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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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	Rhona Peat
ORGANISATION	ScottishPower Energy Retail Limited
ORGANISATION CATEGORY	Energy Supplier
E-MAIL ADDRESS	Rhona.Peat@ScottishPower.Com
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 broadly support the proposed scope and functional components of the Minimum Marketable Product. Limiting the initial scope to the sharing of domestic energy data is a sensible approach that should probably allow industry to assess how effectively the proposed solution delivers benefits for suppliers and ultimately consumers. We note the intention to extend the scope to include non-domestic energy consumers, in future. It is our expectation that such expansion will be subject to an industry consultation, to determine and understand the modalities on how this would operate.	
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 support the intent for SEC Other Users moving to using the CCS as existing consents are renewed.	

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.

No. This could potentially lead to confusion and data protection breaches. Our approach towards customer data is based on the premise that the data subject is the named account holder. As such, all the data relating to that account is treated as the account holder's (ie the bill payer's) personal data.

This approach is premised on the below steps:

- As a data controller, we would not disclose personal data at anyone else's instruction other than the named account holder, or when we otherwise have a lawful basis to do so.
- If the data subject ie account holder/bill payer has not provided consent, we will need to befully satisfied that anyone else who has provided consent has done so with the full authority of our account holder before disclosing data.
- As a data controller, we would not make a disclosure to the ATP without assurance that our account holder has approved it.

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 are unclear on how this verification process is expected to operate. The consultation states:

- for multi-occupancy households "one 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". However, the absence of clear guidelines on how such authority should be evidenced, if indeed the "lead occupant" has the explicit authority of other tenants to grant such consent for the sharing of energy data may *ipso facto* create conditions for disputes.
- For single occupancy domestic premises, an individual may well occupy the property and consume the energy at the premises. However if the bill is being paid by the landlord, suppliers would have no relationship with the consumer and thus no way of verifying their consent to disclose data on that basis.
- These concerns also extend to multi-occupancy households with multiple MPANs where the account holder is different from the occupier.

Please also note the concerns highlighted in our response to Q3.

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

Yes, we support the requirement for a high confidence level when verifying consumer identification for the Consumer Consent Solution. Consent should only be granted by individual(s)/data subject with the appropriate authority to do so to safeguard the integrity of the data sharing process.	
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.
No, our preferred option would be for consumers to establish CCS accounts for the purpose of managing their consent activity. We acknowledge the intention to reduce consumer drop off through the provision of a "guest approach". However, this cannot come at the expense of data security and where it could compromise the integrity of the consent framework. As noted in our response to Q5, it is important that the risk of unauthorised access or misuse of consent management is reduced to the bare minimum.	
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.
Yes, we have no objections to consumers managing their consent activity directly via their CCS accounts. However, clear obligations and liabilities will have to be defined in circumstances where a consumer does not hold a CCS account and instead chooses to manage their consent activity bilaterally with the ATPs, and where consent revocation is not communicated to the CCS. This is to ensure: • That any withdrawal of consent made to the ATPs and not subsequently notified to the CCS,does not create compliance risks for the Energy Data Provider. • Where consumer data is shared in error due to the ATPs failure to notify the CCS, the Energy Data Provider is typically the first point of contact. In such a scenario, the Energy Data Provider should be able to enforce costs against the ATP. The consultation acknowledges that ATPs are responsible for obtaining consent and as such relies on it to demonstrate a lawful basis for processing data. However, this creates a significant risk for the EDP. While the EDP is expected to rely on the consent as much as the ATP, it has no control over that consent and can only validate information available on the CCS. If the EDP therefore discloses personal data in circumstances where the consumer has informed the ATP that they no longer consent and the ATP does not update the CCS, the EDP would be in breach of Data Protection Law. EDPs would in this instance, require protection through the Data Sharing Agreements and clear consequences for ATPs who fail to meet their obligations. However, even if these protections exist, we consider the degree of risk to be significant for EDPs more broadly and at this point are not convinced that this risk is reasonable in the context. The EDPs do not get to choose which ATPs it deals with and it does not get to conduct due diligence on these ATPs (we note REC's intention for an accreditation process). As such, it is not enough that EDPs are	

able to recover financial losses, as there is the risk of reputational damage arising from a mistake by a party that EDPs have limited or no control over. Given the issues highlighted above, it is imperative that RECCo undertakes a thorough review of these risks and establishes mitigating measures to ensure that EDPs are adequately and consistently protected.

