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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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	Nicola Meyrick
ORGANISATION	E.ON
ORGANISATION CATEGORY	Supplier
E-MAIL ADDRESS	nicola.meyrick@eonnext.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?

Scope and Strategic Alignment

We agree that the current scope of the MMP appropriately focuses on the digital-only option, which is an accurate reflection of the productive discussions held during our recent working groups. We believe this focus is vital for ensuring a consistent approach to the development of the tool. By delivering a single, unified version of this consent solution, Industry can prevent a fragmented market landscape where consumers are burdened with varying versions created by different Authorised Third Parties (ATPs). This streamlined approach not only enhances the user experience but also provides essential clarity across the industry.

Regulatory Framework and Compliance

To maintain high standards of security and trust, it is a sensible approach to utilise the regulatory entry requirements already established within the Smart Energy Code (SEC). Provided that ATPs accede to these requirements and demonstrate their "fit and proper" status, leveraging this existing framework in proportionate manner and any differences in entry requirements must be clear to each party, to avoid ATPs side tracking this option to utilise the SEC that would not provide the same level of high standards of security required for sharing personal data, however, we would also recommend that the ATP's are required to accede to the REC for further entry monitoring especially within the initial 6 month period.

While the CCS remains in the MMP phase, we recommend shortening the ongoing compliance checking period from three years to one year to ensure compliance with all relevant code requirements. This increased frequency will provide better oversight and ensure that new entrants are delivering services in line with industry expectations.

Data Governance, Liability, and Synchronisation

As we move toward implementation, we will require further clarity regarding the liability framework in regard to data breaches. We propose that any breach concerning the access or use of data from the CSS be governed by RECCo. This governance should include formal reporting protocols to both the ICO, in accordance with UK GDPR and the Data Protection Act, and to RECCo itself.

We are also looking for confirmation on the synchronisation latency between the CCS and the SDR. To prevent unauthorised data polling by ATPs, it is critical that any withdrawal of consent in the digital tool is reflected in the SDR in real-time. Furthermore, we would appreciate confirmation on whether RECCo intends to inform Suppliers when a breach impacts their specific customers and the intended communication channels for such notifications.

With the implementation of the Tariff Interoperability having been aligned with the CCS, it's essential that there's no significant delays within the implementation of the CCS which could delay other programs. These programs will need to liaise to ensure continued alignment.

Consent Management and Technical Alignment

To ensure full transparency, we understand that a new consent will be obtained for any new or existing agreements that SEC Other Users have with consumers. Currently, consent under SEC Section I is managed via the Privacy Controls Framework and audited through Independent Privacy Assessments; therefore, it is essential to understand how consent for the SDR (Smart Meter Data Repository) will align with these existing obligations.

Specifically, we seek to confirm if SDR access will be strictly limited to instances where consent is recorded within the CCS. From a technical standpoint, we also require clarity on whether the SDR will manage granular consent (such as specific data types or timeframes) or if it operates on a binary access model. This detail is essential to ensure compliance with the "Data Minimisation" principle under UK GDPR.

Mitigating Consumer Confusion and Dispute Resolution

Finally, we note some potential inconsistencies across various Industry Codes regarding consent and access permissions. If liability remains ambiguous, it could lead to significant consumer confusion. Given that Suppliers are the primary point of contact for consumers regarding their smart meter data, they are likely to receive complaints without currently having visibility into who has accessed data via the SDR.

To resolve this, we suggest the SDR provide a transparent audit trail or a read-only "Access Log" to the relevant Supplier. This would allow us to identify which SEC Other User accessed data, and under which specific consent ID, ensuring a swift and professional resolution to consumer enquiries.

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?

Our view is to ensure that the Consumer has clear visibility of all consent, and that existing data migration should happen immediately and be determined by the specific nature of the original consent.

We believe it is essential to obtain explicit consent from the customer before any existing agreement is transitioned into the CCS tool and this must be obtained via the ATP. Access agreements should never be assumed; a proactive approach ensures that the consumer remains in control of their data and is fully aware of how it is being managed within the new digital framework.

To support this transition, there must be a clearly defined and intuitive customer journey. This journey should transparently display the date each consent is due to expire and outline the specific actions a customer needs to take to renew access. This level of clarity is vital for maintaining consumer trust and avoiding service interruptions. Furthermore, before any existing consents are transferred, the SEC Other User must demonstrate that they continue to meet all relevant regulatory requirements and hold a valid, active contract with the consumer for data access.

From a regulatory viewpoint, it is imperative that Other Users remain compliant with their existing obligations under SEC Section I and the Privacy Controls Framework to continue accessing data held at the DCC. Any non-compliance in these areas could significantly impact their standing as an SEC Other User.

We also note that while Other Users may choose to access data from the Smart Data Repository (SDR) using consents held in the CCS, the success of this model relies entirely on the comprehensiveness of the data within the CCS. Given that updates to the CCS are not currently mandatory, we recommend that once past MMP there is a consideration around a modification to the SEC Section 1, which directs the mandate to utilise the CCS as opposed to creating a potential disconnect and ensuring alignment and one version of consent truth.

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.

Occupier vs. Bill Payer Consent

Regarding the proposal in section 5.6 of the consultation, we agree in principle that for consent to be valid under data protection standards, it should be obtained from the Data Subject. In the context of energy usage, this is the occupant whose daily behaviors generate the data, regardless of whether they are also the legal bill payer. While this aligns with the Smart Energy Code (SEC), which recognises the occupier as the consent provider so long as they meet the criteria set out in Section I, we believe several practical challenges must be addressed to ensure this approach is both secure and workable.

One of our primary concerns relates to Houses in Multiple Occupancy (HMOs) and other multi-occupant sites. Identifying these sites accurately within current industry processes is notoriously difficult. We are seeking clarity on the specific mechanisms that will be implemented to ensure HMOs are identified correctly to prevent unauthorised data access. In a multi-occupant scenario where one individual holds the contract with the energy supplier but another engages with an ATP it is unclear how the ATP will verify the number of occupants and/or churn of occupancy or confirm that the Letter of Authority (LOA) provided is valid for all parties whose data may be captured.

To mitigate these risks and simplify the process, we suggest exploring whether the Account Holder (the individual with the direct contract with the energy supplier) should be the primary party allowed to engage with an ATP. This would provide a clearer chain of authority and better protection for the consumer. At a minimum, there must be robust guardrails to ensure consumers fully understand the consent process and the specific contractual obligations they are entering into with a third party.

Moving forward, we recommend a review of how this process currently functions for SEC Other Users ensuring that this process is simplified and transparent is essential to protecting the rights of the occupant while maintaining the operational integrity of the supplier-customer relationship.

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.

Lead Occupant Consent in Multi-Occupancy Households

While we agree in principle that a "Lead Occupant" may provide consent on behalf of a household, this must be underpinned by a rigorous and transparent process that ensures all occupants are fully aware of the agreement with the ATP. To maintain data integrity, all occupants of a property should be explicitly listed within the consent agreement, confirming their permission for the designated lead person to act on their behalf taking into account the high level of churn of residents and revised consent documentation on each subsequent change.

We seek clarity on how the system will manage frequent "move-in/move-out" events, as the departure of a single occupant would potentially render the existing consent agreement invalid.

The complexity of this model increases when considering the various stakeholders involved, such as landlords or property owners. For instance, if a landlord enters into a contract with an ATP to improve property efficiency, but the residents do not provide consent for data access, a clear framework is needed to address this conflict. Furthermore, while a lead occupant model may suffice for simple processes like energy tariff changes, it becomes problematic for third-party disputes involving infrastructure, such as EV charger installations. In such cases, the interplay between tenancy agreements and data consent requires a robust dispute process. We believe the person providing consent must have absolute clarity on their rights, the identity of the company holding the consent, and who is ultimately responsible for data access.

To protect consumers, it is essential that ATPs publish a transparent dispute process with clear contact details. We recommend the development of a formal escalation path for consumers who are dissatisfied with an ATP's response. Escalation bodies which are utilised in the financial sector offer consumer protections that are better suited to these types of digital agreements than the current Energy Ombudsman. We agree with the proposed approach for identity verification and support the requirement for photo identification such as a passport or driving license as the minimum baseline standard.

