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_0701**
DATE	**01 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 CCS Governance and the REC Access Agreement.

2. CCS GOVERNANCE

SJ reminded members of the five key spokes of the CCS Governance Arrangements - Change Control, Qualification, Funding, Issue and Error Resolution and Assurance. SJ advised on the development of a new CCS Arrangements Schedule, which will define participant obligations and operational processes for managing Consumer permissions. SJ noted that existing REC Governance Schedules are also being updated to incorporate CCS requirements.

SJ described the ongoing REC drafting approach for the Arrangements Schedule. This includes drawing on existing energy regulations and policy decisions informed from the design consultation and responses, alongside technical design work being undertaken with the appointed technology provider, Raidiam. Technical artefacts, business processes and security requirements are being refined based on consultation feedback and ongoing working group discussions. These inputs are informing the REC drafting that will be issued as part of the summer consultation. Following consultation, the drafting will be refined before progressing through the established REC Change process via I0318, which will subsequently become a full REC Change Proposal for formal approval and implementation of the Arrangements Schedule and other required legal text.

A member asked about when the consultation is due to be issued. SJ responded that the current scheduled date is towards the end of August.

SJ introduced the CCS Arrangements Schedule further. The Schedule will contain both general obligations applicable to all CCS users—such as qualification requirements and compliance with API technical specifications—and specific regulatory obligations that apply separately to ATPs and EDHs. It will also include non-functional requirements supporting end-to-end customer journeys and translate agreed business processes into operational procedures.

SJ explained that as it will be a REC Schedule, REC Parties will be required to comply where they participate in CCS arrangements. Non-REC parties wishing to access the CCS will be required to comply through separate access agreements. SJ noted that, for consultation purposes, new CCS-specific definitions will initially be contained within the CCS Arrangements Schedule itself before subsequently being incorporated into Schedule 1 (Definitions) later.

SJ then focused on the proposed allocation of responsibilities between ATPs, EDHs and RECCo. The current design assumption is that ATPs will be responsible for ensuring compliance with data protection legislation, determining their lawful basis for accessing data, complying with any relevant energy regulatory requirements regarding CCS use, and using data only for the agreed purpose covered by a consumer's permission. EDHs will be responsible for determining when CCS permission is required for data access and, where applicable, validating that the requesting ATP is an authorised CCS user with an active permission in place. RECCo's role will be to provide and operate the CCS service itself in accordance with the service definition, including delivering centralised identity verification, address matching and MPxN matching services. SJ highlighted these responsibilities as a key discussion area, noting that they underpin the legal arrangements being developed within the REC drafting.

A member noted that, for domestic Consumer consumption data, consent is currently the only lawful basis under existing arrangements, whereas other categories of personal data may be accessed using alternative lawful bases. They asked whether ATPs would be restricted to using consent when accessing consumption data. SJ confirmed that this is the current position. While ATPs remain responsible for complying with both data protection legislation and energy-sector regulatory requirements, existing industry Code arrangements only permit access to domestic consumption data where valid consumer consent is in place. The member asked about non-domestic Consumers. SJ responded that non-domestic markets are out of scope for MMP and separate consideration will be given in the future to this.

A member questioned how the CCS would interact with existing arrangements where EDHs already have contracts with third parties for access to domestic data. They asked whether becoming an EDH would require all such arrangements to be routed through the CCS. SJ clarified that use of the CCS is not intended to be universally mandatory. Instead, whether CCS permission is required will depend upon the relevant energy regulations and code requirements. Where existing industry frameworks continue to permit alternative consent mechanisms, EDHs may continue to rely on those arrangements.

SJ explained that CCS will use and extend the existing REC qualification framework rather than introducing a new process. Schedule 9 will be updated so that organisations seeking CCS access must complete qualification activities including an application, Information Security and Data Protection (ISDP) assessment, system testing and an access agreement. They highlighted that Suppliers participating in Tariff Interoperability (TI) arrangements will be required to become CCS users in their role as EDHs where they are required to share Consumer-specific tariff information.

SJ added that RECCo has been reviewing the ISDP assessment to ensure it appropriately addresses the risks associated with unauthorised access to half-hourly consumption data.

While the overall structure remains largely unchanged, greater emphasis is being placed on data protection controls and consumer safeguards. SJ also confirmed that the proposed minimum information security requirement remains Cyber Essentials Plus certification, with the ISDP assessment being streamlined where reliance can be placed on recognised third-party security assurance.

A member questioned whether Suppliers, which already undergo REC qualification and Smart Energy Code (SEC) security assurance, would need to complete additional ISDP assessments and obtain Cyber Essentials Plus certification. SJ explained that Suppliers are already REC Parties and therefore have an existing assurance framework in place. They noted that the key risk focus of the CCS ISDP assessment is on ATPs, rather than EDHs. As a result, organisations acting only as EDHs may face a different assurance requirement and risk profile than ATPs. On Cyber Essentials Plus, SJ confirmed that the position is still being refined with Ofgem and DESNZ, although organisations holding suitable independently verified certifications, such as ISO 27001, may be able to demonstrate equivalent assurance.

