



Department for
Business & Trade

Smart Data Implementation Guide

July 2023



Department for
Business & Trade

A joint project between the Centre for Data Ethics and Innovation (CDEI) and Department for Business, Energy, and Industrial Strategy (BEIS)

The Centre for Data Ethics and Innovation (CDEI) worked with the Smart Data team in the Department for Business, Energy, and Industrial Strategy (BEIS) to identify the features of ethical and trustworthy Smart Data schemes. The aim of this paper is to build on the three phases of work undertaken by the CDEI: Phase 1 Stakeholder Engagement and Desk Research, Phase 2 Scenario Planning and Phase 3 Public Engagement.

The CDEI, in partnership with BEIS has produced this guide to support decision-makers to consider how to design, develop and implement ethical and trustworthy Smart Data Schemes.

The intended audience of this paper is: government departments, regulatory bodies, data holders, Authorised Third Parties, and consumer interest groups, particularly those that have been involved in the Smart Data Working Group (SDWG).

This is a research paper, and not intended to be a statement of government policy in this area.

Contents

Context	4
Definitions	4
Methodology	5
Using the Implementation Guide	6
Purpose of this guide	6
What this guide does not do	6
How to use this guide	6
Smart data schemes: challenges and benefits	8
Key future challenges for Smart Data	8
Benefits of Smart Data	8
Features of ethical smart data schemes	9
Clear Purpose	11
Clear Purpose – Governing Bodies	12
Clear Purpose – Regulators	14
Clear Purpose – Authorised Third Parties	17
Fair Outcomes	19
Fair Outcomes – Governing Bodies	20
Fair Outcomes – Regulators	22
Fair Outcomes – Authorised Third Parties	24
Function as Intended	26
Function as Intended – Governing Bodies	27
Function as Intended – Regulators	29
Function as Intended – Authorised Third Parties	31
Function as Intended – Data holders	33
Accountability	35
Accountability – Regulators	38
Accountability – Authorised Third Parties	40
Accountability – Data Holders	42
Societal Benefits	44
Transparency	46
Security	47
Privacy	48
Looking Forward	49
Appendix 1: Glossary	50
Appendix 2: Envisioning Smart Data in 2028	52
Appendix 3: Governing Bodies' Checklists	53

Clear Purpose – Governing Bodies	53
Fair Outcomes – Governing Bodies	55
Function as Intended – Governing Bodies	56
Accountability – Governing Bodies	58
Appendix 4: Regulators’ Checklist Collection	61
Clear Purpose – Regulators	61
Fair Outcomes – Regulators	63
Function as Intended – Regulators	64
Accountability – Regulators	66
Appendix 5: Authorised Third Parties’ Checklist Collection	69
Clear Purpose – Authorised Third Parties	69
Fair Outcomes – Authorised Third Parties	70
Function as Intended – Authorised Third Parties	72
Accountability – Authorised Third Parties	74
Appendix 6: Data Holders’ Checklist Collection	76
Function as Intended – Data Holders	76
Accountability – Data Holders	77

Context

Definitions

Smart Data Term	Definition
Smart Data	The secure sharing of customer data with Authorised Third Parties, upon a customer's request.
Consumers with vulnerabilities	Consumers who, due to their personal circumstances, are especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care. N.B. Whether a consumer has vulnerabilities will depend on the context and sector.
Data holder	A business or organisation that holds data on individual customers e.g., a bank. This includes information about the customer, and data which has been generated through the customer's use of their service.
Authorised Third Party	Any business or organisation that a consumer gives permission to access and/or process their data for the provision of innovative services.
Decision-maker	Could include governing bodies, government departments, regulators, data holders or Authorised Third Parties, and consumer representatives or consumer interest groups where relevant.

Methodology

This guide builds on three phases of work undertaken by the CDEI:

Phase 1 – Stakeholder engagement and desk research

Phase 1 involved desk research and stakeholder engagement through structured interviews with 25 stakeholders across the Smart Data ecosystem to understand the features of ethical and trustworthy Smart Data schemes. The final output of this phase, and methods used are explored in detail in our Phase 1 report.

Phase 2 – Scenario Planning

In phase 2 the CDEI ran a scenario planning workshop with stakeholders across the Smart Data ecosystem to envision Smart Data in 2028 and understand its potential evolutions, enabling us to prioritise specific ethical and trust-related concerns. The final output of this phase, and methods used are explored in detail in our Phase 2 report.

Phase 3 – Public Engagement

Phase 3 consisted of public engagement, which tested Smart Data use cases with the public to develop toolkits and practical guidance for Smart Data schemes.

The CDEI ran polling with members of the public to better understand their thoughts and feelings about Smart Data. The methods used in this polling, and the results, are summarised in a blog¹.

The CDEI also conducted focus groups with participants from the public and microbusinesses, to look at their understanding of Smart Data in a more nuanced manner. The methods used in these focus groups, and findings from them, are summarised in a separate blog².

¹ The Centre for Data Ethics and Innovation, Part one: Examining public attitudes towards Smart Data schemes, 2022. Available at:

<https://cdei.blog.gov.uk/2022/06/22/part-one-examining-public-attitudes-towards-smart-data-schemes/>

² The Centre for Data Ethics and Innovation, Part two: Examining public attitudes towards Smart Data schemes, 2022. Available at: <https://cdei.blog.gov.uk/2022/06/22/part-two-examining-public-attitudes-towards-smart-data-schemes/>

Using the Implementation Guide

Purpose of this guide

The CDEI, in partnership with BEIS, has produced this guide to support decision-makers to consider how to design, develop, and implement ethical and trustworthy Smart Data schemes.

This Guide focuses on:

- The features of ethical and trustworthy Smart Data Schemes that may require additional support in development.
- Regulated sectors (e.g., financial services, energy, communications, etc.)

What this guide does not do

This Guide does **not**:

- Prescribe policy for Smart Data schemes.
- Exhaustively cover all relevant questions for decision-makers to consider in these schemes.
- Deal with the legal responsibilities of parties participating in Smart Data schemes.

Participants in schemes should be aware of the legal frameworks they operate under, including those that arise from data protection legislation.

The Information Commissioner's Office³ (ICO) is tasked with regulating information rights and data protection legislation, including the UK GDPR. Users of this guide might also wish to refer to the ICO's Guide to Data Protection⁴ and data sharing information hub.⁵ Compliance with data protection law is an important practice that will help engender and maintain trust.

Smart Data legislation was introduced into the House of Commons on 18 July 2022, as part of the DCMS Data Protection and Digital Information (DPDI) Bill. The Government is seeking powers to enable the Secretary of State or HM Treasury to mandate industry participation in Smart Data across the economy.

How to use this guide

This guide provides context and information on features of ethical and trustworthy Smart Data schemes. A useful starting point for decision makers is considering all of these features in aggregate before diving into specifics. The Open Data Institute (ODI) has also developed a Smart Data Innovation Guide⁶ in parallel with this work which provides useful information for all stakeholders working in this space.

Our focus group research suggests that the public are particularly concerned with the

³ ICO Website. Available at: <https://ico.org.uk/>

⁴ ICO Guidance for organisations. Available at: <https://ico.org.uk/for-organisations/>

⁵ ICO Data Sharing Code of Practice. Available at: <https://ico.org.uk/for-organisations/data-sharing-information-hub/>

⁶ Open Data Institute, Introducing the Smart Data Innovation Guidebook, 2022. Available at: <https://theodi.org/article/introducing-the-smart-data-innovation-guidebook>

following features: Clear Purpose, Societal Benefits, Function as Intended, and Accountability. Therefore, these features are the focus of this document.

Each of these features is considered independently to support relevant decision-makers. However, reading the guide more widely should help inform understanding about the interaction between different decision-makers and the different features.

Decision-makers will be conscious of the sector specific context in which they operate. However, this guide aims to be useful across sectors, and identifies some implications for expanding Smart Data schemes across sectors.

Smart data schemes: challenges and benefits

Key future challenges for Smart Data

Consumers pointed to the key role trust will play in ensuring that they are confident about engaging with, and seeing benefits from, Smart Data schemes.

- Low trust in Smart Data schemes
- Lack of belief in the benefits of Smart Data
- Benefits of Smart Data not realised – Individuals miss out on potential annual benefits of £12 billion per year, while SMEs miss out on £6 billion a year from not using Open Banking services⁷

“New ways of sharing data creates new ways of misusing it.” - Interviewee, 18 – 44 years old, C2DE

“It seems like there are a lot of people who wouldn't benefit from it...seems like there's an ulterior motive behind this sort of data gathering.” - Interviewee, 18 – 44 years old, ABC1

Benefits of Smart Data

Creating Smart Data schemes that facilitate the sharing of data in a trustworthy manner, that are aligned with societal values, and that match people's expectations of ethical behaviours should have benefits such as⁸:

1. Fostering legitimacy and trust in data sharing activities, encouraging consumers to participate
2. Driving innovation in Smart Data schemes
3. Replacing current practices that may be unethical or untrustworthy

⁷ Reynolds. F, Chidley. M et al, Consumer Priorities for Open Banking, 2019

⁸ The Centre for Data Ethics and Innovation, Addressing trust in public sector data use, July 2020 Available at: <https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use>

Features of ethical smart data schemes

The CDEI's Model for Responsible Innovation provided a starting point for identifying the features of ethical and trustworthy Smart Data schemes. These eight features have been tailored to the Smart Data context through incorporating the perspectives of stakeholders and desk research.

Key features for decision makers to consider include:

1. Is there a **clear and defined purpose** for the scheme?
2. Have the tensions between **fair outcomes** for consumers with the potential for future innovation been balanced?
3. Are there measures in place to ensure systems **function as intended**, such that they do not inflict harm?
4. Are there clear lines of **accountability** in and across Smart Data schemes?
5. Does the scheme deliver **clear benefits** to individuals and society as a whole?
6. Is the scheme **transparent** and open to scrutiny by participants and other legitimate sources?
7. Are there stringent data **security** controls in place?
8. Is consumer **privacy** protected and respected in the design and delivery of the scheme?

In order to satisfy the features on the previous slide, certain conditions need to be present. These conditions include:

- **Robust technical design** – This encompasses three aspects: the functional design (how the data-sharing system will behave in relation to outside agents), the technical design (how this functionality is implemented in code), and the architecture needed for these data-sharing systems. For all of the above, industry wide standards may be required.
- **Appropriate, available, and minimal data** – Smart Data schemes should be designed such that the data needed to enable consumers to benefit is made shareable. Beyond existing legal requirements around data minimisation and storage limitation (covered in the UK GDPR)⁹, ensuring that data is relevant, recent and accurate will minimise the risks associated with data loss, help build consumer trust, and reduce the costs associated with data storing and sharing.
- **Clear scope** – Decision-makers should consider, clarify, and communicate the intended outcomes of introducing a new Smart Data scheme, and from this, the appropriate scope for the scheme. A clear scope could help prevent unintended negative consequences, while allowing as much innovation as possible.
- **Available resources** – Those designing and implementing Smart Data schemes will require certain technical, legal, and financial resources to do so effectively.
- **Effective governance mechanisms** – Smart Data schemes, and the systems that facilitate them, will require governance and oversight mechanisms. These should include lines of appropriate responsibility and routes to redress if issues arise.
- **Meaningful engagement** – Effective communication with a diverse group of domain experts, affected stakeholders, and the general public will be important for fostering

⁹ ICO Guidance, The Principles, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>

trust in Smart Data schemes. This includes particular focus on including the voices of consumers in vulnerable circumstances and traditionally underrepresented groups, and communicating to individuals how they stand to benefit from a scheme.

