



Ofgem Consultation Response

Consumer Consent Solution

4th October 2024

**Electricity
Distribution**

nationalgrid

Approval

| | Name | Role | Date |
|----------|---------------|----------------------|------------|
| Author | Ryan Kavanagh | Data Science Manager | 02/10/2024 |
| Approver | Shak Butt | NGED CIDO | 02/10/2024 |

Document Revision & Review

| Date | Comments | Author |
|------------|---|---------------|
| 26/09/2024 | Initial draft shared internally for comments and review | Ryan Kavanagh |
| 02/10/2024 | Approved for submission to Ofgem | Ryan Kavanagh |
| | | |

Document Submission

| | |
|---------------|---|
| | |
| Submitted By | Ryan Kavanagh |
| Email | rkavanagh@nationalgrid.co.uk |
| Date | 03/10/2024 |
| | |
| Respond Name | Lindsay Jones, Tom Lewis, Charles Clark |
| Respond Email | digitalisation@ofgem.gov.uk |

Table of Contents

| | |
|---|---|
| Approval | 1 |
| Document Revision & Review | 1 |
| Document Submission | 1 |
| 1. Chapter 3: Our Vision for the Consent Solution | 2 |
| 2. Chapter 4: Implementation of the Consumer Consent Solution | 5 |
| 3. Chapter 5: Landscape – Current and Future | 7 |

1. Chapter 3: Our Vision for the Consent Solution

Q1. Do you agree with the proposed Design Principles? Would you recommend any additional Design Principles?

NGED agrees with the proposed Design Principles, particularly their emphasis on transparency, security, and inclusivity, which align with our previous responses. Ensuring that the consent solution is interoperable, agile, and scalable is important for meeting the evolving needs of the energy sector. These principles should enable the necessary trust and flexibility required to empower consumers and support a secure data-sharing ecosystem. As outlined in our responses to the call for input earlier this year, a user-friendly and transparent approach is crucial for fostering consumer engagement and ensuring regulatory compliance. Finally, as outlined on our response to Governance of a Data Sharing Infrastructure (DSI) consultation, resilience is an important consideration. If the consumer consent solution is to support wider energy sector systems and solutions it will need to be sufficiently resilient.

Q2. Do you have a preference between the centralised, decentralised or hybrid models? Please elaborate.

NGED supports the centralised architecture, for the Consumer Consent solution, with the understanding that this architecture applies specifically to the management of consumer consent data, rather than the consumer's data itself. This distinction is important, as the purpose of this system is to manage how consent is granted, tracked, and potentially revoked—not to handle the underlying consumer data, which is managed separately by data holders.

Whilst the DSI architecture is still under development, it is essential that the proposed Consumer Consent solution aligns with its guiding principles. The DSI is expected to create a secure, interoperable, and standardised data-sharing framework for the energy sector. Ensuring that the Consumer Consent solution is built to integrate seamlessly with the DSI architecture once established will enable more consistent, secure, and efficient data flows across the sector.

By aligning the Consumer Consent solution with the evolving DSI framework, the Delivery Body managing consent data will benefit from a centralised governance structure, which will provide clear protocols and oversight for data sharing. This alignment will reduce complexity, enhance trust, and streamline the management of consent data, ensuring it is shared consistently and securely across all platforms.

Moreover, this integration will facilitate the future sharing of actual consumer data. Once consumer consent is granted, the DSI can support the secure exchange of personal and usage data between relevant parties, ensuring that consumer preferences are respected. This coordinated approach will allow for greater innovation and consumer engagement while safeguarding privacy and data security.

In conclusion, NGED believes that the centralised architecture, with the flexibility to align with the future DSI architecture, offers the most robust solution for managing consumer consent data and enabling responsible data sharing as the energy sector continues to evolve.

Q3. Do you consider the security measures referenced in this section, including the access control measures, will meet the requirements of a consent solution holding consumer data? Which additional protections would you recommend?

We consider that the security measures outlined in Section 3, including the access control mechanisms, are appropriate to meet the requirements of a consent solution holding consumer data. The application of multi-factor authentication (MFA), such as one-time passcodes, Digital IDs, and biometric verification, provides a necessary level of assurance that only authorised users will have access to sensitive information. These controls align to our expectations for data protection in a consent solution of this scale.

The requirement for ISO 27001 accreditation as a standard for the Delivery Body further demonstrates a suitable focus on ensuring information security management practices are in place. This is a widely recognised standard, and adherence to it is expected to provide the level of security required for handling consumer data. We also acknowledge the value of the proposed Trust Framework, based on established models such as Open Banking, which offers a method for ensuring that data is shared only with trusted and authorised parties.

Additionally, the inclusion of a Data Protection Impact Assessment (DPIA) will help to identify and mitigate risks in line with GDPR requirements.

The process diagrams shown in Figures 4 and 5 of the consultation document, provide helpful clarification on how consent will be granted and managed, and we note the emphasis on ensuring consumers can revoke or adjust their consent easily and securely.

