocated for governance models where technical standards are developed by expert-led bodies that include broad representation but are protected from dominance by any single industry actor. These standards could then be signed off and implemented by regulators.

> *"[Government should] not go too detailed on how, in technical terms, to share data. But just say what we expect data holders to do. We don't have the right expertise to write standards. In Open Banking, having an entity in the middle helped."*
>
> **Regulator**
>
> *"You can't have a situation where incumbents write the rules to suit themselves. It must be independent."*
>
> **Property stakeholder**

There was also consensus that new Smart Data standards should not reinvent the wheel. Instead, they should build on existing standards and infrastructure where available – such as the Smart Energy Code in energy, or the Property Data Trust Framework in housing – to reduce costs and accelerate delivery. Standards should be modular and extensible, allowing for gradual refinement as use cases evolve. Importantly, several stakeholders stressed the need for ongoing maintenance and governance of standards, not just one-off development. Without a sustainable mechanism for version control, issue resolution, and stakeholder input, participants warned that standards would quickly become outdated or contested.

Design preference 4: Data sensitivity classifications should determine security and ATP requirements.

2b. Developing data security classifications: Defining levels of sensitivity for different types of data and adjusting security requirements accordingly.

Participants broadly agreed that not all data is created equal when it comes to sensitivity and security, and that Smart Data governance should reflect this by adopting differentiated standards for data sharing and Authorised Third-party Provider (ATP) accreditation. Several interviewees suggested that certain sectors, particularly finance, should be held to higher security standards than others, citing the potential for financial fraud and the stringent expectations already in place through FCA regulation. However, the majority view was that variation exists *within* sectors as well as *between* them. For example, even within energy or property, certain data types may be relatively low-risk while others – especially when linked or aggregated – can reveal highly sensitive personal information.

> *"You need to know what level of scrutiny a dataset requires before deciding who can access it and how."*
>
> **Telecoms stakeholder**

Given this complexity, many participants called for an expert-led classification framework that could assess and label different types of data according to their sensitivity. This would create a transparent, cross-sector baseline for determining both technical standards (e.g. encryption or

consent requirements) and ATP authorisation levels. Participants stressed that the process for classifying data should be clearly defined, iterative, and responsive to emerging risks, potentially overseen by a cross-sector panel of privacy and cybersecurity experts. It should also consider the risks associated with both 'read only' and 'write' access. Aligning this approach across sectors was also seen as crucial for maintaining consistency and trust, especially as cross-sector data sharing becomes more common.

Design preference 5: Baseline privacy and security standards should be established centrally.

2c. Developing privacy and security standards: Designing the controls, policies and procedures to ensure that data sharing protects user privacy and system security.

While privacy and security standards were not a major focus of debate, participants expressed a preference for a central coordinating body to lead the development of baseline privacy and security standards that apply across all Smart Data schemes, and consider the risks of both 'read only' and 'write' access for ATPs. Sector-specific bodies could then apply and adapt these to reflect the sensitivity of their data and risks specific to their sector if needed. Some participants noted that while not all data requires the same level of protection, consistent approaches to privacy and security help build trust in the system and reduce confusion for users.

Design preference 6: Standards should ensure customer journeys are simple and consistent, in line with mandatory guidelines.

2d. Defining customer experience guidelines: Developing rules for customer data sharing journeys.

Participants consistently emphasised that well-designed customer experience guidelines are important to driving adoption of Smart Data schemes. If requesting and consenting to data sharing is too complex, confusing or time-consuming, users are unlikely to complete the journey, limiting both the scheme's impact and its commercial viability. Several interviewees pointed to examples from Open Banking and international initiatives where data holders created deliberately poor customer experiences (such as multi-step redirects or unclear consent screens) as a way to suppress usage and reduce compliance costs. To prevent such practices, stakeholders advocated for clear and enforceable guidelines based on user-centred digital design principles, and noted that governance frameworks should include appropriate oversight to support simple and consistent Smart Data journeys.

> *"If you don't get the UX right, people just won't use it – and then the whole scheme fails."*
> **Cross-sector technology expert**
>
> *"Standards and APIs are just the start. The customer experience is what will make or break this."*
> **Telecoms stakeholder**

Design preference 7: A core set of common standards with sector-specific extensions should be developed by a central body.

2e. Ensuring cross-sector interoperability of standards: Coordinating standards across sectors to ensure interoperability across industries.

Participants highlighted that cross-sector interoperability of standards is very important to unlocking the full potential of Smart Data. Many noted that different sectors often rely on common data 'touchpoints' (such as names, dates of birth, and addresses) to identify individuals, meaning that misalignment in how this core data is structured or authenticated can create friction and limit the feasibility of cross-sector services. There was strong support for the development of a core set of common technical standards that apply across all Smart Data schemes, with sector-specific extensions where necessary. To manage this, participants advocated for a central coordinating body to be empowered to oversee cross-sector alignment of standards while taking advice from sector-specific experts to ensure the standards remain appropriate and proportionate. To strike

thus balance, a core set of common standards could serve as a shared foundation, building on existing standards wherever possible and allowing for iterative, scheme-specific development. This model would enable schemes to benefit from consistency and economies of scale, while minimising duplication and retaining the flexibility to meet sector-specific needs.

> *"One data standard should work everywhere it's relevant… Cross-sector data sharing only works when the identifiers – like who someone is – are defined the same way in every system."*
>
> **Transport stakeholder**
>
> *"You want consistency where it makes sense, and variation only where it's absolutely necessary."*
>
> **Authorised Third-party Provider**

Design preference 8: Smart Data standards should build on existing sector standards, including those from Open Banking.

Participants widely supported the principle that technical standards for Smart Data schemes should not be developed from scratch where suitable standards already exist. Instead, Smart Data schemes should seek to build on and extend existing sector standards, particularly those developed under Open Banking, which are well-established and widely adopted. In other sectors, participants pointed to industry-led standards bodies and sector codes (such as the Smart Energy Code or Property Data Trust Framework) as valuable foundations. Aligning with these existing standards would reduce duplication, lower compliance costs, and improve early scheme adoption by leveraging systems and data formats already in use.

> *"Open Banking has already done a lot of the heavy lifting on APIs and data schemas: we shouldn't reinvent the wheel when so much of that can be repurposed."*
>
> **Authorised Third-party Provider**
>
> *"We've spent years agreeing a way to format and share this data. If Smart Data just imposes something totally new, it'll lose industry buy-in immediately."*
>
> **Property stakeholder**

F.3 Accreditation of Authorised Third-party Providers (ATPs)

Design preference 9: ATP accreditation should be tiered and have consistent requirements across schemes.

3a. Determining ATP accreditation requirements: Defining the eligibility criteria and conditions Authorised Third-party Providers must meet to be accredited.

Participants agreed that ATP accreditation requirements should include criteria such as regulatory authorisation (e.g. one of the FCA's roles for Open Banking), data security and privacy controls, and evidence of technical competence. Several interviewees noted that accreditation requirements should be proportionate to the sensitivity of the data being accessed, building directly on the data security classifications established elsewhere in governance (see function 2b). This would therefore result in a tiered accreditation process, with more stringent requirements for those ATPs accessing more sensitive data.

> *"We've got to stop duplicating work across authorities – one accreditation or standard should work everywhere it's relevant"*
>
> **Transport stakeholder**

Design preference 10: Shared recognition of ATP accreditation across schemes should be enabled.

3d. Ensuring cross-sector recognition of ATP accreditation: Enabling ATPs accredited under one scheme or sector to be recognised in others without a duplicative process.

