



Department for
Business, Energy
& Industrial Strategy

BEIS: Smart Data Research

Report: Consent

Lead author: Miles Cheetham

Co-authors: Faith Reynolds, Sharon Cunliffe, Gavin Starks

2020-03-31

REF: DGEN-SSD1-V2020-03-06





© Crown copyright 2020

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.

This publication is available from: www.gov.uk/bei
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.
Any enquiries regarding this publication should be sent to us at: enquiries@beis.gov.uk

Commissioned by BEIS
Produced by Dgen.net

Contents

Executive Summary	4
Gaining consent from consumers	5
Impacts of requiring ongoing consent	6
Recommendations	7
Policy	8
Standards	9
Market	10
Guidelines	11
Summary of concepts	12
Overview	13
Consent	15
What we mean by Consent	15
Learnings from Open Banking	17
Regulation	21
Consumer protection	23
Considerations in Open Banking	23
Considerations across other sectors	24
Approaches to consent outside the UK	25
Regulation — summary of implications	27
Regulatory — checklist for development	28
Consumer consent	30
Consumer attitudes and behaviours	30
Consumer comprehension	31
Customer experience	33
Consumer — summary of implications	34
Consumer — checklist for development	35
Market participants	37
Participant issues	37
Consumer issues	38
Roles in the provisioning chain	38
Trusted parties in a data sharing ecosystem	41
Market participants — summary of implications	41
Market participants — checklist for development	42
Impacts of requiring ongoing consent	45
What does this look like to a consumer?	47
Scenario 1: Using a service provided by an agent	47
Scenario 2: Using a loan company	48
Scenario 3: Using a credit broker to find a loan	49
Biographies	50
Glossary & terminology	52

Executive Summary

Data sharing consent spans three domains: regulation, consumer and market.



Our primary recommendation is to:

Develop additional consumer protections
and enhanced rights for consumers through a
Smart Data Right and a Smart Data Consumer Agreement

This will require a number of supporting actions and initiatives.

1. Determine the key policy drivers and values for consent and its management early. These should determine the design of the technology and success of the smart data initiatives.
2. Review the current legislative and regulatory mechanisms, 'test' whether they remain fit for purpose for future initiatives, and propose enhancements, ensuring regulatory consistency for consent and its management in smart data initiatives across sectors.
3. Create cross-sector consistency in participant categorisation and a common terminology.
4. Develop a cross-sector Smart Data Consent Standard
5. Develop API specifications for Smart Data Consent and associated metadata.
6. Consider new approaches and entities that enable consumers to manage their consents.
 - a. Explore the potential for independent Smart Data Consent Contracts
 - b. Explore the potential for privacy enhancing technologies
7. Develop cross-sector Customer Experience (CX) Guidelines for Market Participants.
8. Develop cross-sector Operational Guidelines for Market Participants.

To support these actions and initiatives, research is required in the following areas.

Regulation

- Regulatory consistency for consent across sectors
- Challenges codifying the approach to onward data sharing
- Strengthening of GDPR, its application and enforcement

Consumer

- Informed consent for the transfer of data
- Data cluster design
- Consumer language

Market

- Consumer understanding of data sharing in data provisioning chains
- Onward sharing in the provisioning chain
- Management of consent

Gaining consent from consumers

Neither GDPR nor PSD2 provide comprehensive approaches

We explore potential approaches to set cross-sector rules and principles for third-party providers and suppliers gaining consent from consumers.

Consent is an ill-defined term. It is generally used to describe a consumer sharing data for a particular purpose: in effect giving a third party provider permission to access personal data from a specific source. From a regulatory perspective it can be defined as one of the lawful bases for processing data under GDPR, while in Open Banking/PSD2 consent relates only to the transfer of data.

From a consumer perspective 'consent' is not clear because to access a product regulations require that consumers first understand and agree the Terms and Conditions for the product, then understand and acknowledge the Privacy Notice before going on to share their data. This is a lot of information to absorb.

From the consumer's point of view, they are 'just' buying a single product or service. Given the consumer's ability to assimilate layers of information for both the product and data sharing, alongside known behavioural traits we all exhibit, the expectation set is unrealistic.

Regulation has therefore created an approach which cannot be applied by consumers and genuinely 'informed consent' is in practice impossible. The risk is that consumers do not understand what they have given 'consent' to, especially with regards to the use of their data.

GDPR is the regulation for data protection but it should be made to work more effectively for the consumer. The pioneering UK Open Banking consent model has sought to address both sets of regulation in its approach, which is frequently held up as a model of good practice, but this too has gaps that must be addressed.

At this early stage of development, there are no alternative standardised approaches at scale that can genuinely be considered.

Therefore, we consider consent by learning from the progress made by Open Banking. We consider how this could be developed to create a well functioning cross-sector approach through the lens of consumers, market participants and regulation. For example, there are emerging technical and commercial solutions that serve as signposts in the Open Banking ecosystem, with existing TPPs (AISPs) beginning to provide market driven solutions to consent management.

Further work should consider how to build on this progress, including new approaches and entities that would enable consumers to manage their consents through innovation that would drive competition and economic benefit.

For the full potential of Smart Data to be achieved, the approach to consent should be led by some key principles.

The most important principle is that of trust

Consumers share data because they have a basic level of trust in the system and a cultural belief they will be 'protected' in the event something goes wrong¹. Consumer primacy must therefore lead our thinking. The key principles for consent should be that it is:

- **Controllable:** consent management is core;
- **Transparent:** the way in which data is used is clear and understandable;
- **Balanced:** the value exchange between consumer and TPP must be understood and acceptable to the consumer and TPP;
- **Protected:** the consumer is secure, can get help and be awarded redress if something goes wrong.

Trust is, however, a fragile concept. It must be achieved and maintained in a rapidly growing ecosystem, where increasing numbers of market participants – nodes in the ecosystem network – are handling exponentially growing volumes of personal data in complex chains. This data is an important driver for economic growth. For this reason, the policy decisions, regulations and standards taken now must be designed to evolve to meet the needs of both consumers and market.

Impacts of requiring ongoing consent

As data can be accessed and used on an ongoing basis this creates implications for how consumers can manage and control data in scenarios of ongoing consent. PSD2 provides for 90-day re-authentication to protect against extended periods of sharing without a consumer re-confirming the arrangement. However, it does not work well for either engaged consumers or the market. It has a poor customer journey and can lead to consumer drop-off; or worse, hinder use of the very service that the consumer needs.

¹ https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf

Furthermore, in Open Banking there is a disconnect between the consent which may last longer than 90 days and re-authentication. A firm may still derive value from data the consumer has previously shared using this consent which might be at odds with the consumer's view that they have let the 'consent' lapse.

Additional complexity is encountered when considering data carried through the provisioning chain and the dynamic way in which data can be shared between different data controllers. Without effective tools, consent management will become ever more challenging. This is a gap that must be addressed. Open Banking has only addressed this issue in a limited way, and PSD2 does not provide for consent management tools.

We concur that, as noted in the Smart Data Consultation, additional protections providing enhanced rights above and beyond existing data protection legislation will be required. We propose that these additional protections and enhanced rights could be enacted via a 'Smart Data Right' that would deliver the required level of consumer trust, and could be achieved through introduction of a 'Smart Data Consumer Agreement' between the TPP and consumer.

Our aim here is not to provide a comprehensive answer to these complex questions but to narrate the critical areas for investigation for further consideration and research. We are at the early stages in the development of Smart Data, with the opportunity to ensure it delivers powerful consumer, economic and societal benefits.

The issues identified and recommendations herein will add to the debate on National Data Strategy as we collectively build a world-leading data economy.

Recommendations

Our core recommendation is that BEIS consider development of additional consumer protections and enhanced rights for consumers through a 'Smart Data Right' and a 'Smart Data Consumer Agreement'.

Such an agreement would be between the TPP and consumer and would encompass:

1. A new standard for consent including requiring TPPs to put the interests of consumers first;
2. The requirement for TPPs to provide consent management tools and bring GDPR rights to life;
3. The requirement for TPPs to act as 'Data Custodians' providing for the option to manage or reject onward sharing for services;
4. Consumer access to ADR and redress (see our paper on liability).

This will require a number of initiatives, described below, considering the requirements for policy, standards, market and guidelines.

Smart Data Right & Customer Agreement

Additional consumer protections and enhanced rights:

- Consumer privacy
- Control of consent throughout provisioning chain
- Access to ADR and redress

Key Policy Drivers

Determine the desired consumer, economic and societal outcomes

1. Review and test current legislative and regulatory mechanisms, propose enhancements for consistent approach
2. Develop cross-sector consistent approach to participant categorisation with common terminology

Standards

1. Develop a cross-sector Smart Data Consent Standard
2. Develop API specifications for consent and associated metadata

Market

Consider new approaches and entities that enable consumers to manage their consents

Guidelines

Customer Experience & Operational

1. Determine the key policy drivers and values for consent and its management early. These should determine the design of the technology and success of the smart data initiatives.

The work undertaken should consider and determine the desired consumer, economic and societal outcomes as the starting point, creating a clear vision for a well functioning Smart Data ecosystem: what will this look like at key points in its evolution, and what therefore are the key policy issues that will make smart data initiatives successful?

This should go beyond a functionally driven roadmap, and should challenge existing regulatory and market norms. It should take a holistic approach, noting, for example, the interlinkage between the issues raised in both the consent and liability reports.

2. Review the current legislative and regulatory mechanisms, ‘test’ whether they remain fit for purpose for future initiatives, and propose enhancements, ensuring regulatory consistency for consent and its management in smart data initiatives across sectors.

It will be essential to ensure consistency and familiarity in the regulatory requirements for data sharing across sectors. Regulators must work collaboratively across their sectors to ensure that unnecessary barriers and obstacles do not arise.

How will relationships between regulators work? Where, in particular, will the regulatory perimeters be? This exercise should look beyond the finance, telecoms and energy sectors to include sectors such as healthcare to identify examples of best practice.

3. Create cross-sector consistency in participant categorisation and a common terminology.

Given the evolving nature of the ecosystem, the different roles of market participants and the regulatory boundaries that apply, it will be essential to create a consistent approach to the types and roles of market participants that works and is well understood across sectors.

Standards

1. Develop a cross-sector Smart Data Consent Standard

This would create standardised values for data access, sharing and consent parameters, including the consent purpose as a codified approach. This is envisaged as a common set of parameters and values to capture (and record/manage/revoke) consumer agreement and consent.

A codified standard brings to life data protection laws in a more meaningful way, against which success or failure can be measured. The Information Commissioner's Office (ICO) makes a series of recommendations about what should be included within a data sharing agreement which could be included in such a standard. These include:

- The purpose of data sharing
- Other organisations involved in the data sharing
- What data items will be shared
- The lawful basis for sharing (for GDPR)
- Inclusion of special category or sensitive data
- Access and individual rights of the consumer
- Information governance arrangements (such as accuracy of data, the deletion of data, termination of data sharing and complaints management)
- Review periods for the agreement

This should be developed from the consumer perspective, with emphasis on user experience, and allowing for the interconnected nature of the data provisioning chain. While this must be designed to encourage consumer adoption without undermining competitive innovation, it is against this standard that a regulator can measure accountability and compliance with law.

Development of a standard would, in turn, enable creation of an API endpoint for Smart Data Consent at the TPP, and support the implementation of the Smart Data Consumer Agreement between the TPP and consumer, which would be inextricably linked.