Our focus group research¹⁰ suggests that the public are particularly concerned that the following features may not be given enough attention: Clear Purpose, Fair Outcomes, Function as Intended, and Accountability. Therefore, these features are the focus of this document.

¹⁰ The Centre for Data Ethics and Innovation, Part two: Examining public attitudes towards Smart Data schemes, 2022. Available at: <https://cdei.blog.gov.uk/2022/06/22/part-two-examining-public-attitudes-towards-smart-data-schemes/>

Clear Purpose

Clear purpose can be considered both in terms of the purpose of a scheme itself and of the use cases developed within it. Decision makers should consider how the scheme/service will offer value to consumers. It will be necessary to account for the needs and expectations of a wide range of consumers - including those with vulnerabilities.

Why does Clear Purpose matter for consumers?

Consumers will only participate in Smart Data schemes if they understand the benefits of doing so. The consumers we interviewed highlighted that they would be most inclined to use a Smart Data service that could help them save money, save time, or receive personalised services.

"I can't see any benefits to me, but I can see lots of benefits to [companies]." - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

"I can't think of any other [reason] why companies would collect data... To me it's just for the sheer money of it." - Interviewee, 18-44, CDEI public engagement on Smart Data.

Why else does Clear Purpose matter for decision makers?

Considering the underlying aims of a scheme should help in creating a scope that allows decision makers to identify use cases and clarify their potential benefits and harmful outcomes (this scope will likely need to change over time, as new Smart Data schemes emerge in more sectors).

In each use case associated with a Smart Data Scheme, it will be necessary to clarify the elements of a consumer's data that will be used. This will aid in facilitating data minimisation and storage limitation practices, and give an understanding into what technical infrastructure will be necessary.

Possible cross-sector sharing impacts

Cross-sector data sharing may help facilitate entirely new use cases for consumers, as well as improve the quality of existing offerings.

However, those enabling this type of data sharing should consider how to mitigate potential risks it may bring including:

- Increasing the potential for the development of harmful use cases.
- Unmonitored 'Mission creep' of a scheme and therefore loss of clear purpose.
- Increasing the likelihood of unnecessary elements of data being used.
- Decreasing clarity around who is responsible for regulating participants and their use cases.
- Introducing too many industry specific terms and phrases, confusing consumers.

Clear Purpose – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Are there established goals for the Smart Data scheme? If not, have you considered who is responsible for developing these goals, and anticipating potential use cases?
- Have you mapped out the personal and other information necessary for the scheme, and ensured its sharing and processing will be in accordance with data protection legislation?
- Have potential participants been consulted and engaged whilst determining the above?
- Have you taken learnings from existing schemes into account?
- Where it exists, have you taken learnings from accepted international best practice relating to schemes in your sector?

Further Considerations:

- Have you fully explored the potential lessons from other Smart Data schemes when it comes to establishing the principles for defining, and communicating, the purpose of the scheme to consumers?
- Have you referred to the ICO's guidance on "What is personal data?"¹¹
- Could there be a lawful basis for the processing or sharing of personal data that does not rely on consent? (See the ICO's guidance)
- Have you considered how cross-sector use cases might be incorporated into the design of your scheme?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you determined what scope and standards (both surrounding potential use cases and data used) will be necessary to ensure the goals of the scheme are achieved?
- Have you considered how data holders and/or Authorised Third Parties should ensure that consumers understand the scope of the services they are using?
- Have you ensured there is enough representation of consumers and SMEs within the governing structure of the scheme?
- Have potential participants been consulted and engaged whilst determining the above?

Further Considerations:

- Have you assessed the trade offs between creating firmer scope as to how data can be used/what data is used, and the scope for more innovation?

¹¹ ICO Guidance, What is Personal Data? Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

- Have you determined the scope so that it maximises potential for innovation whilst minimising potential harms?
- What risk mitigation practices could be employed to maximise innovation whilst limiting potential harms?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- How are you ensuring consumers adequately understand the scope of the service that they are participating in?

Further Considerations:

- Have you considered whether it is appropriate to allow data holders and Authorised Third Parties to aggregate data shared by consumers for purposes beyond those directly relevant to the consumer's use case?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Do consumers understand what they are agreeing to in terms of how their data will be used? Do consumers understand routes to redress if their data is used in a way that is inconsistent with this?
- Is there a clear mechanism for consumers to provide feedback about the quality of the communication they receive about the functioning of the service?

Further Considerations:

- Have you considered how consent mechanisms should operate when there is no single specified use case but multiple purposes for which the data can be shared?
- Have you ensured consumers remain able to opt out?
- Have you considered whether further uses of the data are justified by serving the public interest/societal well-being?
- Would a mechanism that allowed consumers to track how their data is being used be helpful?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do consumers understand what they are agreeing to in terms of how their data will be used?
- Do consumers understand routes to redress if their data is used in a way that is inconsistent with this?
- Are you monitoring consumer feedback about the services facilitated by the scheme?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?
- Would consent dashboards for consumers, that track use of data, be helpful in giving a holistic view of data use to consumers?

Clear Purpose – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Are there established goals for the Smart Data scheme? If not, have you considered who is responsible for developing these goals, and anticipating potential use cases?
 - Have you considered what governance model will best enable these goals, and what the role of a regulator/regulators should be?
- Have you mapped out the personal and other information necessary for the scheme, ensuring that its sharing and processing will be in accordance with data protection legislation?
- Have relevant stakeholders been consulted and engaged whilst determining the above?

Further Considerations:

- Have you referred to the ICO's guidance on "What is personal data?"¹²
- Could there be a lawful basis for the processing or sharing of personal data that does not rely on consent? (See the ICO's guidance)¹³
- Have you considered how cross-sector use cases might be incorporated into the design of your scheme?
- Are you engaging with regulators from other sectors to enable cross-sector data sharing?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you considered the scope (around potential use cases and data used) that will be necessary to ensure the goals of the scheme are achieved?
- Have you ensured you have sufficient powers, capacity, and systems to enforce this scope?
- Have you considered what is the appropriate level of monitoring, at the scheme, architecture and consumer outcome levels, to ensure that a scheme, and its participants, are operating within this scope?
- Have potential participants been consulted and engaged whilst determining the above?

Further Considerations:

- Have you assessed the trade offs between creating narrower scope as to how data can be used/what data is used, and the potential for more innovation?

¹² ICO Guidance, What is Personal Data? Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

¹³ ICO Guidance, Consent, Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>

- Have you determined the scope that would maximise potential for innovation whilst minimising potential harms?
- What risk mitigation practices could be employed to maximise innovation whilst limiting potential harms?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested whether the proposed scope is having the intended effects?
- Have participants been given the opportunity to feed back on the scope that is being tested?

Further Considerations:

- Have you considered if regulatory sandbox environments would aid the responsible development of use cases in this space?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you checked the scheme's scope is having the intended effects?
- Have you checked that the anticipated use cases are able to develop and operate within the scheme's scope?
- Are you ensuring participants in the scheme are operating within the scheme's scope?
- Have you ensured consumers understand the scope of their data's use and their routes to redress if this is breached?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you checking that the scope of the scheme is having the intended effects?
 - Are you checking that the anticipated use cases are able to develop and operate within the scope of the scheme?
 - Are you ensuring participants in the scheme are operating within the scheme's scope?
- Are you ensuring consumers understand the scope of the use of their data and their routes to redress if this scope is breached?
- Do structures exist to monitor if the scope of the scheme needs modifying, and to carry out this modification?

Further Considerations:

- Are you considering what safeguards would be necessary to enable cross-sector data sharing?
 - Are you considering which organisation/organisations would be responsible for regulating cross-sector Smart Data sharing?

- Are you continuing to consider context-specific requirements for your sector?

Clear Purpose – Authorised Third Parties

Whilst developing and implementing Smart Data schemes, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with the authorities responsible for establishing the scope of the Smart Data scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you ensured the service you are aiming to provide is fully within the scope of the scheme?
- Have you ensured you have adequate internal governance structures to make sure you comply with the relevant regulatory requirements?
- Have you ensured you have sufficient structures, resources, and systems to make sure that your service operates within the scope of the scheme?
- Have you determined how you are going to communicate the benefits of your service, and the purpose of data processing, with your consumers to enable the gathering consent?
- Have you collected feedback from the consumers to ensure you are clearly communicating the above?

Further Considerations:

- Have you tested a process for the gathering of consumer feedback to understand whether you communicate the purpose and benefits of your service in an easily understandable manner?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you ensured the scope of the service you provide is fully within the scope of the scheme as intended?
- Have you collected feedback from consumers to ensure they understand the purpose of data processing and the benefits of the service you provide?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Does the live service remain fully within the intended scope of the scheme?

- Have you adequately communicated to consumers what elements of their data are being used, how they are used, and the purpose of and limits to this use? (e.g., In simple English, easy to understand, and a standardised format).

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring the service you provide is fully within the scope of the scheme?
- Are you actively reviewing how you communicate to consumers what elements of their data are being used, how it is used, and the purpose of and limits to this use? (e.g., this should be in simple English, easy to understand, and a standardised format)?
- Do you have structures in place to respond to unexpected data sharing beyond the scope of the scheme?

Further Considerations:

- Are you collecting consumer feedback to ensure that any new information about your service does not diminish the level of understanding of its benefits and purpose?
- Are you continuing to consider context-specific requirements for your sector?

Fair Outcomes

There may be tensions in balancing fair outcomes for consumers with the potential for future innovations emerging from Smart Data schemes. Realising the value of sharing consumer data in exchange for better services and future innovation, from a basis of fairness, will be important.

Why do Fair Outcomes matter for consumers?

Consumers who participated in this research believe that the benefits of Smart Data schemes will be unfairly distributed across the population. Several of our interviewees voiced fears that consumers in vulnerable circumstances, particularly those that are either digitally disengaged or with financial vulnerabilities could both miss out on the benefits of these schemes, or actively lose out because of them.

“I’d hate to think that someone who doesn’t have a laptop or doesn’t understand the benefits would miss out.” - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

“[This is] a lot of control to give to groups, and that could be abused against smaller companies, for the bigger companies.” - Microbusiness, CDEI public engagement on Smart Data.

Why else do Fair Outcomes matter for decision makers?

Consumers believing that Smart Data schemes are unfair will likely lead to lower levels of uptake. Alongside this, there is the potential for bias and unequal outcomes to emerge in schemes. For example, services designed on data shared by an unrepresentative sample of the population, could lead to services with inbuilt biases.

Not tackling unfair outcomes would erode trust, and participation, in services and schemes as a whole.