While the proposed measures are comprehensive, we recommend that additional protections be considered, particularly in relation to the use of end-to-end encryption for data in transit and storage. This would offer further resilience against potential security risks, particularly as the solution scales. This recommendation aligns with our previous response to the call for input, where we highlighted the need for robust but seamless solutions, and also with our recent response to the Governance of a DSI consultation, where we highlighted the importance of transparency, security, and trust in data management.

While the proposed security measures provide a strong foundation for the protection of consumer data, particularly with the use of multi-factor authentication, ISO 27001 accreditation, and the Trust Framework, we believe that further assurances could be beneficial. To ensure the highest levels of security, we recommend that the proposed security protocols, including access control and data protection processes, be reviewed and approved by relevant UK security agencies, such as the National Cyber Security Centre (NCSC). The involvement of agencies like the NCSC would provide additional layers of oversight and assurance. Their expertise in cyber risk assessment and secure-by-design principles could enhance the robustness of the system, ensuring it remains resilient to evolving cyber threats. We consider this step crucial for maintaining trust with consumers and ensuring that the system is both secure and aligned with national cybersecurity standards.

Q4. Do you consider these standards are sufficient parameters to ensure inclusivity, accessibility and interoperability for the consent solution? Which standards would you recommend?

We consider the proposed standards for accessibility and inclusivity to be appropriate for the consent solution. The use of Web Content Accessibility Guidelines (WCAG) 2.2, along with the Web Accessibility Initiative – Accessible Rich Internet Applications (WAI-ARIA) suite of web standards, provides a solid framework to ensure the platform will be accessible to a wide demographic, including users with disabilities or additional needs.

The emphasis on ensuring clear, concise communication throughout the user interface is especially important, given that the consent solution will need to be understandable by consumers across various demographics. These guidelines align with the Government Digital Service's principle of creating services that are Perceivable, Operable, Understandable, and Robust (POUR).

To further enhance inclusivity and accessibility, the platform could consider adopting BS 8878, the British Standard for Web Accessibility, which emphasises the importance of involving users with disabilities in the design and testing process. Additionally, integrating Speech Recognition Technology could improve access for users with limited physical capabilities. For interoperability, leveraging Open API standards would enable seamless integration with other systems and platforms, ensuring data portability and collaboration across sectors.

In terms of data interoperability, we recognise that this is also a key focus in the Governance of a DSI consultation response, which highlights the importance of seamless data exchange across systems to avoid siloing. Ensuring that the consent solution adheres to open standards, such as Open API, will promote greater alignment with broader data-sharing infrastructures like the DSI, enhancing collaboration across platforms and preventing fragmentation. This consistency across systems will be essential for ensuring that consumers can manage their data seamlessly across multiple sectors, further increasing trust in the digital ecosystem.

This Ofgem consultation focusses on a technological solution for Consumer Consent and outlines various standards that contribute towards the solution being 'inclusive'; with this we must not exclude Customers who are not technology literate or enabled and understand how they will manage their consents.

While the standards are robust, we recommend continuous monitoring and evaluation of the solution's accessibility features during implementation. The Delivery Body should work closely with relevant consumer advocacy groups, such as those specialising in digital disadvantage, to ensure that the platform remains inclusive as it evolves. This recommendation complements our position in both the call for input and Governance of a DSI consultation responses, where we emphasised the importance of inclusivity and user empowerment in digital solutions.

In conclusion, we believe that the proposed standards are adequate, but ongoing engagement with accessibility experts and further testing across diverse user groups will be critical to maintaining high levels of inclusivity, accessibility, and interoperability.

2. Chapter 4: Implementation of the Consumer Consent Solution

Q5. Do you agree with the options assessment conducted by Ofgem? If not, why?

Yes – NGED agrees with the options assessment conducted by Ofgem.

We have reviewed and understood Ofgem's approach to the options assessment, particularly the application of clear and relevant criteria in the evaluation process. The use of principles-based analysis, focusing on operational capabilities, independence, and engagement, provides a structured approach for assessing the suitability of potential delivery bodies.

The criteria used, such as operational capability and governance, play a key role in ensuring that the chosen delivery body can effectively manage the consent solution and meet the needs of consumers and stakeholders. The inclusion of the RAG rating adds transparency and understandability to the selection process.

Q6. Do you agree with Ofgem's minded-to position that RECCo should be selected as the Delivery body for the consent solution? If not, which of the three proposed organisations should be selected as the Delivery Body for the consent solution, and why?

NGED agree to the four standards to which these potential delivery bodies have been evaluated, however, we question the 'Amber' assigned to ElectraLink for 'Implementation and Governance', especially considering the further implications of the upcoming Code Reform and licencing changes. Whilst it is highlighted within 4.23 that the introduction of these licences may alter the dynamic of drafting a governance framework, we disagree that the drafting of bespoke arrangements would delay delivery, as it also noted that RECCo are currently unlicensed. It has been proposed that the DTS could potentially become a Central Service within the SCR, and there is potential that appropriate governance for the consent portal could also be applied within this mechanism.

There is also potential also to extend the obligation to the Distribution Licence to enable ElectraLink as a delivery body, assuming that necessary funding is also provided. This is already an embedded governance process where ElectraLink demonstrate that they are a well-established delivery vehicle. Distribution Network Operators are well posed to deliver for customers and aid in the delivery of Ofgem's public policy.

