

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

Consultation Response Form **Consumer Consent Solution (CCS) Design Consultation**

Published 11 February 2026

Response Deadline 25 March 2026

Link to the Consultation

[View the Consumer Consent Solution Design Consultation here.](#)

How to Respond

Please complete this document and send your responses to consumerconsent@retailenergycode.co.uk

Where possible, we kindly request that responses are submitted as a Word (.docx) document.

Please be assured that your responses will not be edited or amended in any way.

We've asked for your feedback in each of the questions throughout. Please respond to each one as fully as you can.

We will publish non-confidential responses on our website at <https://retailenergycode.co.uk/consultations/>

Your response, data and confidentiality

Responses can be submitted in one of three ways:

- **Non-confidential** – the full response along with the submitting organisation's name and category will be published; or
- **Confidential** – responses will only be shared with RECCo and its CCS project team, the REC Code Manager and the Authority (where relevant). We will respect this request for confidentiality, subject to any obligations upon us to disclose information. Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or
- **Anonymous** – the full response will be published, but the submitting organisation's name will be omitted (the organisation category will still be published). Details of the response may be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation, and the organisation name will be shared with RECCo and its CCS project team, the REC Code Manager, and the Authority (where relevant).

If you submit a non-confidential response but wish to keep part of your response confidential or anonymous, please clearly mark those sections as "confidential" or "anonymous" as appropriate.

All responses will be treated as non-confidential unless otherwise indicated.

RECCo recommends submitting only financial or commercially sensitive information as confidential, and using anonymous for other cases where the submitting organisation does not wish to be identified. This approach ensures that response details can be included in any consultation summary report(s) and that RECCo's comments on the responses can be published.

Respondent Details

NAME	Dale Lloyd
ORGANISATION	CGI IT UK Ltd
ORGANISATION CATEGORY	SEC Other User
E-MAIL ADDRESS	dale.lloyd@cgi.com
RESPONSE CONFIDENTIALITY	Non-confidential (recommended)

Questions

Scope of the CCS

Q1	Do you agree with the proposed MMP scope, including the core functional components and the inclusion of SEC Other Users and the BSC SDR?
<p>With respect to SEC Other Users (OUs), we understand the aspiration and the potential benefit to energy consumers of including their consent records within CCS. However, there are numerous disincentives for an OU which we would assist REC with resolving. As examples:</p> <ul style="list-style-type: none"> - Changes to current integrated coded system - Change to existing contractual arrangements with current clients. - Introduce new OU to client electronic comms including FAPI2 and mTLS. - Change current ID&V processes to pass to CCS - Contract change with current ID&V partners e.g. bank card verification. - Establish new comms links (2-way) with CCS. - Additional requirement to undertake REC accreditation. - Additional liabilities for costs involving REC breach investigations and accreditation costs. - Dual running of pre and post CCS as both will need to co-exist for several years - Mismatch of who is entitled. OU have used SEC Principles which do not match with REC principles - Small client drop-off. Some clients are small organisations who may not have the capability to comply with CCS requirements. - Due to staggered consent expiry a single client cannot migrate all consumers simultaneously. - Our existing processes cater for those consumers who are not digitally enabled, the REC processes appear to require a degree of digital enablement. - As CCS only manages the ID&V process the OU or client will have to maintain Consent detail such as purpose, duration etc as defined in UK GDPR - Current OU clients, who may become ATPs would need to become WCAG compliant <p>With respect to other MMP candidates consideration could be given to inclusion of Supplier data from their SLC47 obligations. The inclusion of the Elexon SDR data has several dependencies outside of the control of REC which may impact on the MMP delivery date.</p>	

The consultation in section 4.11 advises that REC are seeking ATPs to act as volunteers for MMP. Bear in mind that if an ATP requires to access consumption data direct from the metering systems, then a SEC Other User will be required.

We also note that for SEC Other Users participation in CCS is voluntary. Are there any plans to make this mandatory and if so, how and over what timescale?

