RETAIL ENERGY CODE

This document is classified as **WHITE**.
Information is for public, unrestricted dissemination and publication.

REC CONSUMER CONSENT TOPIC SPECIFIC SOLUTION GROUP
MEETING MINUTES

MEETING	**REC_CCTSSG_26_0722**
DATE	**22 July 2026, 14:30**
LOCATION	**By teleconference**

1. INTRODUCTIONS

The Chair welcomed Members to the meeting of the Consumer Consent Topic Specific Solution Group (CCTSSG). This session would focus specifically on the Consent Schema and Address Misalignment.

2. CONSENT SCHEMA

GR reminded Members of the importance of the CCS Consent Schema in ensuring Consumer Consent is accurately represented, enabling EDHs to retrieve the correct data, supporting data minimisation principles, and remaining adaptable to future data-sharing scenarios. They noted that feedback from a previous Solution Group meeting in June had already resulted in several changes, including the introduction of centrally managed enumerated purposes, new fields for data type and energy flow direction, the removal of frequency, elimination of free-text fields, inclusion of EDH requirements where relevant, and support for different consent types such as one-off and enduring consents.

GR explained the role of the Schema throughout the CCS data-sharing journey. ATPs would submit a push authorisation request containing the initial consent information, which CCS would then validate, enrich and formalise into the consent record. The resulting consent record would underpin the access token ultimately used by ATPs to request data from EDHs. Given its role across the entire process, the Schema needed to support consent management, consumer transparency and data retrieval requirements simultaneously.

GR advised that the primary focus of the discussion was a proposal to separate the schema into two logical blocks:

- A Consent Block containing items such as purpose, consent duration and consent type.
- A Data Block containing data-specific attributes such as fuel type, energy flow direction and other information required by EDHs to retrieve the requested data.

GR explained that this separation would improve maintainability and future proofing as additional data types and services, such as tariffs or PSR data, are brought into CCS. Although

separated logically, both blocks would still form a single consent record and be associated with a single access token.

A member sought clarification on whether the proposed structure would allow a Consumer to provide a single consent covering multiple data sets, citing import and export consumption data as an example. GR confirmed that the current working assumption was moving towards one consent per data type, although design work was still ongoing. The member questioned whether this approach would be appropriate from a Consumer perspective, noting that Consumers typically seek to access a service rather than individual data sets. They suggested that where a service requires multiple data sets, consumers should ideally be able to provide a single consent covering all necessary data sharing activity.

Another member agreed with this position, observing that in real-world customer journeys consent is generally requested in the context of a service. They argued that Consumers would expect one consent to cover all data required for the delivery of that service rather than having to manage multiple consents linked to separate data sets.

A member raised concerns that the emerging design risked conflating technical implementation with the legal concept of consent. They stressed that from a legal standpoint a Consumer grants consent for a defined purpose or service, which may legitimately require access to multiple data types. They recommended testing the technical design against established legal consent processes rather than allowing technical architecture decisions to drive the Consumer experience.

A member strongly supported an outcome-based, service-oriented approach. They argued that Consumers should be asked to consent to a service outcome rather than being expected to understand the technical details of individual data sets. They warned that exposing excessive technical detail could increase complexity, create friction in the consent journey and ultimately reduce completion rates.

GR acknowledged these concerns and agreed that purpose remained a fundamental concept within the schema. They noted that further work was required to understand how multiple data types could sit beneath a single consumer-facing purpose or service.

A member supported the service-based consent approach but highlighted an additional benefit of retaining visibility of the underlying data requirements within the technical design. They argued that the Schema could signal to ATPs the importance of considering precisely what data is needed to deliver a service, rather than requesting broad access to data and determining its use later. The member suggested this would reinforce data minimisation principles by requiring ATPs to identify and justify the specific data required for their service. They envisaged this as a design consideration for ATP integrations rather than something consumers would necessarily see during the consent process. GR agreed that these considerations should be kept in mind during detailed review of the individual Schema fields and in determining which information should be Consumer-facing versus system-facing.

