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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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	Paul Linnane
ORGANISATION	ElectraLink
ORGANISATION CATEGORY	[OrgCategory]
E-MAIL ADDRESS	Paul.linnane@electralink.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 with the proposed MMP scope, the associated core functional components, or the inclusion approach (SEC Other Users and the BSC SDR). We reflect on this position more in the relevant questions, but our key concerns are that: the MMP is too narrow to earn trust, inclusion of SEC Other Users (rather than the DCC as a primary route) creates a structural two-tier model, BSC SDR inclusion is not sufficient on its own and the omission of gas is a fundamental gap, and a centralised, effectively single IDV approach is a strategic mistake that will depress adoption.

The programme's original rationale as set out in Data Sharing in a Digital Future - Consumer Consent is explicit: a consumer consent solution should (1) improve consumer trust in data-sharing services, (2) improve access to personal data across the sector, and (3) develop a consent process or mechanism. The proposed MMP, as described, does not credibly deliver against these objectives and, in several respects, risks actively undermining them. The MMP is being treated a technology delivery program and deferring the difficult issues to future "undefined" phases. This will lead to a piece of work that is not fit for purpose on day one and will unlikely solve the bigger issues as time goes on.

MMP Scope: A consent service will only build trust if consumers can see it as complete, coherent, and improving rapidly. The current MMP scope is so limited that it is unlikely to demonstrate meaningful consumer value early, and the absence of firm, published time-bound delivery commitments for the roadmap creates a multi-year period of partial coverage. That combination is a direct trust risk: consumers will experience a "consent solution" that does not reflect the reality of

their data sharing, then conclude it is incomplete or performative.

Inclusion of SEC Other Users: Including SEC Other Users while not treating DCC as the primary baseline route creates a two-tier access model in practice: some actors participate via one governed path, while others remain outside or operate differently. A consumer-facing trust mechanism cannot be credible if it embeds structural unevenness at the foundation. This will be experienced as inconsistency and will directly erode confidence.

BSC SDR: The inclusion of the BSC SDR focuses on electricity. That is not "good enough" for a consumer trust proposition because consumers experience energy as a combined service. A consent solution that does not address gas in scope at the outset (or at minimum provide a clear, binding plan for how gas is handled) is incomplete by design. If the service launches with electricity but without a coherent approach to gas, the consumer proposition becomes fragmented and will not meet expectations of sector-wide access improvement.

A single IDV approach: We strongly disagree with positioning the CCS around a single, centrally governed IDV mechanism as the default. The consultation itself acknowledges that different data types warrant different levels of identity confidence, and that wider options may come later. In practice, the MMP risks hard-wiring one approach early and then attempting to retrofit plurality later — which is usually costly, slow, and politically difficult. The UK has already seen public sensitivity and backlash around centralised digital identity initiatives; forcing a single route here risks unnecessary friction, uneven consumer experience, and lower uptake. It also suppresses innovation by preventing services from selecting the most appropriate ID&V method for their product context and consumer segment.

The consent model: The consent model as described does not meet the standard of "informed consent". Ofgem's published position is clear: it must be obvious to consumers what they are consenting to, who receives the data, why it is needed, and for how long — not hidden in legalistic language or pushed to secondary pages. The approach described and the way it has been presented to stakeholders risks reducing consent to a formal step rather than a genuinely informed decision. Deferring critical terms and disclosures away from the primary consent step (e.g., to separate pages) is not consistent with a "transparent and informative" consent journey. Any model that results in consumers effectively consenting to "data sharing for all purposes" is not purpose-specific and therefore fails the informed consent standard in practice. It also creates foreseeable long-term trust failure once consumers realise data may be reused in ways they did not expect.

In summary, the proposed MMP is not aligned with the original policy intent and is not sufficient to build trust. It is too limited in scope, structurally uneven in access routes, incomplete across fuels, and paired with consent/ID&V choices that risk poor adoption and long-term distrust. If implemented as proposed, it is more likely to produce a low-value, confusing early experience that damages confidence than a credible foundation for a trusted, pro-innovation consent ecosystem.

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 agree that existing consents could be renewed using the CCS but note that it is an optional requirement for SEC Other Users, rather than a mandatory one. This could create an ongoing two tier system for users which we believe would not be appropriate, if the objective is for the consumer (and industry) to provide consent in one place.

