Consultation Response Form

Consumer Consent Solution (CCS) Design Consultation

Published 11 February 2026
Response Deadline 25 March 2026

Link to the Consultation

View the Consumer Consent Solution Design Consultation here.

How to Respond

Please complete this document and send your responses to consumerconsent@retailenergycode.co.uk
Where possible, we kindly request that responses are submitted as a Word (.docx) document.
Please be assured that your responses will not be edited or amended in any way.

We've asked for your feedback in each of the questions throughout. Please respond to each one as fully as you can.

We will publish non-confidential responses on our website at https://retailenergycode.co.uk/consultations/

Your response, data and confidentiality

Responses can be submitted in one of three ways:

- **Non-confidential** – the full response along with the submitting organisation's name and category will be published; or
- **Confidential** – responses will only be shared with RECCo and its CCS project team, the REC Code Manager and the Authority (where relevant). We will respect this request for confidentiality, subject to any obligations upon us to disclose information. Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or
- **Anonymous** – the full response will be published, but the submitting organisation's name will be omitted (the organisation category will still be published). Details of the response may be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation, and the organisation name will be shared with RECCo and its CCS project team, the REC Code Manager, and the Authority (where relevant).

If you submit a non-confidential response but wish to keep part of your response confidential or anonymous, please clearly mark those sections as "confidential" or "anonymous" as appropriate.

All responses will be treated as non-confidential unless otherwise indicated.

RECCo recommends submitting only financial or commercially sensitive information as confidential, and using anonymous for other cases where the submitting organisation does not wish to be identified. This approach ensures that response details can be included in any consultation summary report(s) and that RECCo's comments on the responses can be published.

Respondent Details

NAME	Faye Widdowson
ORGANISATION	Luxon Group
ORGANISATION CATEGORY	Other
E-MAIL ADDRESS	Regulatoryaffairs@utilita.co.uk
RESPONSE CONFIDENTIALITY	Non-confidential (recommended)

Questions

Scope of the CCS

Q1	Do you agree with the proposed MMP scope, including the core functional components and the inclusion of SEC Other Users and the BSC SDR?

We do not agree. The scope of the consultation has gone beyond what Ofgem's original remit allowed, and we do not currently see how the benefits of the proposed solution will outweigh the costs of implementation.

We are firmly of the view that customer facing businesses are best placed to define the customer journey and own the customer relationship. Mandating a common journey will risk creating barriers to innovation and placing governance above customer experience. We believe this is the wrong outcome if we want customers to engage with the energy market as part of the net zero transition.

Q2	Do you have any comments on the assumption that SEC Other Users would not need to migrate existing consents to the CCS and would instead move to using the CCS as existing consents are renewed?

We fundamentally disagree that the CCS should validate consumer consents because a process already exists via the existing consent arrangements. We do not believe that SEC Other Users should be mandated to use the CCS process and instead the CCS should be limited to acting as a data base to manage existing consents.

Notwithstanding the above, if the proposal proceeds as is, it would seem sensible not to migrate the SEC Other User consents because it would otherwise endure duplication of validation. We request additional clarity on how the CCS will propose to notify EDPs of new consents (and consent changes), the SLA's involved (if any) and how performance expectations will impact end users. We also seek clarity on whether it is REC's intention to use consumer consents obtained by energy

suppliers under SLC 47 in future iterations of the CCS. Currently this consent is only obtainable under mandatory settlement rules and cannot be used in any other capacity.

REC Policy Positions

Q3	Do you agree with the position that consent for access to half-hourly metered data should be provided by the occupier rather than the bill payer, where these are different individuals? If not, please provide your rationale.

Half hourly metered data relates to the household and so it should be the occupier that provides consent to this data; however, we disagree with the proposals for multi-occupancy homes as this may not be compliant with data protection rules.

For the proposed approach to work within the data protection rules, the energy user would have to be a single occupant or a small family household, and the consumption data would have to be wholly used by the individual(s) to provide valid consent.

