

Smart Data Working Group

Spring 2021 report



© Crown copyright 2021

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at: smartdatareview@beis.gov.uk

Contents

roieword	ວ
Summary	7
Introduction	9
Part 1: Update on Smart Data schemes and background information	11
Sectoral schemes	11
Smart Data benefits	12
Open Banking	13
Potential benefits in regulated sectors	13
UK business and innovation	
Use cases	15
Cross sector use cases	16
Vulnerable consumers	17
The customer journey	17
Common challenges	19
Smart Data activities	20
Part 2: Proposals for the delivery of Smart Data schemes	23
Cross-sector coordination	23
Coordination of Smart Data activities	24
Institutional options	25
Part 3: Links with wider work and next steps	31
Links with wider work	31
The National Data Strategy	
Digital Identity	31
Digital markets	32
Centre for Data Ethics (CDEI) and Open Data Institute (ODI)	32
Roadmap for Smart Data	33
Next steps for BEIS	33
Next steps for working group and members	33
Annex 1: Invitation for further feedback	35
Annex 2: Definitions	37

Annex 3: Objectives for Smart Data schemes	43
Accreditation of TPPs	43
User authentication	45
User consent	48
Liability framework	50
Annex 4: Use cases underpinning the customer journey	54
Customer journey	54

Foreword

In a time of change, challenge and opportunity, data is playing an increasingly important role in all our lives. By removing barriers to responsible data sharing and use, we aim to become the world's number one data destination: an open, welcoming, and secure environment where companies from all over the world can innovate and grow, and where data improves life for people across the UK. Unlocking the power of data is one of our 10 tech priorities to build back better, safer and stronger from Covid-19, shaping a new golden age for tech in the UK. We need to harness the potential that data holds, to save consumers and businesses time and money, and reduce barriers for smaller innovative businesses to enter and succeed in markets.

In September last year we published the National Data Strategy, setting out the framework for action this government will take on data. Mission one of the National Data Strategy, to unlock the value of data across the economy, sets out how we will complement our high data protection standards by creating an environment where data is appropriately usable, accessible and available across the economy, fuelling growth in organisations large and small.

The National Data Strategy highlighted Smart Data as a key initiative that would support the delivery of this mission and help us to realise the opportunity at hand. With your permission Smart Data could allow you, as a business or consumer, to enable trusted third parties to help you access, make sense of and use your data. This can help you streamline everyday tasks, reduce admin and choose the deals best suited to your needs. Not only will this improve consumer outcomes, but also reduce barriers to entry, enable innovation, and support fair competition across all markets involved.

Open Banking continues to demonstrate the value Smart Data can bring, with the number of users rapidly rising from 2 million last September to now over 3 million consumers and small and medium-sized enterprises (SMEs). As a direct response to Covid-19, many SMEs are saving time and money by using Open Banking for cloud accounting, cashflow forecasting and to access alternative credit providers. Meanwhile consumers increasingly use Open Banking to simplify and accelerate housing affordability checks, receive targeted debt advice and for many other services.

The UK has been world leading in Open Banking, supported by our FinTech sector which annually contributes £11 billion to the UK economy. As other countries develop equivalent schemes, we need to work together to maximise the benefits of Open Banking across further sectors, ensuring UK businesses can continue to grow and compete internationally. The Kalifa Review of UK FinTech further highlights this potential and the opportunity to enable innovations spanning multiple sectors.

We have committed to introduce primary legislation, as soon as parliamentary time allows, extending the government's powers to mandate participation in Smart Data schemes. That means the potential for more consumers and SMEs across more sectors able to take advantage of the benefits of data sharing similar to those already being delivered by Open Banking. As we work towards this, we continue to work together across government and

beyond to promote, support, and accelerate innovations which will make data more accessible and useful for consumers and businesses. For example, we are considering how we can better support Privacy Enhancing Technologies, which can help drive the value from data whilst protecting privacy, and we are conducting research to consider how wider incentives can support data sharing beyond the Smart Data programme.

Today's publication provides an update on the progress made by the cross-sector Smart Data working group and we would like to thank all working group members for their contributions to date. There remains a lot of important work to do, and we would welcome involvement and feedback on the suggestions for cross-sector coordination set out in this report.

As a government we will continue to support Smart Data schemes as they develop in individual sectors. Beyond this, we are committed to enable better cross-sector innovations and efficiencies to emerge, supported by a vibrant and engaging cross-sector ecosystem.





Paul Scully MP

Minister for Small Business,

Consumers and

Labour Markets

BEIS



Keni budenouh

Kemi Badenoch MP

Exchequer Secretary

HM Treasury





Rt Hon John Whittingdale OBE MP

Minister for Media and Data

DCMS



Matt Warman MP

Minister for Digital Infrastructure

DCMS

Summary

- Smart Data is the secure sharing of customer data with authorised third-party providers (TPPs), upon the customer's request. These providers then use this data to provide innovative services for the consumer or business user, such as automatic switching or better account management.
- The Smart Data working group was announced in the Next steps for Smart Data report, to progress Smart Data initiatives, reduce duplication and maximise the combined potential of these initiatives. This update report was written by BEIS, with the support and input of the working group. A list of working group members can be found in paragraph 12.
- 3 There are three parts to this report:
 - Part 1 updates on the potential benefits and use cases of Smart Data in banking, finance, communications, and energy. It also explores the activities and challenges required throughout the Smart Data customer journey.
 - Part 2 sets out practical proposals for cross-sector coordination and poses questions to help inform future policy development.
 - Part 3 explains the links between Smart Data and wider work and sets out the roadmap for Smart Data beyond this report and ahead of legislation.
- Working with the Smart Data working group, we have identified four key principles that should inform the design of cross-sector coordination and collaboration. These are:
 - **Sectors working together** bringing together all bodies leading sectoral delivery of Smart Data with industry and government to enable coordination.
 - **Develop the Smart Data ecosystem** sharing information and drawing on shared expertise to tackle common challenges and support cross-sector innovation.
 - **Enable interoperability** to address barriers to competition and realise Smart Data benefits for consumers and businesses.
 - Inform the ongoing development of the Smart Data framework ensuring the
 ecosystem remains responsive to changing user attitudes and technological
 developments will be important. Pooling research and findings to develop a cross-sector
 picture of adoption, attitudes and capabilities will provide an opportunity to identify and
 consider emerging opportunities and challenges.
- Further work is required to pinpoint specific areas of coordination and where coordinated activities within Smart Data should sit.
- 6 Current governance arrangements enable Smart Data initiatives to develop independently of one another, with BEIS responsible for Smart Data policy coordination. In this report we propose three different options for evolving the current cross-sector

working group arrangements, in the form of a coordinating layer, to create greater opportunities for cross-sector coordination. These options include:

- Extending the duration of the existing Smart Data cross-sector working group as a forum for meaningful discussion, primarily between government departments and regulators on cross-sector issues. This option is the least resource intense and least coordinated approach.
- Establish a cross-sector Smart Data Council building a voluntary, non-statutory council with a wide cross-sector membership. This would provide an opportunity to involve a cross-section of industry, consumer interests and technical experts.
- Establish a Board to lead a Smart Data Council providing government with advice and recommendations on cross-sector issues. This is the most resource intensive, but would achieve the greatest level of coordination.
- We are seeking feedback on the above proposals and on the outputs that should be delivered by this cross-sector arrangement. Initial feedback from stakeholders suggests a stronger interest in a Smart Data Council, but we wish to gather wider stakeholder views.
- Please send all feedback by 23.59 pm 30 July 2021. Responses can be sent via email: smartdata@beis.gov.uk or via Citizen Space.
- 9 Next steps:
 - BEIS will continue to work towards Smart Data primary legislation, introducing when parliamentary time allows.
 - BEIS will continue to lead the Smart Data working group for at least another 6 months as
 the group continues to share knowledge and lessons learned across initiatives and seek
 wider stakeholder input on areas of cross-sector interest and challenge. The working
 group will support BEIS in delivering a blueprint for a coordinating layer to sit across
 current and future Smart Data initiatives.
 - BEIS will publish an equivalent update report following this 6-month extension to the working group.

Introduction

- 10 Smart Data is the secure sharing of customer data with authorised third-party providers (TPPs), upon the customer's request. These providers then use this data to provide innovative services for the consumer or business user, such as automatic switching or better account management.
- 11 The 2019 Smart Data Review¹ consulted on how best government should support these existing and future schemes. The consultation response² published last September announced the key next steps on cross-sector Smart Data work:
 - primary legislation, when parliamentary time allows, extending the government's powers to mandate participation in Smart Data schemes
 - launch of a cross-sector Smart Data working group to coordinate and accelerate existing Smart Data schemes across regulators and government, focusing initially on communications, energy and finance.
- 12 This report focuses on the activities of the working group and opportunities for further cross-sector coordination, and not the Smart Data legislation. The working group has been pursuing areas of cross-sector interest, set out in this report. Members include the Department for Business, Energy and Industrial Strategy (BEIS), Ofgem, the Department for Digital, Culture, Media and Sport (DCMS), the Department for Work and Pensions (DWP), Ofcom, HM Treasury (HMT), the Financial Conduct Authority (FCA), the Competition and Markets Authority (CMA) and the UK Regulators Network (UKRN). The Information Commissioner's Office (ICO) have attended as observers, while the group has sought engagement and challenge from selected TPPs and expert organisations including the Bank of England, Open Banking Implementation Entity (OBIE), Centre for Data Ethics and Innovation (CDEI) and Open Data Institute (ODI).
- 13 The working group was established to encourage and accelerate Smart Data schemes, reduce duplication, and maximise the combined potential of schemes. Government is playing a coordinating role, rather than directing the policy work of the independent regulators. The aims for the group, as set out in the Terms of Reference³, are to:
 - support the development and delivery of Smart Data infrastructure and standards for the benefit of consumers, particularly vulnerable consumers;
 - where appropriate encourage commonality or consistency of approach across Smart Data schemes to enable interoperability and cross-sector innovations;
 - improve efficiency by reducing duplication across Smart Data schemes and re-using assets or resources from prior Smart Data schemes.

¹ BEIS (Jun' 2019) - "Smart Data: Putting consumers in control of their data and enabling innovation"

² BEIS (Sep' 2020) – "Next steps for Smart Data"

³ BEIS (Sep' 2020) – "Smart Data working group: Terms of reference for the Department for Business, Energy and Industrial Strategy to establish a cross-sector Smart Data working group"

- 14 The Terms of Reference further stated that the Smart Data working group would produce:
 - Updates on the development and timescales of all current and contemplated schemes.
 - Guidance and common resources for existing data portability schemes.
 - Recommendations for existing and future data portability schemes, on areas to standardise across Smart Data schemes in different sectors.
 - Recommendations to BEIS for implementation of interoperable Smart Data schemes which deliver tangible innovations.
- This report provides an update from government on progress made by the working group to date, helping inform the collaborative development of schemes across government, regulators, and industry.