Possible cross-sector sharing impacts

Cross-sector data sharing might further enable access to services by groups that have traditionally faced greater difficulties or been excluded from them.

- However, those enabling this type of data sharing should consider how to mitigate potential risks it may bring including:
- Perpetuating digital disengagement and limiting digital footprints by linking digital services.
- Certain services or organisations gaining data dominance.
- Less clarity on what organisations are responsible for ensuring that consumers receive fair outcomes.

Fair Outcomes – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Have you determined how you will identify which groups face vulnerabilities in your sector?
- What expectations should there be for participating organisations to provide services that support consumers with vulnerabilities?
- Have you considered how to monitor whether bias and unfair outcomes are emerging in a scheme?
- What requirements for participants need to be put in place for transparency and monitoring to identify bias and unfair outcomes?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you considered, and incorporated, the needs of consumers in vulnerable circumstances into your scheme?
- Have you considered the impacts of the scheme on people with protected characteristics?
- Have you determined what data will be needed within a scheme, and developed safeguards to ensure unnecessary data will not be used?
- Have you identified potential unfair outcomes for consumers and considered safeguards that will help minimise the risk of these occurring?

Further Considerations:

- Have you considered if participating organisations in the scheme should be required to ring fence elements of participant's data, to ensure only appropriate data is used?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you reviewed the standards in light of initial feedback and testing?
- Have you tested if bias and unfair outcomes are emerging within the scheme?
- Have you incorporated the insights of representatives of vulnerable customers in the above?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are you in dialogue with consumer groups to review and update the standards to prevent negative impact of the scheme on consumers in vulnerable circumstances?
- Are you continuously reviewing and updating the standards of the scheme to ensure fairness of the outcomes for consumers?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are there processes in place for regular dialogue with consumer groups?
- Are there processes in place to update the standards and prevent negative impact of the scheme on consumers in vulnerable circumstances?
- Are there processes in place to review and update the standards of the scheme to ensure fair outcomes for consumers?

Further Considerations:

- Are consumers being engaged when determining if cross sector data sharing is desirable?
- Are you considering whether encouraging cross sector data sharing would alter which consumers should be considered vulnerable?
- Are you ensuring consumers fully understand the following, particularly given the complexities that cross sector data sharing will add:
 - How their data will be used?
 - Who will use their data?
- Are you continuing to consider context-specific requirements for your sector?

Fair Outcomes – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you considered what protections and processes should be in place at the regulator, governing body and service level and communicated these to consumers and participants?
- Have you determined scope such that it maximises potential for innovation whilst minimising potential harms?
- Have you consulted consumers in vulnerable circumstances, or groups that represent them?

Further Considerations:

- Have you considered how to ensure that allowing cross-sector data sharing will not result in data dominance by specific organisations?
- Have you determined whether standardised formats for data, and cross-sector accreditation, will be needed to ensure interoperability across different sectors?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you provided input into the governing body's considerations around:
 - Ensuring fair outcomes for all consumers?
 - Consumers with vulnerabilities?
- Have you established a mechanism for monitoring the fairness of outcomes for different consumers?
- Have you established a mechanism for monitoring that the data shared and used is handled by the participants of the scheme as per the intended purpose?

Further Considerations:

- Have you considered whether requiring ring fencing of particular elements of data would help to protect consumers in vulnerable circumstances?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you determined, and communicated, what enforcement actions will be taken if participants act outside of the scheme's scope?
- Have you developed routes to redress in situations where the scheme participants are using the data for purposes other than the intended purpose, or in a manner that perpetuates bias or causes unfair treatment towards groups with vulnerabilities?

Further Considerations:

- Is there clear guidance for consumers and services on the expectations for how complaints should be submitted and handled?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured the enforcement measures are preventing participants from violating the scheme's scope?
- Have you tested the routes to redress in situations where the scheme participants are using the data for purposes other than the intended purpose, or in a manner that perpetuates bias or causes unfair treatment towards groups with vulnerabilities?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring the participants in the scheme to make sure that the services they offer are competitive and that there is no concentration of data in the hands of a few Authorised Third Parties?
- Are you monitoring for other competition-related impacts that could arise from the dominance of a small number of Authorised Third Parties?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Fair Outcomes – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you created structures that allow consumers to flag when they face vulnerable circumstances?
- Have you considered the needs of consumers in vulnerable circumstances/with protected characteristics when designing your service?
- Have you considered how you will monitor your service to make sure that it treats consumers fairly?
- Have you designed communications to explain to your consumers what their data is being used for and how it contributes to the operation of the service?
- Have you tested the processes, workflows and other elements making up your service to ensure that any unfair biases are identified?

Further Considerations:

- Have you determined how to ensure that you are only using relevant pieces of a consumer's data for a given use case?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you validated that your service meets the requirements of consumers in vulnerable circumstances?
- Do you have structures in place to alter your service if issues are identified that your service is not meeting?
- Have you tested that your communications strategy will enable consumers to feedback about whether they understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Do you have a feedback process in place to monitor the following:

- Outcomes, ensuring that certain groups are not disproportionately disadvantaged?
- That your service meets the requirements of consumers in vulnerable circumstances?
- Whether consumers understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do you have processes in place to make sure that your service treats consumers fairly? Have you defined metrics to track your performance?
- Are you monitoring the following:
 - Whether your service delivers fair outcomes across the population?
 - Whether your service meets the requirements of consumers in vulnerable circumstances?
 - Whether the consumers understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Do you have processes in place to review whether you are using only necessary elements of a consumer's data?
- Are you continuing to consider context-specific requirements for your sector?

Function as Intended

Decision makers should consider how to ensure that Smart Data schemes function as intended and expected by consumers. It will be important to consider how consumers will give and withdraw consent. Consumer consent should not be assumed from their agreeing to complicated terms and conditions documents that they are unlikely to have read.

Why does Functioning as Intended matter for consumers?

The majority of consumers we interviewed believed that Smart Data offerings are complex and voiced fears that their data would not be used in the ways that they would anticipate. In particular, our focus groups highlighted that consumers are suspicious of long, complex terms & conditions, and whether or not organisations keep within their bounds.

“You’ve got to click through the terms and conditions and say yes, but no one really reads [them] because they’re long.” - Interviewee, 18-44, CDEI Consultation on Public Perceptions of Smart Data.

“It will direct you to who they want to direct you to for commission. It’s what happens with the travel and insurance websites too. The same thing would happen with this smart data.” - Interviewee, 45+, CDEI public engagement on Smart Data.

Why else does Functioning as Intended matter for decision makers?

Those designing and implementing Smart Data services might consider how they can test, and show, that they operate as intended and expected.

Likewise, those governing and overseeing Smart Data schemes should consider how they can validate that the schemes are having the anticipated impact within a sector.

Possible cross-sector sharing impacts

Cross-sector Smart Data sharing might better enable Authorised Third Parties to deliver on consumer expectations, with access to more, and better quality, data.

However, those enabling this type of data sharing should consider how to mitigate potential risks it may bring including:

- Potential for increased confusion for consumers, and less perceived control of their data, stemming from more complicated data sharing relationships.
- Making consent harder to ensure.
- Complicating consent withdrawal mechanisms.
- Creating more potential points of failure as data sharing infrastructure and architecture becomes more complex.
- Lack of engagement between different oversight functions.

Function as Intended – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Have you considered what the intended impacts are from the introduction of the Smart Data scheme?
 - Have you considered what consumers will expect the benefits of using a service within the Smart Data scheme to be?
- Are you consulting relevant stakeholders on issues of consent, liability, and data minimisation and storage limitation in Smart Data schemes?
 - Have you considered how other schemes tackle issues of consent, and whether your scheme deviates from common approaches?

Further Considerations:

- Have you considered developing pilot programmes with stakeholders to test issues around consent, liability, and data minimisation and storage limitation?
- Are you considering encouraging/requiring participants to use privacy-enhancing technologies, when appropriate?
- Are you considering encouraging/requiring use of mechanisms that allow a consumer to track how their data is used?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you begun to develop and test a liability framework with stakeholders?
- Have you begun to develop and test data minimisation and storage limitation requirements with stakeholders?
- Have you begun to develop and test how consumers can provide consent to participate?
 - What information should participating organisations be required to give to consumers?
 - How often should re-consenting be required?
 - What should the process for re-consenting be?
 - How do you ensure consumers are aware they can remove consent?
- Have you determined what technical standards are required to ensure safe, smooth transfer of data between organisations?

Voluntary onboarding and testing

Important:

- Have you created clear lines of appropriate responsibility in your liability framework?
- Have you iterated on the liability framework, data minimisation and storage limitation requirements, and consent mechanisms based on feedback from stakeholders?

- Have you determined how long organisations should be allowed to retain shared data?
- Have you determined what measures need to be in place to ensure that information about a person, inferred from data about another consumer, is not shared if they have not consented to sharing it?

Further Considerations:

- Have you tested the liability framework, data minimisation and storage limitation requirements, and consent mechanisms in practice with stakeholders?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured stakeholders understand:
 - Their legal responsibilities and who is liable for non-compliance?
 - Who is responsible for addressing/ redressing consumer complaints?
 - Their obligations around consent?
 - How to handle consumer data if consent is revoked?
 - Their obligations around data minimisation and storage limitation?
- Have you ensured the above information is readily available, in plain English, to consumers.
- Have you ensured consumers understand their routes to redress?

Further Considerations:

- Have you considered how to handle liability in the event an Authorised Third Party ceases operations? E.g., who is liable for the consumer data an Authorised Third Party holds when it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do you have processes in place to ensure the following information is readily available to consumers:
 - Liability structures within the scheme?
 - Their rights around data minimisation and storage limitation and storage limitation?
 - Their rights around consent and ability to opt out at any time?
- Are you continuing to adapt your liability framework, data minimisation and storage limitation requirements, and consent based on changing use case needs?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you considered what the intended impacts of introducing the Smart Data scheme are for consumers and the sector?
 - Have you considered what consumers will expect the benefits of participating in the scheme to be?
- Have you determined what stakeholder groups (e.g., consumers, consumer groups, data holders, Authorised Third Parties, etc.) you should be engaging throughout the process and when you should be engaging them?
- Have you determined the appropriate level of monitoring, at the scheme, architecture, and consumer outcome levels, to ensure that a scheme is operating as intended?
- Have you determined the primary use cases and intended benefits of the scheme? How will you determine if these impacts are being met?

Further Considerations:

- Have you considered context-specific requirements for your sector? (E.g., Would consumers expect services to perform differently between the finance and energy sectors)?

Development and testing

Important:

- Have you tested the following with relevant stakeholders:
 - What rules and regulations are needed for the scheme to deliver on consumer expectations?
 - What would constitute a service provider securing consent from a consumer?
 - How compliance with data standards will be enforced
 - What an appropriate level of monitoring for the scheme would be?
- Have you considered how regulations that already exist (for example, those around data sharing standards) would impact your scheme?

Further Considerations:

- Have you engaged with stakeholders on how to implement consent mechanisms?
- Have you engaged with stakeholders to gain their opinions on proposed data sharing standards?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you ensured stakeholders are aware, in plain English, of their legal responsibilities around consent?

