

**FDATA Response to OFGEM Call for Input:  
Data Sharing in a Digital Future: Consumer Consent January 2024**

The Financial Data & Technology Association is a not for profit global association for financial services companies operating in open banking and open finance. FDATA's mission is to open up the worldwide financial sector to allow every customer to leverage the benefits of their financial data, ensuring that financial services are delivered in a fair, ethical, compliant, and robustly competitive landscape. We are active in the UK and Europe, Australasia, Latin and North America.

FDATA started at the request of Her Majesty's Government back in 2015-16 to represent third party providers in the negotiations of PSD2 (the second payment services directive legislation that formalised open banking), and has been intimately involved in the work to deliver open banking to the UK market ever since. FDATA's remit is not isolated to just financial services; we have a vested interest in the opening of other sectors including energy, telecommunications, retail, healthcare and transportation. Our members are keenly interested in bringing new value propositions to market that centre on the intersection of multi-industry data sets. As such, we are involved in the Smart Data Council subcommittees, and have been an active public supporter of the Penrose amendment to the DPDI bill. It is for this reason we are submitting this response to the Call For Input, and appreciate the opportunity to do so.

**Q1. Yes/No: Do you agree that a Consumer Consent solution is required as per the taskforce's recommendation?**

Yes, however it should be noted that consent is just one form of permission, and should not be conflated to be entirely inclusive of a robust permissioned data sharing framework.

FDATA does support incorporating learnings from open banking, with an eye on ensuring interoperability with data sharing sectors that have already been delivered.

**Q 2. Could you please provide any reasons why the current methods for obtaining consent from a consumer might be ineffective or inefficient?**

Current consent methods are constrained by 1) the perception of privacy in the context of value exchange, and 2) by entrenched legacy technology. The former stems from the limitations imposed by the latter.

Because consent has mostly been managed using a sales tool - a customer relationship management system - it is subject to fragmentation. Consent is often held in unconnected silos by multiple parties, both within a single organisation across multiple lines of business and across multiple firms. Consent fragmentation means harmonised consent management becomes impossible; this is compounded by the fact that existing cross-sector consent standards are not interoperable. Moreover, legacy tech is unable to recognise the different permission types within 'consent'; this limits the ability to personalise services for the end customer. This also limits the value creation of data sharing, which is counterproductive to the purpose of sharing the data in the first place.

The end consumer is also burdened with managing all of their consents and permissions in individual portals directly with the myriad service providers with whom they have a relationship. Consumers cannot see or manage their consents and permissions in a single place. As the number and complexity of data sharing use cases increase across not just the energy sector, but across the entire economy, the current 1:1 consent management approach will not scale. This results in 'consent fatigue'. This is a significant impediment to building trust and confidence in a data sharing economy.

An absence of granular control over what data is shared, how it can be used, and the perception that access to a service is dependent upon a particular block of data being shared also need correction if consent driven data sharing is to be more widely adopted. Lack of clarity about the scope of consent, the parameters, and what it ultimately means for the consumer must also be addressed. This is especially true in cases of onward sharing of data, as both the consumer and the data provider may not have a clear visibility or understanding of where and how the data is being shared or used by third, fourth, or fifth parties.

Easy consent revocation in the same dashboard is also crucial: consumers require assurances that they are in full control of their permissions, and that those permissions can be retracted at any time.

FDATA supports a consent approach that is consistent and interoperable across sectors in order to maximise the benefits of open/smart data across the whole of the UK economy. We also support an approach that enables individuals and small businesses to engage and control their data more effectively, granularly, and via a single dashboard. This also requires there be simplicity in explaining the value exchange to consumers, and transparency of how the data will be used in delivering that value.

**Q3. Do you believe that consumers are sufficiently motivated to engage with the consent solutions proposed in this Call for Input? Please elaborate on your answer.**

Yes, if the consumer can easily recognise the value of sharing their data. Open banking provides evidence of this as consumer adoption and usage continues to grow month on month since its successful launch in the market. It is not just the UK adoption of financial data sharing propositions, it is a global phenomenon.

However, this is predicated on the consumers perception of value and outcome of the offering. There must be a clear value exchange: what is received for sharing the data, and why that data exchange is worth it. Again pointing to open banking, when firms offer better products, services, and outcomes in exchange for consumers sharing their data, customers will indeed consent for their data to be shared.

FDATA recommends that Ofgem consider adopting a similar approach to the Customer Experience Guidelines (CEGs)<sup>1</sup> that form part of the open banking standard. The Open Banking Implementation Entity (OBIE) and industry collaboratively created these guidelines after considerable research and testing. The CEGs also detail approaches to [authentication](#) that could be adopted for the energy sector<sup>2</sup>, as well as simplifying the re-consent process without tying it to a re-authentication requirement.

The re-consent process/customer experience is critical to both the service provider and the end consumer. Expiration of consent can limit commercial business models as well as negatively impact consumers, who may not realise their consent has expired, and therefore the service they have signed up for is no longer active.

Again, Ofgem can benefit from work already delivered under open banking in respect to customer experience guidelines to create an optimised consent (including authentication and authorisation) customer journey. This would contribute to creating an interoperable cross-sector consent standard for the entirety of the UK open/smart data sharing economy.