The potential for unknown future user pays adds a double jeopardy to Other Users where potential payments are being made to both SEC & REC which are currently unbudgeted.

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?

See our response to Q1 Migrations to CCS would need to be carefully considered. Technically it is not a difficult process but the basis for consent is different between SEC & REC. It would seem sensible not to migrate in bulk but instead at consent expiry. However, due to the different ID&V processes and the different policy approaches it is possible that a successful SEC consent would fail the CCS consent process which may lead to complaints.

If SEC OUs were to migrate in bulk this would only work if the energy consumers did not have to fulfil the CCS ID&V requirements, although this would mean that CCS was holding consent against two different methodologies. If existing SEC OU consumers were expected to complete the CCS ID&V ton bulk migration this would cause contractual, consumer & potentially system issues.

Our current processes allow for vulnerable and those not digitally enabled to participate in consent and data sharing. The absence of a REC CCS process for these consumers potentially results in those consumers failing CCS ID&V and therefore we suggest that these cannot be migrated until CCS has a suitable solution.

REC Policy Positions

<p>Q3</p>	<p>Do you agree with the position that consent for access to half-hourly metered data should be provided by the occupier rather than the bill payer, where these are different individuals? If not, please provide your rationale.</p>
<p>We do not believe that this is an either/or situation. We recognise that this is a grey area given that there is not a concept of data ownership but feel that it is counter-intuitive to prevent a non-resident bill payer, landlord, letting agency, empty property owner or similar not to have access to the granular consumption data of a premise they own or manage.</p> <p>UK GDPR defines Data Subject as:</p> <p>An individual whose personal data is collected, held and/or processed by a controller for varying processes and who can be identified, directly or indirectly by reference to such personal data.</p> <p>From a SEC point of view, we follow two principles: (See SEC Privacy Control Framework for expanded detail.) (See references.)</p> <p>Principle 1: verification of the link between the individual from whom consent is being sought and the relevant consumer premises.</p> <p>Principle 2: verifying the link between the relevant consumer premises and the MPxN (i.e. the Meter Point Administration Number (MPAN) for electricity smart meters or the Meter Point Reference Number (MPRN) for gas smart meters</p> <p>These do not differentiate between occupier and bill payer but instead confirm the identity of the requestor and their association with the premise. We believe this to be UK GDPR compliant.</p> <p>In the same way as SEC has a broader definition of who is entitled to the data REC could consider whether restricting to occupier is appropriate.</p> <p>We have previously provided a number of test scenario to REC where we believe that the bill payer may be entitled to the data. A copy is included for reference.</p>	
<p>Q4</p>	<p>Do you agree with the position that for multi-occupancy households, a 'lead occupant' may provide consent on behalf of other occupants only where they confirm they have the authority to do so and have obtained agreement from all other adult occupants? W If not, please provide your rationale.</p>
<p>As a SEC Other User for the last eight years, we have never received such a request. However, if this is a requirement then consideration could be given to:</p> <ul style="list-style-type: none"> - how to determine/identify the lead occupant. - If the delegated occupant has limited access e.g. read only or read & write - Can a delegated occupant withdraw consent not provided by them? - Can a delegated occupant provide consent? - Is there any risk where a domestic violence situation exists that providing this access could cause issues? <p>Alternatively, it would seem that multiple tenants could fulfil the ID&V requirements in their own right, negating the need</p>	

for a lead occupier. As the CCS consumer screen is MPxN driven all tenants attached to that MPxN would see all details. This itself carries risk of tenant 2 revoking consent given by tenant 1.

We note that the UK Banking Industry has a Financial Abuse Code. (See References) We recommend that REC review that code to identify if there are any similarities or actions that can be taken in the energy sector

It is unclear how and if a 'Lead occupant' may provide and withdraw consent for multiple Energy Services where they may not have been the original consentee.(more than one service)

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

No. Whilst it is subjective, we feel that where the data involved is Half Hourly (HH) consumption data that a GPG45 of Medium is appropriate and that the need for photo or biometric id is not required. This will be the vast majority of consumers using CCS. Placing the burden of High seems disproportionate to the risk. We also note that a study by Manchester University (see references) identified that around 5% of eligible voters were unable to vote due to a lack of photo id. The UK over 18 population is 55.2 million, following the 5% figure this would mean that approx. 2.7 million consumers would fail the ID&V process where photo ID is required.