Part 1: Update on Smart Data schemes and background information

Sectoral schemes

- The initial focus of Smart Data has been on specific regulated sectors. This includes finance, energy, communications and pensions. This also links to government's plans to build back better and develop the regulatory system in a way that supports innovation.⁴ However there could be benefits in any sector whereby a user is unable to easily use data held about themselves.
- 17 Smart Data is not a one size fits all policy area, and the sector specific context is key to the design and development of individual schemes. The working group has created a forum for these schemes, enabling resources and lessons learned to be more easily shared as the schemes develop.
- The schemes continue to develop at varying speeds and are at different stages of policy development. The below box provides an update on the schemes of immediate priority to the working group:

Open Banking – following the CMA's Retail Banking Order 2017⁵ which mandated participation for the nine largest payment services providers in GB and NI respectively, the scheme has continued to gain momentum. Open Banking covers current accounts and credit card accounts as well as some savings accounts. The CMA consulted in March 2021 on the future governance of Open Banking and plan to publish a response later this year. Its consultation invited comments on the future oversight of Open Banking, including the role of the FCA and PSR in this.

Open Finance – the FCA recently published a Feedback Statement to their Call for Input on Open Finance. Open Finance covers the extension of Open Banking-like data sharing to other financial products, such as savings, mortgages, consumer credit, investments and insurance. The FCA has committed to work closely with BEIS and HMT to form a view of what work is needed to inform judgments on the feasibility, timing and design of any future legislation relating to Open Finance. It has also committed to support industry schemes that are already underway and any new ones, as part of a phased and proportionate approach to the development of Open Finance.

Open Communications – a scheme for the retail telecoms and pay TV markets, which would enable people and small businesses to tell their communications provider to share information about their services, easily and securely, with TPPs of their choice. Ofcom

⁴ HM Treasury (Mar' 2021) – "Build Back Better: our plan for growth"

⁵ Competition and Markets Authority (Feb' 2017) – "The Retail Banking Market Investigation Order 2017"

⁶ FCA (Mar' 2021) - "Open Finance - feedback statement"

recently published responses received to their Open Communications consultation⁷ which ran from August to November 2020. Ofcom will set out key findings from the consultation next steps in an update publication in summer 2021. Further consultation on proposals to deliver Open Communications will take place before a final decision on implementation is made.

Midata in energy – aims to enable domestic energy customers to easily and securely share their data with trusted TPPs offering innovative services, such as more accurate tariff comparison and informed switching between time of use tariffs⁸. Ofgem has been responsible for delivery since mid-2018, with key developments including user research to establish a clear proof of concept.9 Work on midata has been paused since 2020/21 to ensure alignment with wider programmes which will substantially change the energy data landscape over coming years. This includes the Retail Code Consolidation Significant Code Review in 2021, the Switching Programme, the Market-wide Half-Hourly Settlement programme, the Smart meter roll-out across Great Britain, and the wider work on Smart Data. These programmes will all impact the availability and quality of energy data, which midata could utilise and will facilitate consumers realising value from their data. Ofgem aims to update stakeholders when work on developing midata resumes. 10

Pensions Dashboards – This scheme will enable consumers to view their existing pension pots in one clear, online dashboard format. The Pension Schemes Act 2021 amends the Pensions Act 2004 to create a legislative framework for pensions dashboards which will make it mandatory for pension providers and schemes to connect to pension dashboards. DWP is now leading on this secondary legislation, considering how the scheme should be staged across different type or size of pensions provider. The Money and Pensions Service (MaPS) has established the Pensions Dashboards Programme team to design and implement the infrastructure that will make pensions dashboards work, and separately MaPS are developing their own a public service dashboard. The Pensions Dashboard Programme have developed data standards and are working on design and service standards, and they are beginning the procurement process for the necessary digital architecture that will allow things such as identification services 11.

Smart Data benefits

19 The increase in data mobility as a result of Smart Data and wider government policies is likely to bring significant benefits to UK consumers, businesses and the wider economy. Greater personal data mobility could increase UK GDP by an estimated £27.8 billion in

⁷ Ofcom (Aug' 2020) – "Consultation: Open Communications – Enabling people to share data with innovative services'

⁸ Time of use tariffs - energy tariffs with different prices at different times.

Ofgem (Oct' 2020) – "Midata Discovery and Proof of Concept User Research Findings"
 Ofgem (May 2020) – "Update on midata in energy programme"

¹¹ Pensions Dashboard Programme (Apr' 2021) – "Pensions Dashboard Programme: Progress Update Report"

total, not including the wider contribution from any digital innovations enabled ¹². Smart Data has the potential to help realise this GDP contribution, by enabling consumers to share their data in an easy and secure way.

Open Banking

- Open Banking indicates how and where these benefits could arise. The annual potential benefits from Open Banking enabled services are estimated as £12billion for consumers and £6billion for businesses ¹³. The uptake and benefits from Open Banking have accelerated due to the increased reliance on data during the Covid-19 pandemic, now with 3 million consumers and business users, up from 2 million in September 2020 ¹⁴. A survey of SMEs by OBIE in Q3/Q4 2020 found that over 50% are now using Open Banking-enabled services such as cloud accounting and cash flow forecasting 86% of whom had started doing so due to Covid-19 ¹⁵. The number of regulated providers enrolled into the OBIE ecosystem also grew from just over 200 in January 2020 to over 300 in February 2021 ¹⁶, highlighting the attractive business opportunity and scope for innovative new entrants.
- Following the success of Open Banking in the UK, equivalent schemes are now being developed internationally. The Consumer Data Right (CDR)¹⁷ was introduced by the Australian Government in 2020 and gives consumers greater access to, and control over, their banking data. This is now being extended to cover energy, with telecommunications currently proposed to follow. Further countries such as Canada¹⁸ and Mexico¹⁹ have begun to adopt Open Banking, and other countries such as the Netherlands²⁰ have stated their vision on business-to-business data sharing. UK expertise is already in demand from other jurisdictions as they begin to develop their own Smart Data ecosystems.

Potential benefits in regulated sectors

There are opportunities to extend the benefits and momentum of Smart Data beyond banking. This will build on and support the work that regulators are doing to tackle consumer issues in other regulated markets. For example, Citizens Advice previously estimated that consumers who do not switch or recontract with their provider collectively pay £3.4 billion per year more than other consumers across five essential markets,

¹² Ctrl Shift (2018) - "Data Mobility: The personal data portability growth opportunity for the UK economy"

¹³ OBIE representatives (Jun' 2019): "Consumer Priorities for Open Banking"

¹⁴ Open Banking (Feb' 2021) – "Open Banking Annual Report 2020"

¹⁵ Open Banking (Dec' 2020) – "<u>Adapting to survive: UK's small businesses leverage open banking as part of their COVID-19 crisis recovery"</u>

¹⁶ Open Banking (Feb' 2021) – "Open Banking Annual Report 2020"

¹⁷ Australian Competition & Consumer Commission (Nov' 2017) – "Consumer Data Right (CDR)"

¹⁸ In Canada's 2018 budget it was announced that the government would begin a consultation to review the merits of Open Banking and in June 2019 the Standing Senate Committee on Banking, Trade and Commerce released "Open Banking: What it Means for You", which included a number of recommendations intended to lay the groundwork for the rollout of Open Banking in Canada.

¹⁹ Mexico has largely adopted the UK's Open Banking implementation model. The law regulating <u>Financial</u> <u>Technology Institutions</u> (The FinTech Law) came into effect in March 2018.

²⁰ Government of the Netherlands (Feb' 2019) – "Dutch vision on data sharing between businesses"

- known as the 'loyalty penalty' 21 (including broadly finance and communications 22). The FCA and Ofcom have already announced measures that will save consumers an estimated £630 million and £332 respectively per annum. 23 There is however an opportunity for Smart Data schemes to help reduce this further.
- The FCA, in its Open Finance Call for Input²⁴, posed Open Finance as a potential long-23 term solution to this 'loyalty penalty' and associated low consumer engagement. A number of wider issues which Open Finance could address were identified, including consumer awareness and the high cost of servicing customers.
- Ofcom's consultation on Open Communications²⁵ similarly highlighted a number of 24 potential benefits to Open Communications. This includes reducing the time and effort needed to search for and find a new deal, better suited to the user's needs. Similar to Open Banking, Open Communications is expected to facilitate innovation and drive more effective competition that could lead to better outcomes for consumers and business.

UK business and innovation

- 25 The UK's early adoption of Open Banking has been a key factor in making London a hub for tech ecosystem in producing and attracting investment in 'Fintech Unicorns' 26 second only to the San Francisco Bay Area by number²⁷. Similar FinTech hubs are emerging in other areas of the UK, such as in the West Midlands²⁸. Smart Data provides a further opportunity to extend the UK's tech leadership into wider finance, communications and energy sectors and attract further foreign investment.
- 26 As a global leader in data portability regulation, there is greater scope for regulatory alignment between the UK and other countries. This creates potential for UK businesses with experience in Smart Data schemes to more easily expand internationally and strengthen the UK's global trade policy. Similar effects have been seen with 'Fintech Bridges' established between the UK, Australia, and Singapore²⁹ that intend to boost exports of Fintech services and bolster digital trade. The Kalifa Review of UK FinTech 30 recommends delivering a strong regulatory strategy and international action plan to build a leading position for UK FinTech. Smart Data can help enable this.

