

A vertical blue bar on the left side of the page.

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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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 Saker
ORGANISATION	EDF
ORGANISATION CATEGORY	Energy Supplier
E-MAIL ADDRESS	paul.saker@edfenergy.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?
<p>No.</p> <p>As noted in our responses to Ofgem’s policy consultations on this subject, EDF disagrees with the introduction of a centralised Consumer Consent Solution (CCS). The case for intervention has still not been made; there is no clear risk of consumer detriment, or evidence that industry parties will not deliver the right outcomes for consumers in the absence of a single, centralised solution, delivered by RECCo. The benefits of the CCS remain speculative at best and are unlikely to be delivered for many years, if at all. However, the costs to suppliers the CCS are very real, and will ultimately be paid by consumers through their bills from this year.</p> <p>At a time when Government is looking for opportunities to reduce energy bills, the costs of implementing the CCS are difficult to justify, especially when there are other initiatives more directly beneficial to consumers that this funding could be used for instead. Examples include the creation of a central Priority Services database using Government health and benefits data that enables vulnerable consumers to be identified and managed appropriately, for example when mode switching smart meters.</p> <p>Where there is a need for consent processes to improve, the commercial pressures of the energy market and the need to engage consumers in new products and services will drive parties to innovate to meet those consumer needs. We already see this in the market with products such as the n3rgy portal created by Smart Metering Systems. The focus should be on encouraging the market to develop innovative solutions that meet a clear consumer need, rather than imposing a single, centralised solution on industry where the purpose and business case are all unclear.</p> <p>Given the uncertainty around the benefits and future use of the CCS, we are concerned that the approach being taken to implement the Minimum Marketable Product (MMP) by RECCo is overly complicated, with a high risk of regret spend.</p>	

We would expect this initial phase to be a low-cost proof of concept that might justify further investment in a more fully developed solution – instead the proposed design of the MMP appears to be unnecessarily ‘gold plated’ and complex. It is not clear that consumers or organisations in the energy sector will want to use it, and certainly not as a mass-market product, especially where there are already existing routes to obtain half hourly consumption data via the DCC which consumers can already grant access to safely and securely. As detailed in our response to Q2, we do not see how the CCS can be used as a tool to manage consent to access data from smart meters via the DCC. Therefore. The CCS risks becoming a stranded asset, paid for by consumers, and used by no one.

As well as the functionality of the CCS, we have concerns about the legal framework that surrounds the CCS and the sharing of data between organisations. The consultation focusses on the necessity of consumer consent for data to be shared; it does not consider which other parties, such as energy suppliers, also need to provide consent for data they have an interest in to be shared.

In the context of the Smart Data Repository (SDR), which is the main use case for the MMP, we require clarity on the legal basis under which Elexon is sharing half hourly consumption data with third parties; especially given that energy suppliers are the data controllers for that data. Suppliers are required under the supply licence to notify the customer of the purpose for obtaining half hourly consumption data i.e. for settlements and forecasting purposes only. This is the data that Elexon will receive from suppliers via MHHS arrangements, and which Elexon are now proposing to make available via the SDR to parties for use for reasons other than settlements or forecasting. We question whether this is legally permissible and require Elexon and Ofgem to urgently consult with the ICO on this matter and demonstrate to us that they are satisfied this is lawful processing.

Furthermore, the underlying assumption is that this is personal data owned by the consumer, however this is also data that suppliers have paid to collect, from meters that they have paid to have installed, based on tariffs they have offered to consumers. This data is also the intellectual property of energy suppliers, however at no point is consent being sought from suppliers for the sharing of this data.

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?

Yes.

We understand that SEC Other Users have already developed robust mechanisms for managing consumer consent to meet their obligations under the SEC so that investment will have been wasted if they are required to migrate existing consent to the CCS. It is not clear that requiring these organisations to migrate this consent management to the CCS, and the associated cost, is in the interests of consumers.

More fundamentally, the CCS does not seem to be fit for purpose for managing access to HH metered data via the DCC, given the proposed technical design. On that basis it is not clear whether migrating existing consents would be possible, let alone desirable or beneficial.