2. Develop API specifications for Smart Data Consent and associated metadata

Develop an API specification and associated metadata that enables the detail of the Smart Data Consent to be checked by authorised parties in the provisioning chain or carried alongside the consumer's data in the API payload. In particular, the metadata could carry the details of the Smart Data Consent and Consumer Agreement. This should be designed in a way that could potentially support development of consent 'contracts' which can only be controlled by the consumer.

Market

1. Consider new approaches and entities that enable consumers to manage their consents

Given the complexity of managing ongoing consents, and the proliferation of consent and access management across the ecosystem, it would be useful to consider how this could be managed most effectively for the consumer and market alike.

This could, for example, include new models such as entities that (using a common Smart Data Consent Standard, API specifications and associated metadata) undertake the management of the consumer's consents on their behalf. An understanding of the consumer and market needs, and how new approaches may be able to address the challenges is required.

2. Explore the potential for independent Smart Data Consent Contracts

Such contracts are envisaged as having parameters and rules agreed by the consumer in the Smart Data Consumer Agreement that are independently recorded and applied in software form, controlled only by the consumer and executed when a change is made to the agreement.

This type of 'smart contract' would provide control, management and enforcement of the agreement, potentially reaching widely across the ecosystem with changes applied automatically.

3. Explore the potential for privacy enhancing technologies

This is an emerging technology that restricts access to parties involved in the provisioning chain where a processing activity can be undertaken without having to access the data itself. The data remains encrypted while the processing activity takes place, and therefore cannot be compromised or misused. This is an emerging area that holds promise for consent management, data privacy and associated liability².

² <https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/>

Guidelines

1. Develop cross-sector Customer Experience (CX) Guidelines for Market Participants

These should describe the optimised customer journey, with the objective that the consumer is clear about the process and how to exercise their rights, and seeks to establish a familiar approach. This should include:

- a. Guidance on language, so that easily comprehensible words and phrases are used that are easy to read and well understood.
- b. Guidance on the parameters for the Smart Data Customer Agreement including consent, so that the terms, conditions, and privacy policy are clearly explained. This should include why the data is needed and what specifically it will be used for, the specific data clusters/types and duration that access to the data is granted for. Moreover, the way in which this data will be used and shared, their rights, and the way in which they can manage their data should be explained.
- c. Guidance on the optimum customer journey at each stage, including annotated wireframes and assistance with interpretation of and compliance with the appropriate regulation.

2. Develop cross-sector Operational Guidelines for Market Participants

These should provide guidance on how to best implement their regulatory obligations, so that market participants act and present themselves to the consumer in the best possible way. The initial focus should be on process and operational capabilities relating to data sharing in the provisioning chain. However, the scope should be defined. Aspects such as information security, data privacy and data ethics could be considered.

Summary of concepts

What is Smart Data?

In its Smart Data Review¹, BEIS explains that 'Smart Data' is an enhanced framework which extends the GDPR right to data portability to the real-time sharing of data via a set of standardised APIs. Data includes both product data (which includes new data sets such as performance data) and personal data.

What is a Smart Data Right?

The Smart Data Right would give consumers the right to port their data from regulated service providers in real-time to a Third Party Provider (TPP) in a safe and secure manner.

What is a Smart Data Consumer Agreement?

The Smart Data Consumer Agreement would confer new responsibilities on market participants and regulators to mitigate risks which occur in complex data chains. It extends and brings to life some of the key GDPR provisions.

What is a Smart Data Standard?

The Standard would be the suite of API standards, specifications and guidelines which underpin the technology across regulated sectors and ensure it is interoperable and consistent. It makes the transfer of data safe and facilitates consumers' control over their data.

What is a Smart Data Consent Standard?

The Consent Standard would codify the parameters of consent that the consumer has granted to the TPP in a consistent way across all sectors. The parameters would include those suggested in the ICO's 'data sharing agreement'.

These concepts require further research and definition.

¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808272/Smart-Data-Consultation.pdf

Overview

What are potential approaches to set cross-sector rules and principles for third-party providers and suppliers gaining consent from consumers, and what is the impact of requiring ongoing consent?

The Department for Business, Energy and Industrial Strategy (BEIS) is carrying out policy work looking at how best to enable and deliver Smart Data initiatives. These are sector specific initiatives aiming to facilitate the secure sharing of consumer data with third party providers, who use this data to offer innovative services for the consumer. This builds on proposals introduced in the Smart Data Review in June 2019. The aim of this policy work is to inform the development of data portability initiatives in energy, telecoms and finance (with scope for applicability across further sectors).

BEIS Smart Data Review, 2019 define Smart Data as follows:

“Smart Data enables consumers, if they wish, to simply and securely share their data with third parties, to enable them to provide innovative services. The UK’s data protection laws already give consumers the right to request that businesses provide their data to Third Party Providers (TPPs) in a commonly used format - this is known as the right to data portability. ‘Smart Data’ represents an extension of this right and provides an enhanced framework for sharing consumer data that allows for further innovation.”

We consider key features of Smart Data initiatives to be:

- the immediate provision of data by the data holder to TPPs following a request from a consumer (rather than the one month permitted in the right to data portability)
- the use of Application Programming Interfaces (APIs) to share data securely, but only once the consumer has verified their identity and the TPP has received their express consent to do so
- where appropriate, an ongoing transfer of data between businesses and TPPs, rather than a one-off transfer
- adherence to common technical standards, data formats and definitions to ensure interoperability and to minimise barriers for TPPs
- provision of certain product and performance data, such as tariffs or geographical availability of services, in addition to consumer data, if necessary, to enable innovation

We propose further research in consumer consent characteristics and guidelines which could be used in Smart Data initiatives (e.g. scope, frequency, expiration and revoking consent). Ultimately, this research aims to inform how consent mechanisms can be designed for individual or cross-sector initiatives in a way that encourages cross-sector interoperability i.e. so that consumers do not face different consent processes and characteristics as they move between sectors and suppliers and can rely on the same processes in different sectors.

Effective implementation of Smart Data initiatives must put consumers firmly in control of both how their data is shared and how it is subsequently processed and managed, in order to encourage trust, promote widespread adoption and thereby enable successful market innovation.

This work has been developed help shape the work of Smart Data by identifying potential options and approaches to developing cross-sector rules and principles for consumer data sharing and consent by third party providers (TPPs) and suppliers, including parties in the provisioning chain.

It takes into consideration the existing regulatory environment and current data request mechanisms such as GDPR and PSD2. It identifies the critical factors that build consumer trust where ongoing consent to share data is required. The aim being that consumers should not face different consent processes as they move between sectors and suppliers, enabling them to benefit from an experience that is familiar and trusted.

Consent

We consider a cross-sector approach to consent and draws upon our direct experience in the banking and fintech sectors in order to recommend suggested next steps for further research and the development of practical solutions.

The recommendations outline the key initiatives required and questions for further research to consider in its development of cross-sector data-sharing standards.

What we mean by Consent

For a consumer, an effective process to provide consent to share their data and then manage this is critical if they are to realise the value from their data and see a direct benefit while exerting their data and privacy rights.

The concept of consent as discussed in this work, should not be confused with consent as defined under GDPR as a lawful basis for processing personal data.

Consent in that regard is a separate and distinct consideration, which comes with its own challenges and wider considerations which will not be explored herein.

Similarly, any references to revocation of consent is not referring to revocation of consent, where consent is utilised as a lawful basis for processing data. Here, consent takes on a meaning, as a basis for the transfer of data.

GDPR defines consent as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. The term “explicit consent” is also used. This is needed when processing special; category personal data in addition to the lawful basis, and requires an express statement of consent. Explicit consent is not defined under PSD2, but is the contractual consent the TPP is granted by the consumer. However, there is no formal guidance from the FCA on how this should look.

Consent to share data has a number of dimensions:

- Providing the consumer with a clear purpose for sharing the data, the actual data being shared, the way in which the data is being used, whether the data will be onward shared in a provisioning chain, and the duration of the agreement.
- Validating that the consumer is who they say they are, and has the authority to share the data (known as authentication).
- Obligations to the consumer to ensure that they agree to continue to share access to their data at intervals (such as the 90-day re-authentication process required under PSD2).
- Enabling the consumer to review, amend or extend the consent that they provided.
- Ensuring that the consumer can stop sharing their data, and where regulations allow, to delete or restrict the use of the data, or prevent any further use.

These dimensions of consent for data sharing can be illustrated in six stages of a customer journey.

Stage One: Set Up. The process to open an account with the service or supplier through an app or website. At this initial set up stage, the consumer is introduced to the current (mandatory) data protection obligations such as the legal basis for processing the data (such as performance of contract, legitimate interests or consent). It will include a Privacy Notice (i.e. highlighting how their data will be used, shared etc.).

Stage Two: Consent. The process utilised by the TPP to obtain the consumer's permission to access their data and for the consumer to agree to share this data with the TPP for the purpose of enabling the service. In Open Banking this is achieved by virtue of an 'explicit consent' (otherwise known as a contractual consent). TPPs are required (prior to any processing taking place) to explain to a consumer the financial information that is necessary for the purpose of the service they are providing (AIS or PIS) and then obtain permission from the consumer to obtain that data from their ASPSP. This explicit consent is in addition to all the mandatory data protection obligations that fall on the TPP (as Controller of data) under GDPR protections outlined in stage one.

Stage Three: Authentication. The process by which the consumer identifies themselves to the data source so that the request can be granted, with the assurance that the consumer has granted consent for the specifics of the data sharing they agreed to in Stage Two..

Stage Four: Consent Management. The stage at which the consumer is able to access tools such as a 'dashboard' in order to view and manage their consent.

Stage Five: Revocation. The process to revoke consent with the TPP so that the consumer's data is no longer shared by the data source. This may be provided for through the provision of a Dashboard as at Stage Four.

Stage Six: End. The process for service cessation including, where appropriate, the deletion of data or the putting out of use of the data by the TPP.

For the purposes of this work, the stages considered are Set Up, Consent, Consent Management and Revocation of Consent.



These stages are shown illustratively but it is important to note that in practice this is not linear. This journey should be regarded as one overall experience, and will vary from TPP to TPP and between subsequent parties with whom data is onward shared. It is important to the consumer that this journey is implemented in a way that is easy to understand, intuitive and as seamless as possible.

The value exchange between the consumer and the service provider or supplier must be clearly communicated and understood

To facilitate the aspirations of the Smart Data initiative the value exchange between the consumer and the service provider or supplier must be clearly communicated and understood by the consumer throughout this process, so they are able to make informed decisions.

Any request made by a TPP to a consumer to share personal data requires, on the consumer's part, a clear understanding of the principles enshrined in law to protect the confidentiality and integrity of the data being shared. Similarly, any desire to onward share personal data or process personal data requires full consideration of the current data protection laws. This work will touch upon the current legal and regulatory framework and explore (where applicable) their shortcomings both in the context of data sharing today and for the future as being explored under Smart Data.

Learnings from Open Banking

The introduction of PSD2 has brought about an additional level of transparency and protection for payments services, while the CMA Open Banking Order provides for standardisation across the largest data providers. The experience of Open Banking demonstrates that:

- Standards reduce complexity, facilitate competition and improve the consumer experience.
- Security, quality of implementation and conformance are key success factors.

Standardisation requires collaboration in the market, leadership and ongoing supervision for conformance to the standards, especially where firms are being required to share data rather than giving it up voluntarily.