Second, this assumption fails to recognise the significant historic investment made by a number of SEC Other Users. Many have already built, implemented, and operated consent mechanisms that meet SEC requirements, often at considerable cost and organisational effort. Forcing those parties to route renewals through the CCS, without a clear, mandatory and consistently applied migration approach, risks destroying value in existing platforms while offering no clear compensating benefit — particularly where alternative IDV options and comparable capabilities are not available through the CCS.

Third, from an operational and consumer-experience perspective, this creates unnecessary complexity. Organisations that have invested in compliant consent journeys will be required to support dual consent models for an extended period, leading to confusing engagement for consumers and increased delivery and support costs for service providers. This is particularly problematic given the current lack of clarity on CCS user journeys, technical integration patterns, service provider responsibilities, or operational service levels. In the absence of this detail, it is not possible to view the proposal as value-neutral; rather, it represents a net erosion of value for those organisations that have acted early and responsibly.

Finally, we are concerned that this approach implicitly penalises early movers — organisations that have pioneered fair, transparent energy data sharing in line with SEC guidance. Rather than recognising and building on that progress, the proposed assumption risks devaluing those investments while failing to establish a clear, equitable end-state for all participants.

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.

A more nuanced approach is required for household consent. The proposal to shift consent for half-hourly data to the occupier has not been adequately thought through in terms of how it interacts with existing industry processes and consumer journeys. Today, bill payers can legitimately grant consent to suppliers for access to half-hourly data to support new tariffs, flexibility services, and other propositions, and this model is well understood by both consumers and industry. The consultation does not explain how this current process will coexist with, transition to, or be reconciled against the new occupier-led consent model. As a result, the market is left with two parallel consent regimes operating for the same underlying data, depending on who is requesting it and through which route.

This creates a de facto two-tier system: suppliers can continue to rely on bill-payer consent for their propositions, while non-supplier parties must obtain consent from the occupier via the CCS. From a consumer perspective, this distinction is opaque and confusing. The same individual may be treated as the decision-maker in one journey and not in another, for the same data, at the same property. From an industry perspective, it undermines the stated aim of a single, trusted, coherent consent framework and introduces inconsistency in how consent validity is assessed and enforced and will mean that ID&V might be different depending on which party is accessing the data. Without a clear and mandatory alignment between the existing supplier consent model and the proposed CCS approach, the policy risks fragmenting consent rather than simplifying it, eroding trust and creating uncertainty over which consent is authoritative in practice.

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 with the use of a 'lead occupant' providing consent on behalf of other occupants. Currently, an energy bill payer can provide consent on behalf of other occupants (including discussing usage or switching). There are some known issues with this method already, including data protection and privacy risks, and the proposed approach should acknowledge the nuances needed. This is a very complex area and we would welcome more development on this in future consultations.

If the lead occupant is chosen for implementation, what evidence will they need to provide to show that they can vouch for all adults in a household?

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

We do not agree with the proposed approach or standard for Identity Verification (IDV) as set out in the Consumer Consent Solution. The current vision appears to hardwire a single, centralised IDV route into the CCS, with limited flexibility or support for alternative mechanisms. This is fundamentally at odds with the stated ambition to build a trusted, inclusive, and future-proof consent framework.

Consumers and service providers have diverse needs, risk profiles, and digital capabilities — a one-size-fits-all IDV model will not serve them equally. By failing to accommodate a competitive or modular IDV ecosystem, the proposal risks excluding legitimate users, increasing friction, and undermining adoption of the service. We note the future ambition to deliver this service but there are no mandated timeframes for this and a single IDV provider will have a significant competitive advantage when this comes to pass. If the MMP is to go ahead, there should be multiple IDV providers from the start to ensure that this service can be opened up quickly or risk losing the entire market.

The direction of travel of REC to pursue a "technology first" approach to the MMP for CCS and IDV is problematic. The IDV is symptomatic of a wider issue: the CCS is being designed as a closed, centrally controlled system, rather than an open, enabling platform. The lack of support for multiple IDV providers, federated identity models, or market-led innovation reflects a broader unwillingness to trust the ecosystem. This is inconsistent with the principles of the Energy Digitalisation Taskforce and the Data Sharing in a Digital Future vision, both of which emphasised openness, interoperability, and consumer empowerment. Without a fundamental rethink of the IDV approach, the CCS risks becoming a bottleneck rather than an enabler and will struggle to deliver the trust, adoption and innovation it was intended to support.

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.