When PSR data is introduced then we would agree that a GPG45 level of High may be appropriate. However, we would also note that many of these consumers on the PSR would fall into the vulnerable consumer category. We note Ofgem's Energy Consumer Archetype Report (See references) which suggests that vulnerable consumers (and others) are less likely to be digitally enabled.

As the inclusion of PSR is likely to be several years away it should be possible to operate consumption data at Medium and when required add a second approach to co-exist following further investigation.

We joined this market in 2018, since that time we have not been aware of any instances where using the SEC Principles, without photo ID, has resulted in any dispute or issues

We note that digital identification services is an evolving market. There are currently 70 providers registered in the UK Digital Identity & Trust Framework. (DIATF.) (See references) Our assumption is that CCS ID&V will be using one of these. The archetype "comfortable data user" may already be registered and verified with one of these services. At present there isn't a single method of checking if a consumer is already verified by a different service resulting in a single consumer potentially having multiple successful ID&V. This may not be an issue for CCS but it may cause some irritation and potential complaint from the archetype above. The Data (Use and Access) Act intends to place DIATF onto a statutory footing and to create a government wallet which would include items such as digital driving licence, digital passport etc. It's possible that this will include some private sector detail. NOTE: This section of DUAA requires a Secretary of State to produce and publish Digital Verification Service trust framework to enable the DUAA clauses. As of February 2026, this document has not been produced.

It is likely that some consumers will have already completed ID&V through other DITAF approved organisations. CCS could accommodate this to avoid consumer complaints.

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? <i>If not, please provide your rationale.</i>
-----------	---

We have not landed on a position for this but would note the following advantages & disadvantages.

- A consumer could consent without the knowledge of other occupiers. This could be both an advantage and a disadvantage.
- It is not consistent with the original aspiration of a consumer being able to view all their consents.
- A consumer providing consent via the guest route will not be able to withdraw consent via the same method. Instead, its withdrawal will have to be via the ATP/EDP. Will this create any misalignment? Also, note that the UK GDPR requirement is that withdrawal of consent must be as simple as providing consent.

We also note that the Office for Digital Identities and Attributes is creating a Trustmark (UK CertifID) We recommend that CCS only uses those organisations for ID&V that have, or commit to have before CCS go-live this Trustmark (See References.)

Q7 Do you agree that consumers should have the option to revoke or renew consent directly with the relevant ATP or via their CCS account?
If not, please provide your rationale.

Yes, although we would also suggest that there needs to be a communication between the ATP and the EDP to ensure that data collection ceases. There is also the possibility of a consumer withdrawing or renewing consent via the EDP.

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.

No. An EDP could retain the consent expiry date within their own systems removing the need to communicate with CCS on each occasion. If a withdrawal occurs, then CCS should notify the EDP as per our response to Q7, enabling the EDP to withdraw consent within its system and commence its own consent withdrawal process (deleting DCC schedules, setting consent status to withdrawn).

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.

See answer to Q8 If Q8 remains as drafted then we agree that the EDP should continue to retrieve data. The risk of consent expiring being coincident with a CCS extended outage is low. We would consider up to 5 days to be a reasonable period before data retrieval needs to cease. Given the proposed up-time of 99.9% then extended outage should be a rare event.

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.

No. FAPI 2.0 was originally used in the UK for Open Banking. In these circumstances all participants are regulated by the Financial Conduct Authority. In the CCS solution only Energy Suppliers are regulated. Other CCS Users would be required to comply with FAPI 2.0 on joining the CCS solution. There is a risk that ATPs may not wish to, or not able to, meet the FAPI 2.0 standard and choose not to participate in CCS. OAuth 2.0 with mTLS may be a suitable alternative.