While we agree that occupants should be able to grant consent as the energy user, there should be a mechanism to ensure consents are reviewed regularly as continuously valid. Occupiers (i.e. not homeowners with or without a mortgage) can change frequently and quickly – particularly for occupancy arrangements such as short term lets or housing associations.

However, REC have identified that the current licence drafting of the supply licence allows energy suppliers to facilitate consents from the bill payer rather than an occupant and therefore this will need to be addressed to progress with this proposal.

We are also concerned that REC's approach would exclude a significant proportion of consumers. We would note that Lloyds Bank Consumer Digital Index 2024 found 11 million adults (one in five) help others with making payments.

Q4	Do you agree with the position that for multi-occupancy households, a 'lead occupant' may provide consent on behalf of other occupants only where they confirm they have the authority to do so and have obtained agreement from all other adult occupants? If not, please provide your rationale.

We do not agree.

We believe this would not be compliant with Data Protection regulations specifically regarding consents being transparent. The proposal seeks to allow the lead occupant to create a portal account or guest account and does not allow for transparency of that consent to reach the other occupants of the household.

There would be too many uncertainties over exactly how many occupants live inside a HMO or other multi-occupancy housing situation. Therefore, it is near impossible to guarantee consent is provided by all occupants particularly if the "obtained agreement from all other adult occupiers" is given verbally. The Data Protection rules state that consent must be transparent and for this proposal to exist, each occupant should, as a minimum, receive a notice to say that they have consented to the sharing of their data. This may arrive in the form of an automated email that can be sent from the CCS, but this is the responsibility for the lead occupant to obtain all email addresses from the other

occupants and provide them correctly. We believe the risk is too high to satisfy Data Protection legislation.

This becomes even more problematic when an occupant vacates the property which can happen frequently and at short notice, particularly in HMOs and student lets. This would only cause more disputes to be raised and the cost of investigating them would not outweigh the benefit of providing data that is, ultimately, shared with other individuals which may or may not benefit each occupant equally.

Lastly there is a risk of a consent-war, where one occupier grants consent and another occupier revokes it. This situation would create unnecessary burden on the organisations who would have to investigate and resolve such situations.

Q5	Do you agree with the proposed approach and standard for identity verification? *If not, please provide your rationale.*

We do not agree.

The current arrangement under the SEC regime already utilises very good and proven validation checks to determine the identity of an individual granting consent. This is less arduous than requiring customers to provide photo ID for the verification. REC have failed to demonstrate why further verification is required and have failed to justify why verification of individuals consenting to sharing household consumption data should be treated the same as accessing NHS data. Creating different requirements under different codes goes against intention of code managers and CACOP as well as creating further regulatory burden.

We believe that it will also disengage consumers as the process requires the consumer to have their ID with them at the time of giving consent and this may not always be possible. Furthermore, consumers may not feel comfortable to do so.

IDV checks will also prevent third party help for any consumer who is digitally excluded and relies on friends or family or trusted third parties to help them.

We are also concerned that REC have chosen an identification solution with no consideration of the costs that this would incur. There also appears to have been no consideration of the customer friction and dropout rates that this would create versus the protections of choosing this preferred method for identity verification. This seems above and beyond the existing processes that are well used within the SEC regime (and which are known to go above and beyond the requirements under the DPA legislation).

Given that REC has chosen to begin with a minimum viable product in which only half-hourly data will be shared, a straightforward verification process should be sufficient at this initial stage. This approach would help maximise consumer engagement by keeping the onboarding experience as low-friction as possible, while also minimising implementation and operational costs for industry participants.

We also question what would happen where the consumer is unable to validate their identity due to historic issues with the industry systems such as crossed meters or incomplete/inaccurate address/MPxN databases. There is a significant problem in the industry where mismatches and false negatives are causing negative consumer experiences. What would be the consumers' course to resolution in this instance?