However, some elements are missing from Open Banking:

- Open Banking focuses on PSD2 and specifically, financial data to the extent it relates to a payment account and in turn a provision of service, such as AIS and/or PIS. This means the customer journey has focused on an explicit consent for the limited purpose of the transfer of payment account information to the extent it is necessary to enable the TPP to perform their service. PSD2 has provided for an explicit consent for the first transfer of data (from the bank to TPP) but it has not provided for informed consent further down the data sharing chain (for anything outside the parameters of PSD2). This must be catered for by GDPR.
- The legal basis relied on by the TPP for using the data under GDPR is most likely to be
 - a. legitimate interest,
 - b. performance of contract or
 - c. consent.

Each of these has advantages and disadvantages. For example, using consent as the legal basis may require the consumer to provide a new consent when the TPP changes some aspect of the way it uses the data (not ideal where ongoing consent is required), whereas legitimate interest may allow firms to hide their business practices behind their Privacy Notices and their Terms and Conditions.

The following table highlights the advantages and disadvantages of the different lawful bases both from a Controller and consumer perspective. The other three lawful bases are excluded as out of scope of the purpose of this work.

Lawful Basis	Implication on Controller	Implication on Consumer
<p>Consent</p> <p>Explicit Consent</p>	<p>Will need to ensure the consent is clear, unambiguous and evidence that it has been freely given Consent may not be bundled so for each purpose that data will be needed for, a consent will be required.</p> <p>When purpose changes a new consent must be sought - no processing may happen outside the parameters of the consent obtained.</p> <p>Applicable if the Controller is also processing special category personal data and is in addition to the above consent.</p>	<p>A consumer can withdraw consent at any time - this is an absolute right - and once withdrawn the Controller must stop processing. This will then also trigger a number of GDPR rights which the Controller will be obliged to resolve.</p> <p>If a change triggers the need to obtain a new consent from the consumer, this may result in inconvenience and has been shown to cause consumers to drop off the service. It's therefore not ideal either to a consumer or TPP.</p>
Performance of Contract	<p>Permits Controller to a potential wider use of data under the guise of provision of service being offered.</p> <p>Could be far reaching as long as it is deemed purpose and use can be legitimately evidenced against Principle(s)1 and 2 GDPR</p>	<p>Gives a Consumer a degree of control over how their data is being used. It may still be shared with third parties if that sharing is required in order to enable the Controller to perform their obligations under the contract but the provisioning chain would understandably be more limited</p>
Legitimate Interest	<p>The broadest and most flexible lawful basis as long as the Controller has satisfied the three-pronged balance and necessity test (known as a legitimate interest assessment - LIA).</p>	<p>A consumer would not necessarily understand or appreciate the extent and breadth of this lawful basis and what is actually happening with their personal data.</p> <p>This means that there is no need to seek a new consent if something changes (and means the TPP has flexibility) but may result in consumers remaining unaware of something that they would not otherwise agree to.</p>

Typically, a Controller relies on a number of lawful bases and will undertake an appropriateness assessment in the context of the personal data in its possession and then apply the appropriate lawful basis against that specific category of personal data. A Controller cannot utilise all lawful bases as a 'catch all'. If the lawful basis changes, the Controller will, if challenged, need to demonstrate the move away from one lawful basis to another and why the replacing lawful basis is more appropriate and what has changed that led to a change in lawful basis. This is likely to be communicated to a consumer via an update to a Privacy Notice.

Open Banking has provided for explicit consent within PSD2 for the transfer of specific data. However:

- TPPs do not always provide clear and transparent information on their key Terms and Conditions of the service and Privacy Notice to consumers, so the implications of giving consent may not be well understood. There is a tendency towards a lack of transparency e.g. the consumer has to scroll to the bottom of the page and agree without reading, or at best skimming the text, in the course of which they may not have paid attention to the Privacy Notice. This is a key issue when considering the balancing of the value exchange between consumer and TPP;

while for Consent Management:

- Open Banking has not provided the ability to fully address the rights afforded by GDPR beyond the creation of basic access dashboards at the data source, which are limited in functionality;
- It is not always easy for the consumer to identify, manage and revoke consent under PSD2 at the TPP, and similarly difficult to cancel access at the Bank (the data source) although this is mandated through the use of an Open Banking ASPSP access dashboard. This can happen, for example when an Agent provides a service through an authorised TPP (providing AIS) but does not provide their brand name to the TPP for reasons of cost and/or lack of resource to do the necessary work;
- Consumers have little control over sharing data that is private or sensitive. This can prove to be a barrier to use, or can have a negative impact such as raising the risk profile of the consumer because they redacted some information or chose not to share data.

Some aspects of the customer journey should work more effectively.

- Authentication at the data provider (the ASPSP for Open Banking) has proven a difficult part of the customer journey to implement consistently and seamlessly. This has been a major hurdle, requiring intervention by the Trustee, supported in his regulatory capacity by the CMA, to ensure an appropriate and consistent journey.
- The requirement for re-authentication at 90 days can lead to very significant consumer drop-off and is generally a poor customer experience. The underlying policy for re-authentication lacks some transparency. For the EU, the purpose was to improve security. However, it was later described in the UK as a way to mitigate the risk of continued data sharing by inert consumers who are no longer engaging with a product or getting value from it. Re-authentication appears to cause attrition even among engaged consumers.

-
- For consumers that switch their bank account using the Current Account Switching Service (CASS), the consents associated with the account that is being switched from are not automatically transferred to the new bank account³. This can mean an interruption to service which might have consequences for the consumer. It is, in any case, a potential barrier to switching and a poor customer experience. The consumer has to connect their new data provider to each of the services that they want to retain. This assumes that the TPP supports the new data provider. This would be the same for consumers switching telecoms or energy provider. It could increase the perceived hassle of switching and make accounts stickier. In cases where popular TPPs only support one or a limited set of providers, this could reduce switching or 'trap' consumers into one data provider.

TPP services often involve several participants in the data chain. TPPs can also play different roles in the data chain, acting as both TSPs and data providers. Data can be shared and ingested by multiple different parties in different ways. This reduces consumers' ability to make genuinely informed decisions about sharing their data. It's overwhelming for the consumer to manage, and potentially provides room for both exploitation and reduction in competition, because the winner takes all. This is evident in online retailing.

Managing consent is therefore a key part of helping consumers enact their data rights and provide protection. Onward sharing creates risks which may be exacerbated when consumers manage consent across multiple sectors with different regulatory regimes. This suggests that new ways of managing the consumer's consent across data provisioning chains (and possibly providing other important services such as allowing consumers to complain) should be considered.

Further work will be undertaken through 2020 in line with the Open Banking Implementation Entity Roadmap⁴ including:

- Evaluation of Efficacy of Consent and Access Dashboards
- Root Cause Analysis on consent success
- Exploring the feasibility and design of capturing consent and enabling traceability and auditability.
- Building on the existing TPP Guidelines to develop standards that address all aspects of consent and permissions, in particular the codification of purpose of data sharing.

3 <https://www.wearepay.uk/enhanced-current-account-switching-in-the-era-of-open-banking/>

4 https://assets.publishing.service.gov.uk/media/5e398d5840f0b609278cd388/Trustee_Roadmap_Proposal_to_CMA_FINAL_-_200203.pdf

Regulation

The current approach to consent is shaped by the regulatory environment, so this work recognises the challenges and implications of this. As noted, when a consumer signs up for a new product or service, a number of consumer protections are triggered such as applicable key Terms and Conditions to the product or service in question, provision of a Privacy Notice, specific regulatory disclosures, as well as mandatory obligations under data protection laws. The communication therefore with the consumer needs to take account of the differing (often complex) and typically 'information heavy' statutory requirements as may be triggered.

Parties in the provisioning chain (while catered for under GDPR) could also be subject to sector specific laws and regulations. However, the extent to which these are relevant in the notion of data sharing (or onward sharing) would be limited. Many would not be operating under sector regulation and therefore would only be operating against a backdrop of compliance with data protection laws. This is explored in the chapter 'Market Participants'.

Sector-specific regulated entities dealing with personal data are generally only required to comply with data protection laws. Any additional regulatory requirements imposed on such entities usually relate to matters such as disclosure of key information (enabling customers to make an informed choice as to whether to take that particular product or service).

Consequently, for the purposes of data protection, the processing, sharing of personal data, compliance with data protection laws is critical. The ICO publishes useful guidance⁵. For non regulated entities, which are not sector specific, when it comes to personal data, the reference point remains data protection laws.

Once a Privacy Notice and its method of delivery has been determined, and prior to any processing taking place, a TPP acting as Controller must identify the appropriate lawful bases for processing personal data. Identification of lawful bases is important in two aspects for the purpose of this work, namely:

- It is a mandatory requirement to communicate this to a consumer (prior to any processing taking place); and
- It is the legal springboard from which a TPP (Controller) uses personal data.

When undertaking an assessment for the selection of an appropriate lawful basis, a TPP will take into account a number of considerations. The most striking and least consumer transparent being:

- Its own business model and profitability; and
- What requires the least explanation and consumer intervention versus maximisation of usage.

5 https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

It is generally accepted that the broadest and most flexible lawful basis is legitimate interest because this lawful basis enables a TPP (or Controller) to maximise its use of the personal data in its possession. Once a Controller overcomes the statutory obstacle(s) of (i) undertaking a satisfactory legitimate interest assessment (LIA), (ii) a determination that legitimate interest is the most 'appropriate' lawful basis and (iii) meeting the transparency requirements of communicating this in a Privacy Notice, a TPP (Controller) can quite legitimately:

- Use that data (or indeed obtain personal data from another source) in a way that perhaps has not fully been understood or appreciated by the consumer;
- Be shared with parties in a provisioning chain that a consumer may not necessarily be aware of, or would not have consented to (had they understood);
- Be used in a way in the provisioning chain in a way that was not within a consumer's reasonable expectations.

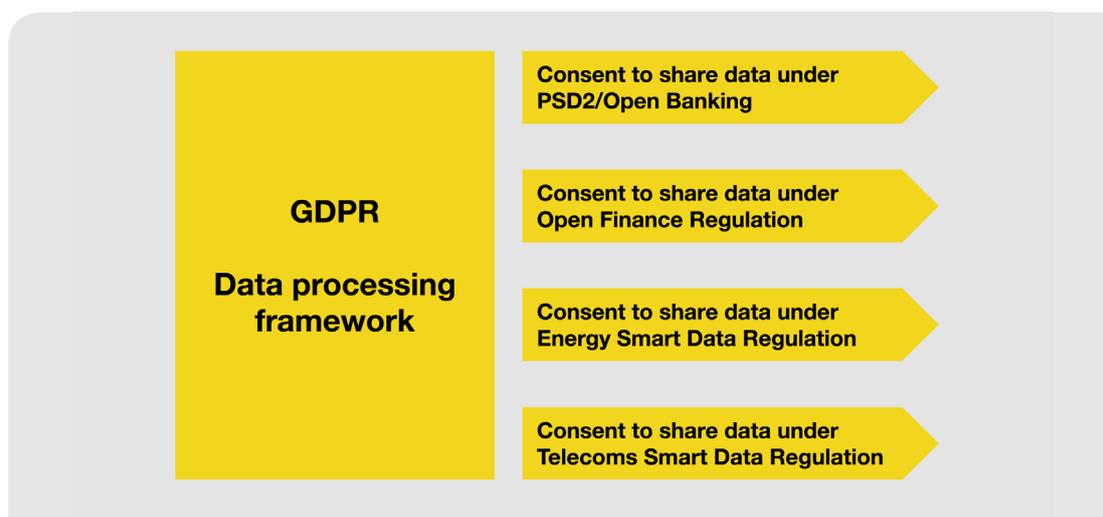
Importantly, this is because, as currently drafted, the law permits a Controller to use or share personal data to meet its own legitimate interests or the interests of third parties. The interests of third parties being the most controversial in that they can include commercial interests, individual interests or broader societal benefits.