It is essential that the level of verification remains strictly proportional to the sensitivity of the data being requested. This correlation must be communicated clearly to the consumer during the CCS onboarding process to ensure they understand why specific security measures are being applied. By mirroring the verification journey and security standards found in high-trust platforms, such as banking or the NHS app, we can foster a sense of familiarity and legitimacy, helping consumers intuitively understand the necessity of robust authorisation.

Regarding the technical standards, we understand that GPG 45 is the proposed framework for identity proofing. While we support the adoption of this standard, we would like to highlight that model.

Finally, we look to RECCo to provide several critical definitions to ensure industry-wide consistency. Similar to the standards set out in the SEC, RECCo must define what constitutes sufficient evidence that a consent provider is an occupant linked to a specific address or meter. Additionally, RECCo must establish clear, standardised protocols for how consent can be removed and how consent related disputes should be handled and treated across the board. We also wish to understand if these "Lead Occupant" rules will apply to the SDR and whether any specific concerns have been raised regarding how multi-occupant data sharing will be gated within that repository.

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

We agree that personal identification is only one half of the verification requirement. To ensure complete security, the link between the individual and the specific address or metering device must be confirmed with the same level of rigor. We support reviewing the current processes utilised by SEC Other Users to determine what they currently deem sufficient and to ensure the proposed approach is aligned with proven industry practices.

Furthermore, we agree that identity verification should be conducted directly within the CCS tool rather than by the ATP. Centralising this process ensures a consistent, high security standard and eliminates the risk of varying or inadequate IDV practices among individual third-party entities. This centralised model is the most effective way to protect consumer data and maintain the integrity of the overall consent framework.

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.

The proposal to allow "guest" access within a CCS presents a fundamental conflict between user convenience and robust data integrity. While a guest approach is often favored in ecommerce for one off transactions, it is fundamentally ill suited for the management of sensitive personal data.

The primary risk lies in the lack of a persistent, authenticated dashboard, which leaves consumers without a clear "single point of truth" to view which third parties currently hold permissions to their data. Without a formal account, the mechanism for a consumer to withdraw consent becomes unnecessarily convoluted; if a user cannot easily log back in to see their active permissions, they effectively lose the right to be forgotten or the ability to manage their data footprint in real time.

Furthermore, the "guest" model fails the test of rigorous auditability and traceability required for high stakes data sharing. In a formal account structure, every consent grant, modification, or revocation is tied to a verified identity with a clear audit trail. In contrast, guest accounts often rely on transient identifiers or cookies, making it difficult to link multiple consent actions across different sessions or devices.

This fragmentation creates significant gaps in the historical record of data sharing, when dealing with sensitive information that carries higher stakes than a simple retail purchase.

There is evidence of historical challenges in the digital landscape, such as issues seen in the early iterations of various public sector and healthcare data sharing initiatives, where guest like or low friction "unregistered" pathways are used, disputes regarding data accuracy or unauthorised sharing become nearly impossible to resolve effectively. Were a customer to raise a complaint or a Subject Access Request (SAR) where they had previously interacted with a guest portal, the organisation may struggle to verify the claimant's identity or reconstruct exactly what data was shared and with whom. The lack of a "paper trail" could lead to regulatory friction and a breakdown in trust between the consumer and the CCS.

Without the centralised control provided by a full account, a consumer who believes their data has been misused has no immediate way to remove the data from the disputed organisation. This delay could lead to prolonged unauthorised data processing, resulting in financial or reputational harm to the user and potential legal liability for the service provider. While it is true that a full account setup may be perceived as more "onerous," this friction serves as a necessary security boundary.

To address those without the technology or digital literacy to manage such accounts, the solution should not be a less secure guest route, but rather the implementation of inclusive support models and delegated authority frameworks that maintain high security standards without excluding vulnerable populations.

Below are outlined the critical security and functional gaps highlighting the contrast between the guest and full account mode in regard to the risks inherent in treating sensitive data consent like a simple retail transaction.

Feature	**Guest Access (Transactional)**	**Authenticated Account (Persistent)**	**Risk/Impact of Guest Model**
Consent Visibility	One-time confirmation; usually lost once the browser session ends.	Centralised dashboard showing all active and historic permissions.	Blind Spots: Consumers cannot see a "real-time" list of who has their data.
Right to Withdraw	Requires manual outreach to each third party or re-identifying via email links.	One-click "Revoke" button for any connected service.	Friction: Makes the legal right to withdraw consent unnecessarily difficult.
Audit Trail	Fragmented; no ability to link multiple sessions to a single identity.	Comprehensive, timestamped log of all grants and revocations.	Compliance Gap: Fails to provide a robust defense during a GDPR audit or dispute.
Identity Verification	Low-level (usually just an unverified email address).	Stronger authentication (MFA/ID checks) ensures the right person is in control.	Fraud Risk: Higher likelihood of unauthorised "consent" being granted by third parties.
Dispute Resolution	Difficult to prove what was shared if the guest session data isn’t available to view consistently.	Clear historical record of data schemas shared with specific vendors.	Liability: Increases the time and cost to resolve consumer complaints or SARs.

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.

We agree consumers should have the flexibility to revoke or renew their consent either directly through the relevant ATP or via their CCS account. Providing this choice is essential for consumer empowerment however, it necessitates a robust and automatic synchronisation process, any revocation of consent must trigger an immediate update to the CCS to ensure the one point of truth remains accurate. To maintain transparency, we propose that a formal confirmation be sent within 24 hours of a revocation being processed by an ATP. Furthermore, when a consumer takes this action through an ATP, the provider should give clear notice regarding the update and how the consumer can verify the update.

To ensure consumers are fully informed, the contract between an ATP and a consumer must include a section outlining their rights to remove consent at any time. A proactive renewal process should be implemented in advance of a consent expiration date, providing “next steps" for maintaining access. Similarly, upon the conclusion of a contract, the ATP must be obligated to remove the consent and provide written confirmation of this within 24 hours.

It is important that if an ATP is also an SEC Other User, they remain bound by the obligations set out in SEC Section I. These regulatory responsibilities are not replaced or superseded by changes made within the CCS, particularly as there is currently no direct interface back from the CCS to the SEC Other User’s internal systems.

This duplicity creates a potential complexity where parties may need to update both the CCS and the SEC Other User independently or where the security standards/encryption are different. We recommend that RECCo and the SEC Panel work closely to define how these dual obligations will be managed to prevent administrative burden on the consumer and providers; ensuring that data access remains strictly aligned with the data subject's intent.

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.

The proposed requirement for EDPs to explicitly verify active consent within the CCS each time data is shared with an ATP is a vital safeguard for the ecosystem. This "zero trust" model ensures that data is only exchanged when centralised proof of occupancy and current consent have been verified.

Adopting this rigorous approach is essential as energy consumption data is deemed highly sensitive and can expose personal occupancy habits or behaviors within the property. Consequently, technical costs or system complexity should not be considered a limiting factor in ensuring that only data explicitly authorised by the consumer is provided to the ATP.

The necessity of these checks is underscored by the potential impact on consumers should unauthorised data sharing occur, for instance, if a consumer has moved out, the ATP is legally required to cease data access immediately. Without a mandatory check against the central ledger, there is a risk that "ghost consents" could persist, leading to the unlawful processing of a new occupant's data.

To mitigate this, we support the proposal that notifications of revoked access must be issued via webhooks to both ATPs and EDPs within 24 hours to ensure local and central records remain synchronised. Furthermore, in the event of a system outage, the priority must remain on data protection and integrity. In alignment with the UK GDPR's "Security" principle under Article 5(1)(f), which requires technical and organisational measures to protect against unauthorised or unlawful processing, it may be necessary to halt data sharing during prolonged outages until system reliability is fully restored.

While the CCS acts as a central trust framework, it does not replace the existing legal and regulatory obligations of the participants. For example, SEC Other Users must still adhere to the SEC obligations, which are verified through annual Independent Privacy Assessments, ATPs bear the primary responsibility for ensuring they have obtained valid consent before attempting to access data via the SDR or other arrangements. The CCS serves to strengthen this by providing a standardised, auditable mechanism with the REC PAF providing the necessary oversight to take action against non-compliance or data breaches.

