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 Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or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** | Emma Johnson |
| **ORGANISATION** | Centrica |
| **ORGANISATION CATEGORY** | [OrgCategory] |
| **E-MAIL ADDRESS** | Emma.johnson5@centrica.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? |

CORE FUNCTIONAL COMPONENTS
We agree with the core functional components listed in 4.5 and 4.6 for the MMP scope.

SEC OTHER USERS
We remain nervous around the approach to SEC Other Users, and the CCS's proposed approach to data accessed through the DCC Other User route. We believe the DCC (as gatekeeper to the individual meters) should be the Energy Data Provider, rather than SEC Other Users. This is for a number of reasons, as follows:

1. Not all SEC Other Users will sign up to the Consumer Consent Solution, given its voluntary status. This will never reach the "single view of the truth" within the original Ofgem (and Citizen's Advice) ambition.

2. The Consumer Consent Solution will not provide a solution for a company acting as their own SEC Other User, rather than through a third party. This seems to be a major gap, even for MMP.

3. Positioning the SEC Other User as the Energy Data Provider limits the ability for third parties to change their SEC Other User should they wish to do so, as their consent permissions will be for "DCC HH data accessed through SEC Other User X", rather than for "DCC HH data". This could have some significant commercial implications, in effect allowing SEC Other Users to increase their charges unchallenged, as it is too complex for their third party customers to switch and recollect all consents for the new SEC Other User.

4. SEC Other Users are not regulated, and offer a commercial service to their third party customers. As such, it seems inappropriate for the Consumer Consent Solution to provide them with a free service, paid for across all Suppliers. This would feel different were the DCC the EDP.

5. The current proposed structure strengthens the value creation for SEC Other Users over time, but puts additional costs on consumers – through necessary cost pass through by Energy Suppliers (to all consumers), and ATPs (to their customers).

We think the DCC should become the Energy Data Provider, although the SEC Other Users should manage the access tokens. Consents should be transferable between SEC Other Users.

BSC SDR
We do agree with the scope including the BSC SDR.

| | |
|---|---|
| **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? |

It must be made clear to consumers that the Consumer Consent Solution will only show an incomplete list of their consents.

However, we do agree with the proposal that existing SEC Other User consents should move to the CCS as existing consents are renewed. Any alternative solution is too disruptive.

Do all SEC Other Users use the same timeframe for renewing consents? We would be concerned if some took much longer than others.

If the CCS project is successful, we believe there should be a date by which all SEC Other User consents are included within the CCS. This would be possible with changes to the legal text in SEC Section I.

## 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?<br>If not, please provide your rationale. |

Ideally this would be the situation, but in practice, it is extremely complex to implement, and could introduce as many issues as it solves, especially with regards to proving residence.

We don't think you will ever reach the situation where you can guarantee consent from all occupants over the age of 18 years old, in all properties. It is impractical and unachievable.

We think it is more important for the CCS MMP to be launched with customer consent (bill payer consent) with a solution that works for 95%+ of properties.

This could be combined with a broader consumer awareness exercise – perhaps led by Citizen's Advice or SEGB.

Please note, the obligation to get occupier consent only applies to third parties accessing the meter data. Rightly or wrongly, as an Energy Supplier, our licence obligations for consent to access HH metered data are with the customer / bill payer.

In 5.4 you reference the September 2017 BEIS letter. The status of this document is a distraction. It is a nine year old letter, representing expectations of a prior team under a prior government, and – today – hidden within the depths of the SEC News section (where very few people know of its existence). It was never enacted into the Smart Energy Code legal text, or SEC Other User onboarding/assurance processes. If it is the expectation for its contents to be mandatory, it needs to be brought into the Smart Energy Code, and SEC onboarding arrangements.

| | |
|---|---|
| **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?<br>If not, please provide your rationale. |

This seems a sensible approach, although there should be consequences for any mis-use, if challenged.

As soon as it is a multi-occupancy household, the HH data is still personal information, but aggregated for all occupants. This slightly reduces its sensitivity.

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

We don't agree with RECCo's interpretation of the GPG 45 guidance. We do not believe it should require a 'high confidence' level of IDV to access HH consumption data, especially when this introduces a practical barrier to some less-digitally accessible consumers.

We note that there is a tiered approach to the NHS interpretation of GPG 45, with only 'medium confidence' required in order to access services such as ordering repeat prescriptions, arranging appointments, viewing vaccination records, etc - unlocking most of the NHS App's functionality, without the requirement for photo ID. 'High confidence' IDV is only required in order to access the most sensitive information on a patient's medical profile.

