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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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	Kevin Hammond
ORGANISATION	Octopus Energy
ORGANISATION CATEGORY	Large Supplier
E-MAIL ADDRESS	compliance@octoenergy.com
RESPONSE CONFIDENTIALITY	Non-confidential (recommended)

Questions

Scope of the CCS

Q1	Do you agree with the proposed MMP scope, including the core functional components and the inclusion of SEC Other Users and the BSC SDR?
We agree with the scope of the Minimum Marketable Product (MMP). Focussing initially on half-hourly metered data and specific Data Sharing Arrangements (DSAs) like SEC Other Users and the Smart Data Repository (SDR) is a sensible, risk-based approach to implementation.	
Q2	Do you have any comments on the assumption that SEC Other Users would not need to migrate existing consents to the CCS and would instead move to using the CCS as existing consents are renewed?
We support this assumption. Existing consents are limited in nature to the data processing activities agreed and consented to at the time consent was provided, which may not include use of data relevant to the CCS. Consents may also be time-bound, so establishing new consent records within the CCS as existing ones renew is a proportionate approach.	

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.
We strongly agree. Under the UK GDPR, the Data Subject for energy consumption data is typically the individual living at or occupying the premises, as they are the ones generating the behavioural data. Consent cannot be validly provided by off-site landlords or bill payers who are not the Data Subject.	
Q4	Do you agree with the position that for multi-occupancy households, a 'lead occupant' may provide consent on behalf of other occupants only where they confirm they have the authority to do so and have obtained agreement from all other adult occupants? If not, please provide your rationale.
We agree in principle, but advise caution regarding the liability model. The proposal requires the lead occupant to confirm they have the authority and agreement of other adults. From a UK GDPR perspective, consent must be freely given and unambiguous. The CCS must maintain rigorous, auditable logs of this "lead occupant" declaration to protect Energy Data Providers (EDPs) from liability if a co-occupant later disputes the processing. We welcome the proposed dispute mechanism where an unexpected consent can be automatically terminated.	
Q5	Do you agree with the proposed approach and standard for identity verification? *If not, please provide your rationale.*
We agree. Given the sensitive nature of half-hourly consumption data (which can reveal lifestyle and occupancy patterns), applying a high level of confidence for Identity Verification (IDV) is legally necessary. Aligning with GPG 45 standards and requiring initial verification via photo identification provides a robust safeguard against unauthorised data access.	
Q6	Do you agree with the position that consumers should have the option to establish an account with the CCS or grant consent via the 'guest' approach? If not, please provide your rationale.
We agree. Offering a 'guest' checkout approach aligns with the UK GDPR principle of Data Minimisation (Article 5(1)(c)), ensuring consumers are not forced to create accounts (and thus provide more personal data than necessary) simply to exercise their right to grant or manage consent.	
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. Article 7(3) of the UK GDPR requires that it shall be as easy to withdraw consent as to give it. Allowing revocation via both the ATP and the central CCS portal ensures consumers have maximum control and visibility over their active consents.	
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 proposal to check CCS for every data share is fine for sporadic API calls (every 15 mins for example), but it introduces challenges to high-frequency data streaming. We are concerned that it could introduce performance issues if the expectation is to do high-frequency data transfers. In which case, it may be preferable to consider a decentralised consent model as this could allow all entities to be more responsive to changes to consent. EDPs could store long-lived consent that is simply updated/revoked via the CCS, rather than a "ask-every-time" approach.	
Q9	Do you agree that if the CCS is unavailable, the EDP should continue to share data unless the CCS outage extends for a significant period of time? If not, please provide your rationale.
We disagree. The consultation proposes that if the CCS is offline, the EDP should treat existing consents as valid by default. From a legal and regulatory standpoint, this introduces a risk of processing personal data without a valid lawful basis. If a consumer withdrew consent shortly before the outage, continuing to share their data would constitute a personal data breach under the UK GDPR. We believe data protection and integrity must be prioritised over temporary service continuity; data sharing should pause during an outage. We suggest contingency plans ought to include a failover/skeleton system which would have access to current data, and some discussion of regular data replication to prevent data loss in the event of data deletion or outage (if all data were lost, we would have to assume zero consent).	
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.
We agree. Utilising FAPI 2.0 and mandatory mutual Transport Layer Security (mTLS) aligns with the UK GDPR Article 32 requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.	

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
We generally support the proposed architecture, particularly the reliance on a token model and an introspection endpoint. From a data protection standpoint, this architecture allows Energy Data Providers (EDPs) to verify consent validity immediately before data provision, which strongly supports our accountability under Article 5(1)(f) of the UK GDPR (Integrity and Confidentiality). We welcome that the architecture is designed to reflect a mature and well-developed approach.	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
We agree with the intention to use the Retail Energy Location (REL) Address, or alternatively the Meter Point Location (MPL) Address. However, we must stress that the accuracy of this matching API is paramount. Under Article 5(1)(d) of the UK GDPR (Accuracy), incorrectly matching an individual to the wrong MPxN would result in the unauthorised disclosure of another household's highly sensitive half-hourly data. We expect rigorous automated testing and validation of this matching capability before go-live. We are concerned that the energy sector has a history of data quality issues, necessitating error rectification procedures for problems such as crossed meters, MPxN/address mismatches, incorrect transfers, and discrepancies between plot and postal addresses. This flaw could result in one customer receiving information applicable to a different individual. Given the clear potential for widespread customer detriment and the resulting loss of confidence in the service, we must stress that mitigation for these data integrity and validation issues must be given further consideration and design refinement before any final implementation of the service proceeds.	
Q13	Do you have any comments on the non-functional requirements detailed within Annex D?
We support the focus on high availability to handle significant increases in demand. Furthermore, we strongly agree with the requirements ensuring data at rest is secure, specifically the use of Role-Based Access Controls (RBAC), Multi-Factor Authentication (MFA), encrypted backups, and ISO 27001 accreditation for the technical service provider. These measures are critical to satisfying Article 32 (Security of Processing).	
Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?