During any period of system unavailability, clear communication and transparency are paramount to maintaining consumer confidence. The CCS should provide visible status reports and clear instructions on the actions a consumer can take to protect their data, such as manual revocation routes. Detailed processes regarding system reliability and dispute resolution particularly concerning the exact date and time a consent was revoked must be published within the consumers tool to ensure a clear path for redress where data may have been processed following a withdrawal.

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.

The approach to data sharing during a CCS outage is primarily contingent upon the duration and nature of the system failure. In instances of short-term outages where a previously issued token remains valid, the risk to the ecosystem is relatively low. For example, outages lasting less than 30 minutes are likely to have a minimal impact on data integrity as the energy data being shared is typically not deemed to be "live". Any outage extending beyond the 30-minute threshold, a more detailed impact assessment must be conducted, and data sharing should be suspended until the system resumes.

It is essential that the system remains accountable to the consumer's right to manage data, even during downtime. Where a consumer attempts to revoke consent while the CCS is unavailable, clear messaging must be provided and the necessary steps to take. Any pending revocation requests initiated before or during an outage must have their requested dates and times strictly honored and all pending updates to remove access tokens must be processed immediately with the original timestamps ensuring no data is shared beyond the relevant point.

Transparency is a cornerstone of this framework, and detailed outage reports must be made available for monitoring reliability of the service and provide an audit trail of any data shared. Special consideration must also be given to specific data sharing arrangements, such as the SDR, access to the SDR during a CCS outage requires a clearly defined management process to ensure that EDPs only share data where valid consent is confirmed and agreed.

A robust Business Continuity Plan (BCP) must be implemented detailing the technical process for managing data sharing and token synchronisation, were the CCS to become unavailable. Upon the CCS resuming operations, a comprehensive post incident report must be provided. This is essential to ensure that each ATP and EDP can process any outstanding consumer requests in a timely manner.

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 adoption of the Financial-grade API (FAPI) 2.0 standard, including the mandatory use of Mutual Transport Layer Security (mTLS) for all data sharing, is proposed as the robust technical solution to secure the CCS. This standard is already established as a proven technology in high-stakes data environments, securing significant ecosystems such as Open Banking in the UK and Consumer Data Rights in Australia. Given that FAPI 2.0 represents the latest version currently employed within the banking sector, it offers a level of security required to deal with the sensitivity of energy consumption data, which can reveal consumer behaviours.

Utilising a publicly accessible and widely documented open standard like FAPI 2.0 provides immediate benefits by reducing the implementation risks and effort typically associated with bespoke or proprietary security models. It aligns with established security practices, ensuring that data exchange is protected at the transport layer through mTLS and further secured via sender constrained tokens. This comprehensive security profile, which underwent extensive threat modeling by academic institutions, ensures that the ecosystem is shielded against token exposure and malicious interception without the need for industry to conduct costly, independent security assessments.

The implementation of FAPI 2.0 fosters long term interoperability, potentially linking the energy sector with other mature data sharing ecosystems overseen by the FCA. Adopting these rigorous controls, the CCS establishes a "Trusted Framework" that provides consumers and industry participants with confidence that only authorised data is shared and that personal identifiers are cryptographically protected. While further consultation with security experts, such as the SEC Security Sub Committee, may provide additional specialised recommendations, the current proposal leverages a globally recognised standard to provide the high level of system security necessary to protect consumer data from Day 1.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?

Based on the design principles and technical architecture, the proposed CCS presents several positive features that should support a smooth implementation. A key strength is the standardised "Consent Data Schema" and the use of the API first, modular design, intended to ensure interoperability and a consistent experience across different market participants. The solution’s reliance on proven open standards, specifically FAPI 2.0 and mTLS, provides a mature security framework that aligns with established practices, potentially reducing the risks and bespoke development effort that's often associated with new technical ecosystems. The centralised Directory and Registry will facilitate the automated discovery of participants and datasets, which should streamline integration for both ATPs and EDPs.

There are certain aspects of the design that may present operational challenges and financial risks to industry parties. A significant area of concern for E.ON is the funding model, as initial development and enduring base costs for the MMP are proposed to be recovered through the socialised RECCo cost recovery model. This effectively places the financial burden primarily on large suppliers, leading to questions regarding the specific controls in place to review and confirm expenditures.

Parties require greater visibility into the cost benefit analysis and the mechanisms RECCo will use to ensure the architecture is designed for minimum financial impact on suppliers, both during the initial build and for future upgrades as the program expands. There is also potential friction regarding the mandatory token introspection, which requires EDPs to verify consent in real-time for every data request, necessitating high system availability and robust business continuity plans.

The project timeline presents a substantial risk to a successful rollout with the MMP targeted for go-live in March 2027, the window for all parties to develop, test, and implement solutions compatible with these complex design documents is notably narrow. Given that detailed REC drafting and technical specifications will not be consulted on until summer 2026, participants will have less than a year for final technical delivery. This compressed timescale is particularly challenging when considering the technical rigor required for FAPI 2.0 and mTLS compliance, alongside the necessity for thorough accreditation and sandbox testing.

The current financial governance of the REC is designed to ensure that all expenditures, including those for the CCS, are subject to rigorous oversight. Under the established REC Schedule 10 Charging Methodology, costs for REC Services are recovered from suppliers based on market share. For the CCS specifically, it is understood that RECCo has committed to using proven technologies to minimise the risks and expenses associated with bespoke builds.

Despite these existing controls, several areas remain where visibility and cost-benefit transparency for large suppliers is limited. While the MMP development is funded through socialised costs to encourage early market adoption, RECCo has indicated that Hybrid Model B will eventually be adopted. Under this hybrid model, the base running costs remain socialised, but organisations will be required to pay for specific assurance activities, such as accreditation audits and breach investigations. However, there is currently no detailed public breakdown of the total forecasted technical costs or the specific "pre-conditions" that will trigger a transition from socialised funding to a more equitable "user pays" model.

The integration of the CCS with existing REC Digital Services such as the REC Portal and Service Desk is intended to reduce duplication and streamline the financial impact. By leveraging these established platforms, it appears that RECCo aims to provide a modular architecture that can be upgraded with minimal incremental cost, with the performance assurance framework allowing for costs related to non-compliance or targeted audits to be recovered directly from the responsible organisation. To improve visibility, suppliers require clearer reporting on the cost-benefit analysis for upgrades, particularly as the roadmap expands to include more complex data sets like the Smart Data Repository (SDR) or the Priority services register.

Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.

We agree that the proposed strategy of utilising the existing gas and electricity enquiry services to match MPxN data to physical addresses is a fundamentally sound approach. This aligns with current utility switching services that rely on ECOES to verify meter and address details, ensuring consistency across industry standards. The preference for using the Retail Energy Location (REL) Address is preferred, as this is the recognised standard for all switching processes within the CSS and management functions. For this ecosystem to function effectively, it is essential that the DCC, CSS, and ECOES remain aligned to prevent any operational discrepancies.

A critical component of this matching process is ensuring that ATPs maintain total alignment between the address used in the CCS tool and the address detailed within their customer contracts. Any identification of a mismatch or address difference must be addressed as a priority at the contract stage to avoid significant complications or "fall out" later in the data-sharing lifecycle. It is essential that the ATP confirms the address matches the physical premises before a consumer enters into a formal agreement. Where a mismatch is identified, a clearly defined process must be followed to correct the data, ensuring that the ATP takes responsibility for the resolution.

Additionally, there must be robust security and governance to protect regulated supplier processes from unauthorised or incorrect data updates. Where an ATP identifies a misalignment, the system must ensure that these updates are not automatically pushed to the DCC, CSS, or ECOES, as this could have a detrimental effect on supplier led regulated activities. It is recommended that where a discrepancy requires a supplier led process to fix a core industry record, this resolution must be completed before the customer proceeds with the ATP's service. This approach preserves the integrity of the industry's "single version of the truth" while protecting consumers from the risks associated with inaccurate data matching.

To ensure that data integrity is maintained a structured data discrepancy workflow is necessary to manage instances where the CCS records do not align with a customer's contractual or physical address. This process ensures that any misalignments are corrected at the source, and the regulated supplier records before an ATP begins data processing:

1. Initial Identification and Verification

The workflow begins at the contract stage, where the ATP verifies the customer's provided address against the CCS record, which is fed by the REL or MPL from the electricity enquiry services. If the ATP identifies a mismatch, they must not proceed with the contract until the discrepancy is investigated. This "guardrail" prevents the escalation of incorrect data ensuring the correct Meter Point (MPxN) is utilised.