- Are you, and stakeholder, testing a variety of approaches to ensure consumers are made aware of their rights around data sharing and consent?
- Have you determined how compliance with consent requirements and data sharing standards should be monitored?
- Have you created measures to ensure data holders/Authorised Third Parties comply with legal requirements?

Further Considerations:

- Have you considered how consumers are informed of their data rights in other data sharing schemes?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you acted upon the lessons learned during the development and testing phase around consent/data sharing standards/appropriate levels of monitoring?

Further Considerations:

- Have you gathered input from stakeholders, particularly consumers, in the development and voluntary onboarding phases?
- Have you considered how to handle liability in the event an Authorised Third Party ceases operations? E.g., who is liable for the consumer data an Authorised Third Party holds when it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring data holders/Authorised Third Parties for compliance with consent standards?
- Are you monitoring data holders/Authorised Third Parties for compliance with data standards?
- Are you regularly assessing whether the data sharing standards are appropriate for the ecosystem and revising regulations as appropriate?
- Are you regularly assessing whether the consent mechanisms are appropriate for the ecosystem and revising regulations as appropriate?
- Are you monitoring consumer complaints to identify systemic issues within the scheme?

Further Considerations:

- Are two-way routes of communication open with consumers, particularly with respect to liability structures?
- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with and contributed to consultations by the relevant authorities designing and overseeing the development of the scheme?
- Have you mapped out the personal and other information necessary for your services, ensuring its sharing and processing will be in accordance with data protection legislation?
- Have you carried out a Data Protection Impact Assessment¹⁴ to identify and mitigate the risks of the planned data processing?

Further Considerations:

- Are you engaging with regulators/governing bodies on the liability framework, requirements, and consent mechanisms in the Smart Data scheme?
- Have you referred to the ICO's guidance on "What is personal data?"¹⁵
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Do you have systems in place to ensure that data is held for the minimum amount of time necessary?
- Have you tested different approaches to how you secure consent from consumers for your use cases?

Further Considerations:

- Have you considered using, or encouraging data holders, to use privacy-enhancing technologies and other forms of data sharing technology aimed at reducing risk?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you provided input and feedback to governing bodies/regulators on liability frameworks, requirements, and consent mechanisms?
- Have you incorporated feedback from consumers on your approaches to gathering consent?

Further Considerations:

¹⁴ ICO Guidance, Data Protection Impact Assessments. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

¹⁵ ICO Guidance, What is Personal Data? Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

- Have you been involved in providing feedback on the liability framework, requirements, and consent mechanisms in practice with other stakeholders?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are you aware of your legal responsibilities and liabilities for non-compliance?
- Is there a clear process for receiving, addressing and where necessary escalating consumer complaints?
- Are there responsible owners for handling complaints in your organisation?
- Are you aware of your obligations around consent? Are you aware of how you handle consumer data if consent is revoked?
- Are you aware of your liability for data shared onwards to other Authorised Third Parties and how they use it?
- Have you communicated liability structures and redress mechanisms in plain English and in a way that is easily accessible to consumers?

Further Considerations:

- Have you considered how to handle liability in the event you fold? E.g., who is liable for the consumer data you hold when your company stops operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring you are communicating all necessary information to consumers when requesting consent?
- Are you ensuring it is clear to consumers how they can withdraw consent?
- Are you communicating liability structures and redress mechanisms to your consumers?
- Are you continuing to revisit your practices based on changing use cases?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Data holders

Whilst developing and implementing Smart Data infrastructure, considerations for data holders include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?
- Have you input into discussions around the types of business data necessary to realise successful services within the scheme?

Further Considerations:

- Are you engaging with regulators/governing bodies on the liability framework, requirements, and consent mechanisms in Smart Data schemes?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you established how you will ensure that a consumer has meaningfully consented to their data being shared?
 - What actions will be necessary if a consumer withdraws their consent?
- Have you considered what data sharing architecture is needed to facilitate data sharing with Authorised Third Parties in a timely and reliable manner (incl. business/commercial data)?
 - How do you ensure that you only share data about a consumer required for a particular use case?
 - How do you determine what data is necessary for a specific use case?

Further Considerations:

- Have systems been put in place to ensure that data is held for the minimum amount of time necessary?
- Have you tested different approaches to how Authorised Third Parties could get consent from consumers?
- Have you considered using or encouraging Authorised Third Parties to use privacy-enhancing technologies?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you established mechanisms to test whether your data sharing architecture is performing as intended?
- Have you tested your data sharing infrastructure/architecture and its performance? (E.g., is it sharing the minimal amount of data? required? Is it working efficiently?)

Further Considerations:

- Have you provided input and feedback to governing bodies/regulators on liability frameworks, requirements, and consent?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured your data sharing architecture is operating as intended? Are you monitoring its performance and rectifying issues where they arise?
- Are you aware of your legal responsibilities and liabilities for non-compliance?
- Are there individuals who are responsible for addressing/redressing consumer complaints in your organisation?
- Have you communicated liability structures and redress mechanisms to your consumers?

Further Considerations:

- Have you considered how to handle liability in the event that an Authorised Third Party folds? E.g., who is liable for the consumer data that an Authorised Third Party holds if it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring your data sharing architecture is operating as intended?
- Are you ensuring it is clear to consumers how they can withdraw consent?
- Are you communicating liability structures and redress mechanisms to your consumers?
- Are you continuing to revisit your practices as use cases evolve?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Accountability

Smart Data schemes and services should have effective governance and oversight mechanisms, with clear lines of appropriate responsibility. The above should be communicated to consumers, in a way such that they are understood. In particular, the roles and responsibilities of governing bodies and regulators - in and across schemes - should be openly and clearly stated.

Why does Accountability matter for consumers?

The majority of consumers in our focus groups believed that a well-regulated system would be a cornerstone for building trust in Smart Data schemes. In particular, participants in our focus groups said they would expect: clear codes of conduct for participating organisations; clear routes of redress, managed by an independent body; and effective deterrents, including fines.

"[I'd want] an independent body that sits above it all just to make sure that the rules are being adhered to." - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

"I think having slightly heavier restrictions [to] make sure they protect the consumer at all costs is a better way of doing it." - Interviewee, 18-44, CDEI public engagement on Smart Data.

Why else does Accountability matter for decision makers?

Consumers we spoke to tend to consider a narrow definition of accountability: they are concerned with the consequences for mis actions, and the oversight functions surrounding these.

Decision makers might consider accountability in a broader sense. Beyond deciding who is responsible in a given situation, they must decide how accountability mechanisms function.

Possible cross-sector sharing impacts

Those enabling this cross-sector data sharing should consider how to mitigate potential risks it may bring including:

- Agreeing roles and responsibilities of different organisations sitting across different schemes and sectors
- Greater uncertainty for services intending to sit across two or more schemes about:
 - Who is responsible for accrediting such services
 - What requirements for accreditation are necessary for cross-scheme services.
- Making routes of redress more confusing for consumers.
- Uncertainty about which organisation has lead responsibility in the event of an issue across two or more schemes.

Accountability – Governing bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Are you clear on the roles and responsibilities of your organisation in relation to the Smart Data scheme in question?
 - Where does your organisation fit in the wider governance model for the scheme?
 - What is the timeline for developing and delivering the scheme?
 - How will you engage with the wider ecosystem whilst developing the scheme?
- Is it clear to participants who are the controllers and processors of personal data? (see - the ICO's Guidance)¹⁶

Further Considerations:

- Have you considered context-specific requirements for your sector?
- Have you considered encouraging data sharing agreements between participating organisations, which would set out their respective responsibilities? (see - The ICO's guidance)¹⁷

Development and testing

Important:

- Have you developed the standards that will underpin the Smart Data scheme?
 - What guidance will you need to provide to participants to help them meet these standards?
- Have you considered whether data holders should be mandated to participate in your Smart Data scheme?
- Have you engaged with the wider ecosystem whilst determining the above?

Further Considerations:

- Have you provided additional guidance for participants beyond that on Mandatory standards? (For example, like the Conditional, and Optional standards employed in Open Banking)
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested the standards and guidance with potential participants of the schemes, and amended them accordingly?
- Have you developed codes of conduct for relevant organisations?

¹⁶ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

¹⁷ ICO Guidance: Data Sharing Agreements. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/>

- Are participating organisations aware of their responsibilities to consumers and the penalties for non-compliance?
- Are the roles and responsibilities of all the different actors in the scheme (including your own) easily accessible and in plain English?

Further Considerations:

- Have you considered context-specific requirements for your sector?
- Have you considered referring participating organisations to the ICO approved codes of conduct¹⁸?

Onboarding and services and services go live

Important:

- Have you provided sufficient guidance and engagement to participating organisations to enable them to adhere to the standards of your scheme?
- Have you ensured that participating organisations communicate clearly about their responsibilities and obligations to consumers?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are there mechanisms in place to alter existing standards and guidance in the scheme if necessary?
- Are you monitoring whether an alternative governance model might be more appropriate now the scheme is fully live?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

¹⁸ ICO Guidance, Codes of Conduct. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/>

Accountability – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you determined who will be responsible for establishing the standards that participants in a scheme must adhere to?
- Have you determined what type of oversight any Governing Bodies within your sector will require?
- Is it clear to participants who are the controllers and processors of personal data? (see - the ICO's Guidance)¹⁹
- Have you communicated to "controllers" that they must have appropriate contacts in place with processors in accordance with Article 28 UK GDPR?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you determined what structures are necessary to ensure that the standards of the scheme, and the responsibilities of the participants, are adhered to?
- Have you considered whether participants in your Smart Data scheme require accreditation?
 - Are you consulting to establish the requirements and responsibilities involved in accrediting services?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you determined lines of accountability for roles across the scheme?
- Have you tested the mechanisms established to ensure the compliance of participating organisations?
- Have you communicated to consumers the role that you as a regulator play within a scheme?
- Are sufficient numbers of organisations passing the accreditation requirements?

Further Considerations:

- Have you considered context-specific requirements for your sector?
- What would be a reasonable number of participating/accredited organisations?

¹⁹ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

Onboarding and services and services go live

Important:

- Are the mechanisms that ensure the compliance of participants fit for purpose and delivering the expected results?
- If implemented, have you checked if the accreditation requirements are allowing for a vibrant marketplace of offerings to emerge in a safe, controlled manner?
 - Are accreditation requirements posing additional burdens on participants operating across sectors?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are the mechanisms that ensure the compliance of participants performing as expected?

Further Considerations:

- If cross sector data sharing is a consideration, will multiple regulators' jurisdictions cover a scheme?
 - If yes, what will be necessary for collaboration between the organisations?
- Are you continuing to consider context-specific requirements for your sector?