Participants largely supported the idea of a centralised ATP accreditation process to enable seamless cross-sector data sharing and reduce administrative burden. A single, unified system, featuring one set of tiered eligibility criteria, one authorised list of approved ATPs, and one accreditation journey, was seen as the most efficient and user-friendly approach. This model would allow accredited ATPs to access data across multiple sectors without undergoing duplicative approval processes and would simplify implementation for data holders, who could use a consistent API call to authenticate accreditation.

> *"Without a shared accreditation process, you'll just create a patchwork: messy, confusing and expensive to scale."*
>
> **Finance stakeholder**

However, a minority of stakeholders argued in favour of sector-specific accreditation processes, particularly where trusted, domain-specific mechanisms are already in place. This most notably includes the Open Banking accreditation process run by the FCA, but may also include existing accreditation processes to access certain data types run by industry bodies (e.g. smart meter data in the energy sector) and other government bodies (e.g. for property data). In this model, each sector would maintain its own authorised list of accredited ATPs, but include a 'passporting' system where sector-specific ATP authorised lists would be linked to allow ATPs approved in one domain to be recognised in others, provided they met the relevant security requirements. There was broad consensus that duplicative accreditation processes should be avoided, with several interviewees proposing letting sectors with the most sensitive data, usually finance, lead on accreditation when an ATP wants access to multiple datasets.

Note that, due to limited relevant contributions from participants, the following governance functions were not addressed in this section:

- 3b. Delivering ATP accreditation process: Running the assessment and onboarding processes that grant or revoke ATP status for third parties.
- 3c. Maintaining an authorised list of ATPs: Keeping an up-to-date public list of accredited third parties that are authorised to access and use Smart Data, that allows data holders and users to confirm ATP credentials.

F.4 Customer protection and engagement

Design preference 11: Redress processes should be coordinated across actors and sectors by a central body.

4a. Handling customer complaints and redress: Managing systems that allow customers to raise concerns and access remedies when issues arise.

Participants agreed that clear, accessible, and trusted customer redress mechanisms are important to maintaining confidence in Smart Data schemes, particularly when something goes wrong. Many interviewees described the current landscape of consumer data complaints as fragmented and difficult to navigate, with overlapping responsibilities between data holders, ATPs, regulators, and ombudsmen. There was widespread support for a more coordinated and transparent redress process for Smart Data schemes, especially as data flows become increasingly cross-sectoral. While few believed a true 'single front door' for data-related complaints was realistic in the near term, many endorsed a model where 'all roads lead to the same destination': ensuring that complaints, regardless of where they are initially raised, are channelled into a common resolution process.

> *"Consumers shouldn't have to navigate a maze of redress options. All roads should lead to the same destination."*
>
> **Property stakeholder**

To achieve this, several participants advocated for a central Smart Data body to play a complaints and redress coordination role. This would include establishing liability models to clarify where responsibility lies in multi-party data sharing chains and bringing in the correct parties to provide redress as needed on a case-by-case basis (e.g. regulators, ombudsmen). The central body could also have powers to revoke or suspend ATP accreditation where serious misconduct is found, ensuring that redress outcomes are meaningful and enforceable. To support joined-up working, stakeholders suggested formal Memoranda of Understanding (MoUs) between the central body, regulators (e.g. FCA, Ofcom, ICO), and ombudsmen to clarify roles and share information. This approach was seen as more feasible than building entirely new redress structures and would allow Smart Data schemes to build on what already exists, while filling gaps in accountability and coordination that currently leave many consumers underserved.

Design preference 12: A centralised, cross-sector consent management solution is preferred.

4c. Defining consent requirements: Ensuring informed customer consent is obtained before data is shared, through either setting clear consent requirements and/or offering shared or standardised customer consent solutions.

Clear and consistent consent processes were seen as important to building consumer trust and enabling adoption of Smart Data services. A widely supported idea was the development of a centralised consent management system, such as a cross-sector consent dashboard, that would streamline how individuals authorise data sharing. This system could be procured centrally and would ensure tokenised consent is captured by ATPs, backed by minimum authentication standards recognised across all participating sectors. Consent tokens could then be passed to data holders as proof of permission, enabling data sharing without requiring repeated checks or duplicative interfaces. To avoid duplication of work, Ofgem's work to create a Consumer Consent Solution for the energy sector[226] was highlighted as a foundation on which a broader cross-sector model could be built. A consistent approach to consent was seen as important not only for security and compliance, but also for delivering coherent user experiences, especially for use cases spanning multiple sectors. It was also noted consent management solutions should consider how often customer consent needs to be reaffirmed for continued data-sharing.

> *"We've learned that consent needs to be clear, not just legally watertight – people need to actually understand what's happening. There's real complexity in making sure it's accessible, not just compliant."*
>
> **Regulator**

Design preference 13: Authentication should be consistent, proportionate, and potentially shared across schemes.

4d. Defining authentication requirements: Ensuring effective processes are in place to confirm the identity of customers providing consent for their data to be shared, through either setting clear authentication requirements and/or offering shared or standardised authentication solutions.

Interviewees emphasised the importance of defining clear, consistent authentication requirements that apply across all sectors, both to simplify the user experience and to support cross-sector data sharing. In particular, there was support for developing or endorsing a shared authentication solution that all schemes could rely on, building upon emerging government digital identity services. Some participants noted that current models, like those used in Open Banking, offer useful technical precedents but would need to be adapted to accommodate a broader range of use cases and risk profiles. Regardless of the technical model adopted, stakeholders agreed that

[226] Ofgem, 2025. Consumer Consent Decision.

authentication should be proportionate to the sensitivity of the data being accessed, aligning closely with the data security classifications established elsewhere in the governance framework.

Note that, due to limited relevant contributions from participants, the following governance functions were not addressed in this section:

- 4b. Promoting customer understanding: Promoting public understanding of Smart Data and encouraging safe and informed participation by consumers.

F.5 Regulatory and compliance

Design preference 14: Compliance monitoring should include light-touch reporting requirements.

5a. Monitoring compliance: Tracking whether organisations fulfil their obligations to comply with data sharing mandates and standards.

Monitoring compliance was seen as a vital function to ensure Smart Data schemes operate fairly and reliably. Several interviewees pointed to the Open Banking model, where an implementation body like OBL tracks compliance and escalates issues to regulators when necessary. Compliance monitoring could include light-touch, automated reporting requirements to flag potential breaches without imposing excessive regulatory burden.

Design preference 15: Enforcement should be led by one regulator in each sector where possible.

5c. Enforcing compliance: Investigating non-compliance and applying enforcement actions such as fines/penalties.

Enforcement of Smart Data rules was seen as essential to maintaining trust, ensuring a level playing field, and deterring misconduct. Interviewees generally favoured having a single, clearly accountable regulator per sector, capable of investigating non-compliance and applying proportionate penalties or sanctions. In mature sectors such as finance, energy, and telecoms, this was seen as straightforward – the FCA, Ofgem and Ofcom were widely accepted as the logical enforcement bodies. However, in other sectors such as property, agrifood, retail, and transport, stakeholders acknowledged that no obvious sector-wide enforcement authority currently exists. Many noted that without clear enforcement, Smart Data schemes risk becoming voluntary in practice, undermining consistency and consumer protections.