HH consumption data feels closer in sensitivity to these 'medium confidence' service categories. It is said that HH consumption data can show patterns of occupancy (ie is someone away?), but equally so can viewing their social media posts, or – literally – seeing if their car is still parked on the driveway.

More importantly, within the NHS, if a customer can't access digital photo ID based IDV, there are face to face alternatives: a customer can turn up in person at their GP Surgery. There isn't this alternative for the CCS.

We are also very concerned about the introduction of a principle that photo ID based IDV will be necessary in order to give permission to access HH data, especially if this were to be extrapolated to Energy Supplier consents in the future. This could result in customers only being able to access a Time of Use tariff (which would need the customer/bill payer to agree to share HH data for billing) if they were prepared to undergo photo ID based IDV. This could considerably discourage uptake of some of the newer tariff products (Time of Use tariffs, and credit products such as Peak Save), undermining a lot of the benefits expected to be associated with schemes such as MHHS, and separately risking longer term uptake of consumer-led flexibility

services.

We would be even more concerned if Energy Suppliers were required to seek photo ID based IDV of other occupants, in addition to the bill payer.

We do agree with the proposed choice of IDV service providers, so a customer can choose one they are comfortable with, although we recognise that a choice of IDV service providers might not be possible for MMP launch.

| | |
|---|---|
| **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?<br>If not, please provide your rationale. |

We are not comfortable with the 'guest account' approach, especially as part of the success of the CCS will depend upon its usage becoming widespread, and it including information on all consents. If the data sharing is challenged by another 'consumer' at that address, there also needs to be a way for the CCS to contact the person who has given consent. This is much simpler if there is a CCS account.

However, it is important for creating a CCS account to be made as low friction as possible. Could the account just be email based, rather than email/user name & password? The login journey could send a link (or confirmation code) to the email address each time, rather than requiring the customer to remember yet a further user name & password.

| | |
|---|---|
| **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?<br>If not, please provide your rationale. |

There must be a way of doing this through the CCS account. The customer may have wider issues contacting the ATP (one of the reasons they may be revoking consent is because they are unhappy with the ATP's services). The customer may also want to go onto the CCS site to double check the consent they removed has definitely been withdrawn.

However, we are happy for consumers to have the choice of also doing this through the ATP, where the ATP has put this functionality in place. In this case, there would need to be clear guidance in the CEGs for the correct wording and process, etc.

| | |
|---|---|
| **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?<br>If not, please provide your rationale. |

In principle we agree with this, but we are concerned that it may impact latency.

Would an alternative be for each token to have an expiry time, of say 48 hours? Then repeated requests (daily, or more frequently) wouldn't need a token every time, if an active token were still in place. It would mean that it could take up to 48 hours to revoke consent, but that seems reasonable, particularly if it had

| | |
|---|---|
| broader system benefits and wider cost savings. It would also allow any short downtimes of the CCS to be accommodated. | |
| **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?<br>If not, please provide your rationale. |
| See our response to Question 8 above. | |
| **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?<br>If not, please provide your rationale. |
| Yes – we agree with using the existing FAPI 2.0 standard, including the use of mTLS for all data sharing. | |

## Technical Design

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

OVERALL SOLUTION ARCHITECTURE
Paragraphs 6.5 to 6.7, and the accompanying diagram (Figure 1: CCS Solution Architecture) seem reasonable as a technical solution to meet the specified functional requirements. We look forward to commenting on the next level of detail, once it is available.

CONSENT MANAGEMENT SYSTEM
The proposals in 6.8 to 6.13, including the two accompanying diagrams (Figure 2: Consent Mechanism and Figure 3: Secure Trust Framework) seem reasonable. Depending on the responses to Question 9 above, you might want to add an 'extra time buffer' to the 4th bullet under 6.8, to allow data sharing to continue for a limited period of time, if the CCS system goes down.

We welcome 6.14's additional security requirements for 'data at rest', in addition to 'data in transit'. This all seems reasonable and appropriate.

USER INTERFACES
We are confused by the references to white-labelling a CCS portal in 6.15. To avoid customer confusion, and ensure customers recognise its central (RECCo?) ownership, we consider the CCS portal should only be delivered under one single brand.

