



Data Communications Company
2nd Floor, IbeX House
42-47 Minories,
London EC3N 1DY
smartdcc.co.uk

03/10/2024

Energy Systems Digitalisation Team
Office of Gas and Electricity Markets
10, South Colonnade
Canary Wharf, London
E14 4PU

By Email only: digitalisation@ofgem.gov.uk

Dear Marzia,

Thank you for the opportunity to respond to Ofgem's Consumer Consent Solution consultation. We have provided answers to the nine questions set out in the document, and where necessary, have raised some questions for consideration.

As the operator of the secure data and communications infrastructure that supports Great Britain's smart metering system and central switching service, DCC is invested in ensuring that the consumer consent solution is robust, secure, integrated effectively within our systems and fully scalable to support broader use.

Through our response we emphasise the following key points:

The importance of cross-sector applicability

We are fully supportive of Ofgem's aims and objectives for a consumer consent solution. We agree that unlocking consumer data, securely, can be a key factor in turbocharging the journey to net zero. Through our Data for Good agenda, we have long advocated for data exchange, both within and across sectors, to enable maximum public value.

Whilst we agree that smart metering data is a sensible use case to focus on initially, early design decisions must enable cross-sector applicability from the outset. We are increasingly responding to inquiries from organisations outside of the traditional energy sector and are engaged with, and supporters of, the Smart Data initiative driven by the Department of Business and Trade. An overly narrow focus on energy data holds potential to stymie development, reduce collaboration opportunities, limit growth and restrict achievement of key government priorities – not least net zero.

Protecting the integrity of smart meter data

Today, the smart metering network securely connects over 81 million devices, in over 19 million premises across Great Britain, transmitting over 2.2 billion messages each month.

Given the sensitivity of the information carried over the network, consumption data in particular, significant time and investment from across Government and industry has been placed on ensuring the security of the system. This has and continues to include substantial input and assurance drawn from GCHQ (now the National Cyber Security Centre). From our experience in managing deemed critical national infrastructure, we strongly encourage Ofgem to consider enhancements to the proposed security framework to ensure it is fully adaptable to evolving threats.

Smart DCC Ltd. Registered Office: 65 Gresham Street, London, EC2V 7NQ
Registered in England No. 08641679



Within our response we address the importance of the trust model to assure token management, the need for privileged access controls and the criticality of protective monitoring to enable early detection of threats. In addition, the consultation does not address how consent information will be communicated to DCC systems if another body is operating the platform. This and other considerations relating to integration with the smart meter system are fundamental to the solution delivery and must be explored further before a delivery route can be determined.

Confirming DCC's role as a critical enabler

The scale, complexity and criticality of the smart metering network make it one of the most complex pieces of digital infrastructure in Great Britain. We remain resolutely focused on delivering a secure and stable service that meets our customer's needs.

Whilst Ofgem acknowledges that '*Smart DCC is likely to be involved in the consent solution....*' we believe, this involvement will be significant given the need to ensure integrity and security of the data, underscored by the complexity of the smart metering infrastructure. The operational consequences of the proposed solution on existing DCC processes and systems will require extensive assessment and careful planning to enable successful integration. This task should not be underestimated.

Accordingly, irrespective of who is selected as delivery body, a significant delivery role for DCC must be clearly defined with appropriate authority on solution design. For example, we interpret Ofgem's reference to DCC involvement meaning the need, as a minimum, to validate existence of a valid consent record to enable technical access to consumption data.

This and several other components of the solution design are critical to ensuring the secure operation of the smart meter system and ultimately, an outcome that works effectively and delivers maximum value for industry and consumers.

We continue to provide our support to this vital initiative and look forward to further engagement with Ofgem and other stakeholders to refine the design and implementation of the solution.

Should you have any questions or require additional information, please do not hesitate to contact us.

Yours sincerely,

Mike Hewitt

Chief Technology Officer



Question 1

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

DCC agrees with the proposed Design Principles outlined in the consultation. We believe these principles are crucial for ensuring a secure, user-friendly, and inclusive consumer consent solution. In particular, the emphasis on simplicity, interoperability, scalability, and security aligns with our methodologies.