2. Resolution through Regulated Channels

Where a genuine error exists in the industry data (DCC, CSS, or ECOES), the ATP is responsible for informing the consumer that a supplier-led correction is required. As ATPs are non regulated entities, they do not have the authority to update core industry address management functions directly, with this in mind the consumer must be directed to their supplier to initiate an address update. The ATP must monitor the status of this update via the CCS enquiry services and only resume the onboarding process once the REL address in the central system matches the contract address.

3. Safeguards Against Automated Updates

To protect the integrity of supplier processes, the CCS architecture specifically prohibits ATPs from pushing automated updates to the DCC or CSS. If an ATP were permitted to override these records, it could cause significant "knock-on" impacts, such as erroneous transfers or billing failures for the primary supplier. Instead, the CCS serves as a "read-only" consumer of address data for matching purposes, ensuring that the master record remains under the governance of the REC and its established switching protocols.

4. Final Validation and Audit

Once the supplier has corrected the record, the ATP performs a final introspection check to ensure the consumer's identity and occupancy are correctly linked to the updated MPxN. This final step must be timestamped and recorded within the CCS central ledger to provide a full audit trail for any future dispute resolution or performance assurance audits.

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

The proposed Non-Functional Requirements (NFRs) outlined in Annex D raises several concerns regarding the oversight and accountability of non-regulated ATPs. While the REC provides a framework for entry and assurance, there is a question as to whether these processes are sufficient to identify and mitigate misuse of the CCS tool by entities that fall outside traditional energy regulations. Clarity is required on how this mechanism links back to the existing SEC Other User process, where organisations currently access personal data and manage consent independently without utilising the CCS.

A particular point to highlight relates to the timing of robust monitoring activities, Annex D states that monitoring will focus on compliance, behaviour, and consumer outcomes, where the product roadmap suggests that essential protective measures such as mystery shopper UX checks, expanded behavioural analytics, and consent pattern anomaly detection are stated for delivery after the MMP launch.

To ensure consumer protection from Day 1, it is vital to understand how these features will be implemented, identifying poor behaviour, with the current entry process treating the reporting of incidents as guidance. To ensure ATPs have the same level of accountability as suppliers, this should be a mandatory requirement as opposed to guidance of the accreditation process.

The practical application of SLAs for query resolution requires further definition. It is unclear how non-regulated ATPs will be mandated to provide complaint data. While raising and managing disputes through the CCS tool provides a trackable measure, there is a persistent risk that any interactions occurring outside the tool via the ATPs directly will become untraceable. Consumers must have a transparent process where they can clearly see raised disputes and track responses from the relevant company. Finally, further transparency is needed regarding the reporting structure for CCS monitoring, including which authorities will receive these reports and at what frequency.

To ensure that the CCS provides robust protection from the launch of the MMP in March 2027, it is essential to move key monitoring and accountability measures from the "Future Roadmap" into the mandatory Day 1 requirements. Relying on voluntary guidance for non-regulated ATPs creates a significant gap in consumer data security and auditability.

Mandatory "Day 1" Monitoring & Compliance Requirements

The following table outlines the proposed mandatory requirements that must be active at launch to ensure ATPs are held to the same accountability standards as regulated Suppliers.

Requirement Area	Mandatory Day 1 Implementation	Rationale for Launch Inclusion
Incident Reporting	Mandatory self-reporting of all data-related incidents or potential breaches to RECCo within a defined window (e.g., 24 hours).	Moving this from "voluntary" to "mandatory" ensures non-regulated ATPs face the same scrutiny as Suppliers to maintain ecosystem trust.
Behavioral Analytics	Automated detection of anomalous consent patterns, such as high-velocity grants or repetitive failed attempts.	Essential for identifying automated misuse or "consent farming" before it causes widespread consumer harm.
Query & Dispute SLAs	Strict resolution timelines (e.g., 5-10 working days) for ATPs to respond to disputes raised via the CCS portal.	Ensures consumers are not left in a "management vacuum" when disputing unauthorized data access.
UX Compliance	Automated CEG checklists and pre-launch "mystery shopper" audits to verify that ATP interfaces are not using "dark patterns".	Prevents poor behavior from being "baked in" to ATP journeys from the start of the MMP.
Reconciliation	Monthly mandatory reconciliation reports submitted by ATPs, comparing their internal records against the CCS central ledger.	Identifies synchronisation failures early and prevents "ghost consents" where data sharing continues after revocation.

Ensuring Traceability and Reporting

To resolve the risk of untraceable "off-tool" disputes, the CCS should mandate that all formal data sharing queries are logged within the central system. This provides a transparent audit trail for the consumer, allowing them to see exactly when a query was raised and the specific response from the ATP. The frequency of compliance reporting to the REC PAB should be set to monthly during the initial MMP phase to allow for rapid intervention if systemic issues with non-regulated entities emerge.

Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?

The proposed hybrid architecture for the CCS, which balances centralised trust functions with decentralised data exchange, represents the most effective solution for meeting Ofgem's objectives in the UK energy market. By centralising the consent ledger and token provision, the system establishes a "single source of truth" that is essential for robust auditing, standardisation, and issue arbitration. This centralised approach is beneficial to consolidate KYC standards among energy suppliers; a central IDV solution raises security standards for all participants without requiring every supplier to develop expensive, bespoke capabilities immediately.

The decision to keep the actual exchange of energy data decentralised is equally critical to the solution's success, as it avoids the risks and costs associated with creating an overburdened central data lake. This model allows data to flow directly between EDPs and ATPs, which preserves the diversity of existing user cases and respects the governance of originating bodies like Elexon, by decentralising the user interface allowing consumers to manage consent either through the CCS portal or directly via their chosen ATP the design minimises "negative friction" and encourages higher market adoption by supporting established consumer provider relationships.

Ultimately, this split is the preferred solution as it resolves the fragmentation of the existing "SEC Other User" market while maintaining a "zero trust" security posture. While the decentralised elements offer necessary operational flexibility, the centralised components ensure that personal energy data which can reveal sensitive occupancy habits is only shared when occupancy and consent have been verified. This balance effectively minimises the single point of failure risk for the data itself while providing the consistent, high standard oversight necessary to build and maintain long term consumer trust as under this model, EDPs must explicitly verify that a consent is active and valid every time they share data with an ATP.

Mandatory Introspection Requirement

The core of the Zero Trust architecture is the requirement for EDPs to call the CCS introspection endpoint before any data is returned to the ATP. This process should ensure that the token provided by the ATP is not only cryptographically valid but also represents a currently active consent record in the central ledger. The introspection call must assess:

- Token Validity: Confirmation that the token has not expired or been tampered with.
- Scope Compliance: Verification that the specific data being requested matches the scope originally granted by the consumer.
- Status Check: A real time check against the central ledger to ensure the consumer provided explicit consent through the central portal or another channel.

Technical Safeguards and Standards

To support this high frequency validation, the CCS needs to be designed with specific technical standards to maintain security without compromising performance:

- FAPI 2.0 and mTLS: The solution should mandate the Financial grade API (FAPI) 2.0 standard, which requires Mutual Transport Layer Security (mTLS) for all data exchange. This ensures that tokens are "sender constrained," meaning they cannot be used by any party other than the specific ATP.
- PKI Services: The CCS provides PKI services issuing the necessary certificates to all participants to secure communications.
- Webhook Synchronisation: Reduce the total reliance on point of access checks, the CCS should use webhooks to push revocation notifications universally and immediately across the ecosystem

Availability and Continuity Strategy

Recognising that 100% uptime is technically and financially difficult, the solution includes a defined contingency for system outages:

- Default Validity: Where the CCS is unavailable and the defined retry strategy is exhausted, EDPs are proposed to treat existing consents as valid by default for a limited period.
- Outage Caps: Requirement to continually measure the system to prevent service degradation but could be subject to an overall time cap to mitigate data exposure risks.

Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?