²¹ Citizens Advice (Sep', '20): "The loyalty penalty in essential markets: Two years since the super-complaint"

²² Includes: Mobile (£182m), Broadband (£485m), Home insurance (£750m), Cash savings (£1.1bn), and Mortgages (£800m)

²³ Citizen's Advice (Sep' 2020) – "The loyalty penalty in essential markets: two years since the super-complaint"

²⁴ FCA (Dec' 2019) – "Call for Input: Open Finance"

²⁵ Ofcom (Aug' 2020) – "Consultation: Open Communications"

²⁶ FinTech unicorns - new businesses who have obtained a valuation of \$1bn whilst remaining private

 ²⁷ TechNation (June 2019); "<u>Unicorn Update - London Tech Week 2019</u>"
 ²⁸ London Tech Week (Mar' 2021) – "<u>12 Clusters of Tech – West Midlands</u>"

²⁹ Australian Financial Review (June 2020): "Fintech bridge to Singapore in the works to lift digital trade"

³⁰ HM Treasury (Feb' 2021) - "Kalifa Review of UK Fintech"

Use cases

- 27 There are a number of both existing and potential use cases that demonstrate how Smart Data can and will bring value to consumers and businesses. It is important to note that many use cases that have emerged from Open Banking that were not anticipated prior to its implementation. Providing Smart Data as the framework for industry to innovate will likely produce new valuable use cases that are not listed here.
- Open Banking was implemented in 2018 and has the most developed use cases with an active service and user base to draw on. One key Open Banking use case is improving understanding and management of your finances. Start-ups such as Emma³¹ and Yolt³² allow users to view all their bank accounts in one dashboard. Another key use case is streamlining processes related to or requiring banking data. Monzo³³ has removed the need to enter banking credentials when making transfers, Flux³⁴ has eliminated the need for physical receipts and loyalty cards, and Mojo Mortgages³⁵ provides personalised advice on improving a customer's credit score. Open Banking has also provided solutions to businesses as well as consumers. Yapily³⁶ empowers lenders with enriched data to make faster and better lending decisions, and accountancy services Amralytic³⁷ and Circit³⁸ provide secure real time access to client's bank statements so that information can be verified in minutes rather than months.
- Open Finance could encompass and unlock new Smart Data use cases not currently possible under the remit of Open Banking. Holistic personal financial management platforms could provide a better overall financial picture, including data not captured by Open Banking such as certain types of savings and investments. This will help improve consumer engagement and understanding of their financial situation, and help consumers make decisions that better meet their needs. Services that provide an overview of a consumer's financial situation could also reduce the time and effort required for financial advisors to understand a consumer's situation and advise accordingly. Additionally, comparison and switching services could help consumers and businesses maximise the returns on their savings accounts and minimise interest on loan repayments.
- Open Communications could enable multiple services, as outlined by Ofcom in the recent consultation³⁹. Improved and tailored product recommendations could be provided when sharing user's data directly with digital comparison tools and other providers. Account aggregation could provide information about a user's

³¹ Emma

³² Yolt

³³ Monzo

³⁴ Flux

³⁵ Mojo Mortgages

³⁶ Yapily

³⁷ Armalytix

³⁸ Circit

³⁹ Ofcom (Aug' 2020) – "Consultation: Open Communications - Enabling people to share data with innovative services"

telecommunications package (such as contract end dates, their monthly payments etc.) in one place. This could be widened further to include all utilities, for example by including your energy tariff information in the same app interface. Users could benefit from better account management under Open Communications. For example, TPPs with access to user data could notify users when their contract is coming to an end and prompt them to switch or re-contract. Much of the hassle and time spent switching could be reallocated from user to third party.

We would expect similar use cases to emerge form a Smart Data scheme in the energy sector, for example in the **midata** project. Midata would enable price comparison websites to access data directly from the consumers energy provider, rather than requiring consumers to input this information manually. This would provide more accurate energy tariff comparisons, potentially saving consumers money if they previously wrongly estimated their energy usage and save consumers time manually entering details.

Cross sector use cases

- The potential for cross sector use cases is clear in communications and energy, given that services will often aim to provide more accurate service comparisons and could fall under the same utilities bracket in account aggregation use cases. However, the potential for cross sector use cases expands across all the regulated sectors.
- One clear example is holistic money management services. Data from Banking and Finance will be required to budget against income or assess options for finance, however this could be supplemented with data from communications and energy to understand expenditure and prove credit worthiness. Greater access to data would enable TPPs that already exist in banking to extend or improve the service they offer, as well as paving the way for new market entrants.
- Linked to this, the Bank of England identified a potential SME lending use case in their Open Data for SME Finance report⁴⁰. More than 50% of UK SMEs only consider one provider when seeking a loan, with 25% of those put off by the hassle or time taken. SMEs would benefit from the ability to compile all their relevant data to create a 'portable credit file' which can be shared more easily with multiple providers to access more diverse and competitive sources of finance. The ability to access alternative and real time data, including from other sectors, will also allow SMEs with otherwise 'thin' credit files to secure funding.
- A further area of cross sector interest is how Smart Data could support the government's wider environmental priorities and the ten-point plan for a green industrial revolution. ⁴¹ Recently commissioned research has highlighted large potential for Smart Data to support environmental priorities, particularly when extended to include industry data. Example use cases include effective management of carbon footprints in supply

⁴⁰ Bank of England (Mar' 2020) – "Open data for SME finance: what we proposed and what we have learnt"

⁴¹ BEIS and No.10 (Nov' 2020) – "The Ten Point Plan for a Green Industrial Revolution"

chains and apps to help consumers identify the most efficient port to charge their electric vehicle. 'Sustainability capital' is also identified as a priority use case, highlighting that mandatory adoption of Task Force on Climate-related Financial Disclosures data from 2025 will enable Fintech investors to prioritise environmentally sustainable projects across the economy, including TPPs in the Smart Data ecosystem.

Vulnerable consumers

- Smart Data presents a valuable opportunity for services to improve outcomes for consumers who find it more difficult to engage in the markets. This difficulty often arises out of the consumers experiencing some form of vulnerability, which can be physical, emotional, or financial.
- The UKRN have recently published research into vulnerable consumer attitudes towards data sharing ⁴². The key findings indicate that the needs of those who could benefit the most from data sharing are being overlooked; those identified as most vulnerable are also the most open to disclosing and sharing their data in order to get help.
- Open Banking has begun to tackle this issue of vulnerability by generating services targeted at vulnerable consumers. The Open Banking for Good initiative has provided £3 million in funding across 7 businesses ⁴³ for this purpose. Each of the fund winning businesses focus on one of three key vulnerable consumer use cases: income smoothing products, money management products, and products that streamline creating income and expenditure profiles (previously compiled by debt advice charities over the phone).
- 39 Charities and debt advice providers could also use vulnerable consumers data from banking and finance to understand consumers income, and data from energy and communications to understand their regular utility expenditure. This would allow the charity or debt advisor to understand part of a consumer's overall financial position far quicker than current conventional methods and enable more personalised debt advice. The need to develop these services quickly and easily highlights a further argument for interoperable data sharing across sectors.

The customer journey

To work towards the implementation of Smart Data schemes and the realisation of benefits, the working group considered the Smart Data customer journey in more detail. The aim of this work was to identify areas of commonality across sectors, and potential areas for coordination. The group compared several use cases across sectors,

⁴² UKRN (Nov' 2020) - "How can we help you? Working together to support vulnerable consumers"

⁴³ Open Banking for Good - "How OB4G works"

- identifying common stages in the customer journey, common challenges that could arise, and the activities needed to both incentivise and protect against these challenges.
- The exact customer journey will vary between use cases, and there will be nuances in the sectoral frameworks. The broad, common customer journey can be visualised in Figure 1.

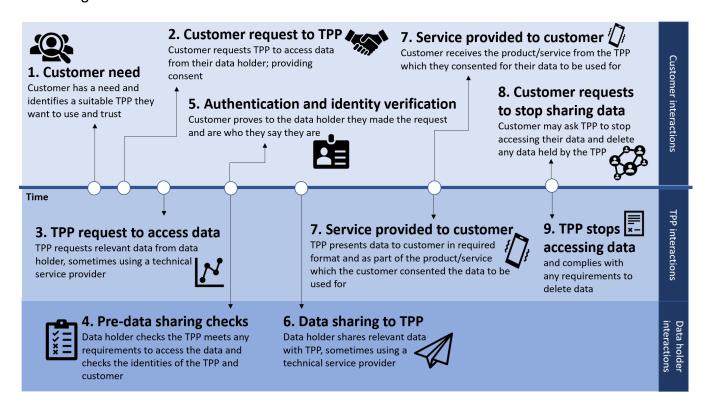


Figure 1: An illustration of the initial stages of the customer journey for Smart Data

- To help understand the customer journey, Annex 2 sets out the working group's agreed definitions to be used across sector examples. This set of definitions was created for use in this report, the cross-sector objectives (annex 3) and future working group publications. The working group separately considered 4 key aspects of the customer journey and developed cross-sector objectives for how they should be taken forward in each sector. The topics include user consent, TPP accreditation, user authentication and liability, and the objectives can be found in Annex 3. These objectives set out what 'good' would look like in regard to these complex topics and provide points that should be considered when designing Smart Data schemes.
- In addition to this, we have commissioned and published research projects looking into accreditation and customer experience guidelines, helping to inform next steps for the working group and sector schemes. 44 Findings from these reports will help inform the development of current and future Smart Data initiatives, while helping shape the direction of the working group. This supplements research into authentication, consent and liability published last September. 45 These research reports have helped inform

⁴⁴ BEIS (Jun' 2021) – "Smart Data: accreditation and customer experience guidelines"

⁴⁵ BEIS (Aug' 2020) – "Smart Data: research on consent, liability and authentication"

policy development for primary legislation and provide a valuable source of information on specific topics of interest to working group members and wider stakeholders. The reports also informed the focus of the working group, for example the need to breakdown the customer journey and the mechanisms needed for trust, the development of cross-sector definitions and common objectives.

Common challenges

- After mapping out the customer journey in more detail, the working group identified that there are common data sharing challenges and a consistent need to protect consumers across sectors. The incentivising and protection activities required to address these challenges were also largely common across sectors. This provides an opportunity for government, regulators and industry to coordinate in finding solutions to these challenges from the outset when designing sector schemes.
- An example of challenges that could be faced at each stage in the customer journey can be seen in figure 2. This is then linked to the incentives and protections needed to manage the risk, and the processes needed to deliver the incentives and protections. The customer journey is explored further in Annex 4, including detail on the use cases considered. This offers a snapshot of the types of challenges that each sector will need to tackle, and the potential activities needed to do so. There are likely sector-specific challenges that schemes will also need to consider but were not in scope of this exercise.

Stage in customer journey	Example of challenge	Example of challenge type ⁴⁶	Examples of incentives and processes needed	Example of protection and processes needed
Customer has a need and identifies suitable TPP	Customer chooses to use accredited TPP that does not meet standard	Communication / information	Accreditation- accreditation provider	Revocation of accreditation if no longer meeting standard - accreditation provider
Customer requests TPP to access data; providing consent	Customer requests to share data they did not want to share due to unclear messaging	Data protection Also a potential communication / information issue	Guidelines for consent messaging - body to issue standards	Revocation of accreditation - accreditation provider

⁴⁶ The Smart Data working group have categorised common data sharing concerns into five non-exclusive risk types: data protection, communication / information, data quality, technical, and user experience.