Yes, we agree with the guest approach.

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 agree that consumers should have the option to revoke or renew consent, however the consultation does not provide sufficient detail on how this will be monitored in practice or how feedback loops will be established to ensure that revocations are respected and acted upon promptly. Without clear governance, auditability, and enforcement mechanisms, there is a risk that

revocation becomes a theoretical right rather than a reliable safeguard. We are worried that like the rest of this solution this will be technically delivered but not enforced or maintained in practice.	
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.
Yes, we agree with the position outlined, However once again it is not clear how this will be enforced on DCC other users. It would need to binding obligations to ensure the success of the solution and without binding obligations on EDPs to implement it, the risk is that this becomes a loosely interpreted principle rather than a hard requirement. If EDPs are left to interpret or implement this differently, it could lead to inconsistent practices, data being shared without valid consent, and ultimately a loss of consumer trust. The CCS must not only mandate this check but also provide the technical infrastructure, audit trails, and compliance oversight to ensure it happens reliably and uniformly across the ecosystem. This again raises the question on why it is being not being hard coded directly into DCC rather than DCC other users.	
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.
As per the drafting, if the CCS is unavailable, an EDP should only be able to share data with ATPs that it has shared with before (and where the token has not expired or been revoked). We understand that REC is proposing an availability requirement of 99.9% so we would not expect this scenario to occur frequently.	
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.
The decision to require FAPI 2.0 and mTLS sets a much higher technical bar for accessing half-hourly consumption data which seems counter intuitive. ElectraLink is comfortable meeting this standard but it may make it harder for smaller or newer organisations to take part. That matters because the CCS will only deliver value if it enables a wide range of new services to emerge. If the technical requirements are too heavy, innovation could be limited to larger, well-resourced players, weakening the overall benefits case. We have seen this with the difficulty of getting access to SEC data through DCC adaptor which has been expensive to integrate with and develop for limiting cost effective data sharing in the market. If this approach is to be continued, REC will need to provide strong and ongoing support, not just technical standards on paper. This means practical help with onboarding, testing environments,	

tools, and day-to-day problem solving. While funding may be available for this, it will land on the consumer ultimately and recent experience raises concerns. Industry services such as EES and GES have not always been easy to implement, and the REC-led Carbon Service has been delayed significantly. The increased cost may not be justified if viewed through this lens. The consultation does not yet explain how REC will avoid similar issues with the CCS, or how it will ensure that high technical ambition does not slow down adoption. If innovation struggles to get going, the core purpose of the CCS is put at risk and the risk and cost falls on the consumer with no value.

The consultation also focuses heavily on securing the point at which data is shared, but much less on what happens after the data has been received. FAPI 2.0 and mTLS are effective at preventing unauthorised access, but they do not address risks such as how data is used, stored, shared onwards, or monitored once it leaves the CCS. Many of the biggest consumer trust risks sit in this later stage, yet these are not fully addressed. This gives the impression that the consultation is trying to build trust mainly through technical controls, rather than treating trust as something that depends on the whole service — including governance, oversight, enforcement, and clear protections for consumers once their data is in use.

Furthermore, this surfaces a separate issue about commercial contracts which RECco has not addressed. Market participants currently access energy data via commercial arrangements and some of these participants will not currently use mTLS. Mandating mTLS for already existing and contracted bilateral data exchanges will either exclude those organisations or provide cost implications for updating their systems, which will not reduce barriers to entry. We also note that the RECco solution assumes that all the heavy lifting is done by the consent token and not commercial contracts, which are far more enforceable than the ICO.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
We consider that the proposed solution architecture does not fully align with the consultation's outcome for the CCS to adopt a hybrid approach. In particular, the current approach introduces unnecessary complexity and centrality, and the level of ID&V specified appears disproportionate to the needs of the service. At this stage, several elements of the architecture require further detail before we can offer a definitive view. Our general observation is that the core concepts are reasonable, but the "devil is in the detail", and the documentation provided remains too high-level to assess operability and proportionality with confidence.	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
We do not agree that using the REC Enquiry Service (EES) for address matching is the appropriate approach. There is a straightforward way to illustrate why this presents a challenge. RECco themselves on the EES website portal state: "The address registered to your MPAN or MPRN. This may be different to the address your supplier puts on your bills". This acknowledgement highlights an inherent limitation of EES. Where a supplier's billing or postal address does not align with the registered address, it is difficult to see how a solution that relies on identity verification (IDV)—potentially requiring photographic evidence to meet the proposed standard—can operate effectively using a strict binary address match. An approach that relies on exact matching is likely to result in a high rate of failed matches, particularly for flats, new builds, and other complex address types. In practical terms, this means that many consumers who should legitimately be able to link to their meter via the CCS may instead be presented with a "no match found" outcome due to relatively minor address discrepancies. This risks frustrating users and undermining trust in the system from the outset. More concerningly, where auto-matching is attempted, there is a risk that the wrong meter could be selected—for example, a neighbouring flat's MPAN—leading to erroneous consent scenarios. This would mirror the erroneous transfer issues that have historically affected the switching process, but with significantly more serious consequences, as personal data could be shared inappropriately, resulting in an immediate breach of GDPR. Ofgem has previously highlighted that erroneous transfer (ET) rates were unacceptably high, often driven by suppliers selecting incorrect meter points due to address confusion. Industry analysis has consistently shown that ambiguous or inconsistent address data is a primary cause of mistaken meter selections. Against this backdrop, a purely binary address-matching	