Q6	Do you agree with the position that consumers should have the option to establish an account with the CCS or grant consent via the 'guest' approach? If not, please provide your rationale.

We do not agree.

We believe that this highlights a failure of the CCS design. We believe that ATPs should be responsible for IDV in line with SEC requirements. This enables ATPs to create the best customer journey and experience as well as fostering innovation. If a consumer wishes to access the CCS to understand what consents they have provided then they would be required to also undertake IDV; however, this could be using a digital identity provider such as Yoti.

Given the future expansion plans, guest accounts should not be an option for accessing CCS database to view what consents had been granted. Full, transparent consent needs to be given by the consumer, and customers need to understand and have records of what they are consenting to as a minimum to ensure the product delivers against Ofgem's direction.

Consents should also be revised each time a new wave of data is added to the scope of the CCS.

The proposals also suggest that an existing login will not have to undertake another IDV check however, what would be the scenario if the customer moved address and did not inform the CCS/ATP/EDP. This is incredibly commonplace in the industry. That IDV will still exist on file, but the consumer could theoretically continue to grant consents to a property they no longer have occupier status over. There should be a robust mechanism in place to ensure quick erasure of consents when a Change of Tenancy is notified.

Q7	Do you agree that consumers should have the option to revoke or renew consent directly with the relevant ATP or via their CCS account? If not, please provide your rationale.

If consent must be given via the CCS, then it should be capable of being revoked there too. This platform should be able to let consumers manage their consents easily and by not including the ability to revoke consents, it would create a confusing and disjointed consumer journey.

This also supports the argument that a guest account should not be made available as a customer cannot log back in to view their consents or manage or revoke them.

Equally, if a consumer does happen to go direct to their ATP (because they have established a relationship with that provider) the consumer should be able to revoke consent and it pull through into the CCS portal and notify EDPs so that data sharing can be stopped.

There should also be a mechanism to ensure that any notification of a home move via the EDP, ATP or CCS must also end that consent. In addition to requiring a new record.

Q8	Do you agree with our position that EDPs should explicitly check that active consent is in place within the CCS each time they share data with an ATP? If not, please provide your rationale.

We do not agree.

The proposed zero-trust model will essentially create three stages of validation of consent which will leave the process feeling arduous, burdensome and costly. Where the proposal suggests that the CCS holds consent and performs verification checks, the EDPs should be able to rely solely on the CCS's platform given the robustness of the proposals. Meanwhile the ATP should be validating that the consent has been granted for the right datasets and time period.

EDPs will need to set up data sharing agreements with the ATPs at any rate which may make this irrelevant.

Q9	Do you agree that if the CCS is unavailable, the EDP should continue to share data unless the CCS outage extends for a significant period of time? If not, please provide your rationale.

We do not agree with the proposals to maintain a 99.9% availability when the Open Banking system is 99.5%. We do not see the consents portal justifying the expense of maintaining that level of availability. We believe cost analysis should be undertaken to assess the cost differential between 99.5% availability and 99.9% availability to assess this.

If an outage happens, the consumer would not be able to log on to accept new consent or change consents in any event and so the continuation of any data sharing can continue at low risk. If the customer does decide to revoke consent, the ATP can notify the EDP directly through the data sharing agreements and/or existing systems.

Q10	Do you agree that the FAPI 2.0 standard should be adopted for the CCS, which includes use of mTLS for all data sharing? If not, please provide your rationale.

Whilst the adoption of FAPI 2.0 standard seems reasonable on paper we would note that there has been no cost consideration of the implications of this.

As recognised by REC, FAPI 2.0 is not currently used in Open Banking or energy, and so implementing this standard would incur additional cost. It is also not clear if implementing FAPI 2.0 would incur further system or validation costs at this stage. We therefore believe further

consideration is given as to what the industry costs of implementing FAPI 2.0 will be above the cost of a standard API. This would enable a cost benefit analysis of this decision to be conducted.