We would emphasise the criticality of scalability both across the energy sector and beyond to ensure investment in the solution is aligned to related cross-sector developments (Smart Data for example) to achieve maximum impact long-term.

We support these principles as a foundation for developing a robust and trustworthy consent management system that will empower consumers and facilitate innovation in the energy sector and beyond.

Question 2

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

At this stage, we believe it is too early to commit to a specific model for the consumer consent solution. The process is still in its early phases, and the design may need to constitute a combination of different models - numerous factors will influence the final decision.

For example (and as we presented to industry during the lead up to this consultation) the tokenisation and exchange of captured consent, lends itself to a decentralised model, whereby industry adopts a standardised protocol for consent exchange (for smart meter data and other data categories). However, a centralised Authority responsible for token issue, in tandem with organisational identity verification would increase trust by ensuring proof of source.

Likewise, visibility of token exchange and ability to revoke consent can be made available to the end consumer via a consumer dashboard – a key feature of the intended end solution. Whilst this could be delivered both through decentralised, centralised or hybrid models we expect that provision by a central entity or controlled to a sub-set of agreed entities, would create greater trust for the end consumer than a fully decentralised model.

Irrespective of the model selected, we see no merit in a single centralised solution whereby all data requests and consent processing are routed through a central system. Such an approach would present substantial limitations to scaling and flexibility to adopt new data categories beyond smart metering.



Question 3

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?

DCC broadly supports the security measures proposed in the consultation, including multi-factor authentication, robust data protection protocols and risk analysis of cyber threats. However, given our experience managing deemed critical national infrastructure, we believe certain enhancements are necessary to ensure the security framework can fully adapt to evolving threats.

Below, we outline our recommendations and concerns regarding specific security measures:

1. **Biometric data:** The use of biometrics for registration appears excessive. Biometric data is classified as special category data under Data Protection Laws and requires additional protection. We believe that alternative methods, such as device IDs, MPANs, or customer account numbers, would suffice for profile creation without the need for biometric data.
2. **Data Protection Impact Assessment:** The proposal mentions a Data Protection Impact Assessment (DPIA) and consultation with the ICO. We agree that this is an effective mechanism for identifying and mitigating data protection risks and should be employed to conduct a thorough privacy risk assessment of the proposed solution. There may be opportunities to engage with the ICOs Regulatory Sandbox¹ to garner further advice.
3. **Function creep:** The issue of function creep, or the use of data for purposes beyond those consented to by the energy consumer, has not been directly addressed. It is crucial to clarify how function creep will be managed to ensure data is used solely for the purposes for which consent has been obtained.
4. **Data sharing agreements:** We suggest implementing an overarching data sharing agreement for all industry participants. This agreement should ensure lawful processing and controlled, secure data sharing. Section 3 references onward data sharing, but it is unclear who will have access and for what purposes. It is essential to address whether data will be extracted from the solution and how this will be managed. Progressing this activity through a trust framework approach as proposed through the Data Sharing Infrastructure may be advantageous in enabling flexibility and efficiency.
5. **Consent:** Consent must be granular, meaning that if there are multiple purposes for data processing, separate consent must be obtained for each purpose. This is necessary for consent to be considered "freely given" under UK GDPR. Figure 4 of the consultation could better reflect this requirement by illustrating how consent will be captured and managed for distinct use cases.

While the proposed measures are a good foundation, several additional security considerations should be factored into the final solution:

¹ [Regulatory Sandbox | ICO](#)



Topology model and security: The security architecture will depend heavily on the topology model selected for the solution (centralised, hybrid or decentralised). For instance, if an Identity Provider (IdP) federation is part of the solution, additional security layers such as control plane management and identity checks may be necessary.

Token management: A comprehensive and defined security model will be required to manage the entire lifecycle of tokens, including their generation, transmission, storage, and revocation. Additionally, a trust model must be established to ensure the consistent and secure handling of these tokens. This approach should be aligned with the chosen deployment model, as previously mentioned above.