We do not agree with the 1st bullet point under 6.18, regarding ATPs being able to recreate their own version of the portal. The portal should be recognised as a central independent platform.

Regarding the 5th and 6th bullet points under 6.18, we consider it very unlikely that consumers will remember to notify the CCS when they are moving out of a property. A customer may only do this when they choose to set up new energy data services for their new home, and even then may not remember to cancel their previous address permissions.

The high level Admin Portal proposals in 6.19 seem reasonable. We assume that an EDP will be able to see all consents related to their data provision, and to download aggregated MI reporting on this, in order to manage their own reporting and internal management? If not included, this should be added.

DIRECTORY / REGISTRY
The principles in 6.20 to 6.22 seem sensible in general, although we had a few questions:

What is the difference between the Directory and the Registry? We were confused by the 2nd and 3rd bullet points under 6.20.

Will all ATPs be able to access information on all EDPs, even where they are not actively contracting with that EDP? This would be useful for ATPs to understand what data may be available from more than one source.

IDV SERVICES
As detailed in our response above to Questions 3, 4 and 5, we disagree with the need for 'high confidence' IDV, and are concerned by the complexities surrounding such photo ID based IDV proposals, which we do not think are necessary.

We are also very concerned by the potential future expansion of any photo ID based IDV requirement to Energy Suppliers, and the broader implications for uptake of HH based tariffs and services.

We agree with the proposed choice of IDV service providers, so a customer can choose one they are comfortable with, although we recognise that a choice of IDV service providers might not be possible for MMP launch.

We believe that the potential for federated IDV solutions outlined in 6.25 may be useful in the future, but agree it is a level of complexity too far for MMP.

ENQUIRY SERVICES
See our answer to Q12 below.

REC PORTAL
The proposals seems sensible. This presumably will also align with registration as an RTI User for tariff interoperability.

TESTING / MONITORING
The testing proposals seem sensible – in particular the sandbox testing, pre-production testing and potential 'live' testing outlined in 6.33.

Some of the monitoring and reporting proposals seem complex for an MMP (see 6.42 for example), but we recognise are standard for any modern cloud setting. We expect these to happen seamlessly in the background, with minimal demands on new EDPs and ATPs, as they commence their testing and usage of the

CCS. We agree with the principle in 6.38 and 6.39 of using automated monitoring wherever possible.

We presume any commercial confidentiality (eg EDP or ATP company names) will be kept appropriately confidential, within data shared with Ofgem and other regulatory bodies (see 6.36).

Should be a grace period be considered before REC PAF intervention (see 6.40), where more informal adjustments could be corrected, rather than entering into detailed assurance, escalation and enforcement from day 1? The proposals in 6.40 seem very onerous for companies who may be trying to get to grips with a new consent operating system.

The Proposed Monitoring outlined in Annex D does not cover the volume of token linked data exchange for individual EDPs – ie information on which EDPs are providing data linked to the CCS in large volumes, and where is usage much lower. This would be interesting information, and could show where the CCS MMP was seeing most usage – ie were most ATPs seeking information from the new SDR, or from the existing SEC Other Users route.

SERVICE DESK
The service desk proposals in 6.46 (specifically for 24/7 x 365 support availability for P1 issues) sound expensive, for the early days of an MMP, particularly when initial take-up may be low. We presume this service support be integrated into other Service Desk support within RECCo's operations, to enable efficiencies and flexibility?

NON-FUNCTIONAL REQUIREMENTS
We agree with the need to design a scalable system. However, longer term demand for the CCS is not proven, and may take many years to materialise. For example, if only a minimal number of SEC Other Users choose to voluntarily use the scheme, and if there are delays to the SDR. There are potential parallels with the 2012 Green Deal framework which never met the target volumes, but left an expensive collections arrangement that needed ongoing funding and delivery through to the late 2030s.

Does RECCo have access to DCC data (or can RECCo request it) on the number or proportion of DCC enrolled meters that are today being accessed by SEC Other Users? This would be an interesting benchmark for the reference in 6.48 to the CCS having "the potential to grow into a solution meeting the needs of a significant portion of the UK population", especially if the future requirement for photo ID discouraged consumers from enabling energy data sharing.

| | |
|---|---|
| **Q12** | Do you agree with the proposed approach to matching MPxN to the address?<br>If not, please provide your rationale. |

The proposals in 6.26-6.28 seem reasonable for residential customers. If (as suggested in 6.28) it isn't possible for the REL Address to be accessed in time for MMP delivery, we agree with using the Meter Point Location (MPL) Address as an alternative, providing there is a work around route for any inaccuracies.