We appreciate the technical and business process diagrams presented in Annex E as these provide a necessary visualisation of the CCS architecture, including critical components such as IDV, the CCS, and decentralised data exchange. The successful execution of this model is entirely reliant on RECCo's designing and implementing a secure, scalable architecture that achieves these objectives at minimum financial cost. It is vital that the system is engineered for cost effective upgrades within reasonable timeframes as the program expands to include wider datasets and consumer segments beyond the initial MMP.

We would like to understand financial governance, as the substantial costs of development and implementation are currently borne by suppliers, primarily the large suppliers through the socialised cost recovery method. It is not clear how future enhancements and necessary system upgrades are to be funded; we would like clarity on the specific controls RECCo has in place to review and justify the expenditures being recovered from suppliers. This will ensure a robust oversight process is essential to maintain the program's viability and prevent the socialisation of disproportionate costs.

There is a need for greater visibility regarding the ongoing cost benefit analysis of the CCS. To protect the interests of the consumers who ultimately fund these industry charges, we would like RECCo to provide transparent reporting on both the actual costs incurred and the tangible benefits realised as the roadmap progresses. This transparency is critical to ensure that the "user pays" transition occurs at the earliest possible threshold and that the financial burden remains proportionate to the value delivered to the market.

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.

The current identification of four primary behavioural archetypes: digitally confident maximisers, cost conscious and financially constrained consumers, high need, high load households, and time poor, digitally capable families provides a robust foundation for designing the CCS.

We agree that focusing on the high need, high load group as a primary design benchmark is a sound strategy, as the simplified structures and plain language required for this group effectively lower barriers for all users without disadvantaging more digitally fluent consumers. While the existing archetypes are comprehensive from a behavioural standpoint, we believe there are specific demographic nuances that warrant further consideration to ensure the solution is truly universal.

One group to further define is consumers who are entirely digitally excluded. While the "cost conscious" and "high load" archetypes acknowledge low digital confidence, a segment of the population remains that does not use the internet at all. For these individuals, the "floor" of Web Content Accessibility Guidelines (WCAG) 2.2 Level AA digital standards will remain insufficient. It is essential that the CCS provides equivalent outcomes through non digital channels, such as telephone based verification or IVR systems, to ensure these consumers are not locked out of the benefits of the energy data market.

There are unique needs for young people and those in rented accommodation should be explicitly cross referenced against these behavioural patterns. Renters, in particular, may have different rights or authority levels compared to homeowners, especially in multi occupancy households or where energy costs are included in the rent. Ensuring that the CCS correctly identifies the "data subject" in these varied living arrangements is vital for maintaining GDPR compliance and consumer trust. Similarly, younger consumers may be "digitally confident" but have higher expectations for mobile first, low friction interactions that avoid clunky systems.

We support the commitment to iterative research to ensure these archetypes evolve as the CCS matures. By grounding future customer experience guidelines in ongoing evidence from real consumer behaviour, RECCo can address emerging gaps, such as the specific needs of neurodivergent users or those with situational barriers like limited English proficiency. This ongoing refinement will be key to ensuring the CCS remains a trusted mechanism that minimises cognitive load for all energy consumers

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 proposed inclusion requirements set out in Annex F provide a strong foundational baseline for accessibility, particularly through the commitment to web content accessibility guidelines (WCAG) 2.2 Level AA standards. By ensuring that content is perceivable, operable, understandable, and robust, the framework addresses a wide array of situational and permanent barriers, such as sensory impairments or cognitive load. We support using high need, high load Households as the primary design benchmark, as features that assist these vulnerable users such as plain language, clear structures, and flexible timeouts tend to enhance the experience for all consumer archetypes.

Further clarity is required regarding the governance of these standards for ATPs. Unlike energy suppliers, who operate under established regulatory oversight, ATPs are currently not governed by regulations that mandate accessibility or clear website navigation. To ensure that critical information remains no more than one click away for the consumer, we recommend that the CEGs be more prescriptive. These guidelines should translate high level accessibility principles into concrete, binding requirements for ATP implementations, specifically focusing on reducing cognitive effort during the consent journey.

To maintain these high standards, it is necessary that the REC implements a proactive monitoring framework. We advocate for the use of the REC PAF to verify that ATPs are meeting the CEGs' accessibility requirements. This should include periodic audits and potentially "mystery shopper" exercises to test the real world accessibility of ATP platforms. Without such robust governance, there is a risk that the floor of accessibility will vary significantly between participants, undermining consumer trust in what is effectively a financial sales journey for many.

Finally, regarding the inclusion of privacy notices, we confirm that our existing digital services are designed and audited for WCAG Level AA compliance, and we believe a similar standard of transparency should be mandated for the CCS. The CCS itself must provide clear signposting and save and return functionality to support consumers with mental health or cognitive challenges who may otherwise abandon a journey due to anxiety or fatigue. By grounding the CEGs in iterative behavioral research, RECCo can ensure that these requirements evolve alongside consumer needs and emerging technology.

Q18	Do you agree that consumers need to know who is requesting consent, what data they want, and for how long? If not, what's missing? Is there a risk of information overload?

We agree that ensuring a clear and transparent consumer experience throughout the entire data sharing lifecycle is fundamental to building trust in the CCS. We agree that consumers must have immediate access to key information, including exactly which organisation is requesting consent, the specific datasets involved, and the precise duration for which that access will last.

To support this, the CCS tool should provide a comprehensive view of every consent an individual has authorised, clearly displaying the original agreement date, the scheduled renewal date, and a record of any past revocations. Every consent record should be identified by a title that is intuitive to the customer and prominently features the primary company name.

A critical component of this transparency is the clear disclosure of data sharing hierarchies. In instances where a company subcontracts its data management activities, the CCS interface must explicitly distinguish between the organisation with whom the consumer has a direct contract and the third party entity responsible for managing the data. This level of granularity is essential to prevent confusion and ensure that the "treating customers fairly" principle is upheld across all sub-processing layers. Additionally, dispute resolution processes must be visible and easily accessible. Any consumer actions, such as revoking or amending consent, should be reflected within the tool in real time. If technical constraints prevent immediate updates, the tool must clearly communicate the expected timeframe for these changes targeting a maximum window of 24 hours to manage consumer expectations effectively.

While providing this essential information, there is a recognised risk of information overload. To mitigate against this, the CCS should utilise a layered information design where core details are presented concisely in plain English, with the option for consumers to drill down into more technical or legal specifics. By standardising the lexicon and format of these disclosures through the CEGs, RECCo can ensure that consumers receive consistent, digestible information that empowers informed decision making without causing cognitive fatigue.

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)

In evaluating the user journey stages presented in the consultation (Figures 7–10), it is clear that the introduction of positive friction or strategic verification steps is essential to safeguard consumer data while balancing the need for a low friction experience. For the MMP, we believe a high level of confidence in IDV is non negotiable because the half hourly metered data being accessed could potentially expose sensitive personal occupancy habits where misused. A critical verification step must be included in the initial verification utilising photo identification, aligned with GDS GPG 45 standards. This step is essential to ensure that the individual granting consent is indeed the data subject with the appropriate occupancy rights.

The most vital point for introducing additional verification is during the grant stage for consumers utilising the guest approach. To protect consumers who choose not to establish a persistent CCS account, the solution must require a full IDV reauthentication each time a new consent is granted. This prevents unauthorised individuals from bypassing security checks through the guest route and ensures that the integrity of the consent record remains robust regardless of the consumer's chosen journey. While this introduces "positive friction," it is a necessary safeguard to maintain the trust framework and prevent misappropriation of energy data.

However, these steps could create disproportionate barriers if they are not applied proportionately to the risk. For instance, requiring high level photo IDV for low risk activities, such as accessing simple tariff data, could lead to high consumer drop off rates. To mitigate this, the CCS should eventually support best practice IDV, allowing consumers to rely on existing, trusted verifications from their bank or government backed identifiers like the NHS. This would significantly reduce negative friction for the consumer while maintaining a high security posture.

What is currently missing from the proposed journeys is a clear mechanism for consolidating guest actions into a full account at a later date. Without this, a consumer may face the disproportionate barrier of having to re-verify their identity multiple times for historical consents they previously managed as a guest. We believe it is essential to prioritise the technical feasibility of this consolidation feature post MMP to ensure the user experience remains seamless as trust in the solution grows.

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?