TPP requests relevant data from data holder	Data holder does not receive the request from TPP	Technical	Technical standards – body to issue standards	Monitoring and enforcing standards
Data holder verifies identities of TPP and customer	Customer decides not to share data as process is long / unclear	User experience Also a potential communication / information issue	User experience guidelines / standards – body to issue standards	Monitoring and enforcing standards
Data holder shares relevant data with TPP	Data holder shares data in the wrong format	Data quality Also a potential data protection risk	Data standards – body to issue standards	Customer redress – complaints management system
TPP presents data to customer in suitable format	Customer is not provided with relevant services and their needs are not met	Communication / information Also a potential data protection risk	User experience guidelines / standards – body to issue standards	Monitoring and enforcing standards
Customer asks TPP to stop accessing their data	TPP does not receive the request	Technical Also a potential data protection issue	Technical delivery and testing services—body to facilitate testing/ sandbox phase.	Monitoring and enforcing standards

Figure 2 – A table describing the risks at each stage of the customer journey and examples of incentivising and protection activities to mitigate these risks.

Smart Data activities

As figure 2 shows, several 'activities' emerge as being needed across all schemes, to incentivise and protect against potential challenges. These activities provide the building blocks for Smart Data schemes, setting out the requirements governing different aspects of a scheme. Not all activities need be delivered by the same body. Instead,

they reflect how different bodies need to interact within schemes and who is responsible at different stages. Common activities can be seen in the box below:

- Data and technical standards the setting, testing, maintenance and enhancement
 of standards needed to enable data holders and TPPs to share data safely and
 securely. Alongside Application Programme Interfaces (APIs), wider standards are
 also relevant, for instance directory and security specifications.
- Technical delivery the design, testing and delivery of technical architecture and infrastructure needed to ensure systems can interact with one another.
- Regulatory rule setting and enforcement Current Smart Data schemes are being developed in regulated economic sectors. As such, appropriate regulatory frameworks will be needed, including setting of appropriate regulatory rules, monitoring, enforcement and periodic evaluation processes.
- Accreditation Identification and accreditation of TPPs is a key feature of Smart Data schemes. In Open Banking, for instance, TPPs are authorised by the FCA before they can be included in the Open Banking Directory.
- Directory of TPPs Providing an accessible list of accredited TPPs ensures data holders can identify TPPs and check the necessary credentials before allowing them to access data on behalf of consumers. It enables TPPs to provide information about regulatory permissions they have and up to date contact information. The Open Banking Directory lists the regulated TPPs and account providers (banks, building societies and payment companies) that operate within Open Banking.
- Authentication this enables a consumer or business to prove to data holders they are who they say they are, for instance through the use of two-factor authentication. Once authenticated, users can then share their data with a TPP. Identification, the process of confirming an identity, for instance through a designated user ID, is different but intrinsically linked to authentication. It is the combination of both that will allow data holders to accurately determine who an individual user truly is.
- Complaint handling and redress mechanisms for handling complaints by
 consumers, TPPs or data holders, as well as ensuring redress are necessary.
 These mechanisms include clear activities for specific bodies. For instance, within
 Open Banking provides routes to both the Financial Ombudsman Service (as a
 route for consumer complaints in the case of regulated financial services activities)
 and the ICO (in relation to consumer complaints involving personal data).
- Monitoring used to identify compliance within the schemes, that data holders and TPPs within the schemes are meeting their respective requirements, and the performance of aspects of the scheme. The OBIE monitors the performance of Open Banking APIs against key metrics such as API availability and response times.

- The working group will continue to consider common challenges and cross-sector activities as sector specific schemes develop and new schemes. It will be able to identify potential shared approaches and possible efficiencies. It will also be able to consider challenges that emerge as the consequences of differentiated requirements across sectors become apparent.
- We want to ensure that existing and future schemes learn from the development, delivery, and maintenance of these activities by other schemes. To do so we consider how to encourage coordination and support dialogue within Smart Data to encourage realise efficiencies, remove unnecessary duplication and ensure ongoing improvement.

Part 2: Proposals for the delivery of Smart Data schemes

Cross-sector coordination

- To realise these benefits will require cross-sector interoperability, as well as coordination and collaboration amongst Smart Data schemes. This section puts forward options for achieving this.
- There will be necessary differences between sectoral schemes, and we continue to support the delivery of Smart Data schemes by sector regulators and their sponsoring departments. However, schemes in finance, communications, energy and pensions face numerous hurdles in the early stages of development. These hurdles, which could delay implementation, range from the need for legislative powers, managing diverging stakeholder views or tackling the inherent complexity of designing and delivering Smart Data schemes.
- We believe there is an opportunity to tackle these challenges collectively whilst these schemes are still at an early stage of development. As these schemes develop, other sector schemes emerge and Smart Data in the UK matures, we expect the ongoing need to coordinate and collaborate across the Smart Data ecosystem to grow.
- Respondents to Smart Data Review⁴⁷ agreed that government should increase coordination across sectors, whilst being flexible to sector-specific needs and being clear on the activities played by different bodies. Our engagement with industry stakeholders and experts emphasises this view, and the Kalifa Review explicitly recommended that government take a cross-sector approach to Smart Data.⁴⁸
- The government will not look to completely align all Smart Data schemes. Individual problems in different markets mean that schemes will need to be differentiated to suit their specific needs. Instead, working with the Smart Data working group, we have identified four key principles that should inform the design of cross-sector coordination and collaboration.
 - Sectors working together: bringing together all bodies leading sectoral delivery of Smart Data with industry and government to enable greater coordination, with a clear understanding of their respective activities and responsibilities.
 - **Develop the Smart Data ecosystem**: coordination should provide opportunities to draw together a broader set of industry, technical/expert and consumer voices within Smart Data. The aim should be to develop a body of knowledge and network to support the delivery of new Smart Data schemes to unlock innovation and growth.

⁴⁷ BEIS (Jun' 2019) – "Smart Data: Putting consumers in control of their data and enabling innovation"

⁴⁸ HM Treasury (Feb' 2021) - "Kalifa Review of UK Fintech"

- Enable interoperability: greater cross-sector collaboration should find practical ways
 to increase interoperability between sectors, to enable greater innovation, address
 artificial barriers to competition and realise Smart Data benefits for consumers and
 businesses.
- Inform the ongoing evolution of the Smart Data: ensuring the ecosystem remains responsive to changing user attitudes and technological developments will be important. Pooling research and findings to develop a cross-sector picture of adoption, attitudes and capabilities will provide an opportunity to identify and consider emerging opportunities and challenges. For instance, challenges faced by specific (particularly vulnerable) groups looking to use Smart Data tools and their potential impact on them. Developing that cross-sector view will help inform the ongoing evolution of Smart Data, and help identify where further support from government is needed.

Coordination of Smart Data activities

- Cross-sector interoperability will depend on how schemes develop and deliver Smart Data activities both within and across sectors. However, it is not obvious where a coordinated approach could be immediately realised. There are currently a limited number of sectoral schemes, led by regulators, being developed and they are at relatively early stages of development. It is uncommon for regulators to develop comparable interventions in a directly-coordinated way (one exception is data protection which is overseen by the horizontal ICO regulator).
- Further work will be necessary to pinpoint where true cross-sector commonalities exist and to establish how they can be capitalised upon to support Smart Data. As a starting point we want to explore where, along a range of possible levels of coordination, activities within Smart Data should sit.

Possible levels of coordination for Smart Data activities		
Complete sectoral choice	No coordination is desirable since both the requirements relating to the activity and its delivery are best left entirely to individual sector regulators to determine for their respective sectors.	
Mutual recognition	Some coordination is possible with schemes in one sector adopting or replicating some or all of the requirements of individual activities and/or their delivery from another sector. Possible in areas where a sector's requirements for a particular activity can be considered equivalent and sufficient in another sector.	
Identical requirements, sectoral delivered	Greater coordination achieved through identical cross-sector requirements for specific activities.	

Identical requirements,	Fully coordinated, since identical requirements for activities are
delivered across sectors	both established across sectors and delivered in each sector by the
by the same body	same body.

- Alongside potential benefits from coordinating activities across sectors, there could also be potential risks, particularly if the delivery of activities was centralised. Depending on the approach taken, it might unnecessarily restrict the capacity for private sector delivery of activities to sectors or overlook important sector-specific considerations in areas like complaint handling and redress.
- However, working group members are interested in exploring how some activities could benefit from identical requirements, delivery across sectors or mutual recognition. These included:
 - Data standards in particular, coordination of API standards and data formats related to core data fields;
 - Accreditation where there is a strong rationale for tackling unnecessary burdens and duplicative requirements for TPPs seeking to operate across markets (whilst recognising additional requirements would be necessary to operate in particular sectors, such as requiring FCA authorisation to operate within financial sectors);
 - Directory services where a coordinated list of accredited TPPs could create efficiencies; and
 - Authentication which enables consumers or businesses to prove to data holders they are who they say they are. In particular, the opportunity to adopt common authentication requirements across sectors.
- We believe further progress can be made by exploring how levels of coordination could be practically achieved for one or more of this narrower set of activities. Dependent on the outcome of any government spending decisions, we propose focusing our attention on two areas: where common data standards could provide greater cross-sector benefits and how schemes should approach mutual recognition of activities from other sectors, e.g. how accreditation requirements in one scheme could be recognised as sufficient for accreditation in other scheme.