Accountability – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with and contributed to consultations by the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you determined what internal governance structures will be necessary to ensure you comply with the relevant legislation?
- Have you considered how to communicate a consumer's rights and routes to redress to them?
- Have you, as data controllers, ensured you have appropriate contacts in place with data processors²⁰ in accordance with Article 28 of the UK GDPR

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested that your internal governance structures will ensure that you comply with the relevant legislation?
- Have you tested that the way you communicate to consumers their rights and their routes to redress in the event of a problem is working?
- Have you ensured you are complying with the Privacy and Electronic Communications Regulations²¹, and the consumer's right to object²² to direct marketing?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

²⁰ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

²¹ ICO Guidance, What are PECR? Available at: <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>

²² ICO Guidance, Right to Object. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

- Are your internal governance structures successfully ensuring that you comply with the relevant legislation?
- Are you actively communicating to consumers their rights and their routes to redress in the event of a problem.

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring if you need to modify internal governance structures to enable you to comply with changing legislation?
- Are you monitoring to ensure the way you communicate to consumers their rights and their routes to redress are working?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Accountability – Data Holders

Whilst developing and implementing Smart Data infrastructure, considerations for data holders include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you created the necessary internal governance structures to ensure you comply with the relevant legislation?
- Have you developed clear lines of internal responsibility about who has what responsibility in relation to Smart Data sharing?
- Have you determined how you will communicate a consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?
- Are you actively communicating consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?
- Are you actively communicating consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?

- Are you actively communicating consumer's rights and routes to redress to them?
- Are you modifying your service to prevent issues from reoccurring when they emerge?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Societal Benefits

Smart Data schemes could deliver significant benefits to society as a whole. On top of unlocking financial benefits worth billions annually for consumers and increasing competition in markets with poor consumer outcomes, they could lead to innovations that tackle economic, social, and environmental challenges. Ensuring these benefits are realised will be an important goal for all stakeholders.

Why do Societal Benefits matter for consumers?

Our interviews with consumers revealed that the potential broader societal benefits of smart data resonate less with people than the immediate, more tangible, personal benefits. Interviewees were most open to the idea of sharing data with institutions like the NHS for public benefit. However, most approached the general idea of sharing their data for broader public good with suspicion. Work needs to be done to convince consumers of potential societal benefits.

“No one should tell us what we have to do.” - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

“The NHS is trusted... but I don't think I would be able to accept it from a third party.” - Interviewee, Digitally disengaged, CDEI public engagement on Smart Data.

Why else do Societal Benefits matter for decision makers?

Whilst the most discussed benefits of Smart Data schemes are those for individual consumers, they also have the potential to create broader societal benefits. In particular they could help towards environmental sustainability goals, economic well-being, and general reduction in inequalities. Consideration of how consumers can choose to use their data for social good might be incorporated into Smart Data scheme design. These types of benefits may encourage greater uptake of Smart Data services by consumers.

Achieving these benefits is not guaranteed though, they rely on further innovation and do not necessarily align with the primary motivations for schemes. That will present a challenge for the organisations responsible for delivering schemes.

It will require a focus on enabling innovation and require join up across sectors. It will also require ongoing involvement by policy makers.

Possible cross-sector sharing impacts

Cross-sector data sharing may increase the potential impact that Smart Data schemes could have. It could facilitate Smart Data schemes tackling broad economic, social and environmental issues.

However, those enabling this type of data sharing should consider how to mitigate potential risks it may bring including:

- Increased risks of societal harms emerging from unintended greater data concentration.
- New examples of unfair outcomes or bias emerging.

- Making it harder to measure the impact of a Smart Data scheme.

Transparency

Ensuring that Smart Data schemes are transparent, and open to scrutiny by participants and other legitimate sources, will be an important task for stakeholders. The use and sharing of data by Authorised Third Parties should be open to scrutiny by consumers, who should have easily accessible routes of redress. Users should note, there are existing obligations towards transparency within data protection legislation.

Why does Transparency matter for consumers?

Our interviewees said that they would only trust organisations that are transparent about what information they are using and why this information is required. They argued that organisations would have to demonstrate that the data being used is both relevant to the service provided necessary to delivering the service.

“I’d want to know who they’re sharing the data with, and the length of time they’d have the data - how it’s stored as well.” - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

“It seems transparent, so you know what you are consenting for and are protected.” - Interviewee, 18-44, CDEI public engagement on Smart Data, in relation to Scenario 1 (High Data Portability and High Trust), from CDEI Futures Research.

Why else does Transparency matter for decision makers?

Transparency can be understood both in terms of process transparency and outcome transparency. Decision makers might consider to what extent they understand, and can communicate: how these Smart Data products work (compared to how they are intended to be used), whether they are providing beneficial outcomes, and how these outcomes are reached.

The level of information that should be available will likely vary depending on the audience. Further, the manner in which this information is presented will likely have to be geared to the expertise and knowledge of the relevant audience.

Possible cross-sector sharing impacts

Those enabling this cross-sector data sharing should consider how they ensure that the following is still communicated to consumers:

- What data is being shared.
- Where this data comes from.
- Who is using the data.
- How the data is being used.
- How long their data will be used for.
- The benefits of the data sharing/processing.
- The risks associated with data sharing.

Security

Smart Data schemes could notably improve the existing landscape by protecting individuals' privacy, while facilitating data sharing. This is particularly true where less secure data sharing mechanisms have arisen instead of Smart Data schemes. As Smart Data schemes are developed, ensuring they operate within stringent data security controls will be an important consideration. Participants may wish to consider the ICO's approved codes of conduct²³, which may aid with data protection issues.

Why does Security matter for consumers?

Data security risks were one of the most commonly expressed concerns by our interviewees. Interviewees were most concerned about risk to their financial and health data. Some noted that they would be more likely to trust already familiar participating organisations, or organisations with some type of accreditation kitemark. Consumers emphasised that a strong regulatory system, enforcing strict data security standards would bring them comfort.

"There's been enough high profile instances of the risks... The systems aren't fully secure." - Interviewee, 45+, CDEI Consultation on Public Perceptions of Smart Data.

"When there's a third party and you're giving your data, there's a risk of fraud." - Interviewee, 45+, CDEI public engagement on Smart Data.

Why else does Security matter for decision makers?

Smart Data systems, as with all technology systems, will require good cybersecurity. Decision makers might consider how to ensure systems protect the information and data of participating consumers, remain continuously functional and accessible to authorised users, and keep confidential and private information secure even under hostile or adversarial conditions. Communicating and showing that data is secure might increase trust from consumers.

Decision makers should look to the existing security standards implemented in Open Banking, or in other Smart Data schemes internationally.

Possible cross-sector sharing impacts

Those enabling this cross-sector data sharing should consider how to mitigate potential risks it may bring including:

- Introducing additional points of vulnerability for malicious actors to target.
- Creating more interdependent points of infrastructure and therefore potential points of failure.
- Increasing the complexity of creating data security standards, particularly when different sectors are at different points of maturity in this regard.

²³ ICO Guidance, Codes of Conduct. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/>

Privacy

Guaranteeing that consumer privacy is respected and protected in the design and delivery of Smart Data schemes is important for all involved parties. Unique approaches to privacy might be sought in sectors where the sensitivity of the data being shared, or the effect of its use on consumer trust, is particularly high.

Why does Privacy matter for consumers?

Our interviewees did not feel confident that data sharing would be contained solely to consented third parties. They were particularly concerned that as a result of data misuse they would receive spam/nuisance phone calls and emails. They argued that a well-regulated system, with clear codes of conduct, would be most important to building trust here.

“The more people you disclose your data to, the more you’re going to be harassed in different ways.” - Interviewee, 18-44, CDEI Consultation on Public Perceptions of Smart Data.

“I don’t think anybody can hide from anything anymore... I’m very careful [with personal data] but if anyone really really wanted to know things, then they could find out” - Interviewee, 45+, CDEI public engagement on Smart Data.

Why else does Privacy matter for decision makers?

Decision makers should consider what information individuals engaging with Smart Data services will need to confidently make decisions around use of their data. They might consider how they can ensure systems are privacy preserving, whilst maximising the value of data, and how they might ensure that the amount of data used is proportionate to a given use case.

Decision makers should consider the potential risks to privacy and negative outcomes from particular use cases, especially those disproportionately affecting specific groups.

Privacy is a feature that may stand in tension with other features explored in this document - for example, optimising Smart Data for Societal Benefits.

Possible cross-sector sharing impacts

Those enabling this cross-sector data sharing should consider how to mitigate potential risks it may bring including:

- Creating additional points of vulnerability from which personal data can be attacked/leaked.
- Increasing the risk of re-identification from anonymised data, through greater data aggregation.
- Increasing risk of data misuse through more parties being involved in data sharing.
- Consumers feeling greater levels of intrusion if specific types of data are shared (e.g., health data).

Looking Forward

- Building trustworthiness and ethics into Smart Data schemes will be crucial in encouraging public participation in them.
- Decision makers may need to account for increasing complexity when enabling the growth of cross-sector data sharing.
- For the UK to remain competitive on the international stage, it may need to expand Smart Data to more sectors, quickly and in a responsible manner.

Appendix 1: Glossary

Term	Glossary
API	API stands for Application Programming Interface. This is code that enables data to be shared between applications.
Consent	Consent given voluntarily and in an informed way, with the person consenting having the capacity to make the decision ²⁴
Cross-sector Smart Data Schemes	Schemes in which data from more than one sector are shared with Authorised Third Party Providers - for example, an automated energy switching service might link up with Open Banking services.
Data minimisation and storage limitation	The principle that personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed, and should be retained only for as long as necessary to fulfil this purpose.
Data ring fencing	A barrier segregating a portion of data from other data.
Data sharing standards	Shared rules prescribing a consistent way of sharing data.
Digital footprint	A unique set of one's traceable digital activities.
Digitally disengaged	Lacking access, skills, confidence or motivation to use digital services.
Futures methodologies	Refers to different approaches to thinking about the future and exploring factors that could give rise to possible and probable future characteristics, events and behaviours. ²⁵
Governance model	A framework outlining the structures and processes for decision making, accountability, control and behaviour within a Smart Data scheme.
Liability framework	A system detailing lines of responsibility between the stakeholders of a Smart Data scheme.
Open Banking	Smart Data scheme within banking. ²⁶
Outcome transparency	Transparency around how the Smart Data products and services generate their outcomes and decisions.

²⁴ ICO Guidance, Consent. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/>

²⁵ Government Office for Science, The Futures Toolkit. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

²⁶ Open Banking Website. Available at: <https://www.openbanking.org.uk/>

Privacy-enhancing technology	Any technical method that protects the privacy or confidentiality of sensitive information. ²⁷
Process transparency	Transparency around how the Smart Data products and services work.
Sandbox environment	Testing environment separate from the production environment that enables approved participants to build an understanding of tools, standards and security requirements.
Scenario planning	A futures methodology that allows practitioners to think expansively about the different plausible futures that could emerge. ²⁸
Scheme scope	A set of regulations and standards that define the allowed range of use cases within a scheme and the data that will be allowed to be used.
SME	Small and medium-sized enterprises.
Technical infrastructure	The set of IT components forming the foundation of an IT service, including hardware, software and network components.
Use case	The uses of a Smart Data scheme in a practical setting. This could include services like displaying multiple accounts in one place, or automated switching services.