Please note the concerns raised above are also valid for where the consumer holds a CCS account and for where the CCS suffers a malfunction and consent records are not reflected appropriately.

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.

No, our preference would be the adoption of a model in which the ATP issues a valid consent token to the EDP. Once this token is authenticated against the CCS, the EDP will provide data for the duration of the token's validity. Data sharing would therefore proceed until the consent token either reaches its expiry date or is revoked. This approach is more cost effective than the "zero trust" model and ensures that all parties operate on a consistent and authoritative record of consent, thus mitigating the risk of data being shared beyond the scope of what has been validly authorised.

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.

No, in the event of a system outage, EDPs should immediately cease all data sharing activities. Data sharing should only resume once the CCS has been restored to an operational state that guarantees reliability and integrity. This is critical to prevent data being transmitted without assurance that the underlying framework is functioning as intended.

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.

Yes, we have no objections to the use of FAPI 2.0 standard.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
We offer no comments on the current high-level approach. MPANs for properties are static and that is a benefit for this process. We do however recommend that there is some performance testing for token issuance, as this is core to every ATP–EDP transaction.	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
Yes, however we seek clarifications on how this will be managed in situations where there are erroneous transfers and/or crossed addresses. It is widely recognised across the industry that address data quality remains imperfect. Daily, operational issues around crossed addresses and plot-to-postal discrepancies particularly for new connections continue to present material challenges. We recommend that a data cleanse activity is carried out prior to implementation date to ensure that address quality is accurately aligned across industry systems, recognising that address quality will remain an ongoing area for monitoring and improvement. We also note that REC Schedule 29 assigns the CSS provider (DCC) the responsibility for maintaining REL Address Quality. As such, where MPANs have been wrongly matched to an address resulting in the unintended sharing of data, EDPs should not be held liable for such disclosures. In addition, it is imperative that in an erroneous switching scenario, an incorrect supplier is not inadvertently placed in a position where it is obliged to provide data to an ATP. Any data sharing must be paused until the erroneous transfer is resolved. Please see our response to Q7 also in respect of delineating clear responsibilities.	
Q13	Do you have any comments on the non-functional requirements detailed within Annex D?
We would note that there could be a proactive expiry alert for tokens and requests we receive, where the response from the CCS is not successful. In these scenarios a process could be included to set up automated resubmission or retry logic in case of temporary CCS unavailability.	
Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?

We understand that centralisation is used for IDV, token management, consent ledger and core trust functions, where decentralisation is used for market flexibility and competition matter (ATPs, EDP interactions). If we want to shift components from centralised to decentralised over time to embrace market opportunities, we should have a defined criteria as additional decentralisation could reduce operational risk while maintaining trust.	
Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
At this stage, we have no objections and are happy with the process diagrams. For more detailed process diagrams, it would be helpful to include the following: • Adding explicit error-handling options (eg failed IDV, ATP timeout, token introspection failure). • Including end-to-end monitoring and audit trail elements in diagrams for traceability.	

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 agree with the identified groups. However, it appears the digitally disadvantaged have not been explicitly or sufficiently addressed. We therefore seek clarification on how this sub-group will be supported in their interaction with, and ongoing use, of the MMP. We would welcome details on the specific accessibility measures, assisted digital pathways, and alternative channels that will be available to support consumers with limited digital skills.	
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?
Please see our response to Q16.	
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?
Yes, the law requires that consent must be specific and informed. The consumer also needs to clearly understand the purpose for which their data will be used, what data is being requested, and for how long the party requesting the data is getting consent to use it. As such, we do not see a risk of information overload.	
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 note that the scope of the MMP is expected to over time include tariff data sets and potentially the Priority Services Register (PSR). This consultation also indicates that, should this expansion happen, differing identity verification confidence levels would be required (lower confidence level for access to tariff data sets and higher confidence levels for the PSR). However, to minimise the risk of data mismanagement and ensure a consistent approach from the outset, it is perhaps better to adopt a single, standardised verification model on the understanding that the CCS Solution could host multiple consents of all different sensitivities.	
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 with the elements set out above. However, in addition, consumers should be provided with clear information regarding the specific purpose associated with each consent they grant. Consumers must also be able to easily understand the mechanisms available to withdraw or amend consent at any time. We would also strongly suggest assessing whether all consents should, by default, be time limited. For example, when a consumer grants consent, a reasonable approach could be that such consent should not remain valid for more than one year (or 12 months) unless renewed. This would ensure that consents remain current, informed, and reflective of consumer intentions. Upon expiry, the consumer would be required to provide a positive affirmation to renew the consent.	
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, consumers must have genuine control of their consents. Consent should be as easy to revoke as it was to give. The consumer should have clear understanding of the distinctions between different consents and who each has been provided to.	
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?
Yes, we agree assisted journeys should give consumers the same scope to manage their consent as digital users.	
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 choosing assisted channels must experience no reasonable disadvantage in their ability to access, update or revoke consent. Relevant processes should be implemented to ensure that non-digital consumers achieve outcomes that reflect their wishes. This may include extended guidance and/or additional explanations, to ensure that consumers are equally informed and protected particularly those with accessibility needs and vulnerabilities. Consumers engaging through telephone or in-person support should experience a secure, structured verification process that upholds the integrity of the CCS. This should include robust checks to prevent erroneous or unauthorised consent and ensures the same level of evidential quality and auditability as digital consent.	