> *"Smart Data only works through the use of hard regulatory requirements. We saw little prospect for voluntary efforts. Data holders with legacy systems have no incentive to share data that might drive customers to their competitors."*
>
> **Regulator**
>
> *"Sector-specific regulators... should oversee enforcement but work with an independent governance entity."*
>
> **Finance stakeholder**

Various options were proposed to address this challenge. One was to assign enforcement duties to a cross-sector regulator, such as the ICO, particularly in sectors without a natural lead. Another approach was to take a sector-by-sector route, extending the remit of existing bodies: for example, HM Land Registry in property, the CMA in retail, or the Food Standards Agency in agrifood. A more collaborative model was also suggested, where coalitions of existing regulators jointly enforce Smart Data rules, particularly relevant in complex sectors like property. While a few stakeholders floated the idea of a new, cross-sector Smart Data regulator, most acknowledged that creating new government bodies is politically and financially challenging at present.

Note that, due to limited relevant contributions from participants, the following governance functions were not addressed in this section:

- 5b. Encouraging compliance: Providing guidance and support to help organisations comply with data sharing mandates and standards and issuing pre-enforcement notices where low-level instances of non-compliance are first identified.
- 5d. Managing API conformance certification: Testing and authenticating whether APIs meet the required technical standards before they are deployed in live environments.
- 5e. Oversight of governance bodies: Holding governance bodies to account to ensure they act fairly, transparently and in the public interest.

F.6 Implementation

Design preference 16: Stakeholder forums should represent a wide range of relevant actors, including SMEs, consumer advocates, and representatives from marginalised or underrepresented communities.

6b. Stakeholder engagement and representation: Ensuring Smart Data governance reflects a range of perspectives, including but not limited to consumers, SMEs and industry.

Stakeholder engagement and representation were widely seen as critical to the legitimacy and effectiveness of Smart Data governance. Interviewees across sectors emphasised the need for balanced and inclusive representation, ensuring that governance structures do not become dominated by large incumbents or disproportionately reflect the interests of a single stakeholder group. To avoid this, Smart Data governance should include forums to engage small and medium-sized enterprises (SMEs), consumer advocacy voices, and representatives from marginalised or underrepresented communities. Engagement is not a substitute for representation – rather, it is the most effective route to achieving it. This was seen not only as a fairness issue but also as essential to surfacing a broader range of use cases and risks, ultimately improving the quality of decision-making.

> *"There's definitely a risk that any scheme could be dominated by whoever has the loudest voice. That needs to be managed explicitly. We'd want to see proper consultation – particularly with SMEs – if rules are being updated."*
>
> **Agrifood stakeholder**

Transparent governance processes were also seen as essential to building industry trust. Several participants emphasised that stakeholders should be able to see how decisions are made, who is making them, and on what basis.

> *"If the rules feel like they're coming out of a black box, people will disengage or try to game the system."*
>
> **Cross-sector technology expert**
>
> *"Any rules about data standards or redress - don't write them behind closed doors. Get industry in the room."*
>
> **Property stakeholder**

Note that, due to limited relevant contributions from participants, the following governance functions were not addressed in this section:

- 6a. Developing implementation plans: Setting timelines, milestones and delivery plans for Smart Data rollout in each sector and across sectors.
- 6c. Facilitating knowledge sharing: Ensuring different actors and schemes are learning from one another.
- 6d. Setting up appeals and dispute resolution mechanisms: Providing clear and accessible routes to challenge decisions or resolve disagreements between parties (excluding customers).

- 6e. Managing funding models: Designing and implementing funding models for Smart Data governance bodies, including who pays and how.
- 6f. International engagement: Engaging with international governments and industry groups to align Smart Data schemes with global best practices and support cross-border data sharing.

Appendix G - Mapping the Smart Data stakeholder landscape

This section sets out the key public, private and third-sector actors which are, or could potentially be, involved in the Smart Data ecosystem in each of the eight priority sectors. It does not aim to be fully comprehensive but has supported the identification of relevant actors to take on roles in the governance of Smart Data across the relevant sectors. For each sector, we list relevant actors and initiatives in six categories, each of which relates to different roles in the recommended Model 3 (Federated).

Table 33 - Role of different categories of stakeholders in the recommended Model 3 (Federated)

Category	Role in Model 3 (Federated)
1. Lead government department	Defines Smart Data mandates within their sector; shapes the work of the SDCE via either positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators.
2. Relevant regulators	A lead regulator enforces compliance with Smart Data mandates and standards within their sector; all relevant regulators shape the work of the SDCE via either positions on the Smart Data Council or a separate forum to bring together relevant government departments and regulators.
3. Other relevant government bodies	Support Smart Data schemes through contributions to the Smart Data Council, providing required data, and/or supporting customer redress processes.
4. Relevant industry bodies	Likely to be key candidates for the role of Sector-specific Implementation Entity, driving forward Smart Data delivery within their sector.
5. Industry representatives	Communicate industry needs and preferences through engagement with the Smart Data Council and Sector-specific Implementation Entities.
6. Existing industry data-sharing initiatives	Provide technical foundations and precedents on which Smart Data schemes in the sector can be built.

G.1 Banking and finance

The banking and finance sector is the most advanced in terms of Smart Data readiness, with Open Banking offering a strong regulatory and technical precedent. The Financial Conduct Authority (FCA) plays a clear supervisory role, and key infrastructure such as technical standards and an ATP accreditation system are already in place. While broader Open Finance initiatives (e.g. including pensions, investments, mortgages) have gained some traction, they remain voluntary.

Table 34 - Smart Data stakeholder landscape in banking and finance.

Category	Actors
1. Lead government department	**HM Treasury** – Leads on financial services policy and holds strategic oversight of data-sharing initiatives like Open Banking and Open Finance.
2. Relevant regulators	**Financial Conduct Authority (FCA) (Lead regulator)** – Regulates financial conduct, authorises Smart Data participants, and oversees compliance in both retail and investment services. **Competition and Markets Authority (CMA)** – Initiated Open Banking through its Order and continues to monitor competition across financial markets. **The Pensions Regulator (TPR)** – Regulates workplace pension schemes and works alongside the FCA to oversee the pensions ecosystem

	Payment Systems Regulator (PSR) – Oversees payment systems that underpin API-based data-sharing infrastructure. **Prudential Regulation Authority (PRA)** – Ensures the safety and soundness of financial institutions such as banks and insurers.
3. Other relevant government bodies	**Money and Pensions Service (MaPS)** – Coordinates the Pensions Dashboards Programme and provides public guidance on pensions and financial wellbeing. **Bank of England** – Supports financial stability and innovation across the broader financial system. **Financial Ombudsman Service (FOS)** – Provides independent dispute resolution for consumers and small businesses who have complaints about financial services.
4. Relevant industry bodies	**Open Banking Limited (OBL)** – Current implementation body for Open Banking which is transitioning to an Open Banking Future Entity. **TISA (The Investing and Saving Alliance)** – Drives standards and policy for digital identity, open finance, and financial wellbeing. **Centre for Finance, Innovation and Technology (CFIT)** – Public-private partnership convening stakeholders to drive innovation and cross-sector collaboration. **Open Finance Association (OFA)** – Represents fintechs and third-party providers developing Open Finance services.
5. Industry representatives	**UK Finance** – Represents a wide range of banking and finance institutions, engaging on policy, regulation, and technical standards. **Innovate Finance** – Advocates for fintech and regtech firms, supporting innovation-friendly policy development.
6. Existing industry data-sharing initiatives	**Open Banking** – A mandated scheme requiring banks to share current account and payments data with Authorised Third-party Providers via secure APIs. **Open Finance** – A voluntary extension of Open Banking aiming to include a broader set of financial products such as pensions, insurance, and investments, with the FCA running an Open Finance Sprint in May 2025. **Pensions Dashboards Programme (PDP)** – A national initiative led by MaPS to enable consumers to view all their pension entitlements in one place through a standardised digital interface.