approach appears particularly ill-suited.

Flats and multi-occupancy buildings are a well-established pain point. Research by Citizens Advice has shown that these property types are disproportionately represented in ET cases due to address details being mixed up within the same building. More broadly, the energy industry's core datasets are known to have limitations in address quality. A recent ElectraLink data quality initiative found that missing flat numbers and other address gaps resulted in an initial match rate of only around 85% between gas and electricity addresses, even after applying advanced matching techniques. This meant that approximately 15% of records could not be matched on first pass due to address misalignment. In some instances, large numbers of meters at a single site were associated with a single generic building address or UPRN, obscuring individual units. These findings underline that a simple exact-match approach will not be sufficiently robust.

While the consultation recognises these issues and suggests the use of the Retail Energy Location (REL) address where available, this is not guaranteed for MMP delivery. In such cases, the fallback is to existing Meter Point Location data, which is widely understood to be of lower quality. The consultation does not set out clear mitigations for handling mismatches, ambiguity, or failure scenarios, despite these concerns having been raised repeatedly through workshops and engagement sessions.

We therefore believe that a more resilient approach is required—one that supports fuzzy matching, makes use of UPRNs where available, enables consumer confirmation where multiple potential matches exist, and includes clear exception handling where an automatic match cannot be made. Without these measures, there is a real risk that the CCS will drive workarounds outside the platform, undermining its objectives and eroding the consumer trust it is intended to build. We would also reiterate that these concerns have been consistently raised in CCS workshops with REC, yet we have not seen a corresponding change in approach or a clear explanation addressing these issues.

Q13	Do you have any comments on the non-functional requirements detailed within Annex D?

The requirements listed seem appropriate to monitor. It would have been useful to have the measures or targets labelled against each non-functional requirement, or a reference to if this information is held elsewhere in the consultation pack, in order to assess their suitability as right now if the measures and targets are too low, then these are next to worthless. Further detail is required on this section for us to comment – this seems like a tick-box exercise.

Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?
We agree with a hybrid model, but do not agree with centralised IDV. Existing IDV solutions should be utilised and a standard should be set for IDV that commercial parties can meet and adopt, so that an IDV solution can be built or bought (eg: by an Energy Switching service). If this was enabled for day one, it would encourage more consumer engagement with the platform. We do agree with a centralised consent ledger but again, the consultation is too vague at this stage and any agreement should be considered as "subject to more detail".	
Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
We do not believe the diagrams are sufficient as they only provide the happy path. Given that this is a new process and many things will need to change, the diagrams should address this issue.	