We support the hybrid model. By decentralising the actual energy data exchange directly between EDPs and ATPs , the CCS avoids the creation of a centralised "data lake". This approach embodies the principle of Data Minimisation and significantly reduces the systemic risk of a single-point-of-failure cyber-attack exposing millions of consumers' consumption habits.	
Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
While the high-level business process diagrams outlining consent management and onboarding are helpful, we recommend that future iterations explicitly map the Data Controller and Data Processor relationships at each step. The diagrams in Annex E mention "Data Provision" without clarifying the timeframe. Without knowing if we need to support 4-hour live data streams vs. one-off pings, it's hard to confirm if this solution is robust enough.	

UX Design

Q16	We have identified four groups of people who will use the consent system, each with different needs (Annex F – Behavioural Archetypes). Have we missed any important user groups? Are there any needs we haven't considered for any of these groups? If yes to either, please tell us what's missing and why it matters.
We note the inclusion of the four behavioural archetypes: Comfortable Data Enthusiast, Careful Budgeteer, Surviving Juggler, and Time-Poor Professionals. However, as a Data Protection Officer, I strongly suggest adding a "Privacy-Anxious / Safeguarding Consumer" archetype. This group includes individuals highly suspicious of data sharing, or more critically, those fleeing domestic abuse where data visibility (e.g., exposing property occupancy habits to a joint account holder) poses a physical safeguarding risk. Their needs for granular control and absolute privacy must be considered.	
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?
Yes, mandating alignment with WCAG 2.2 AA accessibility standards and ensuring clear, predictable patterns is a strong baseline. Furthermore, we fully support the requirement that where digital channels are not appropriate, assisted or alternative journeys must provide equivalent outcomes. Privacy rights must not be contingent on digital literacy.	
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. Providing clear information about who is requesting data, what is requested, and for how long is explicitly required to meet the "informed" and "specific" thresholds of consent under Article 7 of the UK GDPR, as well as the transparency requirements of Articles 13 and 14.	
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)
Positive friction is necessary during the initial Identity Verification (IDV) stage to ensure the individual is the rightful occupier (Data Subject). However, negative friction must be strictly avoided when a consumer seeks to revoke consent. Article 7(3) of the UK GDPR dictates that it must be as easy to withdraw consent as to give it.	
Q20	Do you agree that showing consumers which organisations hold consent, what data is shared, when consent was granted, and when it expires provides adequate visibility? If not, what's missing? What limitations should be communicated to manage expectations?

We agree. Allowing consumers to view active consents, the purpose of access, and the ATP accessing the data provides excellent visibility. It effectively operationalises the consumer's Right of Access (Article 15) and fosters trust.	
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. Explaining the immediate and longer-term consequences of revocation, including the impact on dependent services, ensures the withdrawal of consent is fully informed. The process must ensure revocation is straightforward and as easy as granting consent.	
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. Every Data Subject has equal rights under the law; therefore, assisted journeys must provide equivalent outcomes to digital journeys.	
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?
An assisted journey (e.g., via a customer service telephone line) must allow the consumer to achieve the exact same legal outcomes, granting, reviewing, and revoking consent, with the same speed of operational effect as a digital user.	

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 creation of a dedicated CCS Arrangements Schedule. We particularly welcome the commitment to clarify the boundary between CCS obligations and the obligations that sit with individual EDPs. This clear demarcation of liability between Central Services, Controllers, and Processors is essential for our legal compliance frameworks.	
Q25	Do you agree with the proposed initial funding model, including the ability for the cost of qualification and breach investigation activities to be recovered from the individual organisations? If not, please provide your rationale.
We agree with the transition to Hybrid Model B following the initial MMP delivery, where base costs are recovered centrally but individual costs for assurance activities (like qualification audits and breach investigations) are paid by the specific users. This correctly incentivises compliance and ensures that organisations with poor data protection practices bear the financial burden of the resulting investigations.	
Q26	Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.
We agree that a robust accreditation model is vital.	
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.
Mandating Cyber Essentials Plus or ISO 27001 provides a solid baseline. Furthermore, we strongly support the requirement for all CCS Users to undergo a full REC data protection assessment prior to accessing the ecosystem.	
Q28	Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?
We are concerned that the existing REC change process may mean that changes are proposed by parties in the future which erodes the data sharing safeguards and risk mitigations for the CCS.	

Q29	Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?
No comments.	
Q30	Do you have any comments on the proposed issue/dispute resolution paths defined for the management of CCS issues?
We agree with the proposed dispute resolution path. Automatically terminating consent and pausing data processing when an unexpected consent is disputed by a verified matched consumer aligns with the consumer's Right to Restriction of Processing under Article 18 of the UK GDPR.	

Product Roadmap

Q31	Do you have any comments on the approach to defining the future roadmap within the consultation or the content of the draft roadmap in Annex G?
We note that there is no explicit discussion or quantification of the consumer demand for the consumer consent solution.	

Additional Comments

Q32	Please provide details of any additional issues you feel have not been adequately captured within the consultation document.
We have reservations about the growing complexity and subsequent cost to consumers.	

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