G.2 Retail energy

Retail energy has already adopted some foundational Smart Data elements, such as the mandated rollout of smart meters and the development of the upcoming Smart Meter Data Repository. Ofgem regulates across the sector and is developing a consumer consent solution, while industry bodies like Smart DCC, Electralink and Elexon manage data infrastructure.

Table 35 - Smart Data stakeholder landscape in retail energy.

Category	Actors
1. Lead government department	**Department for Energy Security and Net Zero (DESNZ)** – Leads policy for energy digitalisation, including the development of a sector-specific Smart Data scheme.
2. Relevant regulators	**Ofgem (Lead regulator) –** The principal energy regulator, responsible for licensing, market oversight, consumer protection, and data best practice. Currently developing a consumer consent platform which could support Smart Data schemes.

3. Other relevant government bodies	**Energy Ombudsman** – Provides consumer redress services for complaints related to energy services and disputes.
4. Relevant industry bodies	**Smart DCC** – Operates the national smart metering communications infrastructure and accredits 'Other Users' under the Smart Energy Code (SEC). Plays a central role in data access and privacy compliance. **Elexon** – Manages electricity market settlement services. A potential future host of the Smart Meter Data Repository to support more centralised and efficient data access. **ElectraLink** – Operates the Data Transfer Service (DTS), which enables data exchange between UK electricity market participants. **Smart Energy Code Company (SECCo)** – Oversees the Smart Energy Code (SEC), the primary governance instrument for smart meter data access and security. **Retail Energy Code Company (RECCo)** – Manages the Retail Energy Code (REC), which governs key customer-facing processes including switching and data access.
5. Industry representatives	**Energy UK** – Represents suppliers, generators and stakeholders across the energy industry, providing a key voice in regulatory and Smart Data policy discussions. **Energy Networks Association (ENA)** – Represents electricity and gas network operators, and supports the development of industry-wide data standards and infrastructure.
6. Existing industry data-sharing initiatives	**DESNZ Call for Evidence on Energy Smart Data** – A government-led consultation seeking views on the potential scope, benefits, and implementation challenges of a Smart Data scheme in the energy sector, launched in January 2025. **Smart Metering Implementation Programme** – National rollout of smart meters with associated data infrastructure and regulatory oversight. **Smart Meter Data Repository (proposed)** – A DESNZ-backed initiative to centralise smart meter data and provide API-based access for Authorised Third-party Providers. **Ofgem's Consumer Consent Solution** – A platform in development to allow consumers to manage, grant, and revoke permissions for smart meter data access through a single, centralised interface. **Data Sharing Infrastructure project (DSI)** – An Ofgem-led project focusing on facilitating a secure, trusted, and efficient exchange of data between different systems, organisations, or entities within the energy sector, built using the Digital Twin technology developed by DBT. **Open Energy (Icebreaker One)** – A trust framework promoting consistent and secure data-sharing practices across the energy system, particularly for non-incumbent market participants.

G.3 Telecommunications

The telecommunications sector has introduced a limited number of data-sharing interventions, including the One Touch Switch initiative managed by TOTSCo. Ofcom acts as the primary regulator.

Table 36 Smart Data stakeholder landscape in telecommunications.

Category	Actors
1. Lead government department	**Department for Science, Innovation and Technology (DSIT)** – Holds responsibility for digital and telecoms policy, which may include the development of a sector-specific Smart Data scheme.

2. Relevant regulators	**Ofcom (Lead regulator)** – The primary telecoms regulator, responsible for market conduct, consumer protection, switching processes, and pricing. Oversees compliance for schemes such as One Touch Switch and end-of-contract notifications.
3. Other relevant government bodies	**Communications Ombudsman** – Provides dispute resolution and redress for consumers experiencing issues with telecoms services.
4. Relevant industry bodies	**TOTSCo** – Industry-led implementation entity managing One Touch Switch (OTS); provides a model for future industry-governed infrastructure.
5. Industry representatives	**ISPA (Internet Services Providers' Association)** – Represents UK internet service providers and advocates on issues such as broadband policy, cybersecurity, and digital infrastructure. **UKCTA (UK Competitive Telecommunications Association)** – Represents alternative telecoms providers and promotes competition in the communications sector. **Federation of Communication Services (FCS)** – Represents smaller providers and resellers across the telecoms industry.
6. Existing industry data-sharing initiatives	**One Touch Switch (OTS)** – Mandated system allowing customers to switch providers easily without contacting their current provider. Developed and operated by TOTSCo under Ofcom's oversight. **Ofcom's Open Data portal** – Ofcom maintains an Open Data portal that provides publicly accessible datasets related to the UK communications sector. These datasets include information on broadband coverage, mobile signal strength, telecoms infrastructure, and market performance metrics.

G.4 Property

The property sector presents one of the most fragmented and complex landscapes for Smart Data, with no single regulator overseeing the end-to-end homebuying and selling process. Data is dispersed across local authorities, HM Land Registry, and private property services, with varying levels of digital maturity and standardisation. Some current initiatives (e.g. the Local Land Charges Programme and Property Data Trust Framework) are aiming to improve consistency of data.

Table 37 - Smart Data stakeholder landscape in property.

Category	Actors
1. Lead government department	**Ministry of Housing, Communities and Local Government (MHCLG)** – The lead department for the homebuying and selling sector, with responsibility for housing policy and local government oversight.
2. Relevant regulators	**HM Land Registry (HMLR) (Lead regulator)** – While currently only holding a quasi-regulatory role, HMLR is central to property data infrastructure, responsible for maintaining the land register and involved in ongoing digitisation initiatives such as the Local Land Charges Programme.

	Council for Licensed Conveyancers (CLC) – Oversees licensed conveyancers, ensuring regulatory compliance. **The Law Society** – Sets quality standards for solicitors involved in conveyancing (e.g. Conveyancing Quality Scheme). **Solicitors Regulation Authority (SRA)** – Regulates solicitors in England and Wales. **Chartered Institute of Legal Executives (CILEx)** – Professional body and regulator for legal executives, many of whom operate in conveyancing. **National Trading Standards Estate Agency Team (NTSEAT)** – Oversees compliance of estate agents with consumer protection laws. **Royal Institute of Chartered Surveyors (RICS)** – Regulates surveyors and sets standards for property valuations and surveys. **Property Codes Compliance Board (PCCB)** – Provides oversight for property search providers, ensuring compliance with data quality and transparency standards. **Financial Conduct Authority (FCA)** – Regulates mortgage brokers and lenders.
3. Other relevant government bodies	**Local Authorities** – Hold and manage essential property data (e.g. local land charges, search data), with wide variation in digital maturity and access formats.
4. Relevant industry bodies	**Open Property Data Association (OPDA)** – Advocates for property data standardisation, bringing together stakeholder from across the property ecosystem. **Digital Property Market Steering Group** – A cross-sector forum convened by the UK government aiming to improve data sharing and interoperability across the digital property market. **Home Buying and Selling Council (HBSC)** – Coalition of industry stakeholders aiming to improve the home buying process.
5. Industry representatives	**Propertymark** – A professional body representing estate and letting agents. **The Conveyancing Association** – A professional body representing specialist conveyancers. **The Society of Licensed Conveyancers (SLC)** - A professional body representing licensed conveyancers. **Council of Property Search Organisations (CoPSO)** – A professional body representing property search firms. **UK Finance** – A professional body representing mortgage providers. **HomeOwners Alliance** – A consumer advocacy group that represents and supports homeowners and aspiring homeowners.
6. Existing industry data-sharing initiatives	**Property Data Trust Framework (PDTF)** – An initiative led by the Open Property Data Association to define and promote technical standards for property data sharing. **Local Land Charges Programme** – Led by HMLR, aimed at digitising and centralising LLC data previously held by local authorities.