Conversely, a TPP (Controller) is likely to shy away from 'consent' as a lawful basis unless it is absolutely required to do so, because of (i) the strict statutory requirements of obtaining a valid consent and importantly its restrictive use, thus making the use of legitimate interests particularly attractive. In fact, many Controllers may in fact simply be 'chancing' their use for this lawful basis until such time they come under the scrutiny and challenge from the ICO to explain away its appropriateness. The ICO is yet to undertake any assessments of the appropriateness of usage of lawful bases by any Controller.

Therefore there is an opportunity here to:

- Obtain detailed insights in the usage of legitimate interest and the extent to which it currently may be used too broadly;
- Consider how some of the above identified 'harms' could be mitigated via the introduction of a consent standard - applicable to onward sharing;
- Consider a possible change in the law to prevent legitimate interest as currently defined under GDPR to be used for the specific purpose of onward sharing.

With the TPP having determined the lawful basis, GDPR then provides the core framework for sharing personal data. Against this backdrop the relevant sector-specific regulation, such as PSD2 must be considered. In effect, GDPR supports data sharing across sectors, working in synergy with the relevant sector-specific regulation.



Consumer protection

Current consumer laws do not extend in scope to cover potential harm and damage suffered by consumers as a consequence of unauthorised data sharing. This will need to be addressed either in an amendment in current legislation or via other mechanisms. Further, to add to the complexity this is then overlaid with the existing statutory obligations in respect of the provision of specific goods and services (i.e. ensuring product or service Terms and Conditions meet the CRA 2015⁶ obligations in good time before a consumer is tied in).

Considerations in Open Banking

The Open Banking model in its current form does not provide an appropriate model for the issues and challenges presented with cross sector data sharing for the following reasons:

- There are legislative restrictions as well as inconsistencies and conflicts between PSD2 and GDPR;
 - PSD2 only goes as far as mandating an explicit consent for the sharing of data between ASPSPs and TPPs specifically for the provision of account information and/or payment imitation services respectively;
 - It is limited in scope to payment accounts;
 - The consent is 'explicit' and is limited. It is limited to 'that information which is absolutely necessary' to enable a TPP to carry out its service. The explicit consent under PSD2 does not permit a TPP to process personal data for the provision of other non PSD2 services, in the absence of a separate lawful basis under GDPR.
- Explicit consent has different meanings under PSD2 and GDPR resulting in confusion and an inconsistent/inaccurate application.
- There is a lack of clarity when GDPR obligations are triggered. Under PSD2 the FCA Approach Document⁷ only goes as far as to say that Participants must comply with both and that explicit consent under PSD2 is not to be treated as applying in the same way as GDPR;

6 <http://www.legislation.gov.uk/ukpga/2015/15/contents/enacted>

7 <https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf>

-
- Does not address concerns in respect of onward sharing of silent party data and transaction data which may inadvertently reveal special category data (triggering an explicit consent under GDPR);
 - Under PSD2, contractual arrangements are prohibited (deemed an obstacle) between ASPSPs and TPPs.

Considerations across other sectors

At the start of any customer journey for any product or service, any sector specific adopted approach would need to take into account the following critical factors:

- GDPR requirements
 - What is required at the initial set up stage as a minimum (i.e. a Privacy Notice)?
 - How will this be delivered (e.g. layered / interactively)
 - Audience and characteristics of consumer base (Privacy Notice and transparency must be tailored to consumer) to ensure understanding
- Sector specific product/service disclosures (i.e. pre contract information)
- Terms & Conditions a of product or service: (display and level of information and approach to content would need to comply with CRA 2015)
- Onward sharing of personal data provisions
- Management of onward sharing (i.e. data rights including revocation)
- Display and communication of Controller 2's (C2) Privacy Notice as the Consumer moves from Controller 1's (C1) and C1's Privacy Notice
- How data rights (if exercised) will be managed in the 'provisioning chain'. The immediate challenge is when the lawful basis changes from C1 to C2 and different data rights are triggered as a consequence and how this could be managed?

Energy: Midata

Midata aims to put domestic energy consumers in control of their data. By standardising the way this is done, it will unlock consumer benefits from tariff comparison and other services. Consumers can opt to provide ongoing consent so that automated services run on their behalf.

An example would be an app which checks the consumer is always on the best tariff. Currently, this is accessed through the consumer's online account where the Terms and Conditions and Privacy Notice are presented.

The consumer downloads a .csv file which they can use with price comparison sites. However, this is being streamlined and developed iteratively to deliver a better customer experience⁸.

8 <https://www.ofgem.gov.uk/gas/retail-market/market-review-and-reform/midata-energy-project>

Open APIs for Telecoms and Utilities

Work by the IF on behalf of the Open Data Institute shows how open APIs could enable new types of commercial products and service enhancements⁹. This highlighted that “Company policies like Terms and Conditions are often locked away inside PDFs and are impenetrable to ordinary people. AutoSwap demonstrated giving people choice about a company based on their privacy policy and social responsibility”. It does not, however, consider the actual consent process and management in detail.

Telecoms operators and the GSMA (the industry organisation that represents mobile operators worldwide) have been looking at how they might provide access to customer data, both sharing personal data and aggregated data. However, initiatives such these are still at an early stage and have yet to formally publish operational proposals, and for this reason Open Banking provides the most useful reference point.

Approaches to consent outside the UK

The WEF notes that the concept of dynamic consent promises controllability and transparency in its white paper ‘Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data’¹⁰ stating ‘Dynamic consent allows individuals to change their mind about the amount of data they wish to be used, and for what purpose. This provides a transparent and ethical vehicle allowing individuals to modify or withdraw their consent if they change their mind later. For researchers or other ‘data managers’, dynamic consent allows for better electronic tracking of consent, including the details of that consent. It is also hoped that people will be more inclined to consent to their data being used if they are given more flexibility to change their mind at a later date.

Elsewhere the Australian Consumer Data Right (CDR) most closely matches the objectives of the UK’s Smart Data Initiative. While the CDR has the strong benefit of a cross sector approach and architecture, it is somewhat hampered by a lack of granular detail which can lead to inconsistency in interpretation and implementation.

For example, under the CDR, market participants have been classified as either Data Holders or Data Recipients which brings a degree of consistency to cross-sector terminology. However, this is an area where the types of market participants and their regulatory obligations could benefit from greater granularity in their definition. This is something that should be explored further for the UK.

The CDR also includes Customer Experience (CX) Standards and Guidelines. The CX Guidelines provide detailed guidance on Consent¹¹. The approach to consent is similar to the UK in many ways, with divergence in some areas due to the differing regulatory regimes. Indeed, there has been ongoing informal discussion between interested parties in developing the two approaches. However, the CDR has a major difference to the consent model established by the UK’s Open Banking, in that it includes an authorisation step

9 <https://openapis.projectsbyif.com>

10 <https://www.weforum.org/whitepapers/federated-data-systems-balancing-innovation-and-trust-in-the-use-of-sensitive-data>

11 <https://consumerdatastandardsaustralia.github.io/standards/pdfs/CX-Guidelines-v1.2.0.pdf>

The Consent Flow

1. Consent — where the consumer is asked to consent to a data recipient collecting and using their CDR data

2. Authentication — where the consumer is asked to authenticate themselves with the data holder

3. Authorisation — where the consumer is asked to authorise the disclosure of their CDR data to the data recipient

(extract from the Australian CDR CX Guidelines)

The authorisation step can be viewed as a logical checkpoint for the consumer to review the data about to be shared. This can be seen as an advantage to consumers new to data sharing, but may be viewed as not required once consumers become used to sharing. Authorisation was not included in the UK Open Banking consent flow as it was deemed to be an obstacle to competition by the FCA under PSD2 regulation.

Anecdotally, some observers in Australia have expressed concern about current implementation of the consent model in the Consumer Data Right (CDR). At present the standards have not been implemented consistently (which has also been a challenge in the UK despite the regulatory mandate of the CMA).

In particular, two challenges associated with management of consent are cause for concern:

1. participating data holders or recipients must have a consent dashboard, but consumers have on average 200+ online relationships, which is overwhelming to manage.
2. the value exchange between consumer and TPP is not always communicated clearly. Specifically, the commitment required by the consumer in order to obtain the benefit being offered.

Overall, it is believed that when managing consent a significant problem lies in the proliferation and the complexity of inter-relationships in the data sharing ecosystem. Multiple services are developing, each with potentially multi-party chains. This is leading to a situation which is overly complex. This, it is believed, is not going to work for the consumer and a fresh approach is required. The key to finding a solution is to approach this problem from the consumer's perspective.

Regulation – summary of implications

As a result of this analysis and referencing the learnings from Open Banking, we conclude that cross sector consent regulation must ensure:

- The consumer understands the purpose for which data is being collected.
- That the purpose is not extended without the consumer's knowledge or agreement.
- Communication about what an organisation is collecting, why it is collecting it and what the organisation intends to do with it.
- If and when purpose changes having a mechanism in place to ensure purpose is reaffirmed.
- Data held is accurate or where necessary, kept up to date.
- There are robust controls and processes in place to securely delete, minimise or anonymise data, which is to only store it for as long as it is necessary.
- There are processes in place and robust systems to protect data from unauthorised or unlawful access.
- Concerns in respect of silent party data and transaction data which may inadvertently reveal special category data are adequately considered.
- Management of onward sharing of data between parties in the provisioning chain is clear, including transfer between controllers, the management of respective Privacy Notices and data rights. This may include consideration of measures to ensure privacy by ensuring parties can only access information necessary to undertake their specific role.
- Common terminology and definitions are used by all parties across sectors.
- Consent granted to the TPP and access to the data source must be transparent and manageable by the consumer.
- Consent management must be designed to enable consumer control through multi-party provisioning chains and complex inter-relationships in the data sharing ecosystem.
- Checks and balances are in place to ensure that where legitimate interest is used as a lawful basis, it is not used too broadly.
- Some 'harms' identified could be mitigated via the introduction of a consent standard covering onward sharing in the provisioning chain.

Regulatory – checklist for development

Checklist for development of cross-sector data-sharing standards from a regulatory perspective.

Suggested initiatives
Determine the key regulatory policy drivers and values for consent and its management.
Review the current legislative and regulatory mechanisms, ‘test’ whether they remain fit for purpose for future initiatives, and propose enhancements, ensuring regulatory consistency for consent and its management in smart data initiatives across sectors.
Development of a cross-sector approach to participant categorisation and common terminology.
Development of a cross-sector data sharing and consent standard, that would ensure a consistent approach to the issues identified and would provide a common framework for multi-party provisioning chains.
Development of API specifications for consent, and enabling consent parameters to be provided as metadata thereby ensuring that all parties in a provisioning chain have clarity of the consent parameters.
Explore potential new approaches and entities that enable consumers to manage their consents. This should include the consideration of independent (immutable) consent contracts, and the possibilities provided by privacy enhancing technologies (PETs).