²⁷ The Centre for Data Ethics and Innovation, What are PETs? Available at: <https://cdeiuk.github.io/pets-adoption-guide/what-are-pets/>

²⁸ Government Office for Science, The Futures Toolkit. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

Appendix 2: Envisioning Smart Data in 2028

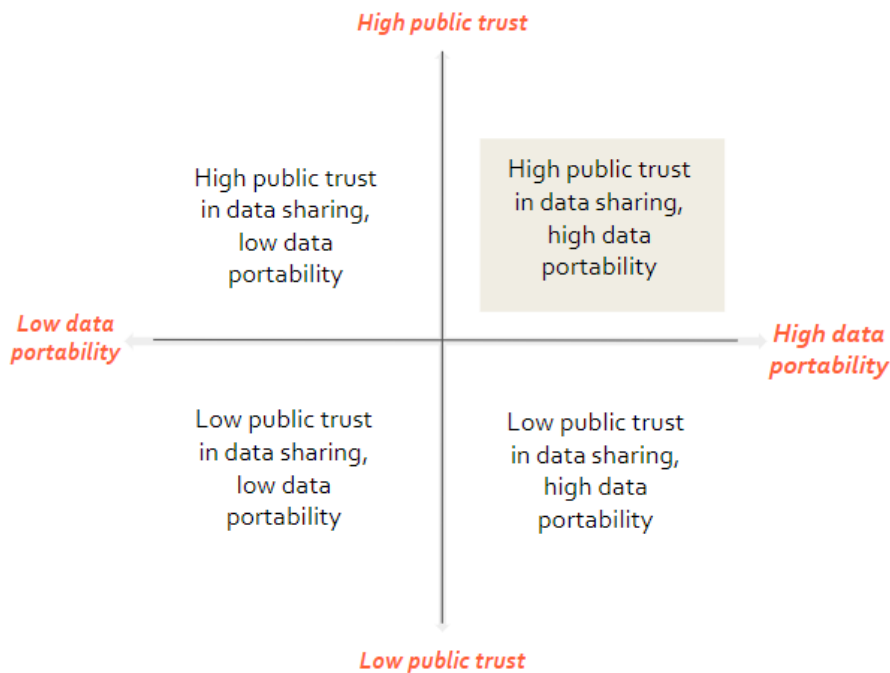


Image description: A two-dimensional graph in which the X-axis represents a spectrum of data portability and the Y-axis represents a spectrum of public trust. The best-case scenarios envisioned in the CDEI's scenario planning workshop are those in the top-right quadrant: high public trust in data sharing and high data portability.

Participants in our Phase 2 workshop highlighted that in the best case scenario of high public trust and high data portability:

1. Consumers would feel they are in control of their data. They would be well-informed about their rights, how their data is being used, and see the benefit of sharing data.
2. There would be robust regulation in place to prevent misconduct on the part of data holders and/or Authorised Third Parties.
3. Participation in Smart Data schemes would be mandatory for data holders and underpinned by common data standards and APIs.
4. The innovation ecosystem would be driven by inclusive and socially beneficial Smart Data applications, addressing unmet needs among consumers.

Appendix 3: Governing Bodies' Checklists

This pack collates our checklists for Governing Bodies across the lifecycle of several features of ethical and trustworthy Smart Data schemes. These are features that the majority of consumers who participated in our focus groups identified as not being given enough attention: Clear Purpose, Fair Outcomes, Function as Intended, and Accountability.

This guidance includes more information about these features, including more contextual and definitional information, and similar guidance for other stakeholder groups.

It also considers four additional features: Societal Benefits, Transparency, Security, and Privacy.

Clear Purpose – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Are there established goals for the Smart Data scheme? If not, have you considered who is responsible for developing these goals, and anticipating potential use cases?
- Have you mapped out the personal and other information necessary for the scheme, and ensured its sharing and processing will be in accordance with data protection legislation?
- Have potential participants been consulted and engaged whilst determining the above?
- Have you taken learnings from existing schemes into account?
- Where it exists, have you taken learnings from accepted international best practice relating to schemes in your sector?

Further Considerations:

- Have you fully explored the potential lessons from other Smart Data schemes when it comes to establishing the principles for defining, and communicating, the purpose of the scheme to consumers?
- Have you referred to the ICO's guidance on "What is personal data?"²⁹
- Could there be a lawful basis for the processing or sharing of personal data that does not rely on consent? (See the ICO's guidance)
- Have you considered how cross-sector use cases might be incorporated into the design of your scheme?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

²⁹ ICO Guidance, What is Personal Data? Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

- Have you determined what scope and standards (both surrounding potential use cases and data used) will be necessary to ensure the goals of the scheme are achieved?
- Have you considered how data holders and/or Authorised Third Parties should ensure that consumers understand the scope of the services they are using?
- Have you ensured there is enough representation of consumers and SMEs within the governing structure of the scheme?
- Have potential participants been consulted and engaged whilst determining the above?

Further Considerations:

- Have you assessed the trade-offs between creating firmer scope as to how data can be used/what data is used, and the scope for more innovation?
- Have you determined the scope so that it maximises potential for innovation whilst minimising potential harms?
- What risk mitigation practices could be employed to maximise innovation whilst limiting potential harms?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- How are you ensuring consumers adequately understand the scope of the service that they are participating in?

Further Considerations:

- Have you considered whether it is appropriate to allow data holders and Authorised Third Parties to aggregate data shared by consumers for purposes beyond those directly relevant to the consumer's use case?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Do consumers understand what they are agreeing to in terms of how their data will be used? Do consumers understand routes to redress if their data is used in a way that is inconsistent with this?
- Is there a clear mechanism for consumers to provide feedback about the quality of the communication they receive about the functioning of the service?

Further Considerations:

- Have you considered how consent mechanisms should operate when there is no single specified use case but multiple purposes for which the data can be shared?
- Have you ensured consumers remain able to opt out?
- Have you considered whether further uses of the data are justified by serving the public interest/societal well-being?
- Would a mechanism that allowed consumers to track how their data is being used be helpful?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do consumers understand what they are agreeing to in terms of how their data will be used?
- Do consumers understand routes to redress if their data is used in a way that is inconsistent with this?
- Are you monitoring consumer feedback about the services facilitated by the scheme?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?
- Would consent dashboards for consumers, that track use of data, be helpful in giving a holistic view of data use to consumers?

Fair Outcomes – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Have you determined how you will identify which groups face vulnerabilities in your sector?
- What expectations should there be for participating organisations to provide services that support consumers with vulnerabilities?
- Have you considered how to monitor whether bias and unfair outcomes are emerging in a scheme?
- What requirements for participants need to be put in place for transparency and monitoring to identify bias and unfair outcomes?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you considered, and incorporated, the needs of consumers in vulnerable circumstances into your scheme?
- Have you considered the impacts of the scheme on people with protected characteristics?
- Have you determined what data will be needed within a scheme, and developed safeguards to ensure unnecessary data will not be used?
- Have you identified potential unfair outcomes for consumers and considered safeguards that will help minimise the risk of these occurring?

Further Considerations:

- Have you considered if participating organisations in the scheme should be required to ring fence elements of participant's data, to ensure only appropriate data is used?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you reviewed the standards in light of initial feedback and testing?
- Have you tested if bias and unfair outcomes are emerging within the scheme?
- Have you incorporated the insights of representatives of vulnerable customers in the above?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are you in dialogue with consumer groups to review and update the standards to prevent negative impact of the scheme on consumers in vulnerable circumstances?
- Are you continuously reviewing and updating the standards of the scheme to ensure fairness of the outcomes for consumers?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are there processes in place for regular dialogue with consumer groups?
- Are there processes in place to update the standards and prevent negative impact of the scheme on consumers in vulnerable circumstances?
- Are there processes in place to review and update the standards of the scheme to ensure fair outcomes for consumers?

Further Considerations:

- Are consumers being engaged when determining if cross-sector data sharing is desirable?
- Are you considering whether encouraging cross sector data sharing would alter which consumers should be considered vulnerable?
- Are you ensuring consumers fully understand the following, particularly given the complexities that cross sector data sharing will add:
 - How their data will be used?
 - Who will use their data?
- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Have you considered what the intended impacts are from the introduction of the Smart Data scheme?
 - Have you considered what consumers will expect the benefits of using a service within the Smart Data scheme to be?
- Are you consulting relevant stakeholders on issues of consent, liability, and data minimisation and storage limitation in Smart Data schemes?
 - Have you considered how other schemes tackle issues of consent, and whether your scheme deviates from common approaches?

Further Considerations:

- Have you considered developing pilot programmes with stakeholders to test issues around consent, liability, and data minimisation and storage limitation?
- Are you considering encouraging/requiring participants to use privacy-enhancing technologies, when appropriate?
- Are you considering encouraging/requiring use of mechanisms that allow a consumer to track how their data is used?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you begun to develop and test a liability framework with stakeholders?
- Have you begun to develop and test data minimisation and storage limitation requirements with stakeholders?
- Have you begun to develop and test how consumers can provide consent to participate?
 - What information should participating organisations be required to give to consumers?
 - How often should re-consenting be required?
 - What should the process for re-consenting be?
 - How do you ensure consumers are aware they can remove consent?
- Have you determined what technical standards are required to ensure safe, smooth transfer of data between organisations?

Voluntary onboarding and testing

Important:

- Have you created clear lines of appropriate responsibility in your liability framework?
- Have you iterated on the liability framework, data minimisation and storage limitation requirements, and consent mechanisms based on feedback from stakeholders?
- Have you determined how long organisations should be allowed to retain shared data?
- Have you determined what measures need to be in place to ensure that information about a person, inferred from data about another consumer, is not shared if they have not consented to sharing it?

Further Considerations:

- Have you tested the liability framework, data minimisation and storage limitation requirements, and consent mechanisms in practice with stakeholders?

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured stakeholders understand:
 - Their legal responsibilities and who is liable for non-compliance?
 - Who is responsible for addressing/ redressing consumer complaints?
 - Their obligations around consent?
 - How to handle consumer data if consent is revoked?
 - Their obligations around data minimisation and storage limitation?
- Have you ensured the above information is readily available, in plain English, to consumers.
- Have you ensured consumers understand their routes to redress?

Further Considerations:

- Have you considered how to handle liability in the event an Authorised Third Party ceases operations? E.g., who is liable for the consumer data an Authorised Third Party holds if it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do you have processes in place to ensure the following information is readily available to consumers:
 - Liability structures within the scheme?
 - Their rights around data minimisation and storage limitation and storage limitation?
 - Their rights around consent and ability to opt out at any time?
- Are you continuing to adapt your liability framework, data minimisation and storage limitation requirements, and consent based on changing use case needs?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Accountability – Governing Bodies

Whilst developing and implementing Smart Data schemes, considerations for governing bodies include:

Setup and planning

Important:

- Are you clear on the roles and responsibilities of your organisation in relation to the Smart Data scheme in question?
 - Where does your organisation fit in the wider governance model for the scheme?
 - What is the timeline for developing and delivering the scheme?