Consent communication to DCC: One critical gap is the lack of clarity around how consent information will be communicated to DCC if we are not operating the platform. Whether token management or another mechanism is used, it is essential that robust security controls are implemented to ensure the integrity and authentication of consent data across systems.

Privileged access controls: Another key consideration is the need for strict privileged access controls. These controls should be defined and established to manage and safeguard access to the platform.

Protective monitoring model: We recommend the introduction of an overarching protective monitoring model, managed by the Delivery Body. This would provide continuous monitoring of the platform's security operations, ensuring early detection of threats and allowing for swift, proactive responses to any security incidents.

Question 4

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

The proposed standards for the consent solution are a good start, but we believe there are additional measures that could further ensure inclusivity, accessibility, and interoperability.

Security standards

While ISO27001 is a robust standard for information security management, we believe additional measures are needed for this specific use case. We recommend independent assurance of the consent solution. This approach is in line with what was done for the Central Switching Service (CSS), providing a higher level of scrutiny and confidence in the security and resilience of the solution.

Accessibility

The consultation acknowledges digital exclusion, which is an important consideration for accessibility. To enhance accessibility, we suggest establishing a fully representative consumer focus group to pilot the solution. This would provide valuable insights into real-world usability issues and ensure that the solution meets the needs of all users, including those who are digitally excluded.



Moreover, it is essential to consider the incentives for energy consumers to engage with the consent solution. For instance, if consumers are already receiving marketing materials for products that can lower their bills, they may not see an immediate benefit to using this new consent solution. Clear communication about the advantages and benefits of the consent solution will be crucial in encouraging consumer participation.

Management and revocation of consent

The process for managing and revoking consent needs to be clearly defined. Consumers will receive an acknowledgement of their consent and a link to the Delivery Body's consent solution, where they can manage or withdraw their consent. It is important to specify whether this link will be sent via email and how accessible it will be for users who wish to withdraw their consent. Ensuring that the process is straightforward and easy to navigate will be essential for maintaining user trust and satisfaction.

Question 5

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

Our response is structured around the following key areas:

- Ofgem's direction of travel
- The role of DCC and clarifications required
- Our operational capabilities and engagement scores

Support for Ofgem's intent

As we have outlined throughout this process, we are supportive of Ofgem's intent in developing the consumer consent solution, and we are committed to being a strong and collaborative partner throughout this process. We share Ofgem's goal of empowering consumers to manage their energy data securely and efficiently and are ready to contribute our expertise to ensure that the final solution achieves these objectives.

We have long advocated for the responsible and innovative use of data, as demonstrated in our *Data for Good* publications, which highlight the potential of data to deliver consumer benefits, enhance market efficiencies, and support the transition to a low-carbon economy. We believe the consumer consent solution aligns with these principles, and we look forward to continuing to support its development.

Clarification on DCC's Role

In the consultation, Ofgem states that "regardless of which Delivery Body is selected, Smart DCC is likely to be involved in the consent solution's infrastructure due to its unique position in the industry as a processor of consumer energy data." While we appreciate this recognition, further clarity on what this role would specifically involve is necessary.

DCC's role needs to be clearly defined, with key principles established to ensure our involvement reflects the complexities of the smart metering system and appropriate authority on solution design.

We interpret Ofgem's reference to DCC's involvement to mean that DCC would confirm, when processing requests for consumption data, that a valid consumer consent record has been registered via



the new consent solution, as required under the Smart Energy Code (SEC). The section on Access Control, which states "the token allows the authorised provider access to the consumer's data from Smart DCC or Elexon's Data Integration Platform" supports this interpretation. We also strongly recommend direct integration of the smart metering system data fields to enhance the robustness of consent management and automating revocation. For example, change of tenancy alerts as a means of automating the revocation of consent, simplifying the process further for consumers.

This is aligned with our previous submissions to Ofgem, and we are strongly supportive of this approach, as it ensures that requests for consumption data are only processed when appropriate consumer consent has been obtained.