Institutional options

The current governance arrangements enable sector schemes to develop independently of each other, with BEIS having current responsibility for Smart Data policy coordination. There are several challenges that emerge from the way the current relationships are constructed:

- New schemes develop independently and do not have any existing body of knowledge or expertise to connect with, risking duplication of efforts and unintended divergence of approaches to Smart Data;
- Current sector schemes have no ongoing connection to other sectors, risking unintended divergence in approaches and a failure to secure interoperability;
- Industry engagement by schemes is currently sector focused, without any established cross-sector space. There is limited scope for sharing information, insights and expertise across sectors, and no networks engaging with companies and groups on practical cross-sector Smart Data issues; and
- To engage with Smart Data, relevant wider public bodies currently need to approach schemes individually.
- The cross-sector Smart Data working group has shown the practical benefits of bringing together relevant bodies to consider common challenges that apply across sectors.
- Our intention is to build on this work and create more opportunities for greater crosssector engagement with industry, consumer groups and technology experts. We want to harness the wide range of relevant work being done by existing organisations to inform other sectoral schemes. To do this, we propose evolving the current cross-sector working group arrangements to bring together the wider Smart Data ecosystem.
- We previously consulted on 'establishing a Smart Data Function (SDF) as a crosssector body working across existing schemes, with responsibilities including setting standards and managing the accreditation of TPPs. 49 Stakeholders had concerns about the potential for a central cross-sector body to be too prescriptive and potentially stifle innovation. Such a body delivering services to sectors might also crowd out other potential service providers and restrict opportunities to grow new delivery models. A more mature Smart Data ecosystem, with more developed sectoral schemes and broader group of TPPs might see a clearer benefit from a body like the SDF. However, stakeholder concerns and a lack of consensus means it is not the right time to develop those proposals further.
- There are different options for how cross-sector engagement could be delivered, with increasing formality. We are not proposing to introduce mechanisms that would establish collective decisions, to preserve the independence of any regulators that are involved. However, where views are collectively agreed amongst regulators, we would expect to see them reflected in individual sectors' schemes. A list of options can be seen in the table below:

Option	Description	Benefits	Limitations
Option 1 - Extending the	Under this option, the current Smart Data	The group could continue under its existing	Without additional resources and

⁴⁹ BEIS (Jun' 2019) – "Smart Data: Putting consumers in control of their data and enabling innovation"

existing crosssector working group working group would continue, involving working-level participation from government departments, regulators, and other invited stakeholders. It would be facilitated by a small BEIS-based secretariat.

The group's terms of reference could be broadened to engage with the wider ecosystem, and encouraging commonality and consistency of approach across sector schemes.

arrangements which would not need to be reestablished.

This arrangement would not require increased resources from contributing members of the working group. commitment, there would be limited scope to engage widely with the ecosystem or develop sub-groups able to draw on expertise and focus on specific challenges facing Smart Data.

Option 2 – Establish a cross-sector Smart Data Council. The government would establish a voluntary, non-statutory council with a wide cross-sector membership.

This would draw together a larger cross-section of the Smart Data ecosystem, involving industry, consumer interests and technical experts, with the aim of utilising their expertise to build a body of cross-sector knowledge and evidence.

A steering group involving government, regulators and wider members of the Council would be established to coordinate and lead the Council's activities.

It provides an opportunity to develop a variety of dedicated sub-groups, drawn from the council's membership, able to deep dive and develop detailed thinking on both specific challenges facing sectors and technical areas requiring expertise.

It would provide a network and body of knowledge for new schemes to draw on as Smart Data in the UK evolves. This option would not require extensive formal arrangements but would require a certain level of pooled resources from steering group members to support the Council's work.

As such, we would expect the Council to focus mainly on engagement across areas of common interest, with a limited number of issues being considered in detail.

This work would develop general recommendations and guidance, which individual sector schemes would consider independently.

This approach has been successfully used within government to foster collaboration with broad communities, to develop evidence and share insights. For instance, the **UK Council for Internet** Safety (UKCIS) brings together government, the tech community and the third sector to work together to deliver strategic goals with the aim of ensuring the UK is the safest place in the world to be online⁵⁰.

A Board would need to have its own resources and government-set remit in order to deliver its priorities.

Option 3 – Establish a Board to lead a Smart Data Council This develops the idea of Smart Data Council further, with a more formal senior representative Board leading the Council's activities.

It would be able to consider government requests for advice on matters of Smart Data policy and reflect on wider policy developments relevant to Smart Data as a whole. For instance, how Smart Data should adapt to future changes in digital policy.

A Board would provide a

government and wider

bodies to interact with the

whole of the Smart Data

ecosystem, rather than

clear gateway for

sector by sector.

A Board would need to balance leadership against the independence of bodies and the need to not stifle a developing ecosystem.

While not guaranteed to

There are examples of government bringing together relevant experts in a Board to advise and decide on recommendations for ministers in relevant area. The Open Standards Board, which was established in 2013. advises the Cabinet Office on the setting of open standards for use by all of government⁵¹. It consists of a selected group of industry, professional, developer and academic

A Board would provide a direct link between regulatory Smart Data schemes and the work of While not guaranteed to be a new public body, it should be noted that the Government prefers to establish a new public body only as a last resort.

⁵⁰ DCMS – <u>UK Council for Internet Safety</u>

⁵¹ DCMS - UK Council for Internet Safety

volunteers, supported by data and technology experts drawn from within and outside of government.

As a starting point, the Board should include representatives from the sector regulators taking forward Smart Data schemes and their respective departments. These bodies are actively exploring the application of Smart Data.

In the medium to long term, as the Smart Data ecosystem matures and more schemes are delivered for consumers and businesses, we propose revisiting the makeup of the Board to ensure an effective balance in representation.

the Council, providing leadership for the Council's activities and identifying clear priorities, including coordinating specific projects delegated its sub-groups.

A Board would also be able to provide government with coherent cross-sector advice and recommendations on Smart Data issues, as and when they emerge.

- Initial feedback from stakeholders has suggested strong benefits to be gained from developing cross-sector Smart Data engagement along the lines presented in these options. There has been particular interest in a Smart Data Council as a possible approach. Subject to government spending decisions, we will use further evidence drawn from stakeholders to establish the most appropriate option and develop detailed plans for how it can be delivered.
- Across all options we would want to ensure a variety of beneficial outputs are produced for those delivering Smart Data and the wider ecosystem. Proposed outputs of cross-sector coordination and collaboration include:
 - Clear priorities for joint-working This could include joint action plans for particular areas of concern (such as protecting vulnerable consumers), shared programmes of research or specific coordination schemes. The intention is members will pool

resources and expertise to deliver more than they would otherwise be able to if working independently.

- Cross-sector institutional agreements the necessary formal and informal mechanisms required for functioning cross-sector engagement. This could be new terms of reference or memoranda of understanding between bodies to enable practicalities like the sharing of information.
- Coordination guidance setting out the various activities and responsibilities of the bodies leading Smart Data sector schemes, as well as the areas where coordination and common approaches exist, as they are developed.
- Advice on cross-sector challenges providing advice to government where
 necessary to guide the further development of the Smart Data legislative framework
 and to consider possible impact on Smart Data of adjacent digital policy areas.
- Engaging the whole Smart Data ecosystem plans for convening broad crosssections of the ecosystem to share best practice, lessons learnt and insights.
- Publish cross-sector insights the group could look to bring together research and draw data from across sectors to provide a clear cross-sector evidential picture of Smart Data and its impact on both consumers and businesses.
- Developing cross-sector industry support building out from work undertaken within sectors, the group could establish joint programmes aimed at supporting crosssector industry innovation through shared learning, best practice and evidence to support interoperability approaches, and areas of international coordination.
- Developing links with the government's wider digital and data policy ensuring the whole Smart Data ecosystem, regulators and industry, has an effective link to wider government digital and data policy schemes.

Part 3: Links with wider work and next steps

Links with wider work

As Smart Data spans across sectors and data driven policies become increasingly prevalent, there are links with a wide range of interventions both within government and the private sector. It is key that these links are clearly established and communicated both across government and industry. Below, we provide more detail on the links to key government policies, including the National Data Strategy, Digital Identity, and the Digital Markets Unit.

The National Data Strategy

67 The National Data Strategy published in September 2020 sets out our vision to harness the power of responsible data use to boost productivity, create new businesses and jobs. It highlights the vision to improve public services, support a fairer society, and drive scientific discovery, positioning the UK as the frontrunner in the next wave of innovation. The National Data Strategy sets out the actions this government will take on data and created a shared frame of reference that brings together and unifies an extensive portfolio of activity. Publication of the National Data Strategy launched a 13week public consultation. The government response to the consultation response was published 18 May. It set out a commitment to adopt a phased approach to future publications, focusing on developments relating to each of the strategy's five missions, including mission 1 to create an environment where data is appropriately usable, accessible and available across the economy - fuelling growth in organisations large and small. Smart Data featured as a key initiative as part of this mission and will remain central to the development of a wider framework for data availability across the economy.

Digital Identity

Smart Data schemes will require users to prove they are who they say they are before their data is shared. One way this could be achieved is by using a Digital Identity. A digital identity gives people more choice about how they prove things about themselves, such as their age or address, aiming to streamline access to public and private sector services by making it easier to prove who you are or something about yourself. Digital identities are a vital building block for a fully realised digital economy. They will enable smoother, cheaper, and more secure online transactions; they will simplify people's lives, and boost business. It should be noted that the Digital Identity work is separate from a National Identity Card scheme. The Government does not support a National Identity Card scheme.

- 69 DCMS are leading work on this and following the response to the Call for Evidence on Digital Identity, a prototype of the Digital Identity trust framework was launched earlier this year. 52 This sets out the rules and standards to enable the use of trusted digital identity products. DCMS will work with the digital identity community to develop the framework and aim to publish the next iteration in the summer.
- 70 Smart Data and digital identity are complementary policy areas which aim to facilitate better use of data for the benefits of people and organisations. They exist independently of each other, but when combined can bolster the projected benefits for the user as well as for market growth. Digital identity tools are not essential to enable Smart Data schemes: acceptable identity verification for Smart Data is commonly achieved by two factor authentication. But digital identity can support Smart Data schemes by providing an alternative, secure means for a user of a private sector service to prove they have the right to access their data. In turn, Smart Data schemes can help further the consumer benefits of digital identity by extending it to other services. BEIS and DCMS are aware of the complementary nature of these projects and will work to ensure no duplication of effort, while considering opportunities for greater coordination.

Digital markets

- 71 The Smart Data Review highlighted the potential benefits of Smart Data in digital markets such as social media, online marketplaces, or app stores. In our Next Steps for Smart Data consultation response, we committed to explore future links between Smart Data and digital markets, with cooperation between the Smart Data working group and the Digital Markets Taskforce. 53 The taskforce focused its expert advice on how to promote competition, and how to address the consumer harms that can arise from the exercise of market power in digital platform markets.⁵⁴ Advice from the taskforce was published in December 2020, building on the recommendations of the CMA's market study into online platforms and digital advertising. Government has committed to establish a new, pro-competition regime for digital markets. A new Digital Markets Unit (DMU), has been set up in shadow form to begin to operationalise a new procompetition regime for digital markets. We will legislate to put the DMU on a statutory footing as soon as parliamentary time allows.
- 72 The future institutional arrangements to deliver Smart Data will need to work with and not duplicate the work of the DMU. Collaboration across government will continue as both digital and Smart Data policy continues to develop and move towards implementation.