Research will be required to inform understanding and decision making.

Suggested research
<p>Achieving regulatory consistency across sectors</p> <ul style="list-style-type: none">• How to avoid consumer overload and build consistency and familiarity into the regulatory requirements?• Ensure regulators work collaboratively across sectors to align, avoid obstacles to competition while sector-mandated requirements are built into any common standards?• How will the boundaries between the regulators be determined?• How will regulators adjust to cope with exponential growth in volume?
<p>Codifying the approach to consent in onward data sharing</p> <ul style="list-style-type: none">• How to improve clarity of purpose by standardising it?• How to standardise consent parameters?• How does a consumer ‘switch off’ ongoing sharing, what rights could be triggered if consent and continued sharing is switched off by the consumer?• How different lawful bases of different controllers sharing data will be managed, and how data rights are understood and triggered by a consumer? What obligations on other controllers with whom data has been shared and managed?

Strengthening of GDPR, its application and enforcement

- Obtain detailed insights in the usage of legitimate interest and the extent to which it currently may be used too broadly; and
- Consider how some of the above identified 'harms' could be mitigated via the introduction of a consent standard - applicable to onward sharing
- Consider a possible change in the law to prevent legitimate interest as currently defined under GDPR to be used for the specific purpose of onward sharing.
- Which 'common' factors from a data perspective, could be converted into 'common data elements' for use across sectors? These could include:
 - Agreed language for the consent for onward sharing;
 - Privacy Notice (i.e. when, how and where it is displayed in a customer journey, making it more familiar to a consumer);
 - Transparency requirements that ensure consumer comprehension;
 - Summary (or pop up) of any change in lawful basis when personal data passes from Controller 1 (C1) to Controller 2 (C2), etc.
 - Agreed language when communicating data rights (or any change) where there is a change in lawful basis for processing personal data.

Consumer consent

The current approach to consent has been largely driven by commercial interests and the regulatory environment as described above. As previously described, this approach means that it is difficult for consumers to give informed consent (PSD2) or to make an informed decision (GDPR & other regulations). From a consumer perspective 'consent' is therefore a blurred term.

To access a product the regulations require that consumers first agree the Terms and Conditions for the product; then understand and acknowledge the privacy notice, then agree to share their data. However, from their point of view they are just buying a single product. Going forward, a more consumer-focussed approach should help design Smart Data in a way that improves outcomes and mitigates unintended consequences.

Consumer attitudes and behaviours

The value of personal data has long been recognised by commercial interests of online retailers, social networks, social networks and 'big tech' companies. The way in which the consumer's data is being used is not generally well understood by the consumer and is all too often presented alongside long, impenetrable terms, conditions and Privacy Notices which the consumer accepts in order to be able to use the service.

Indeed, consumer research on attitudes to data collection and use by BritainThinks on behalf of Which? reveals that the data ecosystem is invisible to consumers, who have limited knowledge of it. People believe, incorrectly, that data transactions are bounded and are unaware of the extent of data sharing.

Consumers are primed to accept the collection of data about them as largely positive, because it is easier to identify and conceptualise benefits than harms. What is more, while consumers judge the acceptability of data collection by what impact it has on them, they often do not have information on which to actually judge this impact¹². Similarly, the DCMS Data Mobility Report¹³ found that

“Consumers have a lack of know how and understanding of the digital market, and limited knowledge about their data, how it is used, and how they could use it. This makes the individuals vulnerable to abuse and lacking in the skills to access the opportunity.”

It is evident that consumers all too often make decisions without a full understanding of the agreement they are making. They feel powerless to engage with organisations that are collecting and using data about them, but want meaningful control over their data. The challenge encountered by consumers is therefore that this can be a confusing experience in which their actions and the consequences, or any data related rights they have, may not be well understood.

¹² <https://britainthinks.com/news/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use-a-report-for-which>

¹³ https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf

However, ‘Unlocking Digital Competition, The Report of the Digital Competition Expert Panel’, Chaired by Jason Furman¹⁴ noted the great consumer benefit to be released if these issues are addressed:

“Personal data mobility means agreeing common standards to give consumers greater control of their personal data so they can choose for it to be moved or shared between the digital platform currently holding it and alternative new services.

By making this easy, consumers could, for example, move across to a new social network without losing what they have built up on a platform, manage through a single service what personal data they hold and share, or try out an innovative digital service that uses their information in a new way. Open Banking has shown the potential for data mobility to provide new opportunities to compete and innovate in this way.”

Consumer comprehension

In order to maximise propensity to share data it is essential to maximise comprehension, and to minimise the time to achieve this. The challenge here is that:

- Consumers are expected to read the Terms and Conditions of the product they want and understand it. This might be a more complex product such as a mortgage or an energy tariff, which are already quite complicated to understand.
- Consumers are supposed to have read a Privacy Notice to understand how their data will be used and processed in providing the product or service.
- Consumers should understand that they are giving explicit consent for the transfer of data.

The large amount of information alone makes unrealistic expectations on the consumer. Factor in their desire to achieve the promised benefit from that product or service, and insufficient notice may be taken of the implications of their actions, or the Terms and Conditions.

This leads to uninformed decision making: the risk being that consumers do not understand what they have given ‘consent’ to. As their data may be accessed and used on an ongoing basis this creates implications for how consumers can manage and control data in scenarios of ongoing consent.

TPPs must implement a customer journey flow that accommodates and enables consumer understanding of a number of different legal and regulatory requirements.

¹⁴ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

During Stage One, 'Set Up', a well designed customer journey flow needs to take into account the following regulatory requirements:

- Presentation of key Terms and Conditions of the product or service being offered;
- Presentation of key information/ disclosures and exclusions - specific to the regulatory environment which the TPP is operating;
- Presentation of a Privacy Notice. This needs to be provided prior to any processing taking place.

Whilst the ICO has provided very clear guidance on good practice on bringing Privacy Notices to a consumers attention in an effective manner, typically, in attempting to design a frictionless, consumer friendly journey, this can be overlooked. It must be recognised that consumers are concerned about use of their data, particularly if it is shared with other brands or service providers and leads to unwanted consequences.

Within this stage of the customer journey it is therefore imperative that a consumer understands the main points before being asked to provide their consent to share their data. The key aspects that should be explained clearly are:

- The proposition. What benefit will the consumer get from this service or supplier?
- How their data will be used, how it won't be used, and how it will be handled if it is shared with other parties in order to provide the service.
- The legal basis that is being relied on to lawfully process the consumer's data.
- How they can manage their data, stop sharing, trigger any data rights together with any consequences that might arise if they do stop.
- How the business makes money. This is particularly important if the data shared by the consumer is the basis for the business model, such as advertising-funded.
- How the consumer can get help if something goes wrong, and how they are protected.
- How the business or organisation is regulated.

At Stage Two, 'Consent', clarity of the consent agreement is essential. It is at this point that the TPP is establishing consent for the purpose of obtaining and/or onward sharing of the consumer's personal data.

However, for the consumer, consent to share data is not yet a familiar experience and is often not expected. It may be unclear within the consent step what it is for, or the impact it has. Therefore, a critical aspect is that the purpose for data sharing is well understood.

Clarity and consistency can be achieved by following a standard approach. For example, in order to address this, Open Banking recommends a purpose statement that follows the following structure:

'To provide a [describe type of proposition] service, we need to [describe data processing activity]'

This could therefore read: 'To provide you with a debt advice service, we need to analyse your income and spending patterns'

Such an approach could be adopted across all sectors and would become familiar to consumers, thereby increasing familiarity and comprehension. This purpose should reflect any regulatory authorisation granted.

Other critical elements of the consent that must be clearly explained are:

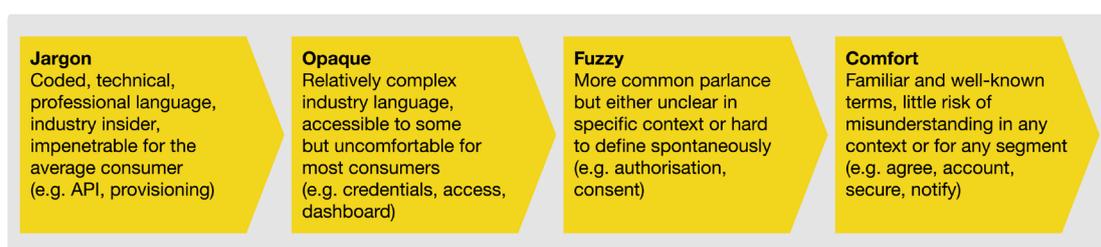
- The data to be shared. The data standard used in Open Banking groups data together into clusters (e.g. account details, standing orders, direct debits) and depending on the data type is available in either ‘basic’ or ‘detailed’ form. Lessons from this could be applied to the energy or telecom sectors. Consumers can then provide their permission to share these data clusters through the consent process.
- The duration of the data sharing. This may be one-off or ongoing.

At Stages 4 and 5, it is essential that the consumer can manage and revoke their consent once it has been granted. This is a critical issue for consumers and is explored more in the Market Participants section of this work, as this is a complex area that needs to take account of provisioning chains and the associated regulatory requirements.

Customer experience

The Open Banking Customer Experience Guidelines (CEG)¹⁵ provide a useful starting point for understanding the management of consent through the customer journey. These guidelines include work done by the Behavioural Insights Team on behalf of BEIS in the Best Practice Guide ‘Improving consumer understanding of contractual terms and privacy policies; evidence based actions for businesses’¹⁶.

Customer Experience (CX) Guidelines would be required in order for different sectors to develop and maintain a common approach that is familiar to the consumer. A particular area which should be considered in detail is clarity and consistency of language across sectors. This should include a glossary of common terms for use by market participants and regulators that consumers understand.



Developing such cross-sector terminology will require a research programme to determine the appropriate language and vocabulary that enables consumers to understand the concepts and capabilities being introduced. It will be critical to use professional and simple language that is easy to understand. Colloquial terms should be avoided, as should overly assertive phrases and words that might risk undermining consumer trust i.e. words that can invoke discomfort or undermine their sense of security. Likewise, ambiguous or unfamiliar language can raise concerns.

¹⁵ <https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/>

¹⁶ https://www.bi.team/wp-content/uploads/2019/07/BIT_WEBCOMMERCE_GUIDE_DIGITAL.pdf

Consumer – summary of implications

The customer journey must
be a good customer experience

As a result of this analysis and referencing the learnings from Open Banking, we conclude that consumer consent must be developed to meet the following needs:

- In future, a well designed consent model should place greater emphasis on consumer attitudes, behaviours and needs, such that consumers can better understand the true value of their data and realise the benefits from having their data work on their behalf.
- Consumers must not face different consent processes as they move between sectors and suppliers, and must benefit from an experience that is familiar and trusted.
- The purpose of data sharing must be well understood, and the value exchange between consumer and TPP (i.e. what the consumer must commit to in order to get the benefit offered) made very clear before the consumer makes the commitment to share their data. The consumer must be aware of the consequences of their actions.
- The way in which data is structured, described and controlled should be consistent across sectors.
- The extent of data sharing should be made very clear to the consumer.
- The customer journey must be a good customer experience whilst meeting the regulatory requirements for the sector and compliance with GDPR.
- Control and transparency should be central to the customer experience throughout the customer journey, from set up, through the consent process and including the management and revocation of consent.