G.5 Transport

Smart Data implementation in transport faces unique governance challenges due to its fragmented structure, variation by transport mode (e.g. rail, road, aviation, maritime), and overlapping public and private responsibilities. Unlike other sectors, there is no single regulator or implementation body currently well-placed to lead a Smart Data scheme.

Table 38 - Smart Data stakeholder landscape in property.

Category	Actors
1. Lead government department	**Department for Transport (DfT)** – The lead department for transport policy in the UK, including oversight of major data-sharing initiatives (e.g. Bus Open Data Service).
2. Relevant regulators	**Office of Rail and Road (ORR) (Lead regulator)** – Economic and safety regulator for rail and strategic roads; could play a regulatory role in some modal areas but lacks cross-sector reach. **Civil Aviation Authority (CAA)** – Regulates UK aviation, including economic regulation and consumer protection. **Maritime and Coastguard Agency (MCA)** – Regulates safety and environmental performance in shipping. **Office of the Traffic Commissioner (OTC)** – An independent regulator responsible for licensing and regulating operators of heavy goods vehicles (HGVs), buses, and coaches. **Driver and Vehicle Standards Agency (DVSA) –** Enforces vehicle and driver standards across Great Britain, overseeing driving tests, vehicle safety, and compliance for commercial transport.
3. Other relevant government bodies	**Local Authorities** – Key players in managing regional data-sharing schemes, such as integrated ticketing and mobility-as-a-service initiatives. **Network Rail** – Manages rail infrastructure and plays a role in data-sharing through initiatives like the Rail Data Marketplace. **Highways England / National Highways** – Holds road transport data and infrastructure information. **Transport for London (TfL) –** A government body responsible for managing and developing transport services across London, often consulted on national transport policy due to its scale and innovation. **Driver and Vehicle Licensing Agency (DVLA)** – Maintains the registration and licensing of drivers and vehicles in Great Britain, managing key data used across the transport sector.
4. Relevant industry bodies	**Open Transport Initiative** – Industry-led initiative advocating for open standards and Smart Data across all transport modes. **ITSO** – Oversees the national standard for smart ticketing in the UK; plays a governance role in technical standards, certification, and security modules **Real Time Information Group (RTIG)** – Supports data standards and real-time passenger information, especially in bus transport. **Transport Technology Forum (TTF**) – Brings together government, local authorities, and the transport technology industry to promote innovation and data-sharing in intelligent transport systems.
5. Industry representatives	**Rail Delivery Group (RDG)** – Represents train operating companies, Network Rail, and freight operators, working to coordinate and improve the UK rail industry. **Confederation of Passenger Transport (CPT)** – The trade association for the bus and coach industry, advocating for operators and shaping public transport policy. **Logistics UK** – One of the UK's largest trade bodies representing freight transport interests across road, rail, sea, and air, including haulage, warehousing, and supply chain.

	Airlines UK – The trade body for UK-registered airlines, representing their interests to government, regulators, and other stakeholders on aviation policy and regulation. **Road Haulage Association (RHA)** – Represents commercial road haulage operators, providing lobbying, training, and advisory services to improve road freight operations.
6. Existing industry data-sharing initiatives	**Bus Open Data Service (BODS)** – Mandated open data platform for timetables, fares, and vehicle locations; funded and overseen by DfT. **Rail Data Marketplace** – A closed-loop system enabling structured rail data sharing between train operators and third parties. **ITSO smart ticketing standard** – National framework used for concessionary travel and integrated transport solutions. **Mobility-as-a-Service (MaaS) pilots** – Local and regional experiments integrating transport services and payments, e.g. in Manchester and the West Midlands. **Open Transport account-sharing standard** – Developed by the Open Transport Initiative to enable third-party services to access customer transport data.

G.6 Retail

The retail sector presents a unique challenge for Smart Data governance due to its lack of a dedicated regulator, high concentration of market power among large retailers, and the commercial sensitivity of consumer data. While the sector has strong foundations in industry-led standards (e.g. GS1), there is limited precedent for regulated data-sharing schemes.

Table 39 - Smart Data stakeholder landscape in retail.

Category	Actors
1. Lead government department	**Department for Business and Trade (DBT)** – The lead department responsible for supporting the growth, competitiveness, and innovation of the UK retail sector, including leading on retail strategy, improving business regulation, fostering digital transformation.
2. Relevant regulators	**Competition and Markets Authority (CMA) (Lead regulator)** – Promotes competition and protects consumers by investigating anti-competitive practices, enforcing consumer rights, and advising on market regulation, including in digital and retail sectors. **Office for Product Safety and Standards (OPSS)** – Responsible for ensuring the safety and compliance of consumer products in the UK, supporting businesses and protecting consumers through regulation and enforcement. **Food Standards Agency (FSA)** – Protects public health by regulating food safety and hygiene across the food supply chain in England, Wales, and Northern Ireland.
3. Other relevant government bodies	**RetailADR** – Ombudsman service offering dispute resolution for retail customers.
4. Relevant industry bodies	**GS1 UK** – Global standards organisation providing product barcoding and interoperability frameworks used across retail. Advocates for voluntary adoption of open, non-proprietary standards and plays a convening role across manufacturers, retailers, and tech platforms **Institute of Grocery Distribution (IGD)** – Provides insight and support for grocery retailers and may play a convening or advisory role in food-related Smart Data schemes.

5. Industry representatives	**British Retail Consortium (BRC)** – Represents large and mid-sized UK retailers on public policy and operational issues. **British Independent Retailers Association (BIRA)** represents thousands of independent retailers across the UK, advocating for their interests on policy, digital innovation, and fair access to data and technology in the retail sector.
6. Existing industry data-sharing initiatives	**GS1 Next Generation Barcoding** – Introduction of QR-enabled barcodes offering expanded product-level data access. **Digital Deposit Return Schemes (DDRS)** – A separate, regulated initiative which has highlighted the need for standardised data formats, legal clarity, and anti-fraud measures, offering governance lessons for Smart Data. **Retail loyalty programmes (e.g. Clubcard, Nectar)** – Proprietary data ecosystems not currently shared between providers, but highly relevant due to consumer-level data insights and value. **University of Leeds Retail Data Environment** – Secure research data sharing model used by some major food retailers; noted for strong safeguards and practical governance mechanisms.

G.7 Agrifood

The agrifood sector spans a highly complex and fragmented landscape, from primary production through to food processing, manufacturing, and retail. It is marked by a high number of small businesses, diversity of sub-sectors, low margins, and substantial data asymmetries across the supply chain. Smart Data governance in this sector must address significant trust gaps and accommodate a wide range of digital maturity levels. Unlike some other sectors, there is no clear regulatory home for Smart Data.

Table 40 - Smart Data stakeholder landscape in agrifood.

Category	Actors
1. Lead government department	**Department for Environment, Food and Rural Affairs (Defra)** – The lead policy department for agriculture and food systems, including oversight of the Food Data Transparency Partnership (FDTP), GHG data standards, and food system governance strategy.
2. Relevant regulators	**Food Standards Agency (FSA) (Lead regulator)** – Regulates food safety and is involved in data transparency and traceability efforts. **Office for Product Safety and Standards (OPSS)** – Oversees product standards including food labelling. **Environment Agency (EA)** – Regulates environmental impacts from food and agriculture, including pollution, waste, and land use data. **Groceries Code Adjudicator (GCA)** – Ensures fair treatment of suppliers by large retailers; suggested as a potential redress body or compliance overseer
3. Other relevant government bodies	**Agriculture and Horticulture Development Board (AHDB)** – Public body funded by farmer levies; involved in carbon data tool pilots.
4. Relevant industry bodies	**Institute of Grocery Distribution (IGD)** – Delivers industry-led research and facilitates data partnerships between manufacturers and retailers; possible convener role.