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 appreciate the need to develop archetypes, though note it does not include an 'average Joe'. For example, a consumer that would engage with the platform to switch, maybe once a year, which we anticipate would be a large percentage of users.	
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?
We agree that the defined areas for vulnerability are covered. We are interested to learn what the offline journey will look like and when this will be developed.	
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?
The current CCS consultation proposes a baseline where the consent interface will identify the requesting organisation, the category of data to be shared, and the duration of access (including an expiry). However, we believe the proposal must also explicitly include a clear statement of purpose ("why") in the consumer consent journey – not buried in terms and conditions but presented upfront in plain language. This was a core principle in the original design papers and Ofgem's 2024 consultation: "It should be clear to consumers what they are giving consent for and to whom – explained upfront and not hidden in legalistic language or fine print." In practice, that means each consent request should transparently answer who wants the data, what data they want, for what purpose, and for how long – all in a concise, digestible format. The consultation's own UX principles echo this, stating that when granting consent consumers should be able to "identify who is requesting access to their data, what will be shared, why, and for how long." We fully support this standard. Any deviation – for example, omitting the "why" or the specific purpose – would undermine the very notion of informed consent and conflict with GDPR guidance that consent must be "specific" (tied to a defined purpose) and "informed" (the individual understands exactly what they are agreeing to). The original Ofgem vision and Energy Data Taskforce recommendations stressed strong transparency and "purpose limitation": consent must be tied to a clear use case and consumers should always know "how and why their data will be used". Early workshops and papers envisioned "clear, unambiguous terms about how and why data is being used at all	

times." In line with GDPR, consent was not just a box-ticking exercise. However the demonstration given at the Engagement Day showed T&C tickboxes and the statements made by REC employees that "data can be used for anything once the consumer has consented" show that there is a significant deviation from this which undermines trust.

Whilst 7.17 of the consultation highlights "why" as a function this needs to remain because Annex F states that the research will get consent clarity on "What information the CCS must present, how it should be structured, and where clarity is essential to ensure consumers understand what they are agreeing to". On its own it could be read as the Why/Purpose is important but combined with RECs demonstration and comments from teams, it could be read as optional. Treating it as such opens the door to data being reused or reclassified years later in ways the consumer never agreed to, fundamentally undermining trust.

There is no inherent risk of overload if information is presented clearly and concisely and other sectors (e.g. open banking) prove this works at scale. If the CCS reduces consent to identity verification and vague data sharing, it adds friction without value. The value of the CCS lies in transparent, meaningful consent — if that is diluted, half hourly data will be widely reused without genuine permission, destroying consumer trust in the long term.

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)

If done well, we do not believe additional verification steps are needed.

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 that showing consumers which organisations hold consent, what data is shared, when consent was granted, and when it expires and for what purpose (which seems to be missing) should be the minimum standard for visibility. However, on its own this view is incomplete and risks giving consumers a false sense of control. In particular, the current approach does not adequately address situations where data access involves intermediaries or onward sharing, nor does it consistently explain why each organisation has access to the data. Without this context, consumers may see unfamiliar organisations listed as holding consent, with no clear understanding of how they relate to the service they agreed to or what role they play.

There is a clear lack of clear visibility over data access chains. Where a Third Party is acting on behalf of another organisation, or where data is passed through multiple parties, consumers

should be able to see how those organisations are linked, who the primary service provider is, and why each party's access is necessary. Simply listing individual organisations that "hold consent" does not explain responsibility, accountability, or relevance. This is particularly important given that the CCS explicitly defines a boundary after which REC oversight ends; without showing these relationships, consumers cannot reasonably understand where their data goes next or who is ultimately responsible for its use.

We also must be honest and explicit about the limitations of the consent model, especially around onward use and reuse of data where REC are leaving enforcement to the ICO. Ultimately this is a tick box exercise without stronger governance and controls (which go far beyond the onboarding process). There are no protections once data leaves the CCS boundary and as it stands data can be reused for different purposes without renewed consent. Failing to address this leaves CCS as a record-keeping or identity-verification tool rather than a meaningful consent mechanism. If consumers cannot see who has their data, why they have it, and who they gave it to trust will erode quickly, particularly if data is later used in ways the consumer did not expect or understand.

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 have the right to this information. However, we do not believe revocation should be reversible. If a consumer revokes their consent and in the future wishes to grant consent, then the same original steps should be followed for granting access.

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?

We agree that assisted journeys must deliver the same outcomes 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?

The same outcomes should be available to consumers who do not use digital services. These methods are particularly important for elderly, low-income, or those with accessibility needs who may not have access to or proficiency in digital technology. We would encourage the UX Design to engage with industry stakeholders who already deal with this issue (via paper-based communications, phone calls, use of community hubs etc) and consider lessons learned from the Vulnerability/PSR space.