Furthermore, if it is Ofgem's intention that the solution should also cover onward sharing of data, as implied in section 3.13, it will be important to ensure the design is robust enough to cover not only the scenario where the consent seeker is using a third party (a DCC Other User) to source consumption data from DCC on its behalf, but also potentially the scenario where that third party is already holding the consumer's consumption data with consent for another purpose.

Clearly, any additional controls required for DCC to manage access to consumption data will have an impact on our systems and the integrity of those systems. While the specific nature of these changes will depend on the chosen solution, possible developments could include:

- Adding an interface to the consent solution to receive or query consent records
- Modifying the DCC User Interface to allow users to present a consent token as part of their requests for consumption data
- Adding new service request processing logic to verify that requests for consumption data are accompanied by a valid consent record or token

To ensure the successful and timely delivery of the Minimum Viable Product (MVP), we propose that DCC work closely with the selected Delivery Body, should we not be chosen for that role. If DCC is not the Delivery Body, it will also be crucial to clearly define and clarify our relationship with the selected Delivery Body, alongside clarifying our role within the overall solution. This collaboration will help guarantee that the solution is developed in a way that meets Ofgem's objectives and integrates smoothly with the existing smart metering infrastructure.

Ofgem should also be mindful that any new SEC obligations relating to access to consumption data will need to be drafted well in advance. This will allow time for DCC system changes to be developed and tested, allow existing DCC Users to modify their systems accordingly and minimise any form of hiatus from prospective users waiting to understand how the SEC may evolve.

In some cases, a period of dual running may be necessary to ensure a smooth transition and we will seek to work closely with SECCo to achieve an optimal outcome for industry and consumers.

In this context, it is also important to note that DCC holds direct relationships with all existing and prospective DCC users – a key stakeholder group, we would expect to leverage these relationships and understanding of emerging business models as a key feed into the solution development.



Implementation and Governance, and Independence

We agree with Ofgem's assessment that as a licenced entity, Ofgem would have the tools to ensure there is a clear remit, governance, rules and transparency were DCC to be selected.

Operational capability

Performance

Ofgem's "Amber" rating does not accurately reflect levels of operational performance and is contradictory to Ofgem's agreed position as established through our Operational Performance Regime. Our system performance is a key metric for measuring success, and we have achieved 100% of the Operational Performance Regime (OPR) target for the last two years. This target is weighted at 70% of the overall OPR, reflecting the critical importance of system performance in maintaining a reliable, available, and timely service for consumers.

It is important to recognise that the smart metering system is incredibly complex, involving over 100,000 different device model combinations across millions of homes and processing billions of messages every month. Managing a system of this scale requires both technical expertise and operational resilience.

In addition to strong operational performance, DCC has significantly improved its contract management scores as demonstrated in the most recent independent assessment commissioned by Ofgem. As Ofgem was made aware during the development of the consultation document, the Interim Audit highlighted improvements, which we trust will be fully recognised on Ofgem's subsequent response and decision making.

Focus on mandatory business

We strongly disagree with the assertion that we are "too focused on supporting future services." Our mandatory business has always been our top priority and there are in fact several policy areas we are unable to get involved in due to the need to focus on regulated activities.

Were DCC to be selected as the Delivery Body, we assume that our role would be part of mandatory business, making the distinction between mandatory and non-mandatory services irrelevant in this context. Finally, if DCC is required to be involved in the consent solution, it is essential that Ofgem allows for the appropriate allocation of resources to meet this obligation efficiently.

Capacity to deliver the solution

We acknowledge Ofgem's expectation that DCC will be involved in the solution's infrastructure, and we would encourage this involvement leverages our capabilities to the very fullest extent. We have a strong track record of managing multiple complex, large-scale projects, and while we recognise the need to balance our licensed activities, we have the appropriate governance structures in place to deliver new initiatives effectively.