At present many Other User clients are micro companies with fewer than 10 staff. Enforcing FAPI 2.0 and mTLS could have the effect of them exiting this market to the detriment of energy consumers. See our response to Q32 regarding a de-minimus approach.

Additionally, data sharing need not be via an electronic flow. In some cases, data can be retrieved by the Other User and placed on secure file sharing site operated by the OU, the client or a third party. See our response to Q32 regarding EDP & ATP being part of the same organisation.

Technical Design

Q11	Do you have any comments on the proposed overall solution architecture and the component descriptions?
<p>There are more detailed, granular processes required. For example, Annex E Fig 1 there needs to be a return process advising the ATP of success or otherwise of ID&V. It would also be useful to understand the timings between Consumer requesting service and ID&V being complete.</p> <p>Similarly, it would be helpful to understand in Annex E Fig 2 the different processes between granting consent and renewing consent. Eg does renewal remove the need for ID&V?</p> <p>For Annex E Fig 3, mandating and prescribing the type of flows does not take into account the type and size of the ATPs. As mentioned in our response to Q32 a de-minimus approach would be helpful.</p> <p>Additionally, more detail is required for Annex 3.</p> <p>At present many existing SEC Other Users (who would be EDPs) currently manage the consent management process on behalf of their clients (who would be ATPs) This is partly to ensure that the consent requirements in UK GDPR are followed.</p>	
Q12	Do you agree with the proposed approach to matching MPxN to the address? If not, please provide your rationale.
<p>Yes, although due to the nature of addresses some tolerance will be required to accommodate vanity addresses and those with similar, but not exact attributes.</p>	
Q13	Do you have any comments on the non-functional requirements detailed within Annex D?
<p>No comments</p>	
Q14	Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?
<p>We agree with the split. However, more work is required regarding the Energy Market Data Specification as to whether that is appropriate in all cases. In many cases (at the moment) we only share consumption data where a simplified approach may be applicable.</p> <p>We currently retrieve consumption on different parameters</p> <ul style="list-style-type: none"> • HH data • Aggregated daily, weekly, annually <p>The current proposed CCS is a one size fits all and does not accommodate the lower level requirements where HH data is not required. E.g. A price Comparison service may only require the previous 12-month consumption as a total.</p>	

Q15	Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?
See Q11	

UX Design

<p>Q16</p>	<p>We have identified four groups of people who will use the consent system, each with different needs (Annex F – Behavioural Archetypes). Have we missed any important user groups? Are there any needs we haven't considered for any of these groups? If yes to either, please tell us what's missing and why it matters.</p>
<p>In addition to those likely to use the system there are those energy consumers who would like to take advantage of the services offered but are unable to do so due to not being digitally enabled. An Ofcom study suggests that this may account for 5% of the UK population. (See references)</p>	
<p>Q17</p>	<p>Do the proposed inclusion requirements adequately address the needs of vulnerable customers, digitally disadvantaged consumers, and consumers with limited English proficiency (Annex F – Accessibility and device constraints)? If not, what additional requirements should be included?</p>
<p>We note that it will be a requirement to meet the WCAG 2.2 AA standard. We have not fully assessed our clients against this standard (they would potentially become ATPs.) We have conducted a free check against many industry websites with a zero-success rate of WCAG compliance. Our assumption is that many potential ATPs currently have corporate website/portals that may not meet the WCAG standards and could result in a barrier to entry.</p> <p>This extends to vulnerable customers, those with disabilities / rely on energy for life support) as well. Any long term consent journey should allow all users the option to engage with CCS to manage and control their data</p> <p>Also, see our response to Q22</p>	
<p>Q18</p>	<p>Do you agree that consumers need to know who is requesting consent, what data they want, and for how long? If not, what's missing? Is there a risk of information overload?</p>
<p>Yes, although the consumer may also want to see:</p> <ul style="list-style-type: none"> - which organisation is retrieving the data - which organisation is the Controller (in case of complaint/query) - how long could perhaps be expressed as consent expiry date. - there are other UK GDPR requirements which the consumer must see. It may be that these can be covered by the ATP or EDP, but it needs to be clear where the responsibility rests. - We also note that Figure 7 includes "why it is needed." It isn't clear if this is to be displayed within CCS. If it is within CCS, then the reason will need to be transmitted to CCS by the EDP or ATP. <p>We highlight that Fig 7 includes why the data is needed but should be framed as why is the data required e.g. for support with pricing...rather than to enable consent management</p>	
<p>Q19</p>	<p>Where should additional verification steps or friction be introduced to protect consumers? Where might such steps create disproportionate barriers? (Refer to figures 7–10: User journey stage)</p>
<p>It isn't clear if Figures 7 & 8 are inside or outside CCS. Our understanding was that a consumer only entered CCS when they had already engaged with an ATP and agreed to the data sharing subject to ID&V. Subsequently consumers would access CCS to view, renew or withdraw consent.</p> <p>Our view which hopefully aligns to REC view is:</p>	