We note Ofgem's recommendation to select RECCo as the Delivery Body for the consent solution. RECCo demonstrated strength in several key assessment areas, including operational capabilities and stakeholder engagement, as highlighted in the analysis framework.

Q7. Do you hold any views as to how the proposed solution should be funded? Please consider the points regarding fairness raised in paragraphs 4.12–4.14 and Ofgem's duty to consumers when providing your answer.

In considering the funding approach for the proposed consumer consent solution, fairness should be a primary consideration. The funding mechanism must ensure that costs are distributed equitably across all relevant market participants, while not disproportionately burdening consumers. Also, It is essential that the solution's costs do not negatively impact vulnerable customers.

Drawing from the Governance of a DSI consultation, a combination of Connection Charges, Usage-Based Charges, and Target Charges offers a fair and sustainable funding model. Connection charges ensure that new participants in the consumer consent solution contribute to its initial setup costs, aligning with the principle that those entering the system help bear the financial burden of integration. Usage-based charges tie the costs directly to the extent of system use, ensuring that high-use entities contribute proportionately. Target charges allow funding for specific services or functionalities, promoting flexibility in covering particular operational or development needs.

To reduce the initial financial burden, particularly during the early development stages, leveraging innovation funds such as the Strategic Innovation Fund (SIF) and Network Innovation Allowance (NIA) would be beneficial. The SIF supports large-scale, transformative projects aimed at driving the UK's net zero objectives. Using the SIF to fund the consumer consent solution would not only provide initial capital but also align the development of the consent solution with broader national sustainability goals. Similarly, the NIA can fund smaller, incremental innovations, ensuring that the solution's design is scalable and adaptable while mitigating the need for heavy upfront costs borne by market participants. Both funding sources encourage collaboration,

innovation, and cost efficiency, ensuring that the early phases of the consent solution are well-supported without placing undue financial strain on consumers or stakeholders.

This combination of funding mechanisms ensures a balanced approach that maintains fairness, reduces risks to vulnerable consumers, and provides the flexibility to scale and adapt the solution as the industry evolves.

3. Chapter 5: Landscape – Current and Future

Q8. Do you agree with our position to make sharing consent data with consumers (via the consent solution) an obligation for licensees?

NGED is generally supportive of requiring obligated licensees to share consent data with consumers via the proposed consent solution. This aligns with the broader regulatory framework, where licensees are already responsible for obtaining consumer consent under UK GDPR and energy sector regulations. Making the sharing of consent data an obligation will ensure greater transparency and enhance consumer trust, reinforcing the principles of data protection and consumer empowerment.

Requiring licensees to share consent data directly with consumers will improve trust and engagement by giving consumers greater control over their energy data. By ensuring consumers have access to their own consent data, the solution provides an important mechanism for increasing participation within the energy system, which is particularly relevant as we transition towards a more flexible and decarbonised energy system. The ability to easily access, manage, and revoke consent will foster a more dynamic relationship between consumers and service providers.

Additionally, mandating this as an obligation for all licensees will help streamline the consent management process across the industry. Consumers currently face a fragmented system, where different licensees may have different approaches to managing and sharing consent data. A standardised, centralised platform would simplify this process, reducing friction and making it easier for consumers to interact with multiple service providers through a unified system. This will also promote healthy competition by lowering barriers to entry for new market participants, allowing consumers to benefit from a wider range of services and innovations.

Overall, making the sharing of consent data with consumers an obligation ensures a consumer-centric approach that enhances transparency, builds trust, and promotes a more accessible and competitive energy market.

Q9. Do you consider SLC 0 an appropriate route for implementing these changes, or should Ofgem create a bespoke licence condition?

NGED supports the notion that implementing changes through a specific Special Licence Condition may be more appropriate than relying solely on SLC 0. While SLC 0 offers an approach for ensuring fair treatment of consumers; we believe the nuanced and evolving nature of consumer consent solutions necessitates a more tailored approach. A bespoke Special Licence Condition would allow for more precise alignment with regulatory objectives, ensuring that any new requirements are clearly defined and consistently applied to obligated licensees.

Unlike Standard Licence Conditions, which apply broadly to all licensees, Special Licence Conditions are tailored to specific obligated licensees. This allows for more direct and targeted regulation of entities where specific obligations, such as consumer consent management, are critical. This focused approach ensures that obligations are clearly understood by relevant licensees, enabling more efficient compliance and reducing the risk of regulatory gaps.

This view aligns with our previous response to the call for input earlier this year, where we emphasised the need for clear and specific regulatory frameworks to build consumer trust and ensure compliance. Additionally, as outlined in our Governance of a DSI response, the complexity of modern data-sharing infrastructures requires detailed governance mechanisms that ensure both interoperability and transparency. A bespoke licence condition would provide the necessary regulatory clarity to address the unique challenges posed by the evolving data-sharing ecosystem, particularly in protecting consumer rights and managing consent effectively.

By pursuing this route, Ofgem can ensure that the implementation of these changes is both targeted and adaptable, fostering greater industry consistency and consumer confidence.