Consumer — checklist for development

Checklist for the development of cross-sector data-sharing standards from a consumer perspective.

Suggested initiatives

- Determine the key consumer policy drivers and values for consent and its management.
- Develop API specifications for data sharing and consent, and enable consent parameters to be provided as metadata thereby ensuring that all parties in a provisioning chain have clarity of the consent parameters.
- Develop a cross-sector data sharing and consent standard, that would ensure a consistent approach to the issues identified and would provide a common framework for multi-party provisioning chains.
- Develop cross-sector Customer Experience Guidelines for TPPs and data sources that describe the optimal customer journey, design best practice for informed consent, controls, regulatory requirements and a consistent approach to the language/terminology used.

Research will be required to inform understanding and decision making.

Suggested research

Informed consent for the transfer of data

- How to educate the consumer that their personal data, when shared under strict control, can benefit them?
- What are the key forces that encourage data sharing vs. those that induce anxiety or distrust and therefore discourage data sharing?
- Test consumer comprehension for different User Interface (UI) approaches that improve the approach currently used for Terms and Conditions, Privacy Notice and consent.
- How and when to communicate the process, ability to manage and revoke data sharing?
- How and when to communicate the onward sharing of data and how this can be managed (Note: attitudes and understanding are covered under suggested onward provisioning research).

Consumer expectations of data types and clusters

- What are the logical clusters that a consumer would expect in the energy and telecoms and wider finance sectors?
- Consumer attitudes towards data cluster sharing choices which lead to differentiated service levels or outcomes?
- What level of detail (granularity) is appropriate for specific data clusters in different sectors?
- Will the consumer expect to have greater control and be able to toggle on/off to decide on the feature set or outcome required from the service?
- Are there consumer concerns that combining data sets will reveal more than they want to share?
- What do consumers consider sensitive data in the financial, energy and telecoms sector?
- How to best offer transparency of what is being shared – the data clusters themselves – in a consistent way across sectors?

With regard to vulnerable consumers, and the more excluded in society:

- How do the more vulnerable (and older) in society view use of their data and what controls should be made available? Are there specific issues?

With regard to small business the research outlined above should also consider these issues from the SME perspective in their respective sectors.

Language that works well

Identify the vocabulary, terms and words that consumers understand and that can be used consistently across sectors.

- When describing elements specific to the data sharing and consent customer journey, including the authentication user experience.
- When developing awareness, benefits and messaging for data sharing in specific sectors, identifying the common and unique aspects for each.
- When describing the main data sharing ecosystem concepts to both consumers and SMEs.
- When describing technical elements (such as the names of the data clusters used).
- How to indicate to the consumer they are dealing with responsible parties.
- How to convey a strong sense of consumer control, such as indicators that the TPP is working with or for the consumer.
- How to convey a sense of security using familiar terminology that consumers can relate to and doesn't raise issues in their minds?

Market participants

In order for any successful data sharing to take place between market participants in a secure and trusted manner, it is essential to reference the current laws and regulations summarised herein. These are pivotal in providing the legal and regulatory framework within which the various actors share data, manage their statutory obligations and importantly attain trust amongst each other. Consumer trust is attained around rights, protections and importantly, security around the data being shared. In considering any solution for data sharing in a provisioning chain, particular regard is therefore required to the following issues in this non-exhaustive list:

Participant issues

- When onward sharing data, is it a Controller to Controller data transfer?
- What data, if anything, is left with Controller 1?
- Will the Controllers be joint Controllers?
- Should there be some formal data sharing agreement in place between the Controllers before data is shared?
- Will any data subject rights alter as a result of the transfer? (i.e. if each Controller has been relying on different lawful basis for processing personal data)
- How will C2 inform the data subject of their Privacy Notice in order to meet transparency obligations?
- Against which Controller does a consumer exercise their rights?
- Which Controller records the 'consent' (if used) for onward sharing?

Against this last point, GDPR Article 30 requires all Controllers and Processors to maintain a central record of processing which could be extended and utilised to capture 'consent' for the purpose of onward sharing. It could potentially be designed in such a way to capture common data elements such as:

- When consent was provided
- Parameters of the consent
- Details of the party with whom it was shared
- Lawful basis of C1 for processing of PD
- Lawful basis of C2 for processing personal data
- Lawful basis for further onward sharing
- Direct / indirect source. Important, because in order for the qualified right of data portability to be triggered, the following conditions must be satisfied:
 - Lawful basis must be consent or legitimate interest
 - Only personal data provided directly by the consumer can be transferred from C1 to C2 so it doesn't include personal data that C1 has obtained from another source.

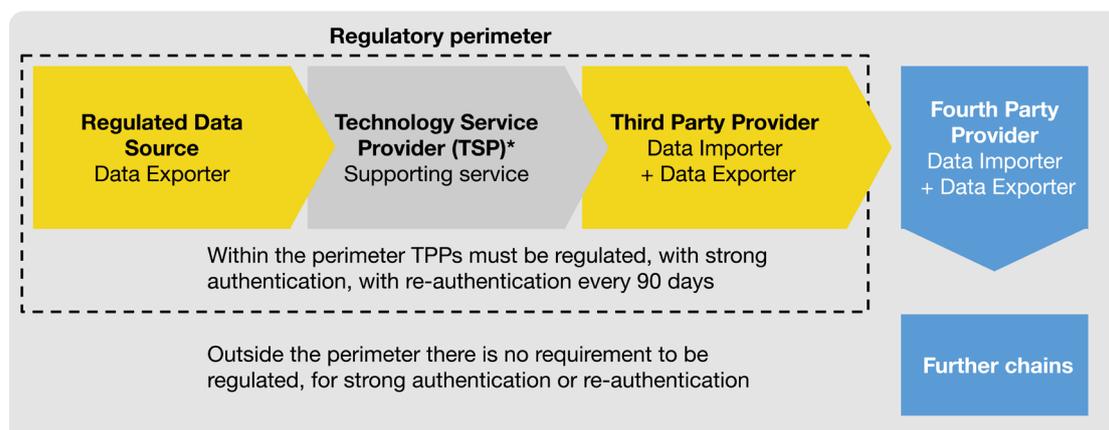
Consumer issues

From a data compliance perspective, it is starkly apparent that balancing the right of consumers against the obligations of Controllers when attempting to onward share personal data is challenging, not assisted by the shortcomings within the current legislation. Consumers could reasonably expect clarity on the following important questions:

- What does the consumer provide consent for, particularly when onward sharing data is likely to take place? This should consider the lawful basis for processing by each Controller in the provisioning chain.
- How does each Controller in a provisioning chain meet their legal obligations as they are triggered (i.e. providing a Privacy Notice)?
- How does a consumer revoke consent?
- What does the consumer's revocation cover (i.e. is it limited to prevent further sharing or does it prevent further processing)?
- What rights are triggered and against whom does a consumer enforce them (i.e. subject access request, right to object, right to rectification etc)?
- How does a consumer check what they have agreed to against each Controller?
- How does a consumer prevent unlawful and unauthorised sharing?

Roles in the provisioning chain

As the ecosystem for Open Banking has developed over two years - and continues to evolve - the role of different actors in the provisioning (value) chain has become clear.



* Regulated party may use a TSP (which does not have to be regulated) in order to access the consumer's account at the data source

This section uses the FCA definition as the starting point in order to illustrate how multi-party provisioning chains are used to provide services. It will be important to understand what the equivalent would look like for market participants in the Energy and Telecoms sectors as they join an open data ecosystem.

The types of participants, and their (FCA) regulatory status in the Open Banking ecosystem are described in the following table.

Participant type	Description and explanatory note
Regulated	
<p>Data Source or ASPSP (Account Servicing Payment Services Provider. e.g. bank)</p>	<p>The company or organisation that holds the consumer data to which the consumer consents the AISP (TPP) access.</p> <p>The bank must provide to the AISP the data it requests (in line with the law) without requiring additional consent from the consumer.</p> <p>A bank cannot require a contract with a TPP to allow the TPP to access the consumer’s data.</p>
<p>TPP/AISP (Third Party Provider or Account Information Service Provider)</p>	<p>Provides consolidated account information to the consumer. They are responsible for compliance with the PSD2/PSRs 2017.</p> <p>The AISP must display back to the consumer the data retrieved. They must do this in all journeys apart from where an Agent works on their behalf.</p>
<p>TPP (providing AIS)</p>	<p>If a regulated AISP provides data to other firms that want to provide AIS, the other firm needs to be regulated for AIS as well. The information provided to a third party must also be provided to the consumer.</p> <p>In the case where an AISP provides a service to another AISP both providers must display the data retrieved back to the consumer. In this scenario, the first AISP is operating in a similar way to a TSP.</p>
Registered (with the FCA)	
<p>Agent of AISP</p>	<p>Regulated AISPs (Principals) can have agents. An agent provides services on behalf of the principal. It cannot provide AIS on its own behalf. The principal must register the agent with the regulator (FCA).</p> <p>In this case the Agent displays the data retrieved back to the consumer on behalf of the AISP.</p> <p>The AISP is responsible for the Agent. Liability for a data breach is likely to rest with the Agent. However, it is possible the AISP may recover damages from the Agent.</p> <p>Accesses consumers’ accounts on behalf of the AISP. They obtain and process account information in support of an AISP but do not provide the information to the user.</p> <p>If a firm does not display the information it retrieves back to the consumer, it is a TSP. TSPs do not fall within the regulatory perimeter. They are not able to access consumer’s data without using the credentials of a regulated AISP.</p>

Participant type	Description and explanatory note
Not regulated by the FCA	
Technical Service Provider (TSP)	<p>Accesses consumers' accounts on behalf of the AISP. They obtain and process account information in support of an AISP but do not provide the information to the user.</p> <p>If a firm does not display the information it retrieves back to the consumer, it is a TSP. TSPs do not fall within the regulatory perimeter. They are not able to access consumer's data without using the credentials of a regulated AISP.</p>
Third Party (not providing AIS)	<p>Where an AISP retrieved data from the consumer in compliance with applicable laws and regulations, it can pass account data to an 'Other Party' or Third Party Not Providing AIS (and not regulated for AIS).</p> <p>The AISP must display back to the consumer the information it has provided to the Third Party Not Providing AIS.</p> <p>Some examples where this may happen are credit scoring, mortgage applications or loan applications.</p>
Fourth Party (not providing AIS)	<p>In the case where the Third Party (Not Providing AIS) onward shares the data to a fourth party, it is termed Fourth Party (Not Providing AIS). This would not be considered a transfer of data under the PSRs 2017 but would, instead be solely covered by GDPR.</p> <p>An example of this is where a credit scoring company passes data to a loan company.</p>

Trusted parties in a data sharing ecosystem

The data sharing ecosystem needs to engender trust across all participating parties, particularly when they are not known to each other. When, for example, a data source receives a request to share a consumer's data with the associated consumer consent, the data source must have confidence that the TPP is trustworthy.

In the Open Banking ecosystem this is achieved through a trust framework enabled by a 'Directory'. All participating organisations are on-boarded and assured both initially and on an ongoing basis. In the case of Open Banking the TPP must have obtained account information or payment initiation authorisation from the FCA or have passported in with authorisation from their National Competent Authority (NCA). In this way, the data source can be sure that when presented with a data access request with consumer consent granted, it is a genuine request and can be trusted.