If it is the expectation that the CCS expects EDPs to share personal data directly with other parties, then a DSA must be in place with that third party by law.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
In light of REC's confirmation that no material changes to the technical architecture can be considered at this stage, it is not evident what substantive value we may add here.	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
Notwithstanding our general objection to the proposed validation checks, in theory we agree with this approach. The use of address-matching is an appropriate mechanism to ensure that the correct customer, correct address, and therefore the correct supplier is identified. However, both REL and MPL address formats carry inherent risks of inaccuracy. These potential discrepancies have implications for ongoing address management, particularly if the consent solution requires the use of an address as a key identifier. However, if address information forms part of the consent process, a robust and clearly defined mechanism will be required to correct, validate, and refresh address data. Without such a process, there is a risk that outdated or inaccurate address records could undermine the reliability of customer identification and consent capture.	
Q13	Do you have any comments on the non-functional requirements detailed within Annex D?
We would need to understand the costs/benefits analysis to comment on the proposal for a 24/7 service desk support. We would also be keen to understand any SLAs with regards to resolution.	
Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?
No comment	
Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
No comment	

UX Design

Q16	We have identified four groups of people who will use the consent system, each with different needs (Annex F – Behavioural Archetypes). Have we missed any important user groups? Are there any needs we haven't considered for any of these groups? If yes to either, please tell us what's missing and why it matters.
We are concerned that the proposal extends beyond the original scope and intent of the CCS as set out by Ofgem. In our view, it may not be appropriate for REC to prescribe elements of the customer experience in this manner. Instead, this should remain the responsibility of service users and market participants, who are best placed to design and deliver consumer-facing interactions that reflect their detailed understanding of customer needs and behaviours. Furthermore, the proposal appears to place disproportionate emphasis on driving customer engagement, rather than prioritising the fundamental objective of enhancing consumer confidence in the consent process. We consider that the CCS should remain focused on delivering a secure, reliable and efficient framework that enables trust, while allowing individual organisations the flexibility to determine how best to engage their customers within that framework.	
Q17	Do the proposed inclusion requirements adequately address the needs of vulnerable customers, digitally disadvantaged consumers, and consumers with limited English proficiency (Annex F – Accessibility and device constraints)? If not, what additional requirements should be included?
While best efforts can be made to increase accessibility of such services to the needs of disadvantaged customers, it can never truly be wholly accessible and there will be a subset of such customers who will not engage. It should not be for the CCS to address this issue. As previously set out, we are concerned that the CCS approach to IDV is likely to exclude a significant proportion of consumers – particularly those who help others with online / digital services.	
Q18	Do you agree that consumers need to know who is requesting consent, what data they want, and for how long? If not, what's missing? Is there a risk of information overload?
We agree that consumers need to know information about how their data is used and we do not think this would be “information overload” if presented well. This information would be the minimum we would expect to comply with DPA regulations. As this is a requirement of DPA regulations we believe that also including this within the scope of the REC design creates regulatory burden. It is the responsibility for ATPs to comply with GDPR and DPA regulation, and for ICO to enforce this.	
Q19	Where should additional verification steps or friction be introduced to protect consumers? Where might such steps create disproportionate barriers? (Refer to figures 7–10: User journey stage)