	Waste & Resources Action Programme (WRAP) – NGO funded by Defra, involved in food systems decarbonisation and data standardisation (e.g. Scope 3 emissions, interoperability standards).
5. Industry representatives	**British Retail Consortium (BRC)** – Represents large food retailers; influential in shaping supply chain data expectations. **National Farmers Union (NFU)** – Represents farmers and landowners; crucial stakeholder for buy-in and data reciprocity discussions. **Food and Drink Federation (FDF)** - Represents UK food and drink manufacturers, working on issues such as regulation, innovation, exports, and supply chain resilience.
6. Existing industry data-sharing initiatives	**Food Data Transparency Partnership (FDTP)** – A Defra-led collaboration aiming to standardise environmental impact and nutrition data. **AHDB's Farm Carbon Calculator and data exchange pilots** – Early-stage platforms offering farm-level data sharing tools. **WRAP–Oxford University interoperability standards** – Define Scope 3 GHG data reporting formats, providing a potential foundation for wider technical standards.

Appendix H – Further evaluation of Smart Data governance models

In addition to the two main (qualitative and quantitative) components of our evaluation of governance models, two supplementary exercises were undertaken to strengthen our assessment and test the robustness of our results:

(1) **Further quantitative analysis** of the governance models, including a concordance and divergence review and the application of different weighting scenarios.

(2) **Indicative costings** of the governance models, drawing on the experiences of Open Banking and efficiency discount factors.

The remainder of this section outlines the results and learnings of these exercises in further detail.

H.1 Further quantitative analysis

Synthetic sector representatives were used to support the scoring of the shortlisted governance models against the critical success criteria for Smart Data governance (see Section 7.2). This section explains what these synthetic sector representatives are, how they were constructed, and also outlines additional quantitative analysis undertaken as part of the evaluation process.

Explanation box 5: What are synthetic sector representatives?

Synthetic sector representatives are AI-generated stakeholder profiles created using transcripts from Phase 2 interviews. For each sector, we developed a single representative using an advanced Large Language Model that captured the views, concerns, and priorities expressed by real participants. For example, using insights from 14 property sector stakeholders, we developed 'PropertyRep': a composite voice designed to reflect the perspectives of the property sector as a whole.

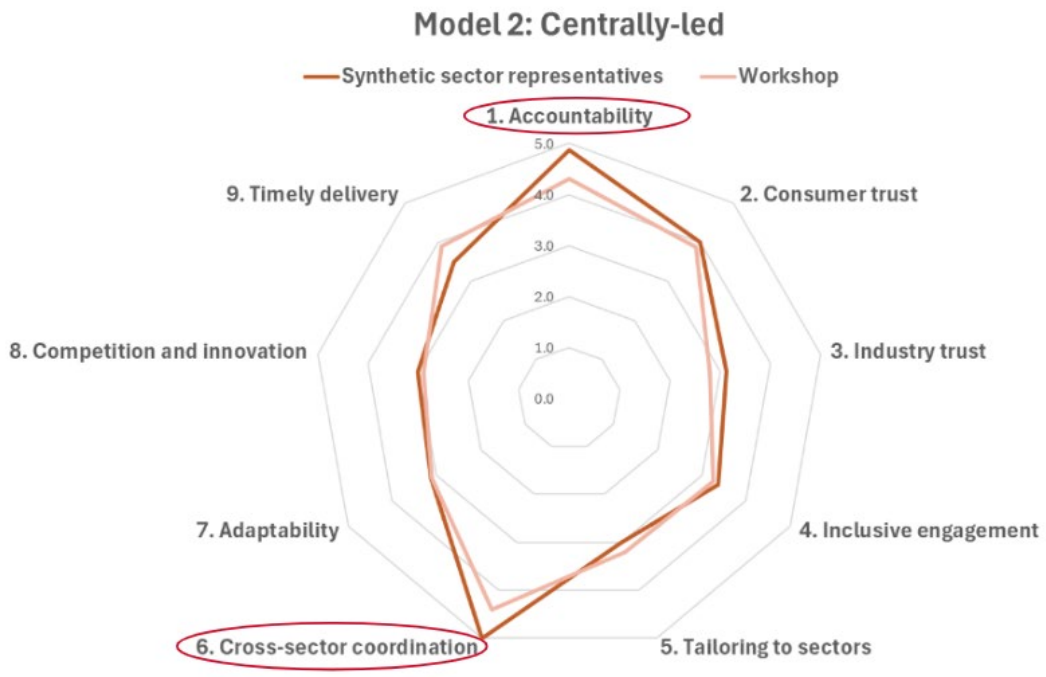
These synthetic actors were used to score the governance models against the critical success factors. This approach avoided the introduction of researcher bias by ensuring each representative drew solely on the views expressed during interviews and focus groups, ensuring that model assessments remained grounded in the evidence gathered during research. However, recognising the potential of Large Language Models to hallucinate, the research team quality assured the scoring of the synthetic sector representatives, triangulating them against our qualitative findings and the scores provided by workshop attendees.

We conducted a concordance and divergence analysis to test the robustness of the quantitative scoring exercise. Where scores from the synthetic sector representatives and the workshop were within 0.5 points of each other for a given criterion, we considered the result concordant and therefore reliable. Where the difference in scores was greater than 0.5, this flagged areas of divergence between the two groups. The purpose of this analysis was not to resolve areas of divergence, but to understand why they occurred. Where significant differences were identified, we revisited qualitative evidence to check whether the differences reflected genuine disagreement or simply varying perspectives. This helped ensure confidence that averaging the two groups' scores was a robust and appropriate approach to scoring.

H.1.1 Model 2: Centrally-led

The Centrally-led model's scoring diverged between sector representatives and workshop participants on 2 criteria: accountability and cross-sector coordination. The radar chart in figure 6 provides a visual comparison of scoring between the two stakeholder groups across ten critical success factors. The red, circled critical success factors indicate where divergence occurred.

Figure 6 - Radar chart of convergence and divergence for Model 2 (Centrally-led).