- Consumer gives consent to ATP
- CCS advises ATP
- ID&V result
- ATP advises EDP of outcome
- Data sharing commences.

We would also like to see the end-to-end process for the 'renew consent' process. The reason being that it is likely that the ATP will be in a contractual relationship with the EDP. A consumer selecting the 'renew consent' option within CCS will presumably trigger an event notification to the ATP. Depending on the contractual position between the ATP & EDP there is a risk that data retrieval will not occur. This may result in consumer complaints.

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?

See Q18

Q21 Do you agree that consumers need to understand which services will be affected, what happens to their data, how long changes take, and whether revocation is reversible? If not, what's missing? Is there a risk of information overload at the point of revocation?

Yes. As an example, withdrawing consent to an app provider may result in the consumer losing access to that data. There needs to be a realistic timescale for when withdrawal takes effect, this is unlikely to be real time but could be a few working days. Presently, we do not allow reversal of withdrawal. Instead, re-consent is required by the consumer.

If the consent has been provided by a CCS account holder, then if reversal is allowed then consideration could be given to not repeating ID&V.

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. Although it is not clear from the consultation documents how assisted journeys will be used. This is an important part of the design with more detail required. It's likely that a one size fits all will not be appropriate particularly given the road map of including PSR data.

Any eventual non-digital consent journey should be fully costed as well to assess financial impact on the sector including existing OUs

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?

Where possible an alternative consent process should be delivered which provides the same outcome as the digital process.

Governance Design

<p>Q24</p>	<p>Do you have any comments on the proposed REC drafting approach, including the creation of a new REC CCS Arrangements Schedule, a new CCS Service Definition, the Customer Experience Guidelines, consequential changes to existing REC artefacts, and the new CCS API Technical Specification?</p>
<p>No comment</p>	
<p>Q25</p>	<p>Do you agree with the proposed initial funding model, including the ability for the cost of qualification and breach investigation activities to be recovered from the individual organisations? If not, please provide your rationale.</p>
<p>No. As SEC Other Users already comply with SEC requirements which are broader & deeper than those of CCS, we do not believe that REC accreditation & therefore payment is required. It also seems that payment for accreditation should be absorbed into the REC charging methodology.</p> <p>With regards to breach investigation this seems to introduce double jeopardy. Where personal data is involved, parties already have obligations to investigate and the ICO has the capability to apply fines.</p> <p>There is uncertainty around the initial funding model and the potential move to a user pays. This unknown future liability causes uncertainty to existing SEC Other Users who already pay for some elements to SEC and could be transactionally charged by SEC.</p> <p>Costs incurred will be passed through to consumers. Socialising the costs across all suppliers results in a lower per-consumer cost increase.</p>	
<p>Q26</p>	<p>Do you agree with the proposed CCS Accreditation model? If not, please provide your rationale.</p>
<p>No. We would suggest that Other Users who are approved under the Smart Energy Code should not have to also complete REC accreditation. Section 8.53 of the consultation document does not accurately reflect the current situation.</p> <p>Prior to going live and communicating with metering systems the OU must:</p> <ul style="list-style-type: none"> - fulfil the requirements of SEC section H1.10 - fulfil the User requirements of SEC section G (Security) - fulfil the requirements of SEC section I (Privacy) <p>Only after each of these three have been independently assessed as complete can the OU commence DCC communication.</p> <p>We believe that combination of these three mandatory requirements meet, or exceed, the accreditation requirements in REC. and therefore that CCS can rely on these approvals.</p> <p>Additionally, OU's are subject to annual external assessment against Section G and Section I to maintain SEC approval.</p>	