Our Enterprise Portfolio Management Office (EPMO) ensures that we can manage our portfolio effectively, allocating resources appropriately. The complexities of the smart metering system are vast,



making it essential that DCC is involved in designing any solution that reflects the advanced infrastructure we manage.

Engagement

DCC undertakes broad ranging engagement on a regular basis – with our customers, Government and regulator, and wider industry. We continuously seek to drive further improvements in our engagement approach reflecting the feedback we receive from industry and through the Operational Performance Regime process.

Over the past few years, DCC has made substantial improvements. For instance, we have seen a 70% increase in our performance against the Customer Engagement OPR between 2020/21 and 2022/23, with a further increase expected for 2023/24. We are also forecast to receive over 90% for our engagement performance through the Switching Incentive Regime and the 4G Comms Hub and Network BMPPA scheme.

In the last 12 months alone, DCC has conducted over 500 formal points of engagement, working through industry governance (SEC and SMIP) as well as leading our own initiatives, including webinars, working groups, and consultations.

Our engagement efforts have been widely recognised, with Angela Love, Chair of the Smart Energy Code Panel, recently stating: *“The Panel recognises the DCC’s efforts in developing the proposals set out in this industry consultation and welcomes the valuable engagement DCC has had with the Panel, the Communications Transition Group (CTG) sub-committee, SEC Parties and DCC Users over the recent months to inform the proposed position. I welcome continued DCC engagement with Panel, its subcommittees and industry over the coming months.”*

Question 6

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?

While we do not have a specific view on RECCo being selected as the Delivery Body, we would welcome visibility into Ofgem’s process regarding the shortlisting of potential delivery bodies, minded-to position as set out within this consultation and ultimately, decision making on the delivery body selected.

We believe it is important for all stakeholders to understand the criteria and rationale underpinning these activities – including the interplay between industry responses and Ofgem’s ultimate position - to ensure transparency and confidence in the chosen body.

As a general point, in context with selection of delivery bodies - we would encourage Ofgem to develop a standardised, robust and repeatable process to options identification, analysis and selection of a preferred option.



Question 7

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.

Our stance on funding remains flexible, as it largely depends on the final design of the solution and the selected Delivery Body, as each entity has different mechanisms for recovering costs. We do agree that fairness should be at the heart of any funding decision, ensuring that consumers are not unduly burdened and that the costs reflect the benefits received.

It is also critical not to underestimate the complexity of cost recovery mechanisms, especially in a multi-stakeholder environment. DCC has the capabilities to navigate these challenges, drawing on our experience with managing complex cost structures. Furthermore, we have identified valuable learnings from the recent Request for Information (RFI)¹ on SEC charging, which could inform how costs are allocated fairly and efficiently across the ecosystem, ensuring that no single group is disproportionately impacted.

Finally, we note consideration of similar challenges for cost recovery in context with proposed uses of the Data Sharing Infrastructure² governance consultation which explicitly calls out the 'Other User' charging framework as a mechanism to support smaller entities who are unable to afford usage-based cost recovery. Exploring potential cost recovery for these initiatives in parallel would help to increase industry standardisation, reduced administrative burden and help to increase uptake.

Question 8

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

Whether licensees will need to be obligated will depend on the perceived value from users of the solution. An effectively designed solution should provide advantages for all industry stakeholders and an agile approach to solution development can test and refine this. The need for obligations should be assessed during this stage.

Question 9

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

Whilst SLC 0 may be a potential route to enable initial implementation, further consideration should be given to the end scope of the solution including breadth of end users and anticipated cost recovery models. For example, the recent Smart & Secure Electricity System consultation from DESNZ set out

¹ [20240430-dp218-review-of-the-sec-charging-methodology-rfi.pdf \(smartdcc.co.uk\)](https://www.smartdcc.co.uk/20240430-dp218-review-of-the-sec-charging-methodology-rfi.pdf)

² [Governance of a Data Sharing Infrastructure \(ofgem.gov.uk\)](https://www.ofgem.gov.uk/governance-of-a-data-sharing-infrastructure)



proposals for licencing Demand-side Response Providers, who would also be intended users of the consent solution.