A member asked whether SEC Other Users would be expected to act as EDHs or ATPs. SJ responded that the base expectation is that they would act as EDHs, but many may also wish to qualify as ATPs in order to engage directly with consumers and access data through future smart data arrangements. They confirmed that organisations may seek qualification in both roles, although a legal view is still being sought on whether an organisation can act as both an ATP and EDH within a single transaction.

A member questioned how RECCo would assess GDPR and privacy compliance given the absence of an equivalent third-party certification scheme. SJ explained that this is the purpose of the ISDP assessment, which will seek evidence that organisations have appropriate data protection controls in place. They noted that the level of assurance and evidence required is expected to vary according to the type of organisation and role being assessed, rather than applying a single approach to all applicants. All CCS applicants will be classified as low, medium or high risk based on several factors. In regard to TI arrangements, access to tariff data only has previously been considered lower risk and therefore would not require a full ISDP assessment, although the potential application of Cyber Essentials Plus remains under review.

A member asked about potential duplication with SEC assurance processes, SJ acknowledged ongoing discussions between RECCo and SEC regarding alignment. They explained that SEC assessments primarily focus on security controls and access to smart meter data via the DCC, whereas the proposed CCS ISDP assessment is intended to focus on the downstream use, handling and sharing of consumer data. RECCo's aim is for a single CCS qualification process to support access to data across multiple routes, including REC, SEC and future SDR arrangements.

A member emphasised that the CCS should be viewed as a long-term, scalable solution rather than one focused solely on MMP. They noted that the service is expected to support access to a broader range of consumer data in future, including personal data associated with traditional and advanced meters, and therefore its assurance framework needs to accommodate a wider range of use cases beyond smart meter consumption data.

SJ outlined the proposed CCS monitoring and assurance framework. Most performance and compliance reporting is expected to be generated directly from the CCS platform, meaning organisations would not be required to submit routine monthly reports. However, CCS Users may be required to retain records relating to activities such as consent revocations and complaints in case further investigation or targeted reporting is required. Compliance with the Customer Experience Guidelines (CEGs) is expected to form part of organisations' annual compliance declarations.

SJ confirmed that security testing, including penetration testing, will form part of the CCS service requirements, alongside continuous monitoring and alerting capabilities. Further confirmation on specific vulnerability scanning requirements will be provided by the technical team.

SJ summarised the proposed charging model. RECCo continues to support a hybrid cost recovery approach whereby core CCS costs are recovered through existing REC charging arrangements, while participant-specific costs such as qualification, accreditation and enforcement activities are charged directly to CCS Users. This approach is intended to encourage early adoption, avoid disproportionate costs for initial users, and align with wider discussions on cost recovery across future smart data initiatives.

3. REC ACCESS AGREEMENT

BOS took members through CCS Access Agreements. They explained that the CCS will operate as a REC service, meaning REC Parties will automatically be able to access it where applicable and will not need a separate contract. The purpose of the CCS Access Agreement is to provide a legal mechanism for non-REC parties, such as ATPs and EDHs, to access the service and become bound by the relevant CCS obligations. The Access Agreement is a short-form contract between RECCo and the CCS User that grants access to the CCS, requires compliance with the CCS rules set out in the REC, and provides Users with the same legal protections available to REC Parties. Existing REC Access Agreements, such as to access the Enquiry Services, will have CCS-specific provisions will be added to the existing arrangements, rather than a new Agreement being needed.

BOS emphasised that the approach is designed to be low-friction, proportionate and aligned with existing REC processes. The agreement ensures that all CCS participants operate under a common set of rights, obligations, liabilities and governance arrangements, while enabling any future changes to CCS arrangements to be managed through the established REC Change Process.

The agreement incorporates standard contractual provisions covering areas such as confidentiality, data protection, intellectual property rights, liability, charging arrangements and dispute resolution. It also sets out the consequences of non-compliance, including protections and liabilities relating to misuse of data, breaches of confidentiality and intellectual property infringements. BOS stressed that these provisions are consistent with standard commercial contracting practices and are already established within the REC framework.

As part of CCS qualification, organisations must sign the Access Agreement before they can participate. The agreement itself is not negotiable because it is governed through the REC. However, signing it does not require organisations to become full REC Parties; it only binds them to the specific CCS-related provisions and associated REC clauses needed to access the service.

BOS added that a key principle of the framework is equivalence, the Access Agreement is intended to ensure that REC Parties, non-REC CCS Users and other service Users are treated consistently, with the same confidentiality protections, liability provisions and governance requirements applying across all participants. This approach avoids creating different tiers of obligations or protections and ensures that all CCS Users are subject to the same standards while benefiting from the same legal safeguards.