There needs to be a work around solution for any inaccuracies, regardless of which address matching system is used. There also needs to be a solution for cross-meter issues, which may be particularly common in new build properties.

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

Please see our comments on Non-Functional Requirements in our answer to Question 11 above.

The additional detail on Non-Functional Requirements in Annex D looks sensible in principle. Under 'Data Retention', how does the retention of consumer data received by ATPs operate alongside any customer request "to be forgotten"?

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

TOKEN PROVISION AND LEDGER - centralised
This needs to be centralised, in order to support the original 'Option One' vision for consumer consent, including a 'single view of the truth' centralised portal.

IDV – centralised
We do not think it is practical for Suppliers' individual IDV processes to be used to support the Consumer Consent Solution – especially when the Consumer Consent Solution is acting as the gateway to energy data that is not accessed through the Supplier. We therefore agree that IDV for setting/amending third party data sharing permissions should be centralised.

However, for the avoidance of doubt, we do not agree with Suppliers being required to use a centralised IDV solution. The CCS should not be overriding how Suppliers manage their customer relationships and meet the requirements for those relationships in their Supplier licences.

DATA SHARING - decentralised
We agree that energy data exchange should be direct between EDPs and ATPs, not via the central CCS technical solution, subject to that data exchange meeting minimum CCS-dictated technical requirements.

You ask specifically for comments on Annex D - Figure 1 Decentralised data sharing in Annex D.

We are nervous about the Commercial Third Party dotted line, in the bottom left of the diagram. The consumer's primary relationship needs to be with the ATP; the ATP should be the entity providing the customer with a service, and the customer should know that the ATP is the entity they need to contact for any changes of consent, complaints, details of home move, etc.

As currently drawn, the Commercial Third Party dotted line potentially(?) opens up the opportunity for SEC Other Users-type organisations to establish a similar unofficial intermediary role around the Elexon SDR, which we didn't believe was the policy intent, and which we don't believe is in consumers' best interests, especially if it reduced the protection offered to consumers by the CCS, by moving that data sharing outside of the CCS control boundary. We would be happy to discuss this further if helpful.

DATA FORMATS & STRUCTURES - hybrid
We agree with the use of the Energy Market Data Specification (EMDS). We agree with the benefits for standardised data formats and structures where appropriate.

We are nervous about your statement that 'ATPs and EDPs [will be] free to format structure data as they wish'. We don't believe a strong ATP should be able to demand bespoke data structure arrangements from EDPs. Especially where an EDP's data sharing is mandatory (for instance for Suppliers with tariff interoperability), there needs to be a standardised data format.

DIRECTORY / REGISTRY - centralised
We agree with the need for a centralised directory and registry. We are confused by your reference to bespoke commercial agreements, and the need for such arrangements to be approved by RECCo. What sort of agreements do you mean? How will RECCo approval work?

DATA STORAGE – hybrid
We agree that energy data itself will not be stored centrally.
We understand Annex D to mean that the CCS will be required to store consent records (both current, and previous), and CCS Users will also be required to store and manage a parallel copy of these consents. If the details differ, which source of information will be confirmed as the correct one? And by CCS Users, do you mean just ATPs, or also EDPs?

Should EDPs also be required to keep a record of who accessed information from each meter and when? This could be useful, especially if there was concern about access to a certain meter's data, perhaps if that data was then onwards shared with other parties, that the customer had not consented to, and there was an investigation.

USER INTERFACES – centralised
We disagree with your hybrid proposal. Even if a consumer considers they may wish to use only one ATP for all of their services, and thereby interact solely with that provider, this may cause issues. For example, if there is consent access to their energy data from another ATP (for example, if the customer has forgotten about something else they signed up for, or if another consumer linked to that address has given data sharing permission), how will the customer see this? One ATP should not be able to see consents that the consumer has granted to other ATPs. So either the ATP's version of the CCS portal will be incomplete, or it will have access to information that should be prohibited.

Information on which other ATPs have also got consent from a customer will be valuable information commercially. For example, if an energy management service can see that a customer is already signed up to a number of different price comparison websites, it may choose to offer that customer a better price versus a customer who does not appear to have shopped around.

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

In Figure 5, will a prospective ATP need to become an actual ATP before they are able to view the Directory / Register? What about new third parties wanting to understand what data may be available?