It is not clear how the proposed technical solution for the CCS and the use of tokens would work where any organisation (SEC Other Users in the short term or potentially energy suppliers in the future) is requesting data from smart meters via the DCC.

It is worth noting that the DCC system is not a data holder – it is an access broker that controls access to the data held on smart meters. DCC Users access data on smart meters by submitting Service Requests (SRs) to the DCC when they wish to obtain that data. It is not clear from the detail provided in the consultation whether it is expected that each SR

submitted to the DCC will need to include within it a CCS token that the DCC will need to verify with the CCS. If that is the case, that would require complex changes to the DCC User Interface that are likely to be very costly and will take months (or more likely years) to deliver – however there is no reference to DCC changes within the consultation.

As well as submitting ‘on demand’ SRs, DCC Users can use a single SR to set up a data retrieval schedule within the DCC – for example they might request the HH data be obtained from the meter on a daily basis. Again it is not clear from the consultation whether it is expected that only the original SR to set up the schedule will include a CCS token, and that the DCC will need to check that token every time it issues a request to the meter in line with the schedule requested by the DCC User. It is also not clear how a DCC User would refresh that token when it is due to expire, and whether they would need to set up a whole new schedule every time token expires, which is unnecessary and burdensome.

Additionally, SRs sent to the DCC do not include the MPxN that the data is being requested for – instead the SR contains the GUID/Device ID of the meter that the data is being requested for. It is not clear how the DCC will be able to check that consent has been granted when it uses GUID and the CCS is based on the MPxN.

It is also not clear how the DCC will be able to determine which SRs it receives from a DCC User need to include a CCS token verifying that consent has been granted. Not only does the DCC not know which MPxNs are associated with domestic premises (which is the current scope of the CCS) and so might require consumer consent, not all requests for HH data that are submitted to the DCC require consumer consent. For example, suppliers are able to obtain HH data without consumer consent for a number of purposes under their supply licences – for example the investigation of potential theft.

The consultation also notes that suppliers will have ‘obtained consent for accessing half-hourly metering data for the purposes of billing and settlement, in accordance with Supply Licence Condition (SLC) 47’ – it should be noted that accessing HH data for settlement purposes does not require explicit consumer consent for domestic consumers – instead consent is on an ‘opt out’ basis. The CCS design is based around obtaining explicit consent from consumers who would access the CCS to grant that consent – it is not clear how ‘opt out’ consent to access HH data for settlement purposes would be managed in the CCS.

Overall, we have significant and material concerns about how the CCS could be used to grant consent to access data via the DCC – until clarity is provided on how this would work it would not be appropriate to require any DCC Users to use the CCS to manage consumer consent.

REC Policy Positions

<p>Q3</p>	<p>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.</p>
<p>No.</p> <p>As noted in our response to Q1, consent can only be provided both by the data subject and by the owner of the data, and who those parties are could vary from scenario to scenario. The approach being proposed for the MMP doesn't seem to cater for this, which is why we have concerns about the approach that's being proposed.</p> <p>Consumption data is regarded as personal data by the ICO, and GDPR mandates that only the data subject can provide consent. In the case of an energy account, this is the bill payer only and not anyone else, even though they may reside at the premises. The proposed solution does not work for energy.</p>	
<p>Q4</p>	<p>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.</p>
<p>No.</p> <p>This is not what data privacy law currently requires, which is one of the reasons why the proposed solution is simply unworkable.</p> <p>Additionally, we do not understand how it will be expected that anybody would be able to validate that a lead occupant has obtained agreement from all other adult occupants. As an energy supplier we often struggle to ascertain who the owner or occupant is on the premises, let alone for multi-occupancy households.</p> <p>On that basis the proposals on obtaining consents from the relevant party are unrealistic, unworkable and unlawful.</p>	
<p>Q5</p>	<p>Do you agree with the proposed approach and standard for identity verification? <i>If not, please provide your rationale.</i></p>
<p>No.</p> <p>A full identification process using photo ID for any data consents is unnecessarily complex, and frankly way beyond what the situation calls for, for the type of data in the scope of the MMP. This requirement may put people off from using the solution and may itself represent a barrier to data sharing, undermining the purpose of the CCS.</p> <p>Overall, the stance on data privacy for the MMP seems to be disproportionate to the risk posed by misuse of HH consumption data. While we recognise that it is deemed to be personal data (as advised by the ICO), is not sensitive personal data; any policies/technical solutions need to be proportionate to the risks posed to individuals and the risk to overall consumer trust.</p> <p>It is also unclear how this approach meets the principle of ensuring this capability is accessible to all (so those without driving licences or passports) and also those without access to digital technology.</p>	