Q27	Do you agree that a minimum standard should be set whereby all CCS Users should be Cyber Essentials Plus certified or ISO 27001 accredited? If not, please provide your rationale.
Yes. Although also see our de-minimus suggestion in Q32	
Q28	Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?
No comments	
Q29	Do you have any comments on applying the existing REC performance assurance framework to cover assurance of the CCS arrangements?
Yes. Although we note that Ofgem & the Energy Ombudsman only have vires (in this context) with energy suppliers.	
Q30	Do you have any comments on the proposed issue/dispute resolution paths defined for the management of CCS issues?
<p>Is it possible to clarify what “publicly” means within Section 8.69. Is it a directory of all ATPs available to all users, or is only available at a consumer-by-consumer level when that consumer is accessing their CCS account.</p> <p>With effect from June 2026 each controller is required to have and publish a formal complaints process, consumers should be signposted to this to enable investigation prior to escalating to the ICO.</p>	

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?
Not at this stage. We assume that the product roadmap changes will be managed through the REC Change Process.	

Additional Comments

Q32	Please provide details of any additional issues you feel have not been adequately captured within the consultation document.
<p>We have been a SEC Other User since 2018, some of our responses reflect our experiences. To assist the understanding we have included some Use Cases where the proposed solution may cause some challenges:</p> <p>For the avoidance of doubt all of the following currently use unambiguous consent and the processes in the SEC.</p> <p>Ofgem Strategic Innovation Fund projects:</p> <p>We have been involved in several Ofgem supported innovation projects which have included sharing consumption data and other parties sharing PSR data. These have tended to be pilots to enable statistical analysis and have involved fewer than 1,000 energy consumers over less than a 12-month period. Requiring the ATP to sit inside the CCS ecosystem with the obligations required may have the unintended consequence of making these innovation projects unviable.</p> <p>Consumer Apps.</p> <p>There are several consumer facing apps, some which are free of charge to the consumer. The ATP may be a sister company to the EDP or a totally separate organisation. As with the SIF requiring the ATP to sit inside the CCS ecosystem with the obligations required may have the unintended consequence of making these apps unviable to the detriment of the consumer.</p> <p>EDP & ATP under same ownership.</p> <p>There are circumstances, such as in the app situation above, where the EDP & ATP are the same organisation with the same systems infrastructure but with both roles. Data sharing would usually be within internal, suitably protected systems.</p> <p>Business Innovators.</p> <p>There are numerous entrepreneurs and business innovators producing intelligence for energy consumers that use consumption data for a variety of purposes including, best tariff, EPC data, energy saving measures, usage analysis.</p> <p>Research Purposes</p>	

Several academic institutions use consumption data for various analytical purposes, this may be a short term requirement covering a large number of premises, perhaps only one data retrieval.

We would like to propose that REC consider a de-minimus approach where an ATP need not be required to fulfil the following CCS obligations:

- the use of FAPI 2.0 – instead standard TLS or OWASP API or sFTP
- REC accreditation – instead Contractual obligations between EDP & ATP
- WCAG 2.2

A de-minimus could be:

- Up to a maximum of 20,000 MPxNs over an extended period. The ATP should move to the full user CCS within X months.
- A maximum of two data extracts.