In Figure 6, the Consumer<-ATP box seems wrong, particularly the first bullet 'Discover and display available data & lexicon from Directory'. A consumer would expect the ATP to focus on what product or service it could offer, not for the ATP to act as a sort of shop-front for data access.

We have struggled to read Figures 7 to 13.

# 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?<br>If yes to either, please tell us what's missing and why it matters. |

We are confused by Section 7 of the consultation document. What exactly is the UX framework (referred to in 7.2 and the first column of Figure 5)? And, what are the four personas to be used for? 7.11 seems to imply that the personas have already done their job in informing the UX framework, but we would expect them also to be used for testing the customer journey once it develops. Have they already been used for the design of the flow charts in Figures 7 to 10?

We are not convinced by the choice of photos for the four personas in the consultation document. The low-income profiles are both shown as female, and both described as not liking complex tasks or services, whereas the Comfortable Data Enthusiast is assumed to be male. This doesn't quite feel right.

There are a couple of other persona we think should be considered:

It would be worth considering the journey from the perspective of an elderly person, potentially with early stage (undiagnosed) Alzheimer's, or potentially just not understanding how technology and services are changing. The first sign that something wasn't right with my Aunt (in her early 70s) was when she started just clicking 'yes' to everything, and ended up inundated with letters from charities or less respectable schemes all trying to get further financial donations from her, some clearly fraudulent. Practically, someone like this may already be relying on a third party (charity, adult child or trusted neighbour) to help them with something like energy bills and consumer consent.

We also think you should include a category for the small minority of people who may have very good reasons to be sensitive to data being leaked or accessed unlawfully – for example, someone who might recently have left a domestic abuse relationship. In this case, their ex partner may already have copies of their driving licence and passport, and other identity information..

| | |
|---|---|
| **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? |

Licensed parties will already have extensive accessibility features, under their obligations to treat customers fairly, but this may not be the situation for all ATPs.

We agree with the principle of the Customer Experience Guidelines (CEGs), but we aren't clear from the consultation and discussions to date how enforceable these may be. In many cases, ATPs will not be subject to wider controls and authorisation.

Your proposals in Annex F under 'Accessibility and device constraints' are sensible, as far as they go, for outlining the requirements for ATPs and their CCS interfaces. However, you will need higher standards around accessibility and vulnerability for the central Consumer Consent portal, matching those provided by licensed energy suppliers.

| | |
|---|---|
| | A vulnerable customer struggling to access the Consumer Consent arrangements digitally may (reasonably) wonder why they can't just phone their Supplier to give them verbal permission to share their data. Could this be considered in certain circumstances for later iterations of the Consumer Consent Solution?<br><br>Please also see our answer to Question 22 below. |
| **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? |
| | Consumers need to know what that data will be used for. For example, will it just be used to show their usage patterns, or might it also be sold on to third parties, potentially for marketing purposes.<br><br>Consumers need to know over what timeframe is data being requested. I.e., is it past historic data, or just data from now onwards, or both.<br><br>Consumers may also need help in understanding company names they may not recognise. For example, if they are signed up to the Loop app, they may not recognise the name Trust Power Limited (the legal owner of Loop) or Procode Technology Limited (the legal entity accessing their data). |
| **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) |
| | Figures 7 to 10 already look relatively complicated, and they don't yet include the 'are you the bill payer or the consumer' dialogue.<br><br>Step 1 "Giving consent" in Figure 7 is slightly misleading, as it talks about an organisation needing to access your half-hourly smart meter data, rather than half-hourly consumption data. However, as discussed in our answer to Question 32 (EXPORT DATA) below, this is interesting. Even though the status of half-hourly export data is not confirmed as personal data, it would be useful for the consumer to be able to give permission for 'half-hourly smart meter data' more generally – thereby including both import and export data, as appropriate.<br><br>Step 7 "Seeing active consents" in Figure 9 is a bit misleading. This won't include all consents, just those consents that have been set up within the Consumer Consent Solution. The fact it is a limited list needs to be made crystal clear.<br><br>We wonder if excessive use of consumer consent granting might somehow be checked. For example, if a customer signed up to 20 third parties accessing their data, should that trigger some sort of check for vulnerability – possibly from the Supplier or DWP, especially if it turned out there were other flags of vulnerability. Note – Energy Suppliers do have a duty to monitor for vulnerabilities, even if the ATPs or EDPs do not. |
| **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? |

If the Consumer Consent Solution is positioned as including all third parties who hold consent, then it is important for it to show a complete list. If it will not be able to show a complete list, this needs to be made very clear.