A member noted that, in practice, customer journeys often include disclosure of the specific categories of data being requested. However, they reiterated that all such data requests should remain associated with a single consent where they support delivery of one service.

A member cautioned against embedding GDPR principles unnecessarily within the industry code framework. They noted that obligations around data minimisation already exist within general legislation and warned against duplicating statutory requirements in industry-specific governance arrangements. MPW acknowledged the point and advised that they would take it away for further consideration.

GR moved onto the inclusion of optional consumer information hints within the CCS Consent Schema. The proposal would allow ATPs, where they already hold Consumer information, to provide details such as names, addresses, email addresses and MPxN identifiers alongside the push authorisation request. GR explained that the primary objective was to reduce Consumer friction by enabling CCS to pre-populate information during account creation and ID&V processes, thereby reducing the amount of data Consumers would need to enter themselves.

Under the proposal, ATP-supplied information would be treated as optional and would always be validated by CCS. Where validated successfully, certain information could be incorporated into the consent record and access token, particularly verified MPxNs. Other information, such as names, addresses and email details, could be returned separately to ATPs via an ID token mechanism, allowing records to be aligned across organisations while avoiding inclusion of unnecessary personal data within access tokens.

A member queried the nature of the proposed ID token and how it would be delivered. GR explained that this would use standard OpenID Connect mechanisms and would be transmitted directly to ATPs via APIs rather than through email or text message. CE added that ID tokens are a widely used industry standard and comparable to authentication mechanisms used in services such as "Sign in with Google".

A member sought confirmation on whether ATPs would be expected to provide Consumer identity information and MPxN details and whether CCS would still undertake ID&V. GR clarified that all ATP-supplied information would remain optional and that CCS would continue to perform its own ID&V process and property verification. Where ATPs did not provide MPxNs, CCS would identify eligible metering points through its own validation process using verified Consumer and property information together with the REC Enquiry Services.

A member also sought confirmation that Consumers would always be redirected into a separate CCS journey rather than having the process fully embedded within ATP systems. GR confirmed that, for half-hourly metered data, Consumers would continue to pass through CCS to complete ID&V and consent, although repeat journeys would become significantly simpler once an account had been established.

A member raised concerns regarding the collection, storage and retention of personal information. They requested clarity on the justification for storing personal data within CCS, the intended retention periods and any associated risk assessments covering the transfer of information from ATPs to CCS rather than collecting it directly from Consumers. They further

cautioned against unnecessarily retaining information that had fulfilled its purpose, noting that some information may be needed for validation purposes without necessarily requiring long-term storage. MPW confirmed that these considerations were being assessed as part of the ongoing design and consultation process and would be reflected in supporting documentation accompanying future code drafting and consultation activities.

A member questioned whether reducing Consumer data entry risked weakening ID&V controls. They noted that providing multiple personal details often forms part of establishing confidence that the individual accessing data is who they claim to be. GR clarified that the information hint proposal would not replace ID&V. Rather, it would simply pre-populate information that Consumers would otherwise need to provide manually. CCS would still undertake all required ID&V checks to establish that Consumers were entitled to consent for the relevant property and associated metering points. Where supplied information was inaccurate or out of date, the ID&V process would identify those discrepancies.

The member sought assurance that personal information would not be displayed to individuals before their identity had been appropriately validated. GR explained that ATPs would initiate the journey through secure redirect mechanisms, ensuring the individual receiving pre-populated information was the same individual who initiated the consent process.

A member described similar discussions taking place within another programme, where organisations such as banks and accounting platforms may already have undertaken robust ID&V on behalf of Consumers or businesses. They outlined a concept whereby trusted organisations could contractually stand behind the quality of ID&V already performed, potentially reducing duplication of verification activities. GR welcomed the comparison and noted that the CCS team was also exploring areas such as Open Banking-based identity verification, although this remained separate from the specific consumer information hint proposal currently under discussion.