It will be critical for trust that parties, particularly when not known to each other, or that work across sectors and have different regulatory obligations and frameworks can be trusted. For example, what would be the equivalent to an FCA authorised AISP in the telecoms or energy sector? How can all parties be confident that they are a 'good actor?'

Market participants — summary of implications

- As a result of this analysis and referencing the learnings from Open Banking, we conclude that market participants will require:
- A common cross-sector approach to implementing and managing consumer consent, including the necessary consumer controls for amendment and management across the provisioning chain. This must ensure consumer visibility of the consumer-facing brand, even when not a regulated entity, and clarity on where/how the consumer's data is being shared and used. This should include management of multiple data sources.
- Common terminology and consistency of definition across sectors for the different types of participant.
- Accepted common practices where data is shared, including where the lawful basis for data processing may change.
- A way for consumer re-authentication, where required, which can be implemented effectively, and which does not impact the customer journey negatively or lead to consumer drop-off (cessation of use).
- Market Participants must be able to identify each other, even when not known to each other, as trusted parties in the smart data ecosystem.
- Guidance on how to best implement their regulatory obligations, so that they act and present themselves to the consumer in the best possible way.

Market participants — checklist for development

Checklist for development of cross-sector data-sharing standards from a market perspective.

Suggested initiatives

- Determine the key market policy drivers and values for consent and its management.
- Develop a cross-sector approach to ensure regulatory consistency in smart data across sectors.
- Develop a cross-sector approach to participant categorisation and common terminology.
- Develop a cross-sector data sharing and consent standard, that would ensure a consistent approach to the issues identified and would provide a common framework for multi-party provisioning chains.
- Develop API specifications for data sharing and consent, and enable consent parameters to be provided as metadata thereby ensuring that all parties in a provisioning chain have clarity of the consent parameters.
- Explore potential new approaches and entities that enable consumers to manage their consents. This should include the consideration of independent (immutable) consent contracts, and the possibilities provided by privacy enhancing technologies (PETs).
- Develop cross-sector Operational Guidelines for Market Participants.
- Develop cross-sector Consumer Customer Experience (CX) Guidelines for Market Participants.

Research will be required to inform understanding and decision making.

Suggested research**Consumer understanding of data sharing in provisioning chains**

- What do consumers need to understand about sharing the data and how it will be used? i.e where it will go and which other parties will have access to it, and for what purpose? What will happen to their data in the future?
- Consumer expectations about how long the TPP has access to their data and the need to re-authenticate themselves?
- Do consumer attitudes vary across different sectors when sharing data and confidence in a TPP?
- How should the consumer recognise that a company is legitimate?
- How to make the consumer aware of the parties in the provisioning chain? The brand that the consumer is doing business with is not always shown through the consent journey or on the Data Source (ASPSP) access dashboard.
- What should market participants provide to consumers to manage their consent, and remain informed, when redirected from party to party?
- What do consumers think when very significant variation in the customer journey exists as in the three scenarios described?
- How to explain the applicability of different regulations such as the relationship between GDPR and PSD2 inside/outside the regulatory perimeter, or where data is shared but rights vary?
- Consumer attitudes in having to agree to more than one set of T&Cs and privacy policy e.g. in an agent/AISP relationship?
- Consumer attitudes when having set up a service with one company, they have to open an account at another (an AISP) in order to enable access to their data or a dashboard?
- How should a consumer cancel two (or more) agreements for a single service at the same time?
- What happens if the consumer fails to recognise the AISP and cancels in error?
- How to manage the cessation of access at the data provider and the management of consent at the TPP?
- As there are two agreements in some scenarios, what does the consumer think about a participant continuing to share old data with another party after their consent has been revoked?

Onward sharing in the provisioning chain

- How to explain to consumers where their data will go and which other parties (if this happens) will have access to it, and for what purpose?
- What will happen to their data in the provisioning chain in the future?
- When, if ever, will their data in the provisioning chain be destroyed? Noting that sector specific regulatory or legal obligations will determine what policy should be followed by the TPP.
- Would consumers welcome an accreditation scheme, for example limiting the nature of organisations to whom data can be onward shared (beyond the regulatory perimeter?)
- Should consumers be presented with options which would limit onward sharing to opt-in consent only basis?
- Is there scope for a tiered approach to consent, aligned to Level of Assurance and drawing from that approach?
- What are consumer attitudes towards limiting the purposes for onward sharing (exclude marketing?)
- What are consumer attitudes towards mixing with other data sets and inferences from this process?
- What are consumer attitudes towards the number of parties and number of times with whom the data can be shared?

Management of consent

- What do consumers expect when managing or amending their consent?
- How do consumers understand the role of consent dashboards (at the TPP) vs. the access dashboard (at the Data Source/ASPSP)? How to align these?
- How should a consent dashboard present the various parties in a provisioning chain i.e. AISP, Agent, Third and Fourth Party relationships?
- Would consumers adopt services that managed their consents and access on their behalf, across all parties in the provisioning chain? Would consumers want to be able to use a single service provider to manage all their consents. Could dedicated data facilitators/consent service providers or Personal Data Stores play a role in managing this and protecting personal data?
- If so, how would consumers expect this to work?
- What models exist already?
- Who would pay for this?
- How would consumers react to new concepts such as consent contracts or the services enabled by privacy enhancing technologies?
- How would this work across different use cases?

Impacts of requiring ongoing consent

As data can be accessed and used on an ongoing basis this creates implications for how consumers can manage and control data in scenarios of ongoing consent. While PSD2 provides for 90-day re-authentication, it does not work well for either consumer or market.

The Open Banking approach is to require each individual data share to require consent and authentication. There is a disconnect between the 'consent' and the 'authentication' which also creates risks for consumers. For instance a consumer may wrongly believe that if they do not re-authenticate a product, the firm must stop processing the data they already have. This is not true: TPPs may not be able to access the data but they could still continue to derive value from existing data shared.

This risk could be reduced by ensuring that any consent is limited to the time period for re-authentication. However, this does not resolve the uncomfortable consumer experience which requires consumers to re-authenticate each single connection with each single provider. Further work should be done to consider the purpose of re-authentication and how it can best be implemented to ensure inert consumers do not continue to share their data without getting value from it, including whether consumers need to re-authenticate or simply re-consent to the data transfer, or, in fact, re-consent to the Terms and Conditions of the product itself.

One approach to addressing this issue is 'data facilitators' as TPPs (AISPs) in this space already exist. Early signs from the Open Banking ecosystem suggest that these AISPs are likely to act as data retrievers for other businesses rather than provide services directly. However, they are driven and incentivised by the needs of the agent or fourth party rather than the needs of the consumer.

A duty to act first in the interests of consumers with specific additional requirements such as the ability to provide simple tools which allow people to enforce their GDPR rights through the data chain (e.g. amendment of data or revocation of PSD2 consent, deletion of data) could enhance the role of these TPPs and ensure they work in the interests of consumers but remain competitive and commercially viable.

Further work is required to understand whether the role of TPPs across all sectors can be enhanced to improve incentives so that they design services which allow consumers to control their data more effectively. It would be helpful for TPPs to develop as 'data custodians' for consumers providing additional services. These could include relevant information about the depth of exposure sharing data creates or alerts to the consumer to key terms in the Privacy Notice of fourth parties intention to onward share data.

Giving consumers the right to access the product provided by a fourth party without having to agree to their data being onward shared could enhance consumer control.

This requires further exploration to address the issues identified and provide effective management of consent across multiple sectors. It will be important to consider how consumers can be protected from ‘inert’ data sharing through provisions akin to ‘90-day re-authentication’ but executed in a more effective way. It would require changes to regulation. We must consider the impact not only of the consent granted to the TPP, but also the access provided at the data source.

So far, we have considered the consumer consent provided to the TPP. This consent may, potentially, be granted for multiple data sources. For example, the consumer may use a service that draws data from their telecoms provider and their bank account. Access to each data source would need to be managed through the appropriate provider, typically in a ‘dashboard’ within the settings function of the website or app.

This implies that the consumer could cancel access at a particular provider, such as their telecoms provider, which would revoke consent to use that specific data source, but would not impact consent granted to access data being accessed from other sources such as their bank. Access at the data provider is therefore not equivalent to consent at the TPP. Consideration should be given to this issue, including the potential for a consent standard that covers multiple data sources that improves clarity, control and friction.

Proliferation of ongoing consents will be complex to manage

As consumers use more services, and the smart data ecosystem grows, the complexity of managing ongoing consents (and the associated access to the data sources) becomes evident. For example, a consumer may have numerous active consents:

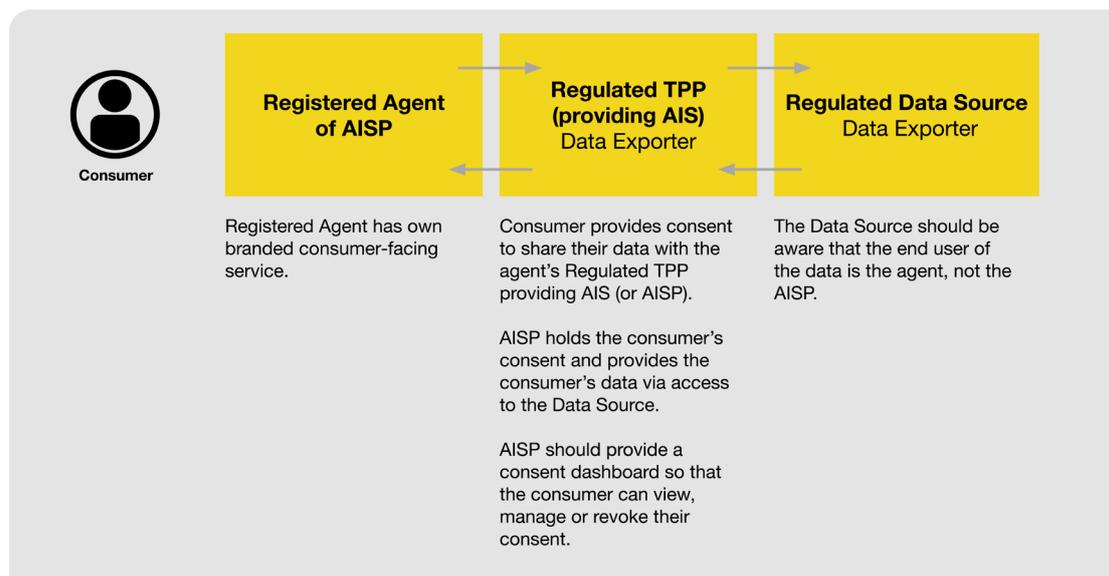
- Each of these may have multiple parties in the provisioning chain.
- Some of these parties may be regulated, some may be outside the regulatory perimeter for that particular sector.
- Some parties may fall within the regulatory scope of more than one sector.
- Some parties in the future could possibly be providing services as a regulated TPP in one sector while simultaneously providing services as fourth or fifth parties in other provisioning chains.
- Not all parties are known to each other, as outlined above, particularly where they fall outside the regulatory perimeter for that particular sector.
- Not all parties will provide a consent dashboard.

This quickly becomes unmanageable for the consumer. It will therefore be essential to provide consumers with the ability to track and manage their consents, and for the market participants to ensure that they are enacting the consumer’s wishes.

What does this look like to a consumer?

It is important to consider a wide range of use cases, but to bring the issues to life we explore three example scenarios, below.