Average score (synthetic sector reps): 3.6

Average score (workshop): 3.5

Average score (both groups): 3.6

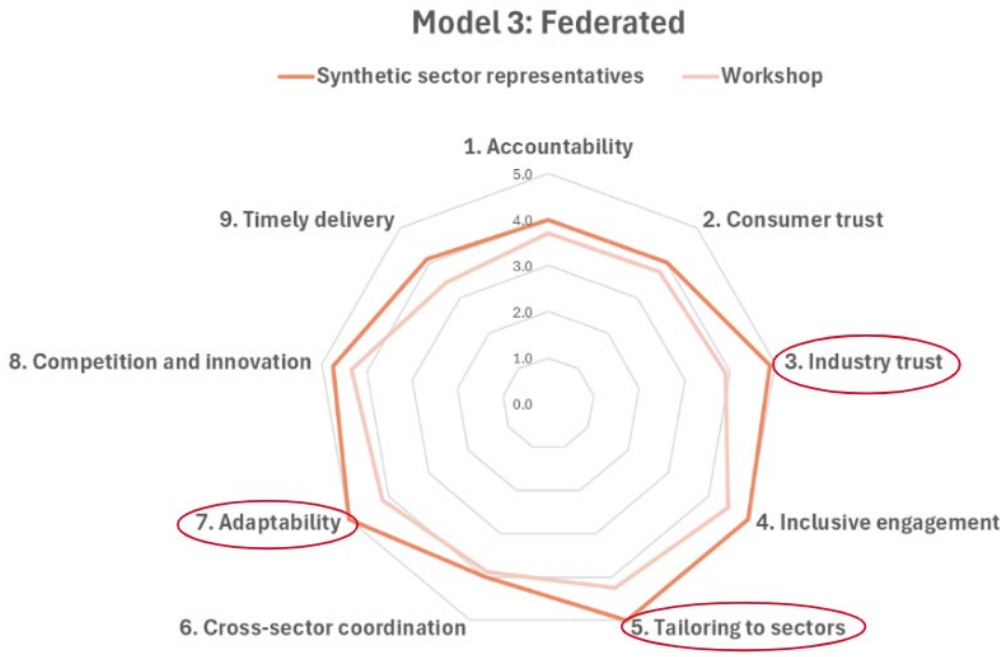
Divergence between the two groups in scoring of Model 2 likely reflects a split in preferences for an 'ideal vs. practical' model. The synthetic sector representatives, which are weighted in favour of industry stakeholders, tend to consider a central Smart Data Implementation Entity as an attractive solution to challenges around cross-sector consistency. More generous scoring here likely reflects a desire for clarity, simplicity, and guaranteed compliance through an umbrella body – particularly in sectors where data sharing is currently voluntary or inconsistent.

Workshop attendees, largely from UK government bodies, appear to score this model with more of an eye toward practical constraints. They are likely more attuned to the realities of how difficult it is to stand up a new government entity with extensive powers and responsibilities. From that perspective, 'accountability' and 'cross-sector coordination' may be more difficult to achieve. Hence, their lower scores may reflect not a rejection of the model's intent, but a more grounded sense of delivery risk.

H.1.2 Model 3: Federated

The Federated model's scoring diverged between sector representatives and workshop participants on 3 criteria: industry trust, tailoring to sectors and adaptability. The radar chart in figure 7 provides a visual comparison of scoring between the two stakeholder groups across ten critical success factors. The red, circled critical success factors indicate where divergence occurred.

Figure 7 – Radar chart of convergence and divergence for Model 3 (Federated).



Average score (synthetic sector reps): 4.4

Average score (workshop): 3.9

Average score (both groups): 4.2

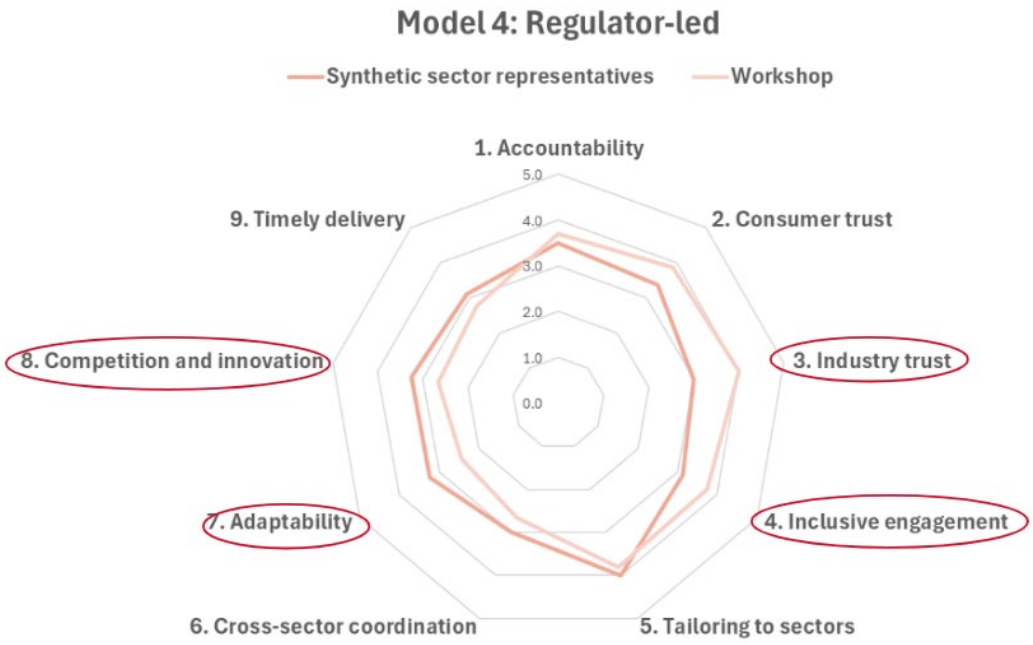
For Model 3, higher scores from synthetic sector representatives are seen across the board. In particular, the synthetic sector representatives seem to trust that Sector-specific Implementation Entities, if given the right remit and accountability, will be best placed to reflect on-the-ground conditions, earning industry trust, tailoring schemes appropriately to each sector, and effectively adapting to change.

Government workshop participants appear more cautious by contrast, consistently scoring this model lower than the synthetic sector representatives. Their lower scores on these criteria suggest concerns about inconsistency, and the risk of slow or partial uptake when sector tailoring is considered. They may worry that, while some sectors (e.g. finance or energy) have well-established governance bodies, others may struggle to unite around a representative delivery actor.

H.1.3 Model 4: Regulator-led

The Regulator-led model's scoring diverged between sector representatives and workshop participants on 4 criteria: industry trust, inclusive engagement, adaptability and competition and innovation. The radar chart in figure 8 provides a visual comparison of scoring between the two stakeholder groups across ten critical success factors. The red, circled critical success factors indicate where divergence occurred.

Figure 8 – Radar chart of convergence and divergence for Model 4 (Regulator-led).



Average score (sector reps): 3.3

Average score (workshop): 3.3

Average score (both groups): 3.3

This model shows the broadest divergence. The scores from synthetic sector representatives are notably lower on industry trust and inclusive engagement. This reflects how industry stakeholders are less likely than government stakeholders to think regulators can deliver optimum outcomes for industry. Meanwhile, perhaps surprisingly, synthetic sector representatives scored this model more generously than government workshop participants for adaptability and competition and innovation. This perhaps reflects how government stakeholders are more acutely aware of the constraints regulators face, including narrow statutory remits.

This process builds confidence in the credibility of the scoring system and allowed us to take an average of scores from the two sources to form a final value. To further test the robustness of the evaluation, we applied different weightings to the critical success factors based on DBT's priorities as set out in earlier stages of the project, and stakeholder design preferences. A comparison of the weighted scenarios with one another and with the original unweighted baseline revealed that the rankings of the models remained unchanged across all scenarios: Model 3 (Federated) consistently ranked the highest, followed by Model 2 (Centrally-led), then Model 4 (Regulator-led).

This scoring pattern is reflective across the full quantitative assessment: Model 3 (Federated) scored the highest across the ten critical success criteria used for analysis with an average of 4.2 points out of 5, followed by Model 2 (Centrally-led) at 3.6 points, with Model 4 (Regulator-led) performing the least well at 3.3 points out of 5. Model 3 was particularly strong on criteria related to flexibility, deliverability, and sector-specific tailoring, reflecting its ability to accommodate differing levels of sector readiness. Model 2 scored highest on accountability and cross-sector coordination, showing its strengths in promoting clear, consistent oversight. Model 4 performed less well overall across most criteria, with especially low scores on cross-sector adaptability, innovation and implementation, perhaps largely due to concerns about regulator capacity and a lack of clear ownership in sectors without a strong existing regulator.

The consistency of this ranking being held true under all weighting scenarios suggests that the final recommendation is not overly dependent on any single set of assumptions about what constitutes success but instead reflects a model that performs strongly across a range of policy priorities and stakeholder preferences.