We believe that customer circumstances such as bereavement, separation and/or domestic abuse or other forms of coercion/control must be carefully considered to avoid the exploitation of the most vulnerable consumers. Any consumer must be able to use a “Say it once” service. For victims of abuse, this must be easy to revoke consent and for data to be deleted/services to be halted as quickly as possible.	
Q20	Do you agree that showing consumers which organisations hold consent, what data is shared, when consent was granted, and when it expires provides adequate visibility? If not, what's missing? What limitations should be communicated to manage expectations?
We agree. This should be shown as a minimum to allow for consumers to make informed choices. This must be in line with the transparency, fairness and lawfulness principle of the Data Protection regulations. We believe that providing this information to consumers is where the CCS can add value. This should be the core of the CCS and anything beyond this represents encroachment on the customer journey. The CCS should return to the original scope as a means of collecting what consent customers had granted and replaying this in a single portal. This would be much simpler requiring API integration with ATPs so consents would be logged, lower cost and deliver a better customer experience than that proposed by REC’s current CCS design. Limitations may arise regarding the specific party to whom consent was originally provided, particularly in scenarios involving multiple organisations—for example, where elements of a service are delivered through white label arrangements or third-party providers.	
Q21	Do you agree that consumers need to understand which services will be affected, what happens to their data, how long changes take, and whether revocation is reversible? If not, what's missing? Is there a risk of information overload at the point of revocation?
Yes, we agree that consumers should have a clear understanding of their rights and of any service levels associated with the process. This is particularly important in relation to consent revocation, which should be simple to initiate and as close to instantaneous as possible in terms of both halting further data collection and ceasing any continued use of the data already obtained.	
Q22	Do you agree that assisted journeys should enable consumers to grant consent, review active consents, revoke consent, and receive the same information as digital users? If not, what additional outcomes are needed to achieve equivalence?
It is not clear from the proposal how the needs of consumers who are digitally excluded will be met, and this represents a significant gap in the current design. Furthermore, additional clarity is required on how the service will accommodate consumers who rely on third-party support to manage their affairs. Many individuals depend on carers, family members, friends, or professional advocates to make decisions, perform administrative tasks, or access online services on their behalf.	

The proposal does not yet propose how such trusted third parties will be recognised, authenticated, or authorised within the system, nor how the service will ensure appropriate safeguards against misuse.

Without such considerations, there is a risk that vulnerable consumers may encounter barriers or exclusions that undermine the service's objectives.

We would also highlight that under GDPR consumers have the right to be forgotten and their data removed. It is not clear from the CCS design how consumers can request for the CCS to delete their data from within the CCS.

Q23	For consumers who are unable or choose not to use digital services, what outcomes should an assisted or alternative consent service journey deliver to be considered fair and equivalent?

Consumers should be offered the chance to provide consent through non-digital channels, including over the telephone or via a trusted third party acting on their behalf. In these cases, the authority to act must be explicit, freely given, and clearly documented to ensure both consumer protection and operational clarity for all parties involved.

To maintain transparency and safeguard the integrity of the consent process, written confirmation of a third party's authority to act—and of the consumer's underlying consent—should be available through hard copy correspondence where required. This is particularly important for consumers who prefer or rely on paper-based communication due to accessibility needs, personal preference, or limited digital capability.

In addition, the provision of regular, hard copy reminders of the consents in place would help ensure ongoing awareness, reduce the risk of outdated or misunderstood permissions, and reinforce consumer confidence in the system. Such reminders would provide a clear record of who is authorised to act, the scope of that authority, and the duration of any consent given.

Taken together, these measures would support a more inclusive, equitable, and trustworthy process, ensuring that all consumers—regardless of digital access or support needs—can participate fully and safely.

This also highlights how REC's proposed approach to IDV for digitally engaged customers has been over engineered. We continue to believe that ATPs are best placed to define and develop customer journeys as they have experience of dealing with customers and developing good customer journeys. REC is a B2B governance expert and not a customer facing organisation.

The current solution risks creating sub-optimal customer outcomes and reducing customer engagement.

Governance Design

Q24	Do you have any comments on the proposed REC drafting approach, including the creation of a new REC CCS Arrangements Schedule, a new CCS Service Definition, the Customer Experience Guidelines, consequential changes to existing REC artefacts, and the new CCS API Technical Specification?

We are strongly opposed to the creation of Customer Experience Guidelines in the REC. We believe this is outside the remit of REC and beyond the scope of the CCS solution. The consumer experience should be owned by ATPs, suppliers and those who engage with customers so that they can develop the best solutions for all their customers. This also drives innovation and enables ATPs, suppliers and customer facing organisations to discharge their regulatory requirements in the most efficient manner possible.