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 would suggest that as part of the CCS Arrangements schedule, clear obligations and liabilities are set between EDPs and ATPs regarding how consent is managed. Please refer to our response to Q7.	
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 note REC's proposal that initial funding for the solution should be provided by Suppliers through the REC cost-recovery model. While we understand the rationale for this approach during the initial development stages, we are concerned that other market participants who will eventually have access to the CCS, in many cases for commercial gain, will be making no contributions, with all of the costs being picked up by suppliers and ultimately consumers. We do not think this is a reasonable approach for the enduring model and welcome RECCo's assessment of alternative models. We consider the initial period should be no longer than six months, with RECCo undertaking a review prior to this point to assess the most appropriate enduring funding model. This is to ensure that consumers are not bearing disproportionate costs for the service for an unduly long period. We acknowledge RECCo's initial view in favour of Hybrid Model B, however at this point we are not convinced that this proposal is a reasonable approach to funding the CCS. While we agree that accreditation and enforcement costs should be covered by the relevant individual users of the service, we also think that there must be an element of transaction cost included, and would welcome further assessment of how to structure a transaction charge in a hybrid model that does not lead to the duplicate charges referenced as a risk in the proposed Hybrid Model A. It is important that all organisations who use the CCS contribute to its funding. This means it is important that the costs of the CCS are structured in a manner that ensures ATP business models take account of all of the costs. This transaction cost could include not only costs for ongoing access to the CCS (and the accreditation and enforcement costs proposed in Hybrid Model B), but also a route to recovering the initial development costs, and ensure that consumers are not disproportionately exposed to the costs when a much broader group of organisations stand to benefit from using the service.	
Q26	Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.
We have no objection(s) to the CCS accreditation model.	

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.
We welcome the proposal that CCS users should be ISO 27001 accredited. However, the primary emphasis should be on ensuring that users maintain robust and appropriate security controls to safeguard the integrity of the CCS as well as the secure flow of data throughout the process.	
Q28	Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?
We offer no comments.	
Q29	Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?
We offer no comments.	
Q30	Do you have any comments on the proposed issue/dispute resolution paths defined for the management of CCS issues?

Our concerns are based off the following.

Queried Consent – where the consent record shows the consent was granted by the individual consumer

- We note the consultation suggests that where consent issues arise, the consumer should raise this with their ATPs through the mandated REC Operational contact list. However in reality, EDPs are most likely the first point of contact when consumers raise a complaint about their energy data. We are unclear on the extent of EDP liability in this scenario and the extent of RECCo's involvement being owner/manager of the CCS If EDPs receive these complaints, we recommend that the rules make it clear that they be forwarded to the ATPs for resolution, with clear guidance confirming that EDPs will not be held liable provided consent was properly validated on the CCS. Queried Consent – where the consent record shows the consent was not granted by the individual consumer

- The scenario described appears to address only circumstances in which consent is disputed within a multi-occupancy household, where consent was previously granted but the consumer subsequently moves property without revoking it, and issues arising from IDV mismatches. However, where the CCS malfunctions, and consent was

validated based on incorrect information held within the solution, EDPs should not be held liable. In such cases, responsibility should rest with the solution provider.

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?
We don't see the Sandbox Suite as being required for CCS core operation (consent creation, token issuance and introspection). Therefore, it could be safely moved to Phase 2 (Next Enhancement and Adoption) to accelerate the launch while preserving compliance, security and supplier interoperability.	

Additional Comments

Q32	Please provide details of any additional issues you feel have not been adequately captured within the consultation document.
We have no further comments.	

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