OTHER POINTS:

1) Change of Tenancy – This is probably the least robust of the industry processes due to dependencies on multiple third parties. At present, SEC Other Users place an MPxN-specific schedule on the DCC such that when the DCC becomes aware of a CoT via Supplier data flows that OU data retrieval stops. We treat this as a withdrawal of consent. There is some reliance on the vacating tenant to advise various industry parties, and the tenant advising CCS is likely to be low on the list and instead will rely on the new tenant (if there is one) providing new meter reads to the supplier. In turn that will trigger a CoT. REC may need to consider how CoT will be managed within CCS and the risks involved.

2) CCS System Security. Whilst we would not expect REC to place the security controls in this consultation, or in the public domain we would like to see some assurance that our systems are protected from any intrusion etc from the CCS systems. We also assume that there will be REC Incident Management and Vulnerability Management.

3) Post Quantum Cryptography - We have not assessed the CCS solution against crypto agility, but as it is a new system we would recommend that REC undertake this assessment.

4) Vulnerable consumers & less digitally enabled consumers. We currently have processes that enable these sets of consumers to participate in the consent solution. It isn't clear how CCS will include these consumers.

5) Penetration Testing. We would recommend that the REC conducts a penetration test on the CCS infrastructure, in particular consumer-facing websites.

6) Non-domestic UK GDPR does not apply to non-domestic and therefore different rules apply when retrieving business data. How will CCS accommodate non-domestics or those businesses with non-SMETS AMR devices.

7) Change of Supplier (CoS). At some points CoS is mentioned. We believe that this is only applicable when Supplier SLC47 data is included. From an ATP/EDP point of view a CoS does not change the consent.

8) Multiple Roles: There should be provision for a participant to hold more than role. Eg Hold both an ATP & EDP for different purposes, hold multiple ATP or EDP roles for different purposes.

SUMMARY:

We have reviewed the consultation and believe that the current design introduces a number of barriers to entry for consumers, ATPs and EDPs:

- Consumers:
 - Strict ID&V process requiring photo id
 - Vulnerable consumer journey unclear
 - Design doesn't provide an end-to-end consent solution, consumer will still need to consent outside CCS to ATP or EDP to be UK GDPR compliant.
 - Restricted use of 'occupier' as the data subject
- ATPs/EDPs
 - Mandating of FAPI 2.0 regardless of organisation size
 - Mandating FAPI 2.0 even for internal communications where ATP & EDP are the same
 - One size fits all does not take into account, innovators, entrepreneurs etc
 - For SEC Other Users many disincentives (see Q1) creating barriers to entry.
 - Use of WCAG AA to existing organisations.

REFERENCES (Added by responder.)

SEC Privacy Controls Framework

<https://smartenergycodecompany.co.uk/privacy-controls-framework/>

UK DIATF

<https://www.gov.uk/government/collections/uk-digital-identity-and-attributes-trust-framework>

UK DIATF Providers

<https://www.digital-identity-services-register.service.gov.uk/>

Office for Digital Identities and Attributes

<https://enablingdigitalidentity.blog.gov.uk/2026/03/16/uk-certifid-a-mark-of-trust-in-digital-verification-services/>

Manchester University voter ID study

<https://www.manchester.ac.uk/about/news/almost-2-million-people-didnt-have-the-right-id-to-vote-in-2024/>

Ofgem Archetypes

https://www.ofgem.gov.uk/sites/default/files/docs/2020/05/ofgem_energy_consumer_archetypes_-_final_report_0.pdf

Ofcom Digitally Excluded.

<https://www.ofcom.org.uk/internet-based-services/technology/exploring-how-people-in-the-uk-are-affected-by-digital-disadvantage>