Centre for Data Ethics (CDEI) and Open Data Institute (ODI)

73 The CDEI is tasked with advising government on how to maximise the benefits of datadriven technology. Given its existing work on trustworthy data sharing, it has agreed to

⁵² DCMS and Matt Warman MP (Feb' 2021) – "The UK digital identity and attributes trust framework"

 ⁵³ BEIS (Sep' 2020) – "Next steps for Smart Data"
 ⁵⁴ CMA (Apr' 2020) – "Digital Markets Taskforce"

- undertake work this year to explore the ethical and trust issues involved in the design and delivery Smart Data schemes.
- The ODI works with companies and governments to build an open, trustworthy data ecosystem. Building on its existing work on data portability and potential use cases for consumers and businesses, it will this year work with the BEIS Smart Data team to explore how to support and incentivise innovation within Smart Data schemes.

Roadmap for Smart Data

Next steps for BEIS

- This report and responses received will inform future policy direction, and in particular the role for government and any coordination of Smart Data schemes. We would welcome further engagement on these proposals and will be organising a series of stakeholder roundtables to discuss key challenges and ideas raised by respondents.
- BEIS will continue to progress work towards Smart Data primary legislation, engaging across government and regulators to ensure the powers are appropriate for use in a variety of sectors, primarily communications and finance. There is however a lot of progress that can be made ahead of primary legislation. To ensure the primary powers are sufficient for use in a range of sectors, further work is required in specific sectors to consider topics such as funding and enforcement, identifying where existing powers are insufficient.
- This report has set out recommended areas and mechanisms for cross-sector coordination, although there is a long way to go for these to be delivered in practice and further work is required across banking, finance, energy, communications and pensions. BEIS will also be considering wider sectors where Smart Data could play a role beyond those included in the working group.

Next steps for working group and members

- BEIS will continue to lead the existing Smart Data working group for at least another 6 months. This extension was accounted for in the group's terms of reference, acknowledging the challenging nature of the group's focus and aims. Due to the current pause on midata specifically, Ofgem will continue to be a member of the working group but may contribute where appropriate outside of the regular meetings. Wider links to energy projects will also be made within BEIS, for example the work on Smart Meters and the Energy Data and Digitalisation Strategy.
- 79 The working group will continue to:
 - Share updates with other members on sector schemes and related programmes in each sector, such as the FCA's regulatory sandbox and the Switching Programme in the energy sector.

- Share knowledge and lessons learned from more advanced schemes and similar projects across government and the private sector, such as Open Energy and work by NHSX.
- Seek wider stakeholder input on areas of cross-sector interest and challenge, such as technical experts and consumer organisations.
- The key role for the working group will be to support BEIS in the delivery of a blueprint for cross-sector engagement for existing and future Smart Data schemes. BEIS will aim to publish an equivalent update report following this 6-month extension.

Annex 1: Invitation for further feedback

We are seeking feedback on the above proposals and on the outputs that should be delivered by this cross-sector arrangement. We are especially keen to hear feedback from stakeholders on the specific areas set out below.

Please send all feedback by 23.59 pm 30 July 2021. Responses can be sent via email: smartdata@beis.gov.uk or via Citizen Space.

Cross-sector coordination

- 1 Do you agree with the principles set out to inform this cross-sector work (para 53, p23)?
- Are there any additional principles for cross-sector work that should be taken into account?

Coordination of Smart Data activities

- Given the interest from schemes, should we focus on exploring how common data standards and a mutual recognition approach could be used to clearly benefit from cross-sector coordination? (para 58, p25)
- 4 Are there other areas where government and/or Smart Data schemes could explore how to practically achieve greater coordination of activities?
- How should government approach the two areas of focus (common data standards and mutual recognition) in order to deliver practical tools and resources for Smart Data schemes?

Institutional options

- Which option from those provided on pages 26-28 presents the most viable approach for gaining greater cross-sector coordination and collaboration, whilst balancing the need for sector-led delivery?
- Do you agree with our approach of not introducing specific mechanisms for collective decisions? (para 63, p26) How else can we ensure the right balance between the independence of the bodies involved and coordinated action in relevant areas?
- Do you agree that the outputs suggested (p29-30) would support greater cross-sector coordination and collaboration? Which stand out as a practical way to achieve our principles for coordination?
- 9 Do you view any of these outputs (p29-30) as an immediate priority for Smart Data and should any be prioritised by any cross-sector group in their first year?

- Are any of the possible outputs (p29-30) already being delivered by existing organisations and where work a cross-sector group should avoid duplication? Similarly, are any existing organisations better placed to deliver these outputs?
- 11 What considerations should inform the delivery of outputs, and should any specific mechanisms be considered to enable involvement from relevant bodies?

Annex 2: Definitions

This annex defines the terms used in this report and agreed by the Smart Data working group. Note these are definitions used for the purpose of this report, the cross-sector objectives set out in Annex 3 and potentially future working group reports. They do not represent the definitions used by other organisations (for example, similar terms used by the ICO).

Term	Definition
Customer	The term customer is used when referring to a customer of a data provider e.g., a customer of a bank.
	Customer Data
	Customer data is any information which is related to an identifiable natural person or that of a small business who is a recipient of Smart Data-enabled services.
User	Any consumer or business that chooses to share data to a specific third party and for a specific use (i.e., a user of Smart Data services) This includes both potential new consumers/businesses who may share data with a TPP, and those that already share data with TPPs. Ultimately, Smart Data will put users in control of their data
Data holder	The business or organisation that holds data on individual customers e.g. a bank. This data includes information about the customer, and data which has been generated through the customer's use of their service. For example, an energy provider holds personal information for their customers, along with generated data related to their tariffs and usage. TPPs will be granted permission by the user to access this data in order to provide their services.
Third party provider (TPP)	Any authorised business or organisation that a user gives permission to access their data or with which they interact to help them navigate the market, other than their data holder(s) in that market. Scope of definition
	This definition covers a wide range of organisations and is flexible to capture new forms of TPPs that might arise as

Term	Definition
	markets develop. The rules around different types of TPPs may differ and will need to be set out clearly.
	Examples of TPPs include (but are not limited to):
	Read-access user facing TPP
	These TPPs have the ability to access, share and display data on the user (e.g. display bank account or energy consumption information)
	Write-access user facing TPP
	These TPPs have the same permissions as read access TPPs, but also have the ability to make changes on the user's behalf (e.g. initiate a payment or switch provider)
	Technical Service providers (TSPs)
	TSPs are organisations that work with regulated data holders and or TPPs to deliver Smart Data enabled products or services (e.g. credit checks)
	Data facilitators
	A TPP may share data with a data facilitator to manipulate or analyse the data so that it is usable, allowing the TPP to provide their service (e.g. converting data file type). This could be considered a data processor under UK GDPR.
Consent workstream	
	Customers have the right to decide with whom their data is shared. A customer must give permission for their data to be shared by the data holder with a specific third party who then uses the data for a specific use.
Consent	Explicit consent
	The above process is referred to as 'explicit consent' under Open Banking. In the context of a banking customer, explicit consent is the permission given by the customer to a regulated TTP to access the customer's payment account held at the bank. Explicit consent under GDPR is consent

Term	Definition
	that must be expressly confirmed in words, rather than by any other positive action.
	Consent under UK GDPR
	Article 4 of UK GDPR sets out that consent must be specific and informed, and a consent request must include as a minimum: the name of the organisation and any other controllers who will rely on the consent, the purpose for processing the data, how the data will be processed and the ability for consent to be revoked at any time. Consent in our documents differs from consent under UK GDPR, as we are interpreting consent as the standard definition of the word, the process of 'giving permission to do something'.
	Under UK GDPR individuals have the right to erasure. Applied to a Smart Data context, this may apply when a user revokes their consent, both ongoing access to the user's data is halted and any existing data held on the user from their period of consent is deleted. There are further circumstances when the right to erasure applies, such as when personal data is no longer necessary for the original purpose of data collection.
Consent framework	A consent framework establishes a series of standards for third parties to adhere to when acquiring, storing and monitoring consent. It also includes a mechanism which monitors ongoing compliance with the standards of consent, and the revocation or expiry of consent.
Accreditation workstream	
	For any TPP to access customer data, they should be expected to meet specified requirements to ensure they are deemed appropriate to handle the data. Accreditation communicates to all parties in the system that the TPP has met these requirements.
Accreditation	Links with regulation
	Accreditation is different from, but linked to, the sectoral regulation of TPPs. The approach taken for accreditation will dictate the level of regulation needed and vice versa. For example, a strict license approach to accreditation may mitigate the need for further regulation. Conversely, legal

Term	Definition
	requirements and wider regulatory powers may lessen the need for strict accreditation requirements.
Accreditation framework	An accreditation framework establishes a series of requirements and ongoing conditions for third parties to meet in order to access data with the consent of the data subject, and the process for becoming accredited by meeting those requirements. It also includes a mechanism which monitors compliance with such requirements, and of revoking accreditation if required. Creating, maintaining, and sharing a record of accredited TPPs is a further aspect of the accreditation framework.
Open Banking Directory	The Open Banking Directory is a list of TPPs (AISPs and PISPs) and account providers (ASPSPs) that operate in the Open Banking ecosystem. The Open Banking Directory enables account providers, such as banks, building societies and payment companies, to verify the identity of regulated TPPs. This is an example of a how an accreditation framework could create, maintain and share a record of accredited TPPs in practice.
Authentication workstream	
Authentication	Authentication is defined as the process of proving that something is real or true. For security reasons, users must be able to confirm to TPPs and data holders that they are who they say they are, so their data can be shared with a TPP and a service can be provided.
	Types of authentication
	There are three main types of authentication: Knowledge, Possession, and Inherence. Knowledge is based on authenticating against something you know, such as a password. Possession is authenticating against something you possess, such as a digital token. Inherence is authenticating against something you are, such as the use of biometrics.
Verification	The distinction between authentication and verification is important. Authentication involves checking a user's identity against information the user and only the user should know

Term	Definition
	(e.g. one-time passcodes). Whereas verification involves checking a user's identity against non-user provided information (e.g. driver license records).
Identification	Authentication is different, but intrinsically linked to, identification. Identification is defined as 'proof of who someone or something is'. It is possible to have identification without authentication and vice versa, it is the combination of both that will allow data holders to accurately determine who an individual user truly is.
Authorisation	Authorisation is the act of giving someone permission to perform a specific action. Identification does not guarantee authorisation e.g. identification of an individual does not in itself provide authorisation to access a certain bank account. A user is first identified, then authenticated to check if that identity is true, from which you can authorise the individual to access an account.
Digital Identity	A digital identity is information used by computer systems to represent a unique person, organisation, application or device. For a citizen or consumer, a "digital identity" is a trusted way of proving one or more attributes about themselves online or offline and the linkage of those attributes to that same person as a uniquely identifiable individual.
Liability workstream	
Liability	Liability is defined as the 'state of being legally responsible for something'. Liability clarifies who is responsible for problems incurred at different stages in the data chain, and what it is they are accountable for.
Liability framework	The liability framework should establish clear liability that covers all and any form of interaction between users, data holders, TPPs, silent parties, government bodies and regulators. This should include clear routes to redress and mechanisms for dispute resolution.
Data breach	A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, user data (both individual users and SMEs, mirroring the UK GDPR definition of a personal data breach.). This includes

Term	Definition
	breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Onward sharing	Onward sharing is the process of a TPP sharing data they have received directly from data holder(s) to further parties.
Redress	Redress is linked to, but different from, liability. Redress involves remedying an unfair or undesirable situation. Redress and liability should be separated, as a consumer needs to know exactly where to go when something goes wrong but may be less concerned with who is at fault.
Silent party	A silent party is a user who is not the direct individual or business involved in the data sharing process, but the individual or business that is linked with the direct user's data traffic. For example, a person who has had their name or bank account number directly or inadvertently shared in the data chain by being on the other end of the direct user's payment transaction.