A member asked whether any CCS information would only be available after signing an Access Agreement. SJ and BOS confirmed that access to the system itself would require participation agreements, but they were not aware of any broader non-public governance documentation and agreed to take the question away for confirmation.

A member asked how Consumers would be protected if an ATP misused data obtained through CCS and whether there would be mechanisms to identify and address poor participant behaviour. BOS explained that the primary relationship would remain between the Consumer and the ATP. If an ATP used data for a purpose beyond that authorised by the Consumer, the Consumer would raise the issue with the ATP directly. Such behaviour would also constitute a breach of the ATP's obligations under both the relevant regulatory framework and the CCS arrangements, potentially triggering assurance or enforcement action.

SJ added that the current design principle is that CCS will not act as a central consumer complaints body. Consumers will initially direct complaints to the ATP, which is required under the Data (Use and Access) Act framework to maintain complaints procedures. RECCo is separately considering how Consumer support and issue escalation should operate and plans to return with further proposals on issue resolution arrangements at a future working group.

There was further discussion on how CCS could identify problematic participant behaviour. BOS noted that Consumers can revoke permissions through the platform, immediately ending data access where concerns arise. MPW explained that the platform will record revocations, disputes and other Consumer interactions, enabling monitoring of participant behaviour over time. Trends such as unusually high levels of consent withdrawals or disputes could be used to target assurance activities and investigate potential misconduct. They confirmed that RECCo will explore additional ways to capture Consumer feedback and use it to strengthen trust and oversight of ATP behaviour as the platform evolves.

A member highlighted the need to consider CCS within the wider context of smart data trust frameworks rather than as a standalone solution. They stressed that future arrangements should include clear Consumer redress processes, oversight of participant conduct, and mechanisms to assess whether organisations remain suitable to access the system. The member noted that best-practice discussions within the Smart Data Council favour a clear, Consumer-centric complaints and redress process, with consideration given to how complaints

are reported, investigated and used to determine whether a participant should continue to operate within the scheme. They encouraged RECCo to engage with a broader range of regulators and stakeholders to ensure the CCS framework is future proofed for wider smart data initiatives. SJ responded that RECCo is considering consumer redress and issue resolution arrangements as part of ongoing engagement with Ofgem, DESNZ and wider digitalisation initiatives.

A member sought clarification on whether parties could pursue legal claims relating to data shared through CCS. BOS explained that the Access Agreement is intended to support liabilities and obligations directly associated with CCS and does not create a route for disputes unrelated to CCS. However, where a participant fails to meet obligations connected to the service—for example, providing incorrect information where accuracy is part of the agreed service obligations—the contractual framework could provide a mechanism for affected parties to seek redress. BOS clarified that the agreement uses bilateral contracts supported by third-party rights provisions, allowing participants involved in a specific CCS data-sharing arrangement to pursue remedies where another party breaches obligations linked to that service.

A member asked whether revoking consent would require an ATP to delete data. SJ and MPW noted that this is still under consideration but highlighted that existing GDPR obligations, including data protection rights and retention requirements, would continue to apply regardless of CCS processes.

A member raised concerns that Consumers are more likely to contact their Supplier if they suspect misuse of their data, rather than approaching CCS or the ATP directly. AP and MPW acknowledged the point and agreed that guidance may be needed to help Suppliers identify CCS-related issues and direct Consumers to the appropriate organisation. They noted that clear signposting will be important to maintaining Consumer trust in the service.

A member questioned how RECCo would identify organisations that repeatedly misuse data or generate high levels of complaints. MPW explained that monitoring and reporting arrangements are still being developed but agreed that trend analysis and broader assurance monitoring will need to be considered. They committed to further work on how CCS can identify patterns of poor behaviour, support investigations, and provide assurance that unsuitable participants do not continue operating within the framework.

A member also requested follow-up clarification on how the EES, which underpins aspects of the CCS solution, will interact with assurance and monitoring arrangements. The Chair agreed to provide further information at a later date.

4. FORWARD PLAN

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

There is a provisional date for the next Engagement Webinar on 22 July, which will cover a review of RECCo's quarterly plan. The next Topic Solution Group meeting on 16 July will focus on Identity and Verification, and MPW added that more topics may be added ahead of the

meeting. The Chair advised that Topic Solution Groups will continue on a fortnightly basis, with future topics to be confirmed as soon as possible.

The Chair advised that any members with queries are welcome to email consumerconsent@retailenergycode.co.uk, and the RECCo project team will be happy to respond. TT 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
Teresa Thompson	Retail Energy Code Company	TT	Chair
Sarah Jones	Retail Energy Code Company	SJ	Presenter
Brian O'Shea	Retail Energy Code Company	BOS	Presenter
Matt White	Retail Energy Code Company	MPW	Presenter
Ann Perry	Retail Energy Code Company	AP	Presenter
Edma Hyskaj	REC Code Manager	EH	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