<p>Q6</p>	<p>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.</p>
<p>Customers should not be required to create yet another online account, with a password to remember, and the unnecessarily onerous level of IDV proposed. This is a barrier that will deter consumers from using it.</p>	
<p>Q7</p>	<p>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.</p>
<p>Yes.</p> <p>In line with GDPR, we agree that consumers should be able to revoke or renew consent directly with the ATP. This would appear to make the CCS completely redundant as consumers can do this already.</p>	
<p>Q8</p>	<p>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.</p>
<p>No.</p> <p>The expectation that consent is checked each time data is shared imposes significant scalability and latency considerations on the CCS platform, if it is to be used at the scale intended. The design and proposal seem to focus on individual consumer requests. It is not clear how consents for a batch of consumers would be facilitated; for example, if a collection of consumers chooses, or are constrained by, shared energy infrastructure (local area micro generation consortia, shared development boilers, etc).</p>	
<p>Q9</p>	<p>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.</p>
<p>No.</p> <p>We prefer a model where each ATP holds local consent data which is periodically refreshed, the CCS acts as the master for this data with ATP synchronisation mechanisms, and consumer consent is provided locally (if required in an CCS outage). This would build resilience into the overall system and reduce the high availability requirements the CCS would need to meet.</p>	
<p>Q10</p>	<p>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.</p>
<p>No.</p> <p>The design could be simplified and the same outcomes achieved with strong signing and TLS 1.3 for all but the CCS to EDP integration, which is the highest risk.</p>	

Regardless of the use of FAPI 2.0 and mTLS, the methods used to secure the service should be consistent across all industry data sharing initiatives (e.g. CCS and NESO Data Sharing Infrastructure) as diversity will lead to unnecessary complexity and further cost.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
<p>Yes.</p> <p>The proposal includes duplicated capabilities (data catalogue and data provider, security mechanism for data sharing, point to point data sharing, shared data standardisation) that will also be available in the NESO Data Sharing Infrastructure. The CCS appears to be duplicating capability and therefore cost. At a minimum, these duplicate capabilities should align technologically, or we risk asking participants to build and use differing methods for the same ends.</p> <p>The architecture ATPs build, and that the CCS has internally, will require more than simple request response APIs. A queueing mechanism will be required by both parties to ensure data is not lost in the event of an outage of either party, particularly to ensure the integrity of consent change data passed in messages between them.</p>	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
<p>Yes.</p> <p>Given the significant investment that has been made in creating the Retail Energy Location (REL) Address and the significant ongoing cost that suppliers incur in relation to DCC activities relating to address management, it seems sensible to leverage that investment wherever possible. If the REL is only ever used for switching, that would appear to be a wasted opportunity, as well as a waste of consumer's money.</p>	
Q13	Do you have any comments on the non-functional requirements detailed within Annex D?
<p>No.</p>	
Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?
<p>Yes.</p> <p>As noted in our response to Q9, we prefer a model where each ATP holds local consent data which is periodically refreshed, the CCS acts as the master for this data with ATP synchronisation mechanisms, and consumer consent is provided locally (if required in an CCS outage). This would build resilience into the overall system and reduce the high availability requirements the CCS would need to meet.</p>	

Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
No.	