Annex 3: Objectives for Smart Data schemes

The working group considered 4 key aspects of the customer journey and developed cross-sector objectives. These aspects were chosen as they are applicable across sectors and are particularly difficult issues when considering cross-sector coordination of Smart Data schemes. The objectives set what 'good' could look like and provide points to consider when designing Smart Data schemes.

The topics covered by the objectives are:

- Accreditation of TPPs
- User authentication
- User consent
- Liability framework

Accreditation of TPPs

Purpose

- Accreditation should provide assurance to users and data holders that third parties have met predefined access conditions and have arrangements in place to ensure that these continue.
- Accreditation should give users and data holders a certain level of confidence that third parties will handle customer data appropriately, ethically (e.g. in compliance with DCMS' data ethics framework and data protection legislation) and for customer-authorised purposes only.
- Accreditation should provide administrative efficiency for TPPs in demonstrating suitability to access data across the economy, speeding up access to data.
- Subject to meeting the initial requirements and ongoing compliance checks, TPPs are permitted to access data and execute specific actions on the user's behalf with their consent (note separate workstream for consent).

Links with sectoral regulation

Accreditation, combined with sectoral regulation, should ensure that the way data is used by third parties is transparent, does not abuse the trust of users, and does not lead to negative or harmful practices for users - such as profiling users (e.g. linking low-income users to only specific packages/providers), unfair or undesirable price

- discrimination and personalisation (e.g. pricing the same service differently for consumers based on their income/past expenditure). As such, accreditation should be used in compliance with existing data protection legislation.
- The accreditation system must balance with further regulatory requirements for TPPs, with clarity where one ends and the other starts. For example, the extent to which accreditation plays a consumer protection role should be set out.
- There should be a clear hand off between any accreditation body and the regulator, and the relationship between the two should be clearly defined.

Accreditation requirements

- 8 The accreditation framework should ensure, in a manner that delivers robust value for money and without unnecessary gold plating, that data is used only in line with specific access conditions.
- The requirements should clarify how third parties should design aspects of their services inclusively so that everyone is able to enjoy the benefits of sharing data. This could include, for example, ensuring issues of vulnerability are tackled and the appropriate security measures are in place to protect all users.
- The accreditation scheme should take into account the size of an organisation it is imposed upon. It should be sufficiently strict to be meaningful, but flexible enough to ensure it is not a barrier to smaller organisations gaining accreditation. The burden placed on TPPs and mechanisms to weigh against this should be considered specifically, such as support services or sandboxes.

Accreditation process

- 11 The accreditation process must be transparent for all parties.
- The process for accreditation should be proportionate, in both cost and time, to the level of risk which the data to be shared carries. Fastest is not always best, however unnecessary frictions for TPPs should be minimised.
- The accreditation framework should be clear on who requires accreditation and whether it extends to all types of TPP and other actors in the ecosystem, for example fourth parties or technical service providers.
- There should be a level playing field for all TPPs aiming to become accredited, to ensure competition is fair.

Monitoring compliance

The accreditation system should include ongoing monitoring of compliance. The accreditation framework needs to balance the time and resources that are required a) up front to assess the requirements that applicants have to meet prior to gaining access

- to the ecosystem, and b) on an ongoing basis through an assurance regime that checks compliance on an initial and enduring basis with the access and accreditation conditions.
- The accreditation system should be risk-based to play a mitigation role. This includes but is not limited to the risk of criminal misuse, fraud and the unethical use and general misuse of data.

Record of accredited firms

- 17 The accreditation framework will create an ecosystem of known and named third parties, in which accreditation is the key to entering. This way users and data holders can be assured that data will be shared securely and used only for agreed purposes.
- There should be a clear record of who is accredited, such as a directory, to give users and data holders assurance that they can trust the organisations they are dealing with. It should be ensured that users and data holders understand the difference between a firm that is accredited and a firm that is not.
- The liabilities on TPPs for failing to meet the accreditation requirements should be clear and explicit. The removal from the ecosystem of accredited TPPs should carry a credible threat for non-compliant TPPs. The potential for enforcement (e.g. blacklisting) should be communicated clearly to incentivise compliance.

Links with wider work

- The accreditation and assurance framework will not seek to duplicate the activities of other competent authorities in enforcing third party legislative compliance (e.g. ICO). There should be a process to notify impacted third parties in the event of a data breach, including data protection breaches, as in line with data protection legislation.
- Any approach to accreditation should aim to be consistent across sectors as far as is possible, balancing user protection and burdens for TPPs. Core accreditation standards should be built for all third parties, and the specific needs for each sector should be further defined through additional sectoral standards via regulation. Note, we are not necessarily imposing a single cross-sector accreditation system; the structure of the accreditation system is still to be decided.
- Technology which facilitates the accreditation framework, including compliance monitoring and maintaining a shared record of accredited TPPs, and drives more efficient accreditation of firms should be embraced.

User authentication

Purpose

- The authentication framework should ensure that TPPs and data holders can confidently, accurately and quickly check whether the user consenting to their data being shared is the same person for whom they hold data or are providing a service to.
- 24 It should also provide certainty to the user that the organisation asking for their data is who they claim to be.
- A robust authentication framework should provide a layer of protection to both the user and data holders and TPPs, by ensuring all parties are protected against some potential harms, such as the misuse of personal data or fraud following identity theft.
- The authentication framework, in combination with the accreditation, consent and liability frameworks, should help to install trust and security in the overall data sharing ecosystem. Authentication alone is not sufficient in achieving trust in the system.

Process

- The authentication process should be smooth and user friendly, learning from the successes and failures from Open Banking, sector specific authentication process and relevant research.
- An appropriate level of friction in the authentication process should strike a balance between user experience and security. Some friction is necessary and instils trust in the authentication process, and it provides users with the confidence that the necessary checks are being done to protect them against potential identity theft and fraud. Excessive friction, such as multiple clicks or a slow process, that does not provide necessary additional security will impair user experience and would likely lead to reduced user uptake and increased user drop off.
- Authentication of user identity should only require information that is easy for users to access.
- Authentication must not create an excessive barrier that inhibits TPPs from being able to provide their services. It will be important to balance the regulatory burden on TPPs with security and user experience.
- There should be mechanisms in place to ensure a good user experience. This could come in the form of customer experience guidelines.
- 32 Specific considerations should be given to those users who may be less digitally engaged. For example, one-time passcodes sent via SMS will not be possible for those users that do not have access to a mobile.
- 33 Specific considerations should also be given to those organisations who hold limited information on their customers which could be used in the authentication process e.g. digital records. There should be methods to authenticate offline to encourage participation from organisations that lack the ability to authenticate digitally.

User authentication should be periodically revisited to ensure all parties continue to be who they say they are. An effective timeframe for re-authentication should be decided, this may vary by sector and should be flexible to the specific use case to balance security with friction for users. The decided reauthentication period should be clearly communicated to all parties.

Proportionate approach

- An appropriate level of authentication should be proportionate to the varying sensitivity of data both within sectors and between sectors. This could, for example, determine the need for single factor verification (e.g. username and password) versus multiple factor verification (e.g. biometrics, one-time pass codes, trusted apps etc.).
- The level of required authentication should be determined by the proposed purpose of the data, be appropriate to the level of risk as well as the sensitivity of the data itself.
- Any approach to authentication should aim to be consistent across sectors as far as is possible and appropriate. For example, one approach could be to establish a baseline level of authentication that is common across all sectors, and only further authentication steps required where necessary for sectors or use cases involving more sensitive data.
- In the scenario where multiple data requests are involved with differing levels of authentication requirements, the highest level of authentication from the data requests should be required.

Communication

- Authentication messaging should use easily comprehensible phrases and avoid technical jargon. This is to protect all users, including vulnerable users, who may not understand complex terminology. ICO data protection requirements have similar requirements for transparency communications, and this should be leveraged where possible to avoid duplication of regulatory burden.
- Authentication messaging should also be consistent across sectors where possible.

 Differing or conflicting authentication messaging could create a poor user experience and undermine confidence in the overall trust framework.
- The distinction between authentication and consent should be made clear and how reauthentication links with consent should be understood. For example, users should understand that when they are reauthenticating they may not be reconsenting.

Links with wider work

The authentication framework should be consistent with any relevant existing regulation, such as in the anti-fraud, anti-money laundering, cybercrime and data protection space.

- The authentication framework should seek to use existing federated authentication standards (e.g. SAML, OpenID Connect and OAuth) where feasible, to avoid duplicating or contradicting existing processes.
- Development of a digital ID might assist consumers to authenticate with multiple providers. The authentication framework does not seek to duplicate this work and should be flexible to its inclusion to improve the authentication process.
- There may be situations where others are able to make a request on behalf of the user in question. Provisions for authenticating on someone else's behalf should be consistent with existing Power of Attorney law and other relevant regulation (such as data protection legislation).

User consent

Purpose

- The consent framework should ensure that customer data is not being used by third parties without the knowledge or willingness of the user. The user should have an appropriate level of awareness of what data is being used by TPPs, and why, in line with transparency requirements set out in the UK GDPR.
- A robust consent framework should provide protections both for users, and also data holders and TPPs, by providing clarity about responsibilities against which any claims of harm can be assessed. Clear consent records would aid in establishing liability, should a given party fail to adhere to the standards of the consent framework.
- The consent framework, in conjunction with the accreditation, authorisation and liability frameworks, should help to install trust and an overall sense of security for all parties involved in the data sharing process.
- Standards should include the definition and parameters for consent, so that terms and conditions, and privacy policy are clearly and consistently explained to users across sectors. This should be in line with existing data protection legislation.

