

Consumer Consent Solution consultation, Ofgem

Energy Saving Trust written response: 4 October 2024

About Energy Saving Trust

Energy Saving Trust is an independent organisation dedicated to promoting energy efficiency, low carbon transport and sustainable energy use to address the climate emergency.

Our work focuses on reaching net zero targets by taking action to reduce energy consumption, installing new infrastructure and accelerating a move to sustainable, low carbon lifestyles.

A trusted, independent voice, we have over 25 years' sector experience. We provide leadership and expertise to deliver the benefits of achieving carbon reduction targets: warmer homes, cleaner air, healthier populations, a resilient economy and a stable climate.

We empower householders to make better choices, deliver transformative programmes for governments and support businesses and community groups with strategy, research and assurance – enabling everyone to play their part in building a sustainable future.

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

While we agree with the proposed Design Principles which recognise the importance of security and transparency, they don't explicitly address privacy, which is becoming an increasingly familiar term to users. We therefore believe the principles should be expanded to include a clear focus on this area. Privacy is distinct from protection against bad actors; it ensures that even without a breach, users' data remains accessible only to those they have explicitly given consent to. A privacy principle should also include mechanisms to ensure explicit and periodically refreshed consent, and ensuring users know how to revoke consent if they wish. Including a privacy principle will be crucial in building trust and safeguarding user autonomy.

Additionally, in relation to the agile, flexible, scalable principle, as an impartial, trusted organisation with experience delivering tailored and expert advice to consumers, Energy Saving Trust believe we would be well placed to be considered as a partner of the chosen Delivery Body.

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

Energy Saving Trust think that Ofgem's proposal of a hybrid model is a logical choice as it presents a balanced approach between a centralised / decentralised model. It would also allow for flexibility and scalability as third parties start to use consumer smart meter data, while maintaining robust security and compliance. The hybrid approach should provide a flexible framework that can accommodate future use cases and data types without compromising on

the ability to control access securely. It's similar to the model adopted by Open Banking which uses a centralised standard but allows third parties to manage data sharing through APIs.

As a potential third-party provider of smart meter data, we would stress the importance of any Trust Framework not introducing insurmountable barriers to accreditation, at the risk of limiting the value this data can deliver to consumers. We have experience as an 'Other' user of smart meter data (via Smart DCC) and the costs associated with auditing / managing the consent frameworks eventually resulted in us stopping providing a smart meter data driven service to our users. Data security and compliance is important, but Ofgem and the Delivery Body must strike a balance that does not stifle innovation or place excessive demands on third party providers who may not have the resources to meet excessive auditing requirements.

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?

Given the Delivery Body's role, we would expect to see transparent and independently audited verification of the commitment to data security that goes beyond relying on adherence to a security standard. We would therefore suggest that more consideration should be made for security controls built into any system design from the start, following secure by design principles:

- **Encryption at Rest and In Transit:** While the document mentions regular security checks and protocols, it does not explicitly mention encryption of data both at rest and in transit. Given that the system will handle Personally Identifiable Information (PII), this will be crucial to prevent unauthorised access.
- **Zero Trust Architecture:** As the consent solution interacts with multiple stakeholders and external systems, adopting a Zero Trust Security Model will further enhance protection. This would mean that no internal or external systems are inherently trusted, and verification is required at each access point.
- **Real-Time Threat Detection:** In addition to regular security checks, implementing real-time monitoring systems such as Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) solutions will be essential to detect potential breaches or anomalies in real-time, allowing for swift responses to emerging threats.
- **Granular Access Controls:** The document mentions MFA but should also implement role-based and least-privilege access controls (RBAC). This would limit data access based on the specific roles and requirements of each user, reducing the risk of overexposure of consumer data.
- **Consumer-Focused Auditing and Logging:** To enhance transparency and trust, a system should allow consumers to view a log of when, why, and by whom their data has been accessed. This would ensure that consumers have clear visibility and control over their data usage.

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

We agree that these parameters are sufficient to ensure inclusivity, accessibility and interoperability. However, we would suggest incorporating a user-centric focus within the parameters by considering not just technical accessibility but also the language and readability. Many of the proposals are quite technical but will be consumer-facing, so adhering to current government guidelines on readability¹ will be crucial to ensure clarity and ease of understanding for all users.

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

We agree with the analysis criteria used by Ofgem to compare the three potential delivery bodies.

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?

We do not have a view.

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.

We do not have a view.

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

N/A

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

N/A.

¹ <https://www.gov.uk/guidance/content-design/writing-for-gov-uk>;
<https://design.homeoffice.gov.uk/accessibility/readability>