- How will you engage with the wider ecosystem whilst developing the scheme?
- Is it clear to participants who are the controllers and processors of personal data? (see - the ICO's Guidance)³⁰

Further Considerations:

- Have you considered context-specific requirements for your sector?
- Have you considered encouraging data sharing agreements between participating organisations, which would set out their respective responsibilities? (see - The ICO's guidance)³¹

Development and testing

Important:

- Have you developed the standards that will underpin the Smart Data scheme?
 - What guidance will you need to provide to participants to help them meet these standards?
- Have you considered whether data holders should be mandated to participate in your Smart Data scheme?
- Have you engaged with the wider ecosystem whilst determining the above?

Further Considerations:

- Have you provided additional guidance for participants beyond that on Mandatory standards? (For example, like the Conditional, and Optional standards employed in Open Banking)
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested the standards and guidance with potential participants of the schemes, and amended them accordingly?
- Have you developed codes of conduct for relevant organisations?
- Are participating organisations aware of their responsibilities to consumers and the penalties for non-compliance?
- Are the roles and responsibilities of all the different actors in the scheme (including your own) easily accessible and in plain English?

Further Considerations:

- Have you considered context-specific requirements for your sector?
- Have you considered referring participating organisations to the ICO approved codes of conduct³²?

Onboarding and services and services go live

³⁰ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

³¹ ICO Guidance, Data Sharing Agreements. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/>

³² ICO Guidance, Codes of Conduct. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/>

Important:

- Have you provided sufficient guidance and engagement to participating organisations to enable them to adhere to the standards of your scheme?
- Have you ensured that participating organisations communicate clearly about their responsibilities and obligations to consumers?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are there mechanisms in place to alter existing standards and guidance in the scheme if necessary?
- Are you monitoring whether an alternative governance model might be more appropriate now the scheme is fully live?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Appendix 4: Regulators' Checklist Collection

This pack collates our checklists for Regulators across the lifecycle of several features of ethical and trustworthy Smart Data schemes. These are features that the majority of consumers who participated in our focus groups identified as not being given enough attention: Clear Purpose, Fair Outcomes, Function as Intended, and Accountability.

This guidance includes more information about these features, including more contextual and definitional information, and similar guidance for other stakeholder groups.

It also considers four additional features: Societal Benefits, Transparency, Security, and Privacy.

Clear Purpose – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Are there established goals for the Smart Data scheme? If not, have you considered who is responsible for developing these goals, and anticipating potential use cases?
 - Have you considered what governance model will best enable these goals, and what the role of a regulator/regulators should be?
- Have you mapped out the personal and other information necessary for the scheme, ensuring that its sharing and processing will be in accordance with data protection legislation?
- Have relevant stakeholders been consulted and engaged whilst determining the above?

Further Considerations:

- Have you referred to the ICO's guidance on "What is personal data?"
- Could there be a lawful basis for the processing or sharing of personal data that does not rely on consent? (See the ICO's guidance)
- Have you considered how cross-sector use cases might be incorporated into the design of your scheme?
- Are you engaging with regulators from other sectors to enable cross-sector data sharing?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you considered the scope (around potential use cases and data used) that will be necessary to ensure the goals of the scheme are achieved?
- Have you ensured you have sufficient powers, capacity, and systems to enforce this scope?

- Have you considered what is the appropriate level of monitoring, at the scheme, architecture and consumer outcome levels, to ensure that a scheme, and its participants, are operating within this scope?
- Have potential participants been consulted and engaged whilst determining the above?

Further Considerations:

- Have you assessed the trade offs between creating narrower scope as to how data can be used/what data is used, and the potential for more innovation?
 - Have you determined the scope that would maximise potential for innovation whilst minimising potential harms?
 - What risk mitigation practices could be employed to maximise innovation whilst limiting potential harms?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested whether the proposed scope is having the intended effects?
- Have participants been given the opportunity to feed back on the scope that is being tested?

Further Considerations:

- Have you considered if regulatory sandbox environments would aid the responsible development of use cases in this space?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you checked the scheme's scope is having the intended effects?
- Have you checked that the anticipated use cases are able to develop and operate within the scheme's scope?
- Are you ensuring participants in the scheme are operating within the scheme's scope?
- Have you ensured consumers understand the scope of their data's use and their routes to redress if this is breached?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you checking that the scope of the scheme is having the intended effects?
 - Are you checking that the anticipated use cases are able to develop and operate within the scope of the scheme?
 - Are you ensuring participants in the scheme are operating within the scheme's scope?

- Are you ensuring consumers understand the scope of the use of their data and their routes to redress if this scope is breached?
- Do structures exist to monitor if the scope of the scheme needs modifying, and to carry out this modification?

Further Considerations:

- Are you considering what safeguards would be necessary to enable cross-sector data sharing?
 - Are you considering which organisation/organisations would be responsible for regulating cross-sector Smart Data sharing?
- Are you continuing to consider context-specific requirements for your sector?

Fair Outcomes – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you considered what protections and processes should be in place at the regulator, governing body and service level and communicated these to consumers and participants?
- Have you determined scope such that it maximises potential for innovation whilst minimising potential harms?
- Have you consulted consumers in vulnerable circumstances, or groups that represent them?

Further Considerations:

- Have you considered how to ensure that allowing cross-sector data sharing will not result in data dominance by specific organisations?
- Have you determined whether standardised formats for data, and cross-sector accreditation, will be needed to ensure interoperability across different sectors?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you provided input into the governing body's considerations around:
 - Ensuring fair outcomes for all consumers?
 - Consumers with vulnerabilities?
- Have you established a mechanism for monitoring the fairness of outcomes for different consumers?
- Have you established a mechanism for monitoring that the data shared and used is handled by the participants of the scheme as per the intended purpose?

Further Considerations:

- Have you considered whether requiring ring fencing of particular elements of data would help to protect consumers in vulnerable circumstances?

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you determined, and communicated, what enforcement actions will be taken if participants act outside of the scheme's scope?
- Have you developed routes to redress in situations where the scheme participants are using the data for purposes other than the intended purpose, or in a manner that perpetuates bias or causes unfair treatment towards groups with vulnerabilities?

Further Considerations:

- Is there clear guidance for consumers and services on the expectations for how complaints should be submitted and handled?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured the enforcement measures are preventing participants from violating the scheme's scope?
- Have you tested the routes to redress in situations where the scheme participants are using the data for purposes other than the intended purpose, or in a manner that perpetuates bias or causes unfair treatment towards groups with vulnerabilities?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring the participants in the scheme to make sure that the services they offer are competitive and that there is no concentration of data in the hands of a few Authorised Third Parties?
- Are you monitoring for other competition-related impacts that could arise from the dominance of a small number of Authorised Third Parties?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you considered what the intended impacts of introducing the Smart Data scheme are for consumers and the sector?

- Have you considered what consumers will expect the benefits of participating in the scheme to be?
- Have you determined what stakeholder groups (e.g., consumers, consumer groups, data holders, Authorised Third Parties, etc.) you should be engaging throughout the process and when you should be engaging them?
- Have you determined the appropriate level of monitoring, at the scheme, architecture, and consumer outcome levels, to ensure that a scheme is operating as intended?
- Have you determined the primary use cases and intended benefits of the scheme? How will you determine if these impacts are being met?

Further Considerations:

- Have you considered context-specific requirements for your sector? (E.g., Would consumers expect services to perform differently between the finance and energy sectors)?

Development and testing

Important:

- Have you tested the following with relevant stakeholders:
 - What rules and regulations are needed for the scheme to deliver on consumer expectations?
 - What would constitute a service provider securing consent from a consumer?
 - How compliance with data standards will be enforced
 - What an appropriate level of monitoring for the scheme would be?
- Have you considered how regulations that already exist (for example, those around data sharing standards) would impact your scheme?

Further Considerations:

- Have you engaged with stakeholders on how to implement consent mechanisms?
- Have you engaged with stakeholders to gain their opinions on proposed data sharing standards?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you ensured stakeholders are aware, in plain English, of their legal responsibilities around consent?
- Are you, and stakeholder, testing a variety of approaches to ensure consumers are made aware of their rights around data sharing and consent?
- Have you determined how compliance with consent requirements and data sharing standards should be monitored?
- Have you created measures to ensure data holders/Authorised Third Parties comply with legal requirements?

Further Considerations:

- Have you considered how consumers are informed of their data rights in other data sharing schemes?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you acted upon the lessons learned during the development and testing phase around consent/data sharing standards/appropriate levels of monitoring?

Further Considerations:

- Have you gathered input from stakeholders, particularly consumers, in the development and voluntary onboarding phases?
- Have you considered how to handle liability in the event an Authorised Third Party ceases operations? E.g., who is liable for the consumer data an Authorised Third Party holds when it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring data holders/Authorised Third Parties for compliance with consent standards?
- Are you monitoring data holders/Authorised Third Parties for compliance with data standards?
- Are you regularly assessing whether the data sharing standards are appropriate for the ecosystem and revising regulations as appropriate?
- Are you regularly assessing whether the consent mechanisms are appropriate for the ecosystem and revising regulations as appropriate?
- Are you monitoring consumer complaints to identify systemic issues within the scheme?

Further Considerations:

- Are two-way routes of communication open with consumers, particularly with respect to liability structures?
- Are you continuing to consider context-specific requirements for your sector?

Accountability – Regulators

Whilst developing and implementing Smart Data schemes, considerations for regulators include:

Setup and planning

Important:

- Have you determined who will be responsible for establishing the standards that participants in a scheme must adhere to?
- Have you determined what type of oversight any Governing Bodies within your sector will require?
- Is it clear to participants who are the controllers and processors of personal data? (see - the ICO's Guidance)³³

³³ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

- Have you communicated to "controllers" that they must have appropriate contacts in place with processors in accordance with Article 28 UK GDPR?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you determined what structures are necessary to ensure that the standards of the scheme, and the responsibilities of the participants, are adhered to?
- Have you considered whether participants in your Smart Data scheme require accreditation?
 - Are you consulting to establish the requirements and responsibilities involved in accrediting services?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you determined lines of accountability for roles across the scheme?
- Have you tested the mechanisms established to ensure the compliance of participating organisations?
- Have you communicated to consumers the role that you as a regulator play within a scheme?
- Are sufficient numbers of organisations passing the accreditation requirements?

Further Considerations:

- Have you considered context-specific requirements for your sector?
- What would be a reasonable number of participating/accredited organisations?

Onboarding and services and services go live

Important:

- Are the mechanisms that ensure the compliance of participants fit for purpose and delivering the expected results?
- If implemented, have you checked if the accreditation requirements are allowing for a vibrant marketplace of offerings to emerge in a safe, controlled manner?
 - Are accreditation requirements posing additional burdens on participants operating across sectors?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are the mechanisms that ensure the compliance of participants performing as expected?

Further Considerations:

- If cross sector data sharing is a consideration, will multiple regulators' jurisdictions cover a scheme?
 - If yes, what will be necessary for collaboration between the organisations?
- Are you continuing to consider context-specific requirements for your sector?

Appendix 5: Authorised Third Parties' Checklist Collection

This pack collates our checklists for Authorised Third Parties across the lifecycle of several features of ethical and trustworthy Smart Data schemes. These are features that the majority of consumers who participated in our focus groups identified as not being given enough attention: Clear Purpose, Fair Outcomes, Function as Intended, and Accountability.