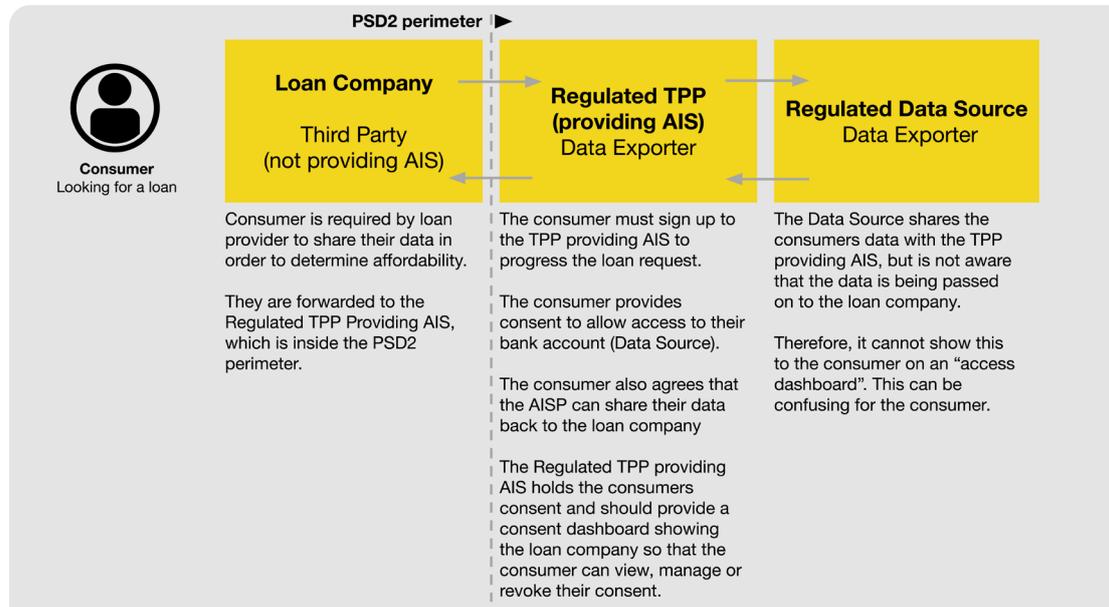
Scenario 1: Using a service provided by an agent



It is common to see the agent relationship, which, for example, makes up 12 of the 15 in the finalist cohort for the Open Up 2020 Challenge currently underway. From a regulatory perspective, this is within the PSD2 perimeter.

- The consumer sets up a service provided by a Registered Agent.
- The consumer provides their consent to share their data with the Agent's regulated TPP (providing AIS).
- The Regulated TPP Providing AIS holds the consent and provides the consumer's data, provided via access to the data source. The Data Source should be aware that the end user of the data is the Agent, not the TPP Providing AIS.
- The TPP Providing AIS should provide a consent dashboard so that the consumer can view, manage or revoke their consent. The bank provides an 'access' dashboard where the consumer can revoke the TPP's access if they choose.

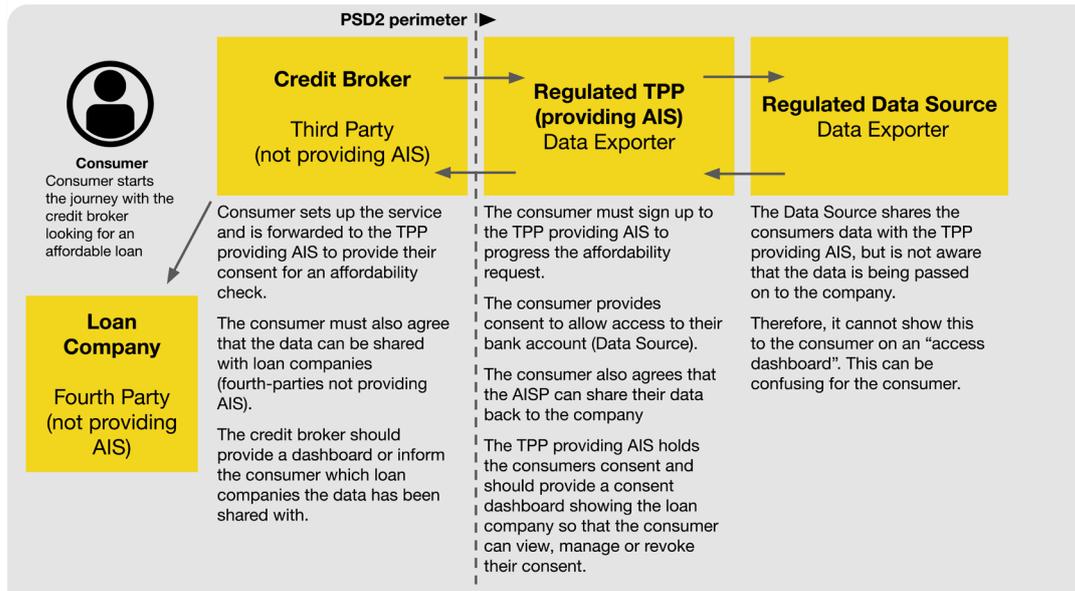
Scenario 2: Using a loan company



This is a common model and would include affordability checking, credit scoring as used by loan providers as well as letting agents in the home rental market. It is more complex than scenario 1. The loan company is outside the PSD2 regulatory perimeter.

- The consumer starts a loan provision application. This is a loan company 'third party not providing AIS' (TPNPA) and is outside the PSD2 perimeter.
- They are forwarded to the Regulated TPP providing AIS. They are now inside the PSD2 perimeter.
- The consumer provides consent to the TPP providing AIS to allow access to their bank account (the Data Source). This data is duly shared with the TPP providing AIS.
- The consumer also has to agree that the TPP providing AIS can share their data with the loan company (TPNPA). Therefore, they have entered a second agreement.
- The TPP providing AIS holds the consent and provides the consumer's data to the loan company.
- The TPP providing AIS should provide a consent dashboard showing the loan company so that the consumer can view, manage or revoke their consent.
- The Data Source (the consumer's bank) is not aware that the consumer's data has been passed on to the loan company and cannot display this on their own access dashboard. The only company shown is the TPP providing AIS, which may not be familiar to the consumer, or may be providing a service to other organisations which the consumer uses. This could lead to a situation where the consumer sees this TPP providing AIS multiple times on the Data Source access dashboard, but cannot differentiate between the purpose of each access granted.

Scenario 3: Using a credit broker to find a loan



This is a more complex provisioning chain in which the credit broker is a ‘third party not providing AIS’, that passes the consumer to the loan provider, which is the ‘fourth party not providing AIS’. The credit broker is reliant on a TPP providing AIS to access the consumer’s data at their bank (ASPSP/Data Source). Overall, the consumer must agree to provide their consent to the TPP providing AIS, agree that the data obtained can be shared with the credit broker, which then in turn will need the consumer’s agreement to share this same data with the loan company.

- The consumer starts the journey with the credit broker (third party not providing AIS), looking for an affordable loan.
- The consumer is forwarded to the AISP to provide their consent
- The consumer also has to agree that the data can be shared with the loan providers (fourth parties not providing AIS)
- The consumer provides consent to the TPP providing AIS to allow access to their bank account (ASPSP/Data Source). This data is duly shared with the TPP providing AIS by the Data Source.
- The consumer must also agree that their data can be shared by the TPP providing AIS with the credit broker.
- The TPP providing AIS should offer a consent dashboard, which should display the name of the credit broker.
- The Data Source (ASPSP) is not aware that the consumers data has been passed on to the credit broker nor of the relationship with the loan company and cannot display these on their own access dashboard. The only company shown is the TPP providing AIS, which may not be familiar to the consumer.

Biographies

Miles Cheetham



As Head of Proposition at The Open Banking Implementation Entity (OBIE) since its inception in 2016, Miles has been responsible for understanding what consumers want from open banking enabled services, acting as the voice of the customer across the programme.

He led the development of the ground-breaking and highly regarded Customer Experience Guidelines, a key part of the Open Banking Standard, which focuses on consent and customer authentication as central to the data sharing journey. This was achieved through extensive engagement with the market, customer interest groups and primary customer research. He has deep experience of customer-led digital product development across banking & telecoms. Prior to joining OBIE he worked in senior product development and strategy roles for major brands including Vodafone, MTN Group, Sky and Verizon.

Sharon Cunliffe



An experienced lawyer specialising in data privacy, with deep expertise in the General Data Protection Regulation (GDPR) as well as financial services regulation.

Sharon has until recently been leading legal and regulatory support in payment services and data privacy at the OBIE, with a particular interest in data privacy and the regulatory and statutory challenges that data privacy is currently presenting at domestic and European level both in the context of payment services and data privacy on a standalone basis. She engages with the Information Commissioners Office (ICO), the Financial Conduct Authority (FCA) and government departments (e.g Department for Digital, Culture, Media & Sport (DCMS) to find practical solutions arising out of challenges and conflicting statutory provisions contained within both PSD2 and GDPR.

Faith Reynolds



Faith Reynolds advises regulators and industry on technology, innovation and business conduct in the financial services market. She is Independent Consumer Representative for the Open Banking Implementation Entity, significantly influencing policy, design and implementation of the trust framework, consent flows and dashboards.

Gavin Starks



On behalf of HM Treasury, Gavin co-chaired the development of Open Banking Standard, leading banks, trade associations, startups, regulators and consumer rights organisations to lay the foundations for new regulation.

He has worked with public and private sector organisations internationally, with Ministers, C-suite leaders and startup founders. He was the founding CEO of the Open Data Institute, has sat on the GLA Smart London and the Ministry of Justice Data Science and Evidence boards and provided evidence to a Parliamentary Select Committee on 'Big Data'. As a serial entrepreneur he has cocreated over a dozen companies, creating economic, environmental and social impact. His work has led to recognition as one of the most influential people in data, awards for innovation and expertise, and frequent international presentations on innovation, the web of data and its impact on society.

Glossary & terminology

Term	Definition
AISP	Account Information Service Provide. rIn this report an AISP is a type of TPP.
Agent	Regulated AISPs (Principals) can have agents, providing services on behalf of the principal.
ASPSP	Account Servicing Payment Service Provider (for example Bank, Building Society acting as the Data Source)
Controller	Data Controller (GDPR)
CMA	Competition Markets Authority
CRA 2015	Consumer Rights Act 2015
C1, C2, C3	(Data) Controller 1, Controller 2 etc.
DPA 2018	Data Protection Act 2018
DS	Data Subject
FCA	Financial Conduct Authority
FPNPA	Fourth Party Not Providing AIS
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
LB	Lawful Basis
LI	Legitimate Interest (as a lawful basis under GDPR)
PD	Personal Data
PISP	Payment Initiation Service Provider. In this report a PISP is a type of TPP
PN	Privacy Notice
PoC	Performance of Contract (as a lawful basis under GDPR)
Processor	Data Processor (GDPR)
PSD2	Second Payment Services Directive
PSRs	Payment Services Regulations 2017
TPP	Third Party Provider. In this report we use the term to mean a TPP which is accessing data like an AISP. In PSD2 a TPP can also be a PISP which initiates payments.
TPNPA	Third Party Not Providing AIS

Acknowledgements

With thanks to Nathan Kinch and David Pollington.

Limit of Liability and Disclaimer of Warranty

The authors, researchers and contributors have used their best efforts in preparing this work. Dgen Network Limited makes no representation or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential, or other damages.

Trademarks: all trademarks are acknowledged.