Including the Customer Experience Guidelines risks creating a vanilla customer journey that increases friction and drives a poor customer experience as well as creating regulatory burden. The creation of the Customer Experience Guidelines also goes against Ofgem's move to customer outcomes and away from prescriptive regulation.

We believe that inclusion of the Customer Experience Guidelines within the REC would be a backwards step and create a barrier to innovation and change.

Q25	Do you agree with the proposed initial funding model, including the ability for the cost of qualification and breach investigation activities to be recovered from the individual organisations? If not, please provide your rationale.

We do not agree with the proposal. In our view, early users of the service should bear an appropriate share of the associated costs, rather than these being passed through to energy suppliers and ultimately recovered from customer bills. Recent government policy has been to reduce the burden of policy and operational initiatives on consumers' energy bills, not increasing it. Government also committed at Budget 2025 to subject any additional costs, including new levies, to enhanced scrutiny under a new framework to ensure they are affordable, represent value for money and do not impose unnecessary costs on households and businesses. These proposals have not been subject to this scrutiny. Shifting the cost of early adoption onto consumer bills would be counterproductive at a time when affordability remains a significant concern for many households and businesses.

While we acknowledge that applying charges to early users may, to some extent, reduce the incentive for rapid uptake, these users are likely to derive commercial benefit from the services they offer to consumers. It is therefore reasonable that the costs of enabling these services should be borne by the organisations delivering them and, where appropriate, by the end users who choose to engage with those offerings. This approach supports a fair and proportionate allocation of costs aligned with the principle that those who benefit should contribute.

Furthermore, the consultation is unclear on the extent to which EDPs will be required to contribute to the costs of the service. Given that EDPs may also benefit from the sharing of consumer data with ATPs under consent-based arrangements, there is a clear rationale for cost-sharing among the early

ecosystem participants. Ensuring that all parties who gain value from the service contribute to its funding would help to avoid inappropriate cost transfers to consumers and promote a balanced and sustainable model for long-term operation.	
Q26	Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.
We are concerned that the proposed CCS accreditation model will create further regulatory burden and goes against the intent of code manager reform as it fails to recognise cross code working or efficiencies. In particular we note that DCC Other Users have to undergo significant SEC accreditation and assurance processes to access half hourly data through the DCC. REC appears to be proposing further accreditation and assurance to access the same data, and Elexon is seeking to develop their own assurance process for accessing SMEDR through P494. We believe there should be a single assurance regime with CCS users able to rely on SEC assurance and accreditation if they already have it.	
Q27	Do you agree that a minimum standard should be set whereby all CCS Users should be Cyber Essentials Plus certified or ISO 27001 accredited? If not, please provide your rationale.
It is our understanding that it is not possible to set a minimum standard for CCS users to be certified or accredited unlike the SEC. Companies may be asked to be compliant with a framework for how they should protect data but cannot be mandated to pay for certification or accreditation.	
Q28	Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?
We are concerned about the use of the REC Change process for managing future expansion of the CCS. We believe that the current solution as proposed is unworkable from a supplier perspective and would require fundamental redesign to be delivered. It is unclear why development of CCS now is being undertaken outside of REC change process, but fundamental redesign could be accommodated within the change process.	
Q29	Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?
Any performance assurance activity should be proportionate to the nature, scale, and likelihood of the issues being addressed. A proportionate approach ensures that the level of oversight and intervention aligns with the actual risks posed, rather than imposing unnecessary burdens on market participants.	

Assurance should be co-ordinated across code managers to reduce regulatory burden and ensure that the same assurance is not being undertaken multiple times.

We are concerned that REC's proposed performance assurance framework duplicates existing code assurance, adds regulatory burden and does not align with code manager principles of facilitating cross code working.

Q30	Do you have any comments on the proposed issue/dispute resolution paths defined for the management of CCS issues?

It is unclear whether, during a dispute, the data sharing arrangement should be revoked or suspended.

If there is a dispute in progress, it should be taken to mean that the consent should be revoked to safeguard personal data.