A significant discussion arose regarding customer drop-off rates. A member argued that the fundamental source of friction was not data entry itself but the requirement for Consumers to leave an ATP's service journey and complete a separate consent and verification process within CCS. Drawing on their experience of consent solutions, they suggested that consent processes work best when fully embedded within the context of the service being provided, maintaining Consumer confidence and continuity throughout the journey. They expressed concern that introducing a separate validation process could lead to substantial Consumer abandonment and encouraged the CCS team to undertake testing to understand likely completion and drop-off rates. MPW acknowledged the concern and agreed that minimising consumer friction and abandonment throughout the consent process remained a key design objective.

A member noted that the usefulness of ATP-supplied MPANs would depend heavily on the quality of underlying address-to-MPAN matching data. They observed that many ATPs already obtain this information from the same Enquiry Services available to CCS and highlighted known data quality issues and edge cases where address matching can be difficult. They questioned whether the additional complexity introduced by ATP-supplied MPANs would provide any meaningful value if both ATPs and CCS rely on the same underlying data sources. Another

member supported these concerns, highlighting longstanding challenges associated with address standardisation, inconsistent address records and metering data quality issues.

Multiple members also raised liability concerns. They noted that inaccurate address matching could create two distinct risks:

- Incorrectly providing access to data associated with the wrong property.
- Incorrectly denying ATPs access to legitimate customers because CCS records do not match ATP-held information.

They emphasised that denial of access to valid Consumers due to data quality discrepancies could become a significant issue.

GR presented a low-level proposal of the CCS consent Schema containing consent type, consent model (one-off or enduring), purpose, duration, and a linked consent field to support consent history and renewals. The associated half-hourly meter data block would contain fuel type, import/export status, data range ("from" and "to"), and EDH information.

Members challenged the inclusion of a predefined purpose field. While the field was intended to improve Consumer transparency and align with broader smart data principles, multiple members raised GDPR and data minimisation concerns, questioning whether REC-managed purposes could accurately reflect ATP intent and whether restricting purposes could potentially mislead consumers. GR agreed further legal and ICO input would be required.

Members also debated whether the EDH should be tied to the consent. They highlighted practical scenarios where ATPs may wish to change data providers during the life of a consent without requiring customers to reconsent. CE noted that, in Open Banking, consent is generally linked to a specific data holder, meaning a change would require a new consent, although Members agreed the energy market presents different challenges. Another member also raised questions about whether a consent should support multiple data types, which could introduce more complex relationships between consents, data holders, and access tokens.

GR presented the proposed post-validation CCS Consent Schema, explaining that while much of the information mirrors the original ATP request, CCS enriches and validates the data before issuing an access token. Members discussed whether certain data fields were necessary for EDHs to receive, particularly given that CCS would already hold the MPxN and consent details. A member questioned why EDHs would need fields such as the consent purpose or linked consent information, arguing that only the MPxN, date range and requested data were required. GR agreed this was a valid challenge and committed to reviewing the Schema.

A detailed discussion followed on whether fuel type and energy flow direction remained necessary fields. A member initially suggested fuel type should be retained and later clarified that where a single identifier could potentially provide access to both electricity and gas data, fuel type remains important to ensure only the consented fuel is collected. The member and MPW confirmed that import/export direction must be explicitly identified for electricity, given the agreed assumption within REC arrangements that export data also requires consent. They

concluded that retaining fuel type and direction within the consent information likely remained beneficial.

3. ADDRESS MISALIGNMENT

GR took Members through a proposal on how CCS should handle situations where an address provided by an ATP does not align with the address CCS can verify through its ID&V processes.

GR explained that ATPs may provide address details to CCS to reduce customer friction and proposed that ATPs could optionally specify whether an exact address match is required before data sharing can proceed. CCS would compare the address supplied by the ATP with the address verified through ID&V and determine whether any mismatch exists.