While we agree that providing visibility on which organisations hold consent, the types of data shared, and key dates is a necessary baseline, the CCS must include more granular detail to manage consumer expectations effectively.

A primary concern is the clarity of corporate relationships if the ATP subcontracts the actual data management to another entity. Both the name of the contracted company and the entity managing the data must be explicitly visible within the tool. Transparency regarding these sub-processing layers is critical for consumer trust and for ensuring that the "treating customers fairly" principles are upheld across the entire data supply chain.

To avoid confusion, the visibility provided must include a clear "title of consent" and a specific, non technical description of the data being shared. The transition between consent states must be managed with high transparency. Consumers need to know whether their data consent will automatically expire on a set date, requiring no proactive action from them, or if they must manually intervene to revoke consent. If manual action is required, the CCS must provide clear instructions and timely reminders that emphasise a "call to action" to ensure the consumer remains in control of their digital footprint.

Robust governance must be in place to ensure that data sharing strictly ceases upon the contract's expiration within the CCS tool. We believe the consultation should detail the specific controls used to prevent data leakage beyond agreed dates, especially in instances where a consumer fails to manually revoke access after a contract ends. Dispute processes must also be prominently displayed within the visibility of the consumers CCS dashboard. By ensuring that the consumer can easily identify who is using their data and how to stop it, the CCS will provide the "adequate visibility" required to build long term confidence in consumer led flexibility service.

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?

We agree that for the CCS to be effective, consumers must have a comprehensive understanding of which services are affected, the timelines for changes, and the reversibility of any revocation. All information provided throughout this process must be clear, transparent, and easily accessible to the consumer. It is essential that these details are not only embedded within the primary contract between the consumer and the ATP but are also clearly visible and trackable within the CCS tool itself.

To ensure clarity without causing information overload, the data should be presented at a high level while remaining sufficiently detailed to enable the customer to make informed decisions. As a minimum, the consumer must be able to identify the specific ATP they have contracted with, the entity responsible for handling the data if different from the ATP, and the formal title of the service or product being provided. Key data, such as the initial consent grant date and the expected expiry or contract end date, must also be prominently displayed. The ATP must also clearly present information regarding any third party employed to manage or process the consumer's data.

By standardising these data points including the specific types of data being shared within the CCS interface, it can provide a consistent experience that empowers the consumer. This structured approach mitigates the risk of confusion or information fatigue, ensuring that the consumer remains in control of their digital footprint without being overwhelmed by technical complexity.

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 enable consumers to grant, review, and revoke consent with the same level of transparency and detail as digital users. Every consumer journey, regardless of the channel used, must be clear and transparent from start to finish, ensuring that all action points are easily understood.

To achieve true equivalence, the service must be inclusive, offering accessible pathways for those who are not digitally knowledgeable or who lack access to online tools. This alignment with “Treating Customers Fairly" principles ensures that no consumer is excluded from the benefits based on their technical literacy. The framework should mirror the inclusive approach currently mandated for energy suppliers, who are obligated by Ofgem to provide access to all and not exclude customers unable to use digital services.

Ultimately, the goal of an assisted journey should be to provide a seamless and non discriminatory experience that protects the consumer’s rights to manage their data. Clear standards must be set to ensure that any "off-line" consent is tracked and consolidated with the same rigor as digital entries, particularly during the transition from guest access to full accounts. By having the right rigor in place for these equivalent outcomes, the CCS will foster greater trust and confidence across the entire consumer base, supporting the broader transition to consumer-led flexibility.

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?

To ensure that the CCS remains inclusive, the assisted and alternative consent journeys must be designed to achieve outcomes that are functionally equivalent to the digital experience. At E.ON, we recognise that a portion of the consumer base may be unable or unwilling to engage with digital only platforms. It is essential that the CCS supports a multi channel approach, incorporating established communication routes such as voice, WhatsApp, social media, email, and traditional postal services. The primary outcome of an assisted journey should be the ability for a consumer to grant, review, or revoke consent with the same level of security and transparency as a digital user, without facing additional administrative hurdles or delays.

Under existing Ofgem regulations, suppliers have stringent obligations to ensure that their services are accessible to all consumers, particularly those in vulnerable circumstances or those who are digitally excluded.

These obligations mandate that no customer should be disadvantaged by their choice of communication channel. In the context of the CCS, REC must define how these non-digital interactions will be managed to maintain a level playing field. We seek clarity on how REC, as the owner of the CCS tool, intends to facilitate these alternative journeys. It is critical that the responsibility for providing non-digital access is clearly defined between the ATP and the REC to prevent a fragmented experience where consumers are passed between parties without a clear resolution.

The governance for assisted consent should be a core component of the REC framework. If the responsibility for alternative contact rests solely with the ATP, there is a risk that consumers will encounter inconsistent service levels, especially if the ATP is not governed by the same licensing mandates as energy suppliers.

To mitigate this, the REC should establish a centralised assisted service standard or facility that ATPs can utilise, ensuring that the burden of managing complex non digital consent does not fall unfairly on the consumer. This approach would ensure that the CCS remains a truly universal tool that upholds the principle of access for all and aligns with the broader regulatory focus on consumer led flexibility and inclusive innovation.

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 support the proposed REC drafting approach, as it utilises a proven and robust framework to govern the CCS arrangements. The creation of a specific CCS Arrangements Schedule and a new Service Definition is an appropriate strategic move to ensure technical and operational consistency for all parties seeking to access the tool.

Given that the REC already maintains well established schedules and definitions, we are confident that the existing governance model built on principles of clarity and transparency is the right foundation for these new artifacts. The proposed technical specifications for the CCS API also align with industry expectations, providing the necessary checks to ensure system performance and reliability from the outset.

The integration of CCS into the REC's issues and change process is particularly beneficial, as it offers a structured environment for the continuous improvement of the tool. Following the existing change management structure, any additions or amendments to REC documentation will be clearly articulated, ensuring that all parties have a fair and formal opportunity to provide input through the standard consultation process.

However, a critical consideration for the successful implementation of this governance model is how it will accommodate ATPs. While the REC's Change Issues Group is a highly effective forum for registered parties like suppliers, there is currently a lack of clarity on how RECCo intends to engage with non traditional participants such as ATPs. To maintain the integrity of the "open to all" approach, the governance framework must define a specific pathway for ATP engagement within the change process. This is essential to ensure that the technical evolution of the CCS is informed by a wide variety of key stakeholders and remains future proofed as the energy data landscape continues to mature.

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.

While we recognise the practical necessity of an initial funding structure to launch the CCS we have significant concerns regarding the proposal to socialise the foundational costs through suppliers.

Under the current proposal, the design, development, and implementation of the CCS tool are funded by suppliers based on registered metering points. This "get users in, charge later" approach effectively means that suppliers who may not be the primary users of the service are subsidising the infrastructure for ATPs. A clearly defined duration period is required for the initial funding period. Further work is needed to establish clear requirements and timescales to trigger a transition to a "user-pays" model.

We agree that the costs associated with the qualification process, connection, and ongoing assurance activities should be recovered directly from the individual organisations seeking to use the tool. It is essential that the cost of a breach or an investigation is not socialised or hidden within broader supplier charges. By ensuring that the individual organisation responsible for a breach, repeated failed qualification requirements and inappropriate behavior bears the full financial burden. The framework creates a necessary incentive for high standards of compliance and operational integrity. This principle of financial accountability should apply immediately, including during the MMP phase, to protect suppliers and their customers from subsidising the failings of third party market entrants.

The lack of transparency regarding the long term commercial viability of the tool presents a risk to the industry. If the CCS does not achieve the anticipated traffic or utility, the ongoing costs of maintenance could become disproportionate to the benefits provided. If CCS eventually becomes mandated, it is vital that all charges remain transparent and proportionate to actual usage. We would welcome a comprehensive review of the wider REC funding mechanism to ensure it is sufficiently agile to adapt as the energy market evolves. This alignment is necessary to ensure that costs are distributed fairly across the market and that the financial model remains sustainable as we move toward the 2030 flexibility target.

Q26	Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.

We agree and support the implementation of a single, robust accreditation model for the CCS.

The five proposed pillars identity verification, user agreement, information security, data protection, and testing form the necessary foundation for any comprehensive accreditation process. The high level detail provided aligns with the rigorous checks we expect of any organisation before they are authorised to share sensitive consumer data.