We do not believe that the CCS should absolve itself completely of the duty to investigate complaints relating to consent – particularly when it is proposing to conduct the IDV checks which is a key part of validating the customers' ability to grant consent and facilitating the use of data sharing, in addition to managing the performance assurance framework. Any part of the consumer journey may be at risk of failing and the consumer should be able to raise a complaint or query directly with the CCS. ATPs, EDPs and the CCS should investigate their systems to confirm where the issue occurred. This is particularly important where REC is assuming that a single individual can grant consents for a multi-occupancy home which is not within the ATPs or EDPs remit to control if it becomes enforceable as a consumer option.

Equally, from a consumer's perspective, they would have granted consent through the CCS, and so, in their view, the complaint should start and end with the CCS to avoid customer confusion where multiple parties are at play.

Product Roadmap

Q31	Do you have any comments on the approach to defining the future roadmap within the consultation or the content of the draft roadmap in Annex G?

Any proposals should be led by the consumer experience and feedback. A suitable Impact Assessment must also be delivered against each step of the roadmap to ensure the costs are balanced and achieve consumer needs and wants.

Additional Comments

Q32	Please provide details of any additional issues you feel have not been adequately captured within the consultation document.

This response is submitted on behalf of the Luxion Group of companies, including Utilita Energy Limited (energy supplier), Procode Technology Limited (DCC Other User), Trust Power Limited (trading as Loop) (Authorised Third Party) and Canary Care Global Limited (data-driven care technology provider).

Overall position
We do not support REC's proposed CCS design. We support Energy UK's response to this consultation and endorse the points raised; accordingly, we do not duplicate those points here. Our responses to the questions in this consultation should be read in the context of our fundamental view that the proposed CCS, as designed, will not deliver the stated project objectives. We also consider that existing consent models could be leveraged without the additional cost and complexity of developing a new end-to-end solution.

Key concerns
We are concerned that the proposed design is disproportionate and has been developed without sufficient evidence of cost-effectiveness, proportionality or consumer benefit. We believe the model is over-engineered (e.g. mandated photographic identity verification and 99.9% service availability) that is likely to increase cost and customer friction without commensurate benefit. There are exclusion risks arising from assumptions about household composition and digital behaviour, including consumers who rely on trusted third parties for support and those in multi-occupancy settings, where the proposed approach may be incompatible with data protection requirements. In addition, there is considerable scope creep into the customer experience design and consumer journeys, which should remain with consumer-facing organisations best placed to innovate and meet diverse customer needs. Embedding customer experience requirements in code governance risks delay, reduces flexibility and inhibits innovation.

We request that an updated impact assessment is undertaken and published, supported by clear evidence, to substantiate the assumed positive outcomes of the CCS and to demonstrate that costs and implementation impacts are proportionate.

To align delivery with Ofgem's original intent and minimise unintended consequences, REC should refocus the CCS on a minimum viable design, with any additional requirements made optional and/or subject to robust cost-benefit analysis.

As a minimum, we recommend that REC should:

- Deliver a core Consumer Consent Service database to record consents (dataset and duration) provided to Authorised Third Parties, enabling efficient integration via open APIs and supporting batch processing where appropriate.
- Provide a simple consumer-facing interface enabling consumers to view which organisations hold consent, what data is shared, the duration of that consent, and clear routes to withdraw consent with the relevant ATP.
- Undertake a full review of identity verification requirements and options (including costs, exclusion risks and customer friction) and publish the associated impact assessment, setting out minimum standards for ATP-led processes.

In our view, delivery beyond these core requirements represents scope expansion and should only proceed where supported by demonstrable consumer benefit and a proportionate, evidence-based business case which is fully costed.

Thank you for responding

Your response is greatly appreciated.
If you have any questions or
want to keep up to date with our
latest news, please contact us below.

LinkedIn

retailenergycode.co.uk

consumerconsent@retailenergycode.co.uk