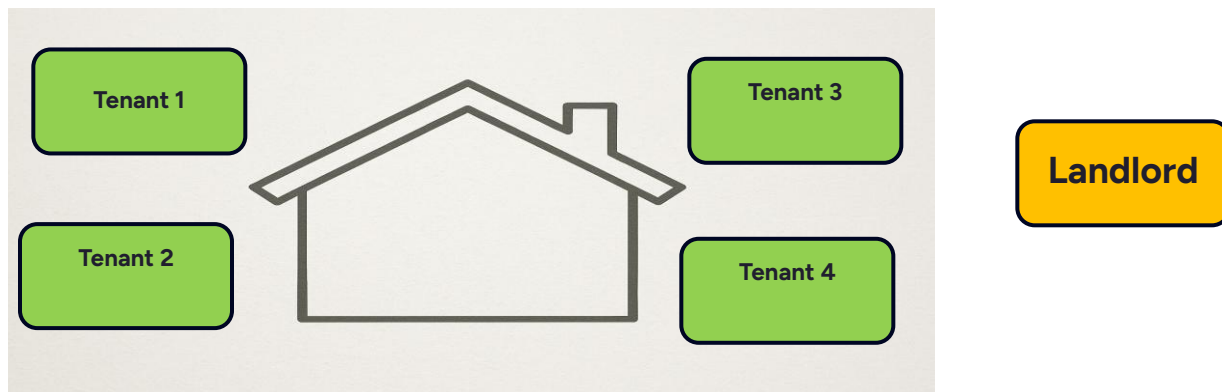
Financial Abuse Code

<https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/financial-abuse-code>

TESTS PREVIOUSLY PROVIDED TO REC CCS

USING OCCUPIER AS CONSENTEE

Not sure how ID&V will work in these new arrangements. Under SEC Other User we have two principles: a) confirmation of applicant details and over 18 and b) connection to premise.



Test 1

Student residence – All utilities included within rent

Landlord is private individual and is the utility bill payer. (Lives 50 miles away)

Premise is exempt from council tax

Test 2

Student residence – All utilities included within rent

Landlord is letting agency and is the utility bill payer for 50+ properties

Premise is exempt from council tax

Test 3

Student residence – Utility bills paid by students (Tenant 1 is on bill)
Landlord is private individual. (Lives 50 miles away)
Premise is exempt from council tax

Test 4

Tenants 1 & 2 married couple. Tenants 3 & 4 19yo children of couple.
Property owned by tenants – Tenant 1 named on bill
Landlord not involved

Test 5

Tenants 1 & 2 married couple. Tenants 3 & 4 16yo children of couple.
Property owned by tenants – Tenant 1 named on bill
Landlord not involved

Test 6

Tenants 1 & 2 married couple. Tenants 3 & 4 12yo children of couple.
Property owned by tenants – Tenant 1 named on bill
Landlord not involved

Test 7

Tenants 1 & 2 married couple. Tenants 3 & 4 19yo lodgers.
Property owned by tenants – Tenant 1 named on bill
Landlord not involved

Test 7

Tenants 1 & 2 un-married couple. Tenants 3 & 4 19yo children of couple.
Property owned by tenants – Tenant 1 named on bill
Landlord not involved

USING MPxN AS THE PARAMETER

This is more about how Change of Tenancy is managed. SEC Other Users place a schedule via the DCC which when a Supplier data flow indicates a CoT the OU treats this as a withdrawal of consent. The CoT notification process isn't as reliable as it could be, partly due to the reliance on the leaving tenant notifying their supplier.

As an example:

MPxN	DATA PROVIDER	DATA USER	COMMENTS	WITHDRAW CONSENT
1112345678912	Supplier 1	Supplier	This tenant has moved out	
1112345678912	Other User 1	Debt Relief Organisation	This tenant has moved out.	
1112345678912	Other User 2	Usage app	This is a new tenant	
1112345678912	Supplier 2	Supplier	This is a new tenant	

On this basis Tenant 1 has provided consent to a debt relief organisation, they have left the premise without any notification.

Tenant 2 has moved in and has selected a different supplier and given consent via an OU to retrieve their consumption data for use in an app. It takes some time for the changes to flow through the system. At this point Tenant 2 can see all the consents given by Tenant 1. The DRO may be considered to be Special Category.

RECCo may well suggest they are acting in good faith as they are only displaying data provided by third parties. I'm assuming that RECCo have completed a DPIA for this and identified risks where a third party hasn't updated their data.

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