Process

- Access to a customer's data should only be permitted to TPPs once the user gives consent to do so.
- There should be clarity as to whom users give consent and what party holds the given consent, whether that is the data holder, the TPP or a further party. It should not be the responsibility of the user to provide consent to personal data access without prompt.
- Rules should stipulate whether TPPs are permitted to request continuous access to personal data (e.g. to continually monitor usage in order to provide up-to-date

- recommendations), or whether consent only grants TPP's one-off, time limited access to data.
- A one size fits all approach across differing use cases may be inappropriate. Guidance should be provided to assist TPPs and data holders on the approach to consent that is required, for example this could come in the form of consumer experience guidelines.

Recording and managing consent

- User consent must be accurately recorded and managed by the TPPs who have access to customer data, for example tagging consent with relevant information such as purpose and time for which it is valid. It should be easy for the user to locate and access these consent records for both active and inactive permissions. This should include but is not limited to which TPP is using their data, what data is being used, how long the data will be held for, and the purpose for TPPs accessing this data.
- Consent should be periodically revisited to ensure that the user continues to agree to their data being used. An effective timeframe for re-consenting should be decided, this may vary by sector and by the specific use case. This should balance the need for user consent to be informed, with friction which may discourage users.

Ability to revoke consent

- Users should have the right to revoke their consent easily and at any given time, and the required mechanisms for this must be in place.
- 57 TPPs should make it clear that users have the right to revoke their consent and explain clearly how they can do this.
- When revoking consent, it should be clear to the user and TPPs what happens to data records. Rules should also set guidelines for how TPPs communicate information relating to the deletion of data to users, this should not contradict the right to be forgotten under UK GDPR.

Communication

- Across all workstreams, there should be minimum communication standards, and these should not act as a constraint to innovation or competition for TPPs.
- 60 Communication between users, incumbent firms and TPPs should be secure throughout the consent process to protect all entities involved.
- Mechanisms are needed to provide consumers with the information they need (and in an appropriate format) to provide, revoke, or decline to renew consent initially and over time.
- 62 Consent messaging, including consent agreements and Privacy Notices, should use easily comprehensible phrases and avoid technical jargon in line with data protection

- legislation. This is to protect all users, including vulnerable users, who may find it harder to understand what they are consenting to.
- Users should be provided with an appropriate level of information on what consent they have provided, revoked or decline to renew both upon the initial provision of consent and continually over time. Such information should include what data that has been consented to is being held, for what reasons, and for how long it will be stored. This information should be accessible, in an appropriate format and in line with requirements of data protection legislation.
- Users should also have an appropriate level of awareness if their data will be shared with other parties in a provisioning chain (onward sharing) that a user may not necessarily be aware of or would not have consented to had they understood.
- The distinction between consent and authentication should be made clear, and how consent links with reauthentication should be understood. E.g., users should understand that when they are reconsenting they are not reauthenticating and vice versa.

Links with wider work

- The consent framework will not seek to duplicate or contradict the requirements for consent set out in UK GDPR and enforced by the ICO, or in PSD2/PSR 2017. The consent framework should allow firms to comply with UK GDPR and PSD2 as appropriate in their sectors and extend beyond existing regulation as necessary to provide additional detail or requirements needed to meet the objectives set out here. For example, UK GDPR does not protect SMEs (other than sole traders).
- Any approach to consent should aim to be consistent across sectors as far as is possible, balancing user protection and friction for users. The consent process can confuse and deter users and third parties, an effect which could be exacerbated if different consent journeys are required in each sector.

Liability framework

Purpose

- 68 Lines of accountability and liability should be effective in incentivising all participants to maintain a secure and trustworthy ecosystem.
- The liability framework should make it clear which party owes redress and to who, should there be a breach of standards or a data breach, i.e. anything that triggers a loss for a user or group of users. This is to ensure that individual parties cannot deny liability unfairly.
- There should be clear data trail from the user, through the data holder, to the TPP and any further recipient (e.g. onward sharing). This is so in the event of a data breach it

- should be easy to identify where in the data chain this occurred, from which you can assign liability. This should be in line with or in addition to existing data protection requirements.
- 71 There is the need for enforceable standards on the quality of data, process and technical requirements in the data sharing ecosystem. For example this may encompass required metadata standards.

Scope

- The liability framework should cover disputes related to users, data holders and TPPs, both between and within these groups. The framework should cover disputes relating to both consumer data and product data.
- The protections available to users, against a particular type of harm or in relation to a particular type of data, should not vary according to the activity undertaken by the TPP they are interacting with. Although this might vary depending on the user type e.g. consumer vs SMEs, where SMEs may not be covered under UK GDPR but will still need adequate protection.
- Where liability may cross sector jurisdictions, clarity is required on the process to establish liability, resolve disputes, and provide redress for cross-sector data breaches. It should be clear when and where liability rules and standards apply, so as not to infringe on existing liability processes in sector specific regulations.

Dispute resolution

- All participants in the data chain including consumers, data holders and TPPs must be able to raise and resolve disputes between all parties.
- All parties should have access to a dispute resolution service. For example, there should be no pitfalls in the liability framework where third parties and data providers have no dedicated means for raising disputes.
- 77 Where parties have a choice of dispute resolution provider, it should be made clear all of the options available to them. It should also be made clear the conditions involved in dealing with each dispute resolution provider, such as costs.
- There should be clear timelines for raising an issue and any redress payments.

 Disputes should be resolved in a timely manner, and guidance should make clear what constitutes a timely resolution. That is without compromising the quality of the dispute resolution service being offered, and appropriate to the needs of each use case and sector.
- The liability framework should also give consideration to aggregated complaints data and how it may be used to improve the dispute resolution process. For example, using data surrounding the types and volume of complaints to monitor effectiveness and facilitate continuous improvement.

The dispute resolution process will require monitoring and enforcement in cases of noncompliance.

Redress

- Alternative dispute resolution services should have clear enforcement guidelines that cover issues such as the proportionality of redress.
- How a user enacts their right to redress should be as consistent across sectors as possible, to avoid confusion.
- Users who are not currently covered by existing liability frameworks should still have access to redress (e.g. larger SME's who are not currently covered by UK GDPR).
- Redress should be free or affordable, accessible, and timely. Each redress case, whether individual or collective, should be handled with consideration for the specific circumstances in which a data breach occurred and its impact on the user.
- 85 Monitoring and enforcement in cases of non-payment of redress will be required.
- Further to redress, the repair of harms to the user that are not financial (e.g. damage to credit score) should be addressed within the liability framework.

Sanctions and fines

- Where there is a breach of standards or requirements by TPPs or data holders, fines and sanctions may be required. These fines and sanctions should provide a credible threat to incentivise compliance.
- The sanction or fine on the liable entity should be proportionate, taking into account factors such as the harm incurred by the affected party, the type of data breach etc.

Communication

- Clear documentation and governance are needed to ensure sufficient standardisation across and within sectors and minimise subjective interpretation of liability requirements.
- The liability framework should be designed to be as accessible as possible to vulnerable users, including the redress process. For example, data holders and TPPs may be required to provide tools that allow users to easily enact their right to redress.
- The liability framework should consider how liability is included and communicated in the enrolment contract under which data was shared, any standards and guidance, and the accreditation scheme. This should be clear in what it is explaining and easily accessible to all parties.
- Occidented and consistent liability and redress communication between parties should be pursued both across and within sectors. This will help all parties understand their rights and responsibilities.

Links with wider work

- The liability framework should remain dynamic so it can evolve with changing markets and future business models. For example, this could include developments in technology, changing user needs, or the emergence of new use cases.
- The liability framework will not seek to duplicate or contradict the requirements for liability and redress under current data protection legislation. The liability framework should comply with and extend beyond current obligations in existing regulation. The extent to which requirements go beyond current obligations in existing regulation should be clearly established.

Annex 4: Use cases underpinning the customer journey

Customer journey

- This annex sets out the use cases considered by the Smart Data working group when considering the customer journey. The exact customer journey will vary between use cases, and there will be nuances in the sectoral frameworks. However examining this common journey will allow government, regulators, and industry to identify the commonalities across sectoral schemes. There are common challenges and a consistent need to protect customers throughout the journey.
- 2 It is useful to contextualise this journey in each sector. The use cases considered by the working group include:

3 Banking:

Customer need: The SME (customer) uses an expense management TPP that will allow them to track bills, expenses and receipts easily and quickly, so they know how much they've spent and are ready for the taxman.

How it is met: The TPP uses a TSP to connect with banks (data holder). Only the TPP and TSP will access the data. The TPP checks the bank's API⁵⁵ 4 times per day for any changes, and imports any activity posted by the bank. This provides a dynamic time flow of banking data.

4 Finance:

Customer need: An individual (customer) currently has savings accounts and a credit card debt with different providers (data holders). Due to the death of a relative, the customer suddenly inherits £10k. The customer would like to use some form of digital investment service (TPP) to decide how best to use or invest the inheritance.

How it is met: The TPP requests the customer's data from the banks and credit card providers, with data being shared via a TSP. The TPP uses specific customer data to present the customer with potential investment scenarios, potentially including some that involve paying off some or all of the credit card debt with a portion of the inheritance.

5 Telecommunications:

⁵⁵ Application Programming Interface; a software intermediary that allows two apps to talk to each other.

Customer need: Residential consumers (customer) can use a digital comparison tool (TPP) which allows them to share information about themselves held by their Communications Provider (data holder).

How it is met: The digital comparison tool can draw on information from the user's current provider to offer recommendations that take into account what services the user already takes, when their contract ends and their usage, as well as what services are available at their address from a range of providers.

6 Energy

Customer need: An individual (customer) would like to access accurate price comparisons. The comparison website (TPP) needs three key pieces of information: the postcode of the premises, the consumer's current tariff, and the consumer's annual energy consumption.

How it is met: The TPP would be able to access tariff data from the customer's supplier (data holder) or other industry central systems. In real time, the supplier/industry systems would provide information about the consumer's tariff and historic consumption, avoiding the need for the consumer to find a bill or use estimates.

These use cases again demonstrate the tangible benefits of Smart Data to customers, from giving consumers better prices to offering SMEs efficient ways of managing their accounts.

This publication is available from: www.gov.uk/government/publications/smart-data-working-group-spring-2021-report
If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk . Please tell us what format you need. It will help us if you say what assistive technology you use.