The consent granting also needs to show basic categories of what that data can be used for.

If the customer starts receiving unsolicited offers for solar & battery (for example) that have clearly been based on their actual HH Consumption Data, they need to be able to understand which of their list of third parties is using their data for third party marketing.

It should be clear in UX that removing consent will not delete the data that the ATP holds (and has already received).

| | |
|---|---|
| **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 presume this question relates to revocation of consent. If so, it sounds sensible.

It needs to be made clear that any revocation of consent under the CCS can not get back information already shared with third parties. It can only stop further information being passed to that third party.

In terms of reversibility, in later iterations of the CCS (post MMP), could revocation be put in a temporary bin, allowing the consumer to reverse their revocation request if they wish within 30 days. This could allow customers to promptly reinstate consent, if they accidentally – eg – stop energy data sharing with their heating controls provider.

| | |
|---|---|
| **Q22** | Do you agree that assisted journeys should enable consumers to grant consent, review active consents, revoke consent, and receive the same information as digital users? If not, what additional outcomes are needed to achieve equivalence? |

Yes we agree with this in principle. However, the need for an ATP assisted journey for consent will depend on whether the ATP offers an assisted journey for its product offering already, or whether its service is already digital only.

If many ATPs (eg price comparison websites) only offer digital customer journeys, then it is reasonable to assume that automated assisted consent journeys won't be necessary, at least for the lower volumes anticipated for MMP. A manual workaround could be used for MMP, with an enduring assisted journey built later.

Assisted journeys will be needed for the central CCS portal.

| | |
|---|---|
| **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? |

See answer to Question 22.

# 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? |
| It seems sensible in principle.<br><br>We are not sure of the legal standing of the Customer Experience Guidelines, and how its use will be enforced.<br><br>We agree that there needs to be a new CCS Arrangements Schedule, and accompanying CCS Service Definition and CCS API Technical Specification.<br><br>Should EDPs be made to become REC parties – especially those sharing data under "Market Governed DSAs"? | |
| **Q25** | Do you agree with the proposed initial funding model, including the ability for the cost of qualification and breach investigation activities to be recovered from the individual organisations? If not, please provide your rationale. |
| We are concerned about the number of data and flexibility related schemes which are being funded by Suppliers – especially as this puts extra costs on all consumer bills, including those of customers who will not be using the services that benefit from these schemes. This seems to run counter to the current broader focus on reducing energy bills. We are concerned that Suppliers are being seen by government effectively as a 'blank cheque book' for data sharing initiatives, which will result in increases to customer bills, and that the aggregated cost of all of these schemes is not being recognised.<br><br>As already expressed in our response to the draft Consumer Consent IA (November 2025), we do not believe there is a robust business case for the CCS.<br><br>A free to use CCS for ATPs and EDPs may also result in certain distortions, where because the ATP or EDP makes no contribution to the CCS costs, they are not incentivised to always access it in the most cost-effective manner. (Caching requests, etc.)<br><br>We do agree with your proposal of Hybrid model B. These will be costs directly associated with ATPs and EDPs, and as such should be borne by those customers. We would also prefer to see the Hybrid model A elements included as soon as appropriate.<br><br>We agree with taking a similar approach to the Gas & Electricity Enquiry Services.<br><br>Finally, forecast costs for the scheme need to be as accurate as possible, in order to not retrospectively impact future price caps. | |
| **Q26** | Do you agree with the proposed CCS Accreditation model?<br>If not, please provide your rationale. |