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 have no overarching concerns with the proposed drafting structure; however, we are unable to comment substantively on the API Technical Specification at this stage due to the limited detail available.	
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 are comfortable with the initial funding model.	
Q26	Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.
We agree that the areas outlined for inclusion in the Accreditation journey (user agreements, information security, testing and data protection) are key foundations for the model. We note the assumption that 'SEC privacy assessments will reduce in scope with the focus being organisations who are not utilising the CCS for all of their consent validation'. We are interested in the development of this area, as REC and SEC should be aiming to minimise duplication of arrangements where possible. We further note that all users would be subject to a full REC data protection assessment, regardless of assessments under other codes, and if this is the case, then it will cause duplication of effort across all industry parties who have already been subject to these assessments. While we support the robust process due to the sensitivity of the data, we hope that REC has aligned their CCS assessment to those already used where possible, to reduce the administrative burden on parties.	
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 believe that all CCS users should have both Cyber Essentials Plus and ISO 27001. We believe this standard should be higher but agree that this will need to be managed by the onboarding.	
Q28	Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?

We believe this will be sufficient and would encourage REC to start providing regular updates at the Change Issues Group as the CCS continues to develop (pre-implementation).	
Q29	Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?
No comments	
Q30	Do you have any comments on the proposed issue/dispute resolution paths defined for the management of CCS issues?
We are concerned that the proposed issue and dispute resolution paths focus too narrowly on administrative or oversight errors, and do not address the more serious risk of organisations deliberately misusing consumer data. Based on ElectraLink's experience, the most significant problems in data sharing environments often stem from actors accessing or using data beyond the scope of consent. The consultation does not explain how such misuse would be detected, investigated, or stopped, nor does it clarify what powers RECCo would have to suspend or remove parties who breach the rules. This creates a serious governance gap. If consumers must escalate to the ICO to resolve misuse, and RECCo has little role in enforcement, then the CCS risks becoming a passive registry rather than a meaningful trust framework. While the REC PAF is mentioned, there is no clear pathway for identifying, tracking, or resolving misuse cases, and no visibility over whether issues are being addressed. Without a robust, transparent process for handling misuse — not just system errors — the CCS cannot deliver on its promise of protecting consumer data or maintaining trust. More broadly, we are concerned that the CCS is drifting away from Ofgem's original vision. The current design appears to focus heavily on technical identity verification and token issuance — essentially a secure login and consent timestamping service — rather than delivering a full consent framework that empowers consumers and governs how their data is used. Ofgem's original requirements emphasised specific, informed, purpose-limited consent, with strong governance and consumer protection at its core. That included not just who has access, but why, for what purpose, and with what safeguards. The current model risks reducing consent to a technical handshake, with little oversight of what happens to the data once it leaves the CCS boundary and little enforcement or tracking if it goes wrong. If RECCo's role ends at the point of token issuance and the process has to wait for enough	

consumers to work through the long ICO process (rather than removing bad actors), then the system cannot credibly claim to protect consumers. Worse, it may give the illusion of control while leaving consumers exposed to misuse or overreach. We urge RECCo to revisit the governance model and ensure that the CCS includes clear, enforceable mechanisms for addressing misuse, not just technical faults — and that it remains aligned with the original policy intent of building a trusted, consumer-centric data sharing framework.

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 assume that the roadmap will be a living, strategy document and can evolve with the industry. As it currently stands, it lacks clear timeframes, sequencing, or prioritisation and offers little confidence that the CCS will evolve in a structured or timely way.

Without defined milestones or delivery commitments, the roadmap cannot be relied upon — it simply highlights how little is currently being delivered and how long it may actually take to realise the full vision.

Given the scale of ambition and the number of unresolved design issues, we believe a pause may be more appropriate. This would allow time to properly align stakeholders, clarify the product scope and develop a more realistic and accountable roadmap. Rushing to implement a partial solution without a clear path forward risks undermining trust and delaying the benefits the CCS is intended to deliver.

Additional Comments

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

The consumer consent solution is meant to give customers control over who can access their energy data and how it's used, by actively managing their consent and helping them make informed choices. The design is also meant to support a more competitive and innovative retail energy market by reducing barriers for trusted third-parties and delivering better consumer outcomes. We do not believe that the MMP solution will deliver this, especially the trust element.

The development of the MMP was supposed to be shaped with industry participants, via the Working Groups, which were designed for REC to have access to people who have experience dealing with issues like consent, data sharing and governance controls. While the Working Groups have provided a discussion space for members, there has been little transparency on the outcome of industry feedback. Working Group suggestions that deviate from the REC desired route have been overlooked and it would be beneficial for REC to share the suggestions

proposed by industry Subject Matter Experts, and the rationale for why specific routes have been chosen in the CCS design.

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