This guidance includes more information about these features, including more contextual and definitional information, and similar guidance for other stakeholder groups.

It also considers four additional features: Societal Benefits, Transparency, Security, and Privacy.

Clear Purpose – Authorised Third Parties

Whilst developing and implementing Smart Data schemes, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with the authorities responsible for establishing the scope of the Smart Data scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you ensured the service you are aiming to provide is fully within the scope of the scheme?
- Have you ensured you have adequate internal governance structures to make sure you comply with the relevant regulatory requirements?
- Have you ensured you have sufficient structures, resources, and systems to make sure that your service operates within the scope of the scheme?
- Have you determined how you are going to communicate the benefits of your service, and the purpose of data processing, with your consumers to enable the gathering consent?
- Have you collected feedback from the consumers to ensure you are clearly communicating the above?

Further Considerations:

- Have you tested a process for the gathering of consumer feedback to understand whether you communicate the purpose and benefits of your service in an easily understandable manner?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you ensured the scope of the service you provide is fully within the scope of the scheme as intended?
- Have you collected feedback from consumers to ensure they understand the purpose of data processing and the benefits of the service you provide?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Does the live service remain fully within the intended scope of the scheme?
- Have you adequately communicated to consumers what elements of their data are being used, how they are used, and the purpose of and limits to this use? (e.g., In simple English, easy to understand, and a standardised format).

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring the service you provide is fully within the scope of the scheme?
- Are you actively reviewing how you communicate to consumers what elements of their data are being used, how it is used, and the purpose of and limits to this use? (e.g., this should be in simple English, easy to understand, and a standardised format)?
- Do you have structures in place to respond to unexpected data sharing beyond the scope of the scheme?

Further Considerations:

- Are you collecting consumer feedback to ensure that any new information about your service does not diminish the level of understanding of its benefits and purpose?
- Are you continuing to consider context-specific requirements for your sector?

Fair Outcomes – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you created structures that allow consumers to flag when they face vulnerable circumstances?
- Have you considered the needs of consumers in vulnerable circumstances/with protected characteristics when designing your service?
- Have you considered how you will monitor your service to make sure that it treats consumers fairly?
- Have you designed communications to explain to your consumers what their data is being used for and how it contributes to the operation of the service?
- Have you tested the processes, workflows and other elements making up your service to ensure that any unfair biases are identified?

Further Considerations:

- Have you determined how to ensure that you are only using relevant pieces of a consumer's data for a given use case?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you validated that your service meets the requirements of consumers in vulnerable circumstances?
- Do you have structures in place to alter your service if issues are identified that your service is not meeting?
- Have you tested that your communications strategy will enable consumers to feedback about whether they understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Do you have a feedback process in place to monitor the following:
 - Outcomes, ensuring that certain groups are not disproportionately disadvantaged?
 - That your service meets the requirements of consumers in vulnerable circumstances?
 - Whether consumers understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Do you have processes in place to make sure that your service treats consumers fairly? Have you defined metrics to track your performance?
- Are you monitoring the following:
 - Whether your service delivers fair outcomes across the population?
 - Whether your service meets the requirements of consumers in vulnerable circumstances?
 - Whether the consumers understand how their data is being used and how it contributes to the operation of the service?

Further Considerations:

- Do you have processes in place to review whether you are using only necessary elements of a consumer's data?
- Are you continuing to consider context-specific requirements for your sector?

Function as Intended – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with and contributed to consultations by the relevant authorities designing and overseeing the development of the scheme?
- Have you mapped out the personal and other information necessary for your services, ensuring its sharing and processing will be in accordance with data protection legislation?
- Have you carried out a Data Protection Impact Assessment³⁴ to identify and mitigate the risks of the planned data processing?

Further Considerations:

- Are you engaging with regulators/governing bodies on the liability framework, requirements, and consent mechanisms in the Smart Data scheme?
- Have you referred to the ICO's guidance on "What is personal data?"³⁵
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Do you have systems in place to ensure that data is held for the minimum amount of time necessary?
- Have you tested different approaches to how you secure consent from consumers for your use cases?

³⁴ ICO Guidance, Data Protection Impact Assessments. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

³⁵ ICO Guidance, What is Personal Data? Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>

Further Considerations:

- Have you considered using, or encouraging data holders, to use privacy-enhancing technologies and other forms of data sharing technology aimed at reducing risk?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you provided input and feedback to governing bodies/regulators on liability frameworks, requirements, and consent mechanisms?
- Have you incorporated feedback from consumers on your approaches to gathering consent?

Further Considerations:

- Have you been involved in providing feedback on the liability framework, requirements, and consent mechanisms in practice with other stakeholders?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are you aware of your legal responsibilities and liabilities for non-compliance?
- Is there a clear process for receiving, addressing and where necessary escalating consumer complaints?
- Are there responsible owners for handling complaints in your organisation?
- Are you aware of your obligations around consent? Are you aware of how you handle consumer data if consent is revoked?
- Are you aware of your liability for data shared onwards to other Authorised Third Parties and how they use it?
- Have you communicated liability structures and redress mechanisms in plain English and in a way that is easily accessible to consumers?

Further Considerations:

- Have you considered how to handle liability in the event you fold? E.g., who is liable for the consumer data you hold when your company stops operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring you are communicating all necessary information to consumers when requesting consent?
- Are you ensuring it is clear to consumers how they can withdraw consent?
- Are you communicating liability structures and redress mechanisms to your consumers?
- Are you continuing to revisit your practices based on changing use cases?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Accountability – Authorised Third Parties

Whilst developing and implementing Smart Data solutions, considerations for Authorised Third Parties include:

Setup and planning

Important:

- Have you engaged with and contributed to consultations by the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you determined what internal governance structures will be necessary to ensure you comply with the relevant legislation?
- Have you considered how to communicate a consumer's rights and routes to redress to them?
- Have you, as data controllers³⁶, ensured you have appropriate contacts in place with data processors³⁷ in accordance with Article 28 of the UK GDPR

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you tested that your internal governance structures will ensure that you comply with the relevant legislation?
- Have you tested that the way you communicate to consumers their rights and their routes to redress in the event of a problem is working?
- Have you ensured you are complying with the Privacy and Electronic Communications Regulations³⁸, and the consumer's right to object³⁹ to direct marketing?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

³⁶ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

³⁷ ICO Guidance, Controllers and Processors. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>

³⁸ ICO Guidance, What are PECR? Available at: <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>

³⁹ ICO Guidance, Right to Object. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

- Are your internal governance structures successfully ensuring that you comply with the relevant legislation?
- Are you actively communicating to consumers their rights and their routes to redress in the event of a problem.

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you monitoring if you need to modify internal governance structures to enable you to comply with changing legislation?
- Are you monitoring to ensure the way you communicate to consumers their rights and their routes to redress are working?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Appendix 6: Data Holders' Checklist Collection

This pack collates our checklists for Data Holders across the lifecycle of several features of ethical and trustworthy Smart Data schemes. These are features that the majority of consumers who participated in our focus groups identified as not being given enough attention: Function as Intended and Accountability.

This guidance includes more information about these features, including more contextual and definitional information, and similar guidance for other stakeholder groups.

It also considers additional features: Clear Purpose, Fair Outcomes, Societal Benefits, Transparency, Security, and Privacy.

Function as Intended – Data Holders

Whilst developing and implementing Smart Data infrastructure, considerations for data holders include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?
- Have you input into discussions around the types of business data necessary to realise successful services within the scheme?

Further Considerations:

- Are you engaging with regulators/governing bodies on the liability framework, requirements, and consent mechanisms in Smart Data schemes?
- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you established how you will ensure that a consumer has meaningfully consented to their data being shared?
 - What actions will be necessary if a consumer withdraws their consent?
- Have you considered what data sharing architecture is needed to facilitate data sharing with Authorised Third Parties in a timely and reliable manner (incl. business/commercial data)?
 - How do you ensure that you only share data about a consumer required for a particular use case?
 - How do you determine what data is necessary for a specific use case?

Further Considerations:

- Have systems been put in place to ensure that data is held for the minimum amount of time necessary?
- Have you tested different approaches to how Authorised Third Parties could get consent from consumers?

- Have you considered using or encouraging Authorised Third Parties to use privacy-enhancing technologies?
- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Have you established mechanisms to test whether your data sharing architecture is performing as intended?
- Have you tested your data sharing infrastructure/architecture and its performance? (E.g., is it sharing the minimal amount of data? required? Is it working efficiently?)

Further Considerations:

- Have you provided input and feedback to governing bodies/regulators on liability frameworks, requirements, and consent?
- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Have you ensured your data sharing architecture is operating as intended? Are you monitoring its performance and rectifying issues where they arise?
- Are you aware of your legal responsibilities and liabilities for non-compliance?
- Are there individuals who are responsible for addressing/redressing consumer complaints in your organisation?
- Have you communicated liability structures and redress mechanisms to your consumers?

Further Considerations:

- Have you considered how to handle liability in the event that an Authorised Third Party folds? E.g., who is liable for the consumer data that an Authorised Third Party holds if it ceases operating?
- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are you ensuring your data sharing architecture is operating as intended?
- Are you ensuring it is clear to consumers how they can withdraw consent?
- Are you communicating liability structures and redress mechanisms to your consumers?
- Are you continuing to revisit your practices as use cases evolve?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Accountability – Data Holders

Whilst developing and implementing Smart Data infrastructure, considerations for data holders include:

Setup and planning

Important:

- Have you provided your perspective to the relevant authorities designing and overseeing the development of the scheme?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Development and testing

Important:

- Have you created the necessary internal governance structures to ensure you comply with the relevant legislation?
- Have you developed clear lines of internal responsibility about who has what responsibility in relation to Smart Data sharing?
- Have you determined how you will communicate a consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Voluntary onboarding and testing

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?
- Are you actively communicating consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Onboarding and services and services go live

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?
- Are you actively communicating consumer's rights and routes to redress to them?

Further Considerations:

- Have you considered context-specific requirements for your sector?

Transitioning to BAU

Important:

- Are your internal governance structures operating as intended?
- Are your internal governance activities recorded end-to-end to ensure auditability?
- Are you actively communicating consumer's rights and routes to redress to them?
- Are you modifying your service to prevent issues from reoccurring when they emerge?

Further Considerations:

- Are you continuing to consider context-specific requirements for your sector?

Lectus convallis consequat eget in ante. In quis ornare eros, in vestibulum felis. Sed volutpat, lectus et maximus hendrerit, nunc mauris eleifend quam, lobortis porta ligula dui eget sapien. Donec dignissim dictum magna. Nunc dignissim justo vitae quam consequat, at maximus mi rutrum. Vestibulum sit amet justo varius, iaculis justo eu, luctus enim. Nullam a tristique purus. Praesent sit amet dui id lectus scelerisque tempus ac ullamcorpe.

Legal disclaimer

Whereas 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, and no warranty is given or responsibility accepted as to the standing of any individual, firm, company or other organisation mentioned.

Copyright

© Crown Copyright 2023

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@trade.gov.uk.