H.2 Indicative costings

Estimating the costs associated with different governance models for Smart Data schemes is a necessarily imprecise exercise. A wide range of uncertainties mean that cost estimates presented in this section should be treated as indicative rather than definitive. These are not forecasts or budgets, but rather structured approximations designed to support comparative analysis between models. Their main purpose is to surface potential cost drivers and relative differences between governance options, rather than deliver exact figures.

International evidence provides limited guidance for this task. No country has yet implemented Smart Data schemes across a range of sectors at a national scale, and there is no empirical data available on the comparative costs or savings of centralising governance functions. This makes it difficult to draw robust conclusions about the economies of scale or efficiencies that might be achieved by reducing duplication through a central implementation entity.

Three main sources of evidence have therefore been used to inform the following cost assumptions. Firstly, qualitative input from research participants revealed mixed views: some believed centralisation would reduce costs by avoiding duplication (e.g. in delivering ATP accreditation or authentication), while others thought the savings would be negligible or even negative, as costs may simply be shifted around or amplified by the overhead of a new central entity. Secondly, cost data from Open Banking Limited (OBL) has been used as a benchmark for understanding both set-up and ongoing costs for Smart Data implementation entities. Third, the broader literature on shared services in the private and public sector - though itself inconclusive – has informed assumptions around efficiency discount rates where governance functions are centralised.

Costs have been modelled on the following basis:

1. **Cost estimates include solely the costs of implementation bodies**, whether central or sector-specific. We exclude costs associated with the roles of government departments or regulators on the basis that these would not differ significantly across models.
2. **Cost estimates assume schemes in all eight priority sectors are launched in Year 1.** Although we know this will not be the case, without clarity on which Smart Data schemes will be progressing when, this approach provides the most straightforward way of comparing costs cross models.
3. **Cost estimates are built using the experience of Open Banking Limited** as a reference point, broken down into set-up and ongoing costs. These are then scaled across the seven remaining priority sectors considered in this report and allocated according to the structure of each governance model.
4. **Efficiency discounts are applied** when central implementation bodies are assumed to carry out functions across multiple sectors, reflecting potential economies of scale. Given the significant uncertainties here, a range has been used to reflect the potential efficiencies expected.

Explanation box 6: Establishing efficiency discount assumptions

In modelling the cost impacts of centralising governance functions within Smart Data schemes, an efficiency discount of 10% has been applied to reflect the potential for reduced duplication and streamlined operations. This is accompanied by a sensitivity range of 0–20%, recognising

the considerable uncertainty in the literature as to whether centralisation reliably delivers cost savings in practice.

Evidence from UK local government shared service initiatives highlights this variability. A study by the Local Government Association found cost savings of only 5% in some cases, with a high of 20% in more mature partnerships, though these outcomes were context-dependent and not universally replicable.[227] Similarly, PwC reports savings of 20–30% from shared services in private sector organisations, but these results were largely based on offshoring centralised services to lower-cost countries: a strategy not applicable to UK Smart Data governance functions.[228]

The literature also cautions against assuming efficiency gains. Research from the University of Oxford outlines five risks that can prevent shared services from delivering cost savings, including complexity, loss of flexibility, and failure to realise synergies.[229] This aligns with findings from the National Audit Office, which observed that while the UK Government's Shared Services Strategy aimed for 10–15% savings, actual savings had not been demonstrated and implementation was fraught with delivery challenges.[230]

Given these mixed findings, the base-case assumption of a 10% efficiency discount strikes a balance between optimism and realism. The upper bound of 20% reflects best-case outcomes from comparable UK public sector initiatives, while the lower bound of 0% acknowledges that centralisation could yield no efficiency benefits, especially if coordination costs or structural complexity outweigh potential savings.

The results of this analysis provide estimated costs for the three models across a 2-year, 5-year and 10-year horizon, as outlined in Table 39. Please note that: (a) these costs are presented cumulative rather than annual basis, (b) for each model both a ‘best estimate’ and a range of likely costs is provided, and (c) all costs have been rounded to the nearest £5m to avoid spurious accuracy.

Table 41 - Indicative costs for the three shortlisted Smart Data governance models.

	Total cost (Y1-2)	Total cost (Y1-5)	Total cost (Y1-10)
Model 2: Centrally-led	£280m (£255m - £310m)	£735m (£660m - 810m)	£1,390m (£1,240m - £1,540m)
Model 3: Federated	£275m (£260m - £290m)	£740m (£690m - £790m)	£1,420 (£1,325m - £1,520m)
Model 4: Regulator-led	£270m (£260m - £280m)	£745 (£710m - £775m)	£1,440 (1,380m - 1,505m)

The cost estimates across the three shortlisted governance models suggest only marginal differences in total expenditure over the 2-, 5-, and 10-year horizons. Across each time period, the ranges of estimated costs for all models substantially overlap. For example, while Model 2 is estimated to cost £1,390m over 10 years, Model 3 and Model 4 come in slightly higher at £1,420m

[227] Local Government Association, 2016. Services shared: costs spared? An analysis of the financial and non-financial benefits of local authority shared services.
[228] PwC, 2016. Shared services: Multiplying success.
[229] University of Oxford, 2016. Five risks to cost saving from sharing services.
[230] National Audit Office, 2022. Government shared services.

and £1,440m respectively – yet all within broadly similar confidence intervals. As a result, cost has been assigned a consistent "medium" score in the evaluation of options for all models. This reinforces feedback from research participants who noted that the governance models have greater impact on how costs are distributed between organisations than how much is ultimately spent. Cost is therefore unlikely to be a key basis on which to choose a preferred governance model from the shortlisted option.

A slight pattern does emerge showing that Model 2, the centrally-led approach, appears somewhat more expensive during the initial set-up phase (Years 1–2). Its £280m projected cost exceeds that of Model 3 (£275m) and Model 4 (£270m), reflecting the additional resources needed to establish a new large, centralised implementation body within government. By contrast, the other two models benefit from leveraging existing institutions, either industry bodies (Model 3) or regulators (Model 4), which reduces start-up organisational costs. However, Model 2's more centralised structure enables the consolidation of governance functions, reducing duplication across sectors and allowing for more streamlined operations over time. This results in marginally lower ongoing costs compared to the other models, with Model 2 ultimately emerging as the least costly option over the full 10-year horizon, albeit by a small margin.

It should also be noted that there is a greater degree of uncertainty in the cost estimates for Model 2, as shown by the wider range of its cost projections. This stems from uncertainty around how effective centralisation might be in reducing duplication and delivering efficiency gains. With more functions consolidated under fewer entities, there is a larger scope for potential savings, but also a higher risk of cost escalation if integration proves complex or slow. This variability is less pronounced in the more distributed governance approaches, where roles are clearer and tied to pre-existing organisations with established cost structures.

In summary, **while cost differences between the models exist, they are not substantial enough to serve as a decisive factor in model selection**. Instead, cost should be understood as a reflection of structural choices – who pays and who delivers – rather than a measure of overall affordability or value.

Legal disclaimer

While every effort has been made to ensure that the information in this document is accurate, the Department for Business and Trade does not accept liability for any errors, omissions or misleading statements.

Copyright

© Crown Copyright 2026

You may re-use this publication (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence visit:

www.nationalarchives.gov.uk/doc/open-government-licence or email: psi@nationalarchives.gov.uk.

Where we have identified any third-party copyright information in the material that you wish to use, you will need to obtain permission from the copyright holder(s) concerned.

This document is also available on our website at gov.uk/government/organisations/department-for-business-and-trade

Any enquiries regarding this publication should be sent to us at

enquiries@businessandtrade.gov.uk.