The success of this model depends on its alignment with existing code body accreditation processes to ensure they complement one another. While providing a cohesive level of assurance and consumer protection is the priority, RECCo must also avoid creating costly duplication for market participants. We recognise that aligning these various frameworks could be a complex and lengthy undertaking; therefore, this alignment must be a central consideration in the development of the CCS MMP to ensure the timeline remains viable.

A significant area of concern is the apparent exclusion of the SEC Trusted Framework for "SEC Other Users." Currently, these users must comply with stringent SEC Section I (Privacy) and Section G (Security) requirements, which are independently audited. These SEC obligations, which must be passed before DCC access is granted, offer a degree of reliance and specialised assurance that the proposed ISO 27001 or Cyber Essentials Plus certifications may not fully replicate in an energy specific context.

We recommend integrating the SEC Trusted Framework to ensure the highest level of security. This integration should also streamline the process for existing energy market participants.

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.

While we agree that establishing a minimum security standard is essential for the CCS, the adoption of Cyber Essentials Plus or ISO 27001 must be accompanied by a clear and transparent vetting process for the accreditation providers themselves. These certifications offer a foundational level of assurance regarding information security and data privacy. However, their effectiveness as a regulatory gatekeeper depends on the consistency and reliability of the auditing bodies. We recommend that a formal "approved list" of accreditation providers be established to ensure that all CCS users are evaluated against a uniform benchmark, preventing any potential dilution of security standards across the ecosystem.

The consultation should explicitly address why the existing SEC trusted framework is not being considered as a viable alternative or complementary standard, particularly for SEC "Other Users." Many prospective CCS participants may already be subject to the SEC's technical and security governance, which is designed to support cyber security for those controlling load and accessing energy data.

Given that the SEC already provides enduring technical and security governance functions, leveraging this existing framework could prevent unnecessary duplication of compliance efforts for parties already operating within the energy sector's established security protocols.

The choice of security standard must be proportionate to the risks associated with the specific activities being undertaken. As the government aims for significant consumer led flexibility by 2030, the security requirements for CCS users should align with the broader "Clean Power 2030 objectives of maintaining grid stability and building consumer trust. Whether through ISO 27001, Cyber Essentials Plus, or the SEC Trusted Framework, the priority must remain the implementation of appropriate and proportionate technical and organisational measures to manage risks to security effectively.

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

We support the application of the existing REC change process to the management of CCS arrangements. As an established framework, the REC change process possesses the necessary robustness and technical rigor to manage the complex evolution of the CCS tool. Utilising this proven structure ensures that any modifications to the consent ecosystem undergo a thorough and transparent assessment, maintaining system integrity while adapting to emerging market requirements.

A significant benefit of migrating CCS management to the REC issues process and (CIG) is the opportunity for broader socialisation of future technical developments and background issues. Historically, the CCS has operated within a relatively closed environment within specific working groups. Transitioning to the REC framework provides a more open forum to engage with wider market participants.

It is essential that the REC defines a clear strategy for engaging with ATPs throughout this process. If these sessions remain restricted to traditionally registered REC parties, such as suppliers. The REC change process will ensure there is future proofing any approved changes to prevent the need for repetitive and costly modifications shortly after implementation. For significant or complex shifts in CCS functionality, we recommend the formation of dedicated working groups comprising all impacted stakeholders. This inclusive approach ensures a diverse range of input during the early drafting stages, providing the necessary depth of information for participants to impact, assess urgency and technical consequences effectively. By fostering this collaborative environment, RECCo can ensure that the CCS evolves in a way that is technically sound, cost effective, and fully aligned with the needs of consumers, suppliers and third party innovators.

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

We support the application of the existing REC performance assurance framework to the CCS arrangements. The current REC assurance process is well structured, providing the necessary pathways to progress non compliant parties through to Ofgem escalation and where necessary, recommending the removal of accreditation. We are comfortable that the established processes for measuring performance are sufficient; however, we must emphasise that the integrity of this framework depends entirely on the accuracy of the performance data.

There is a concern that the ATP market could expand rapidly, potentially repeating the poor practices observed with some TPIs. To prevent this, we recommend that REC use the principles set out in the Code Of Practice for Non-Domestic Third Party Intermediaries as a framework to develop a robust code of practice for ATPs. Longer term it would benefit consumers to use a full governance scheme that mirrors the fully licensed approach DESNZ has proposed for TPIs.

Compliance obligations for ATPs should be aligned with those of suppliers, DNOs and MEMs, specifically regarding the requirement to complete an annual maintenance and compliance statement as a minimum standard for participation in the CCS tool. These statements should be integrated into a mandatory self-assessment process, ensuring that any business changes common in agile ATP environments are formally declared to the Market Entry Assurance team via existing change processes.

The evolution of the assurance framework must also consider cross sector risk drivers, particularly those from the financial markets. Since consumers will likely enter into financial contracts with ATPs, it is vital that these activities are monitored with the same vigilance as those overseen by the FCA. This includes establishing a clear escalation route to the appropriate authority whether it be the ICO, FCA, Ofgem, or DESNZ to ensure there are robust consequences for parties that fall outside of traditional energy licensing.

REC issue I0189 was officially closed on the 25th February careful consideration must be given to any “voice of the customer” survey design, particularly as the service expands to include business consumers.

Any non compliance or performance concerns must be addressed with appropriate urgency. To protect the wider market, the costs associated with implementing remedial actions for specific performance failures should be borne solely by the non compliant company rather than being socialised among the wider users of the CCS tool. This financial accountability, combined with strong inter agency cooperation (such as engaging with the ICO for data specific breaches), will ensure a high standard of consumer protection and market integrity.

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

The proposed dispute resolution framework for the CCS requires significant strengthening to ensure it is fit for purpose.

While the technical issues outlined in the consultation cover the expected areas, their effectiveness is entirely dependent on the implementation of robust, real time reporting. We advocate for mandatory, high frequency performance data sharing to ensure all market participants remain confident that system issues are addressed with appropriate urgency. For ATPs, who may not be subject to the same regulatory rigor as licensed suppliers, this reporting should not be voluntary. To protect consumers against poor behavior, ATPs must be mandated to provide monthly reporting, mirroring the existing obligations for suppliers, with clear accountability for performance failures.

A significant concern remains with the "guest account" model and how it interacts with queried consent records and disputes raised by consumers. Without a clear account structure, there is currently no clear mechanism for a consumer to view, track, or query historical consent actions, which is a fundamental requirement for consumer protection. This complexity is amplified in scenarios involving houses of multiple occupation (HMOs) or changes of tenancy (COTs). A clear simplified process must be established to ensure consumers can dispute consent without being burdened by disproportionate evidentiary requirements.

Regarding the escalation of disputes, we disagree with the reliance on the energy ombudsman (EO) for addressing financial loss or contract specific grievances. The current challenges within the EO, specifically high workloads and inconsistent decision making suggest it is not the appropriate body to handle the specialised, often finance heavy disputes arising from ATP services.

It is essential that the EO, if appointed to resolve these outstanding consumer disputes, receives thorough and comprehensive training. Furthermore, the decisions made must be relevant and provide effective support to both consumers and the ATPs and EDPs. Given that ATP contracts are frequently based on financial products or projected savings, the Financial Ombudsman Service could be a more suitable investigator for assessing direct economic loss. This is particularly important since the ICO generally expects consumers to exhaust all complaint procedures before intervention. The current roadmap lacks a clear, unified consumer protection body to facilitate this for non energy supply issues.

The suspension of disputed consent is a necessary safeguard, but its execution must be seamless. If a consumer disputes a consent record, the service must be terminated or suspended immediately until resolution. However, without the ability through a guest account to trace access back to the correct individual the system risks failing to provide a transparent audit trail. To maintain trust in the CCS tool, we must ensure that the "voice of the customer" is not lost in a fragmented process and that the burden of proof for unauthorised data access does not rest unfairly on the consumer.

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?

While the draft roadmap provided in Annex G successfully identifies the high level pillars required for continuous improvement, there is a distinct lack of clear timelines or success criteria to underpin these developmental stages. For the program to remain viable, it is critical that the roadmap includes specific success metrics and "stop-go" triggers to ensure value is being added and that the cost of progression does not outweigh usage.