Two principal scenarios were discussed. For first-time CCS users, minor address discrepancies would generally be resolved through ID&V processes, while more significant differences could result in CCS either continuing with data sharing using the verified address or stopping the process if the ATP had requested an exact match. For existing CCS users, CCS would identify mismatches against the address already associated with the consumer's account and could present options to the consumer to confirm or update their address.

Several participants highlighted the significant complexity associated with address matching. A member described address validation as a longstanding industry challenge, noting that ATPs have often invested years improving address quality and matching processes. They cautioned that CCS should expect multiple implementation iterations as address-related issues emerge.

A key concern raised was how CCS would determine whether the ATP-held address or central system records were correct when discrepancies occur. GR acknowledged this challenge and suggested CCS could initially provide visibility of mismatches, with future processes potentially developed to help resolve underlying data quality issues.

A member emphasised that address validation is more complex than comparison with REC Enquiry Services alone. They noted that address records can differ across systems, particularly between Enquiry Services and the Smart Meter Inventory, and questioned whether CCS had fully considered the implications of SEC requirements and multiple address repositories. They suggested that CCS map the entire address-validation process in detail before determining how mismatches should be handled.

Members broadly agreed that exact address matches are relatively uncommon in practice and that mismatches should be expected rather than treated as exceptional. A member argued that presenting competing address options directly to Consumers could introduce unnecessary friction and suggested that ATPs should instead manage any follow-up interaction with customers. Another member similarly questioned whether a hard failure was appropriate and proposed that CCS instead provide a warning or flag when addresses differ, allowing ATPs to make an informed decision.

The member also noted that many ID&V verification schemes do not return a corrected address but simply state that the supplied address has failed validation. They encouraged the CCS team to examine how other verification schemes handle such situations and to consider placing

greater trust in address validation work already undertaken by ATPs and other market participants.

GR confirmed that CCS is working with industry stakeholders to better understand address validation flows and determine how CCS can identify discrepancies, provide visibility of issues and potentially support wider industry efforts to improve address data quality over time. The team also agreed to consider how Smart Meter Inventory requirements interact with CCS processes and noted that handling Consumers with multiple addresses remains an area requiring further development.

4. FORWARD PLAN

The Chair concluded the meeting by outlining upcoming sessions and encouraged ongoing feedback and engagement from all participants.

The next Topic Solution Group meeting on 29 July will focus on ID&V, Bill Payer/Occupier, Shared Signals Framework Profile, and OIDC Registration Framework. Another Topic Solution group is scheduled for 12 August, with the agenda to be confirmed at a later date. The next Engagement Webinar is due to be held in September.

MPW advised that any members with queries are welcome to email consumerconsent@retailenergycode.co.uk, and the RECCo project team will be happy to respond. They added that RECCo are looking for early adopters of the CCS solution and asked any interested parties to scan the QR code at the end of the meeting slides.

ATTENDEE ORGANISATIONS

Attendee	Representing	Initials	Role
Michael Walsh	Retail Energy Code Company	MJW	Chair
Matt White	Retail Energy Code Company	MPW	Presenter
George Roberts	Retail Energy Code Company	GR	Presenter
Christian Eloysio	Raidiam	CE	Presenter
Harry Firth	REC Code Manager	HF	Secretariat

Ofgem	Publicis Sapient
Department for Energy Security and Net Zero	Centrica
Citizens Advice	CGI
Which?	SECCo
Consumer Scotland	SMS Energy
ScottishPower	PayPoint
Elexon	GreenSync
Perse Energy	National Energy System Operator
SSE	N3rgy
E.ON	Flock Associates
East Lothian Housing Association	One Utility Bill
Smart DCC	ESG Global
Raidiam	PRIME
Electralink	ScottishPower
Cadent	Ohme
Stark	Smart Energy GB