| | |
|---|---|
| Does there also need to be a requirement for financial stability or credit cover?<br><br>Would you also expect there to be any requirement to show the ATP was responsible towards consumers in general. Ie – no red flags, such as low Trust Pilot scores for existing services, or a significant number of CCJs. This feels potentially in scope, considering Figure 13 (Why the CCS requires robust accreditation) in paragraph 8.41.<br><br>For an EDP would you also check with other Code PABs for any existing compliance concerns (eg if a SEC Other User had a history of challenging compliance issues under the SEC Privacy Framework already). This might be a broader compliance requirement for EDPs sharing data under "Market Governed DSAs" (as defined in 8.37). This might be included within the measures you suggest in 8.53.<br><br>Is it possible to share more information on the "existing risk-based assessment mechanism" mentioned in 8.48, and how this would be applied to different types of EDPs or ATPs?<br><br>In paragraph 8.50, have you considered how the approach might also work for Load Controllers wanting to become ATPs, alongside their Load Control licence application? | |
| **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?<br>If not, please provide your rationale. |
| This seems reasonable. | |
| **Q28** | Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements? |
| We presume that ATPs and EDPs won't have voting representation in the REC Change process, but this could be managed through the engagement you mention in 8.34. Does 8.34 also need to include engagement with the ICO, and/or other Industry Code committees (such as the SEC Privacy Sub Committee) where the ICO is also sharing advice?<br><br>Also see our comment in Question 24 above, as to whether EDPs be made to become REC parties – especially those sharing data under "Market Governed DSAs". | |
| **Q29** | Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements? |
| In principle this seems sensible. However the requirements should not be excessive (especially during the MMP stage when all parties may face teething issues), and the SEC Other User aspects may need alignment with the SEC privacy assurance team.<br><br>What will be the legal status of the CEGs (Customer Experience Guidelines) for ATPs – will these be mandatory or non-mandatory, or a mix? Will ATPs need to demonstrate compliance with all elements? | |

How far will REC's performance assurance framework extend? For example, if an ATP has said they will not sell energy data forwards, nor allow the energy data they collect to be used for marketing purposes, but then do carry out these activities, how will this be handled? If there is proof or suspicion that the ATP is not being honest with consumers and the consumer consent process with their use of the data, will this be considered by REC's performance assurance team, or ignored as 'out of scope'? This seems to be important, to ensure consumer trust.

Finally, we note that the bullets in 8.58 only seem to specify ATPs, not EDPs. Is this correct? We would assume that both needed to be covered by performance assurance – especially EDPs sharing data under "Market Governed DSAs".

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

It is important for a robust presence from the RECCo CCS team with regards to disputes.

We suggest holding a series of workshops to talk through specific example issues, understand where the consumer may be left at unacceptable detriment, and agree alternatives.

TECHNICAL ISSUES
The principles shared on Technical Issues seem sensible as a starting point. We presume there will be appropriate availability and response time SLAs. It will be particularly important for some use cases.

QUERIED CONSENT (CONSENT GRANTED BY THE INDIVIDUAL CONSUMER)
In the first instance we would expect consumers to use the CCS to remove any consents they did not recognise. However, we are concerned by paragraph 8.69 and 8.70, which relate to more complex concerns, and where the consumer will need to access the ATP for any more concerning enquiries on incorrect consents.

If an underperforming ATP is perhaps not offering the clearest or best customer experience (which may have led to the concern or an incorrect consent), it is unlikely to be particularly good at dealing with complaints.

We would expect the RECCo CCS to offer an escalation process, for a number of reasons:

1. RECCo and the CCS are authorising ATPs (literally – it is an Authorised Third Party), and do need to take responsibility or action of those ATPs are not acting correctly, for individual consumers.

2. The proposed escalation to the ICO seems impractical – they are not set up to assist with individual requests, and will not understand the practicalities of the CCS framework.

3. In the absence of a RECCo CCS escalation process, complaints will come to the Energy Supplier, and yet we will not be in a position to assist. As the Energy Supplier, we will have no authority over either the SDR or the SEC Other User access framework, nor the CCS or any ATPs.

QUERIED CONSENT (CONSENT NOT GRANTED BY THE INDIVIDUAL CONSUMER)
The principles proposed here seem sensible as a starting point. We wonder (8.72, 8.75) whether it might be better to Suspend access, pending investigation, rather than Terminate access. I am also not sure about the scenario where the consent is needed in order to deliver flexibility services around assets (for example

| |
|---|
| charging or discharging a battery, owned by the landlord in a rental property).<br><br>How will 8.78 (requiring ATPs and EDPs to report any ICO data breach referrals to RECCo) work in practice? How does this align with the recent SEC requirements – SEC mod MP283 Data Breach Reporting? |