UX Design

<p>Q16</p>	<p>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.</p>
<p>Given the number of consents customers are asked to provide and manage on a day to day basis (for example, all the accidental “subscribe” emails we receive and have to unsubscribe from), and the number of passwords they have to remember, it is unclear that any archetype – maybe beyond the “data enthusiast” – would actively seek to engage with the CCS.</p>	
<p>Q17</p>	<p>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?</p>
<p>Yes.</p> <p>However, we are concerned that the design of the CCS is being ‘gold plated’ while it remains uncertain that the system will be used by any consumers, let alone vulnerable or digitally disadvantaged consumers. While any solution must be as inclusive as possible, the cost of that must be minimised as far as possible as it will ultimately be borne by those vulnerable consumers through their bills.</p>	
<p>Q18</p>	<p>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?</p>
<p>If existing consent mechanisms are used i.e. the consumer directly interacts with the party that they wish to share data with, there are already requirements for that party to make it clear what data they require and for how long. The CCS is simply adding another unnecessary layer into the customer experience of sharing data.</p>	
<p>Q19</p>	<p>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)</p>
<p>It is unlikely that consumers will want to engage with the CCS in the first place. Introducing additional verification steps and friction is likely to further reduce the likelihood that consumers will engage with it, and increase the risk that the money being invested in the CCS will be wasted.</p>	
<p>Q20</p>	<p>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?</p>
<p>Consent is only one of the legal grounds for processing data; all of the other grounds and the parties that rely on those grounds to process data will remain completely opaque to the customer. Consumers will already know which organisations they have provided their consent to and what data they have permitted those organisations to access.</p>	

Therefore, the CCS is not necessary or useful and only gives the customer a small piece of the data sharing landscape, but at a high cost.

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.

As noted previously, it is unlikely that consumers will want to engage with the CCS in the first place. Introducing additional complexity and overloading the consumer with information is likely to further reduce the likelihood that consumers will engage with it, and increase the risk that the money being invested in the CCS will be wasted.

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.

All consumers should be able to achieve the same outcomes, irrespective of whether they are digital users or not. The CCS is ultimately being funded by all consumers; excluding any of those consumers from the scope of the CCS would not be fair.

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?

As noted in the response to Q22, all consumers should be able to achieve the same outcomes, irrespective of whether they are digital users or not. The CCS is ultimately being funded by all consumers; excluding any of those consumers from the scope of the CCS would not be fair.

Governance Design

<p>Q24</p>	<p>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?</p>
<p>Yes.</p> <p>As noted previously, we disagree that the CCS is needed at all, and therefore that any changes should be made to the REC. RECCo appears to be seriously ‘gold plating’ the requirements, and should urgently reconsider what a Minimum Marketable Product actually means.</p> <p>Furthermore, we strongly disagree with the proposal to include Customer Experience Guidelines within the REC and to mandate that organisations follow these. The proposed approach is unnecessarily prescriptive and not aligned with the overall direction towards outcome-based regulation. We support a clear, outcome-based regulatory approach to regulation that empowers organisations to achieve defined consumer outcomes without being constrained by rigid, process-heavy requirements.</p>	
<p>Q25</p>	<p>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.</p>
<p>No.</p> <p>We don’t agree that funding for the CCS should come from suppliers, as these costs will ultimately be recovered from all customers (including those that don’t or can’t use the CCS) through their bills. At a time when Government is looking for opportunities to reduce energy bills, the costs of implementing the CCS are difficult to justify, especially when there are other initiatives more directly beneficial to consumers that this funding could be used for instead.</p> <p>The assumption appears to be that suppliers will fund the development of the CCS, with the potential for some of that up-front investment to be recovered from future users of the consent solution, should any emerge. In our view the future use of the CCS by third parties is highly uncertain and given that suppliers already have consent management solutions in place it is unlikely they will choose to use the CCS unless forced to.</p> <p>RECCo appears creating something which serves its wider commercial purposes in the future, but which is being funded by suppliers via consumers’ bills; however, neither suppliers nor consumers are likely to benefit from the CCS. The main original use case no longer exists as Ofgem and RECCo have postponed the supplier consent aspects – which may never be able to be incorporated into the CCS. Until Ofgem or RECCo can demonstrate an actual customer need for the CCS, or that data can’t be shared without it, it should not go ahead.</p>	
<p>Q26</p>	<p>Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.</p>
<p>Yes.</p>	

We agree with the proposed accreditation model. Utilising the existing risk-based qualification process for Non-Party REC Service Users is sufficient and reduces unnecessary duplication.