If a Guest account is developed for CCS, ID&V and guest to account consolidation should be in MMP Phase 1. The current proposal Phase 1 "guest account" with delayed consolidation leaves a significant gap in the consumer's ability to maintain a single view of their data permissions.

Having guest access without immediate consolidation capabilities compromises the core objective of the tool to provide a centralised "single source of truth" for consent. Aligning these features within the initial delivery phase is essential to ensure that all consents are accurately tracked and manageable from the very first interaction. By including this in the MMP, we can provide the "trust and confidence" required for consumer led flexibility and ensure that the digital experience is seamless rather than fragmented, thereby preventing potential confusion that could undermine long term engagement with the platform.

Ecosystem and Data Experience

This must be more tightly integrated with wider industry programs to ensure value for money and consumer safety. Specifically, delaying the tariff interoperability data set until a later phase risks fragmenting the consumer journey, as these large programs should be aligned to maximise potential savings.

We also seek clarity on how the SDR and SEC programs are coordinating to prevent the creation of redundant consent tools outside of the CCS framework and ATPs using the current SEC other user process to gain access to consumer data.

Finally, the governance and trust framework requires strengthening to ensure the tool is marketed and managed effectively. Cross code alignment and robust reporting should be mandatory requirements for entry in the MMP rather than voluntary, especially for ATPs not currently governed by supplier regulations, any governance framework reporting must be agile and adaptable to new licensing arrangements such as FSP and Load controller licence obligations due to be implemented in 2027.

Governance & Trust framework

We recommend a robust and mandatory reporting structure rather than a voluntary participation model. This is essential to ensure that all ATPs are held to the same rigorous standards as existing energy suppliers, particularly since many ATPs may not currently fall under the same regulatory oversight for complaint handling. Cross code alignment must be integrated into the MMP phase to ensure that the REC activities are fully synchronized with the existing obligations found in other industry code bodies.

A critical point of concern in the current draft is the designation of the energy ombudsman as the primary body for dispute resolution. The financial ombudsman service may be better positioned for this role, as the contracts between consumers and ATPs are frequently financial in nature, specifically focused on cost savings and product service agreements rather than traditional energy supply issues. There are ongoing challenges with the energy ombudsman's current workload, decision making and lack of consistency that could negatively impact consumer outcomes. The current ombudsman system is often burdened by high case volumes, leading to delays that could discourage consumers from engaging with new flexibility services. There is a risk that the energy ombudsman lacks the specific financial sector expertise required to navigate the complex, contract based disputes typical of the ATP landscape.

Communication & Transparency & Education

Establishing a foundation of trust through comprehensive communication and consumer education is the most critical factor for the success of the CCS. Currently, there is a significant gap in public awareness regarding the role of RECCo and the specific value proposition of the consent tool. To overcome this, the programme must deliver a clear, high level marketing strategy that moves beyond technical implementation to explain how the tool directly empowers the consumer. Without proactive education and transparent messaging, the platform risks being perceived with skepticism, which would stifle the adoption of the very flexibility services it is intended to enable.

Consumer trust is intrinsically linked to the clarity of the onboarding journey and the strength of the underlying governance. We believe that onboarding guidance should be directly integrated into the wider governance and trust frameworks to ensure a consistent and reliable experience for all users. Marketing efforts must focus on the tangible benefits of the tool such as ease of use, security, and the ability to unlock energy savings while reassuring consumers that their data is managed within a regulated, "level playing field" environment. Building this trust early is essential; if consumers do not feel confident in how their consent is tracked and protected, the initiative will struggle to deliver its intended benefits, regardless of its technical sophistication.

Transparency must extend to how the tool is monitored and evaluated against its original goals. Robust reporting and behavioral analytics should be part of the MMP to provide immediate evidence that the tool is delivering value and functioning as expected. By fostering an environment of open and co-operative engagement, and ensuring that the voice of the customer is captured as early as possible, the programme can demonstrate a commitment to continuous improvement. This level of transparency not only builds trust with individual users but also ensures that the industry parties funding the MMP can see a clear path toward a viable, long term digital ecosystem.

Additional Comments

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

Level Playing Field and Open Data Access

The move toward an "open to all" data approach must be carefully balanced to ensure a genuine level playing field between suppliers and new market entrants. While we support the principle of data transparency to drive innovation, it is critical that the regulatory framework does not inadvertently create a multi-tier market where certain entities benefit from data access without the corresponding service delivery obligations. A level playing field requires that all parties accessing consumer data are subject to equivalent standards of data hygiene and security, ensuring that competition is based on service quality and innovation rather than regulatory arbitrage.

Consumer Impact and Costs

A concern that remains unaddressed is the risk of a widening "digital divide" as the CCS transitions into a pay to use service. While initial phases focus on technical delivery, the long-term sustainability of the platform must prioritise inclusive design to ensure that all consumers regardless of their digital literacy or engagement levels can benefit from CCS. Without a clear framework for how the service is funded and accessed beyond the initial implementation, there is a significant risk that vulnerable or less engaged households will be excluded from the benefits of smart data while indirectly bearing the system's foundational costs.

The consultation must clarify how it will prevent a scenario where the most tech savvy consumers gain exclusive access to cheaper, data driven tariffs, leaving the less digitally enabled to subsidise the infrastructure through their standing charges.

As the model moves toward a transactional "pay to use" phase, we must ensure that the costs associated with data management do not manifest as "hidden" barriers to entry. True consumer protection in this space requires that the repository functions as a public good that empowers the entire market, rather than a specialised tool that primarily advantages a small segment of highly engaged users at the expense of the wider consumer base.

Licensing and Obligations for Authorised Third Parties (ATPs)

There is a notable regulatory gap regarding the obligations placed on ATPs compared to licensed energy suppliers. Currently, ATPs can access data via the SEC as "Other Users" without being subject to the same rigorous licensing conditions or consumer protection mandates that govern suppliers. Without a robust licensing framework for ATPs, there is a risk of fragmented accountability, particularly in instances of data misuse or poor consumer outcomes. We recommend a more stringent authorisation process that aligns ATP obligations with the high standards expected across the wider energy industry. Confirmation is necessary for new requirements for FSPs and Load controllers to sign up to the REC including all ATPs. Should they remain exempt there is a risk of fragmented accountability. Harmonising these requirements to ensure all parties accessing sensitive data must meet the same rigorous industry benchmarks to protect consumers and place the risk onto the data providers.

The current proposal for a centralised consent tool lacks a clear value proposition for ATPs who already possess the technical capability to access data through existing SEC channels. If ATPs can obtain data without being governed by a specific licence or obligated to use the new consent framework, the incentive to adopt the new tool is significantly diminished.

In the later phases of the CCS tool development, integrating the proposed Load Control (LC) licensing regime with the CCS tool creates a robust framework for consumer protection and market stability. By formalising the roles of Flexibility Service Providers (FSPs) and load controllers, the regulatory framework ensures that the shift toward consumer led flexibility is built on a foundation of trust and accountability. This licensing structure is specifically designed to protect domestic and small business consumers by mandating participation in the energy ombudsman's ADR scheme and enforcing TCF standards. These protections ensure that as consumers engage with automated energy management, they are provided with clear, accurate information and are shielded from high pressure sales or unfair exit fees the CCS tool can develop with these changes.

The proposed licensing regime further benefits the consumer by addressing technical risks that could otherwise lead to system wide disadvantages. By requiring load controllers to comply with rigorous cyber security standards and grid stability "load control checks," the framework mitigates the risk of unintended or adverse consequences to the electricity system. For consumers, this means a more resilient energy supply and the assurance that the data driven tools they use are governed by the same "fit and proper" and operational capability standards expected of traditional suppliers. Preventing misalignment of regulatory gaps resulting in third parties accessing sensitive data without the mitigations of a licensed entity.

These regulatory advancements facilitate a level playing field that encourages innovation while prioritising equitable access. As the market moves toward a "pay to use" model for the CCS tool, the licensing of ATPs and load controllers ensures that the infrastructure remains a transparent and interoperable resource. By mandating that only suitable services are recommended to consumers based on specific customer characteristics, the regime ensures that the benefits of flexibility are accessible to all, preventing a scenario where vulnerable or less engaged consumers are left behind in the transition to a smarter, more flexible grid.

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