**Q4. Do you agree that the four use cases referenced are high priority use cases? Can you describe any other high priority use cases?**

FDATA does not hold an opinion on the relevant priorities of the proposed used cases. We can, however, affirm that a number of its members have a vested interest in being able to obtain energy data in order to deliver value 'in-the-wings' financial services value propositions. Our members are developing cross-sector use cases blending energy and open banking data sets to address green financing for SMEs and home improvements, and particularly at this time, identifying consumer vulnerabilities in the cost of living crisis.

---

<sup>1</sup>

<https://standards.openbanking.org.uk/customer-experience-guidelines/appendices/themes-identified-from-consumer-research/latest/>

<sup>2</sup> <https://standards.openbanking.org.uk/customer-experience-guidelines/authentication-methods/latest/>

What is important for FDATA members is that cross-sector data sharing frameworks have common infrastructure and standards based on recognised best practices and principles.

**Q5. Do you believe that a new Consumer Consent solution would enable the improvements to the energy system described in the four use cases? If not, could you please elaborate?**

Yes, in principle.

Holistically, consent includes other functions like authorisation, authentication, third party regulatory permissions and licenses, technology and data standards development and maintenance, reporting, consumer education, an approach to onward sharing, and the liability model.

**Q6. Do you agree with our method and scoring of options?**

In principle, yes. However we noted that consumer groups were not directly consulted in this process. From our experience in being part of the delivery of the UK's first open data sharing economy - open banking - direct consumer representation participation in every phase of development and delivery has been critical to the success and adoption of open banking. Open Energy would similarly benefit from including consumer reps in this process.

**Q7. Which of the options referenced in this chapter do you believe would be the most appropriate Consumer Consent solution, for the industry, the government, and the consumer?**

- **Option One:** A single technical solution to obtain consent, such as a Consumer Consent dashboard. This proposal builds on the Energy Digitalisation Taskforce's recommendation to deliver a technical consent solution.
- **Option Two:** A set of principles outlining a consistent way for trusted market participants to obtain consent, such as Data Best Practice.
- **Option Three:** An industry-developed code of conduct outlining a consistent way for trusted market participants to obtain consent, such as the Confidence Code.

FDATA supports Option One: a single technical solution.

**Q8. Please can you explain why you chose a specific option? Do you have any suggestions on how to improve this option?**

FDATA supports a single technical solution, based on our experience in delivering open banking. We see specific benefits to this option including:

- **Interoperability:** a multi-/cross-sector common solution and standards mean obstacle free data sharing, reduction in duplication, improved efficiency and re-use of assets, and economic optimisation of infrastructure investment.
- **Improved transparency for the end consumer:** the ability for consumers to see and manage their permissions in a single view also improves their control over their data, and their trust in the system; being able to manage cross-sector permissions in a single dashboard improves engagement and adoption
- **Risk mitigation for regulators, providers, and consumers:** a single consent standard means oversight and enforcement on performance and conformance is simplified, standards development and maintenance is rationalised for regulators; providers do not have to worry about building multiple flows or databases; consumers have a consistent and reliable process for managing consent - which also simplifies customer education requirements and cost.
- **A common shared open protocol for consent:** building on open standards ensures a scalable future proof solution that can adapt to evolving regulatory requirements, new technical developments, and enhanced privacy best practices.

Potential improvements to the solution:

- Ability to manage consent at both the data provider and data recipient sides: this would require that all parties be able to update records across the system in real-time.
- Ability to track data beyond the initial sharing/receiving parties: onward sharing tracking would improve transparency *and* traceability in cases where a breach occurs. This also enhances risk mitigation, and will impact the overall cost of the liability model.

## Q9. What barriers do you see to the successful implementation of a new consent solution?

First and foremost, the lack of a mandate for universal adoption and implementation. Without one, customers are left with inconsistent, inaccurate, and unequal abilities to share their data. Any asymmetry in the solution will erode trust in the system, defeating the entire point of creating a data sharing economy.

There also needs to be a single protocol for the consent solution, without which, interoperability is not possible. We offer up two examples of why a single protocol matters: email (POP, IMAP, SMTP) and GPS. Irrespective of the email provider and the user interface of the email application, all emails can be exchanged because they conform to those protocols. The innovation and differentiation between email applications is at the *application* layer, not the protocol layer. Same with GPS: irrespective of the application used to pinpoint location (be it maps, navigation, weather, or retail shopping), all of those applications use the same protocol. The same principle should apply to a consent management system that enables cross-sector permissioned data sharing: a single universal protocol which enables innovation, competition, and value creation at the *application* layer.

**Q10. What do you think are the roles of Ofgem, industry and other stakeholders in enabling a simple and effective consent solution?**

Ofgem has the convening power to bring other regulators to the table, to coalesce a multi-sector agreement on implementing a scalable, future-proof consent solution. Part of this is to also incorporate lessons from industries and regulators who have already delivered an active data sharing ecosystem.

Ofgem also has the supervisory and enforcement authority to ensure consistent consumer experience in the consent journey, as well as transparency in the explanation of the purpose and use of the data, and service provider conformance to the standards.

Ofgem is also in a position to set the pace of delivery and implementation (via a mandate). Without a mandate, industry will be slow to make changes and invest in the infrastructure required for secure, robust, scalable and interoperable permission based data sharing.