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.

Yes.

We agree that the minimum requirement of Cyber Essentials Plus or ISO 27001 is acceptable. Where organisations already hold relevant certification/accreditation the REC accreditation process should be able to rely on that existing certification. Organisations that are already accredited under the REC in other roles (such as energy suppliers), or who meet similar requirements under other codes such as the SEC, should be able to rely on that existing accreditation, to avoid unnecessary duplication and cost.

It would be useful to understand whether the scope of these certifications will be reviewed. In addition, we would expect transition periods or guidance for smaller organisations should be included to support organisations in meeting these requirements.

Q28 Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?

Yes.

To minimise the cost and impact of the CCS, existing REC governance arrangements should be used wherever possible.

Q29 Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?

Yes.

To minimise the cost and impact of the CCS, existing REC governance arrangements should be used wherever possible.

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

Yes.

The proposed escalation and dispute resolution pathways are sensible. The ability to escalate issues to the PAB or Ofgem, and to terminate Access Agreements where necessary, provides clear accountability.

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?
<p>Yes.</p> <p>In our view the future use cases are speculative at best, with uncertainty about whether many of those schemes will proceed, and even if they do, whether the CCS would be a necessary or appropriate mechanism for managing any consent that might be required.</p> <p>Therefore, RECCo must stop building this with consumers' money, until such time that an actual need for this system can be demonstrated.</p>	

Additional Comments

Q32	Please provide details of any additional issues you feel have not been adequately captured within the consultation document.
<p>As noted in our response to Q1, we have concerns about the legal framework that surrounds the CCS and the sharing of data between organisations. The consultation focusses on the necessity of consumer consent for data to be shared; it does not consider which other parties, such as energy suppliers, also need to provide consent for data they have an interest in to be shared.</p> <p>In the context of the Smart Data Repository (SDR), which is the main use case for the MMP, we require clarity on the legal basis under which Elexon is sharing half hourly consumption data with third parties; especially given that energy suppliers are the data controllers for that data. Suppliers are required under the supply licence to notify the customer of the purpose for obtaining half hourly consumption data i.e. for settlements and forecasting purposes only. This is the data that Elexon will receive from suppliers via MHHS arrangements, and which Elexon are now proposing to make available via the SDR to parties for use for reasons other than settlements or forecasting. We question whether this is legally permissible and require Elexon and Ofgem to urgently consult with the ICO on this matter and demonstrate to us that they are satisfied this is lawful processing.</p> <p>Furthermore, the underlying assumption is that this is personal data owned by the consumer, however this is also data that suppliers have paid to collect, from meters that they have paid to have installed, based on tariffs they have offered to consumers. This data is also the intellectual property of energy suppliers, however at no point is consent being sought from suppliers for the sharing of this data.</p> <p>While the legality of data sharing via the SDR is a matter for Elexon and Ofgem to urgently consider, the underlying issues have a material impact on the viability of the CCS. The CCS roadmap suggests that it could in the future be used to manage consent related to schemes such as the Data Sharing Infrastructure (DSI), the Flexibility Market Asset Register (FMAR), and potentially an Energy Smart Data Scheme should DESNZ decide to proceed with its proposals. It is, however, unclear whether these schemes will proceed, and specifically whether there is a legal basis for data to be shared under</p>	

these schemes where it is owned by suppliers, network operators, flexibility service providers and other third parties.

Without clarity on the legal basis for those future developments of the CCS there is a material risk that it becomes a costly 'white elephant', with complex and over-engineered functionality developed to support use cases that don't materialise or which are subject to legal issues. The energy industry has been here before with scheme like midata that resulted in a lot of cost to develop technical solutions, but very little benefit as they were rarely used. We are in real danger of recreating the same issues with the CCS and wasting consumers' money.

Given these material concerns regarding the viability of the CCS, we recommend that further development of a centralised Consumer Consent Solution should be immediately halted by RECCo until these critical matters are resolved, and until a credible business case, backed by actual customer need is demonstrated

A vertical blue bar on the left side of the page.

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