## 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 had the following comments on the draft roadmap in Annex G:<br><br>CONSENT LIFECYCLE MANAGEMENT - EXPORT DATA<br>You have listed "Consent for Export/Generation Data" in the third column ("Later"). While this may be right for standalone export/generation consents, would it be possible to include export data with HH consumption data earlier?<br><br>We note that the customer journey examples in Section 7 refer to domestic "half-hourly smart meter data", which would be taken as covering import meter data, as well as any export that might be happening. There is uncertainty at the moment as to whether export data is personal data or not, with some conflicting advice coming from the ICO. If a customer had given permission to share it anyway, it wouldn't matter whether it were personal data or not. This is particularly significant with the governments increasing ambitious for domestic solar, and consumer led flexibility.<br><br>Put simply, could the MMP be for "half-hourly smart meter data", rather than "half hourly consumption smart meter data".<br><br>GOVERNANCE & TRUST FRAMEWORK<br>We would expect this to include when a more enduring funding model (user pays) might be considered – at least mentioned in the third column ("Later").<br><br>COMMUNICATION, TRANSPARENCY & EDUCATION<br>Assuming the CCS project is successful, we believe there should be a date by which all SEC Other User consents are included within the CCS. As mentioned in our response to Question 2 above, this would be possible with changes to the legal text in SEC Section I. | |

## Additional Comments

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

EXPORT DATA
We believe it would be useful for a number of policy initiatives and use cases for HH consumption consent to be extended to cover both import and export data. We understand that there is already a mix of views amongst SEC Other Users as to whether export data can be collected through the DCC Other User mechanism, with some SEC Other Users collecting it and others not. Please see our comments in Question 31 above, and our observation that it already appears to be included in Figure 7.

CONSENT vs SEC OTHER USERs
We have outlined our general concerns on the designation of the SEC Other User as the EDP in our response to Question 1 above. We also had some concerns on the applicability of CCS consents in relation to SEC Other Users in general:

1. Under SEC Section I, the SEC Other User is only able to collect the consumption data from the consumer's meter (via the DCC, under SEC Section I) once they have the consumer's consent. However, as currently proposed, the consumer consent granted under CCS would only be for the EDP to pass the information to the ATP; we don't believe it would cover the SEC Section I consent requirements to allow the EDP to collect that data from the meter. If SEC Other Users are to be an EDP, the CCS consent gathered needs to be amended to cover the EDP accessing the DCC, not just the EDP releasing their data to the ATP.

2. Furthermore, the consumer consent needs to address what the EDP does with their meter data after retrieval and passing it forwards to the ATP, not just what the ATP does. For example, does the EDP hold on to the data, just in case someone else asks for it? Do they process it further – for example using HH data to create daily data? If a second ATP asks for the data for that meter, does the EDP reuse what they already have (which would be sensible, but technically wasn't under the original consent). Does the EDP do anything else with the data – for example provide it on an aggregated basis (5+ households) to Local Authorities etc?

SEC OTHER USERS & DATA INTERMEDIARIES
We generally are worried about SEC Other Users. By positioning them as EDPs on the Consumer Consent directory, it will infer a certain level of approval, although very little is visible about how they manage and handle data between accessing the DCC meter, and passing it through to the requesting party. They are not Ofgem regulated, yet are emerging as a strong player in the energy sector, and that position will become stronger as they are validified by the links with the Consumer Consent solution.

We are also nervous about a similar informal intermediary role being created between the SDR and other third parties, and there are various aspects of the CCS consultation that troubled us in this regard. Specifically, we are nervous about the Commercial Third party dotted line in the bottom left of Figure 1 Decentralised data sharing in Annex D. Further down in Annex D, we also do not agree that an ATP should be able to produce their own ATP version of the CCS portal, or anticipate being in a situation where a consumer uses just a single ATP for all of their energy data services. Both of these seem to be potentially opening up a new intermediary opportunity, which we don't believe was the policy intent, or in consumers' best interests, and could undermine the CCS working effectively with the clarity and protections that are intended.

DCC OTHER USER
The term SEC Other User is used repeatedly throughout the consultation; however, it is not correct. It should be 'DCC Other User', which is a sub-category of 'Other SEC Parties'. For more details, please see https://smartenergycodecompany.co.uk/becoming-a-sec-party/. The documents appear to be using a blend of these two terms, which is incorrect.

OFGEM AI GUIDANCE

Finally, we would suggest that ATPs and EDPs should be encouraged to follow the Ofgem AI Guidance – particularly if their use of energy data is used for business models that have an impact on the customers' use of energy. We have made a similar suggestion in our response to the Tariff Interoperability consultation for RTIs.

The requirements in the Ofgem AI Guidance are not excessive, but represent best practice. All licensed energy parties are already required to follow them.

# 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