The Consumer Consent Solution

Frequently Asked Questions

Published: 27 February 2026

Contents

What is the Consumer Consent Solution?

The Consumer Consent Solution (CCS) is a standardised, secure framework that lets people give, manage, and revoke consent to share their energy data with trusted third parties. It will be part of the Retail Energy Code (REC).

The Retail Energy Code Company (RECCo) leads delivery, while the Office of Gas and Electricity Markets (Ofgem) provides policy direction.

Why is it necessary?

People need a simple, trusted, and consistent way to control their data. As the energy system becomes smarter and more digital, data helps people make informed choices. This solution puts control back in people's hands and builds trust.

- ➔ People can share data confidently for their own benefit
- ➔ Tailored services become easier, such as flexible tariffs, energy advice, and switching support
- ➔ Confusion and duplication are reduced across the market
- ➔ Privacy and security improve through clear rules and audits
- ➔ Innovation grows, which helps people save money, cut carbon, and choose services that fit their needs

Who does it impact?

1. Consumers gain greater transparency and control over how their data is used
2. Energy suppliers, service providers, and third-party intermediaries (TPIs) adopt the solution to support new services and migrate existing consents into the solution
3. Data holders and infrastructure operators integrate with the framework to enable secure, consistent data sharing
4. Regulators, policy makers, and consumer groups use it to ensure fairness, privacy, and consistent practice

Does it include non-domestic customers?

No. The first release covers domestic customers only. Non-domestic customers are out of scope, as their data sharing is permission-led rather than consent-led.

How will it benefit domestic consumers?

- Clarity to view and manage consents
- Choice to access a broader range of services
- Confidence that data is used properly
- Control to revoke consent at any time
- Longer-term benefits will unfold for consumers, the market, and the system

How will it build on existing consumer mechanisms and avoid duplication?

The approach is to **reuse** first. It will align with existing mechanisms, such as smart meter opt-in and open banking, where it adds value. It will not replace working solutions unless there's a clear benefit. The goal is to reduce fragmentation, avoid duplication, and make it easier for people to give informed consent through familiar channels. Changes will be delivered through the REC, including a new REC Schedule and updates to the REC Data Specification.

How will it interact with other industry initiatives?

The goal is a cohesive, interoperable data ecosystem that reduces duplication and works seamlessly for consumers and the market. This means it will complement and integrate with several industry initiatives:

- Data Sharing Infrastructure (DSI)
- Flexibility Market Asset Register (FMAR)
- Smart Data Repository (SDR)
- SEC Other User (SOU)
- Tariff Interoperability (TI)

How can industry and third parties use it?

- Obtain and manage consent in a standardised, secure, and auditable way
- Reduce the cost and risk of fragmented or bespoke consent systems
- Launch innovative, data-driven services with confidence
- Build consumer trust with a consistent, easy-to-understand consent experience across energy services
- Meet regulatory and data protection requirements, such as the UK General Data Protection Regulation (UK GDPR)
- Unlock new opportunities, such as supporting adjacent initiatives like the Smart Data Repository (SDR) and

Smart Data work

How can consumers use it?

- Share data with switching and comparison services
- Enable personalised energy advice
- Join demand flexibility offers, including off-peak savings
- Access social support or tailored tariffs (for example, through housing providers or charities)
- Access new services as they emerge

How is it different from existing consent tools?

Consent is fragmented. Many journeys rely on bilateral contracts between service providers and data holders. This slows sharing and adds complexity. The new approach changes that.

- Standardises and simplifies consent across the energy sector
- Provides one consistent, interoperable foundation across the market
- Enables faster, more secure data sharing between organisations
- Focuses on simple journeys, transparency, inclusivity, and security by design
- Reduces reliance on separate bilateral contracts between service providers and data holders
- Replaces fragmented, duplicative approaches with a single trusted route
- Helps businesses meet regulatory and data-sharing requirements, and supports consumers' rights under the Data Use & Access Act 2025 (DUAA), subject to the legislation being in force

When will the framework be available, and how do MVP and MMP differ?

➔ A Minimum Viable Product (MVP) will be developed and tested in 2026. It proves the service with the smallest feature set.

➔ A Minimum Marketable Product (MMP) will follow in Quarter 1, 2027. It will add what's needed for broad market adoption and deliver the first market-ready release.

➔ Iterative releases will follow through 2027 and beyond.

The timelines seem tight. Is this realistic?

Yes. The programme is phased, with delivery broken into quarters and two-week sprints, enabling us to keep a tight focus and have early awareness of risks and challenges etc. Governance, assurance, and delivery move in parallel to achieve the first market-ready release (MMP), leveraging existing governance frameworks and system functionality to accelerate progress and minimise disruption

We'll continue to share progress through the REC Portal Consumer Consent Hub and the Consumer Consent Digest newsletters.

What data will be available?

It enables and manages a person's consent to share data through other agreements. The MMP will initially support Half–Hourly metered data. Additional data types will become available as more sources are added to the framework.

How is the ongoing use or onward sharing of data prevented?

- ➔ Common journey and language
- ➔ Clear what's shared, when, with whom, and for what purpose
- ➔ Access is only permitted for that purpose
- ➔ Other third parties cannot access that data
- ➔ Breach of conditions if shared onward, with removal from the Trust Framework
- ➔ A directly of approved providers

How will it be governed?

It will be underpinned by a governance framework in the REC, which will set obligations, roles, and service levels. A new REC Schedule and updates to the REC Data Specification will codify the model. Accreditation, onboarding, and audit will sit in the Trust Framework, with compliance managed through the Performance Assurance Framework (PAF). Further details will be shared once the REC Change is agreed upon.

How does it link to the Data Use & Access Act 2025?

It aligns with the Data Use & Access Act (DUAA), and RECCo acts as the Interface Body. This ensures secure and fair data sharing.

How will industry be consulted and informed?

- Through 2025, we ran three working groups with representatives from across the sector, providing expert input and open, transparent engagement. Each working group published a recommendation paper, which, in turn, fed into initial design proposals.
- Following stakeholder feedback, the previous three groups have been streamlined into a clearer, more flexible structure with less overlap and duplication:
    - An umbrella CCS working group (meets twice per quarter): Webinar-led sessions providing market-wide updates, the overall delivery plan, and a summary of key topics; and
    - Topic-specific solution groups (meets every two weeks): Focused deep dives into priority issues in greater depth.
- Further information, including details of how you can express an interest in joining the CCS working groups can be found here: Register your interest: Join our CCS working groups
- Updates are shared on the REC Portal Consumer Consent Hub, Consumer Consent Digest monthly newsletters, RECCo Consumer Consent Service Hub, and engagement days.

Will the session be recorded or summarised for stakeholders who cannot attend?

General update sessions are expected to be recorded. Clear summaries and read-outs will be shared so stakeholders can stay informed even if they cannot attend live.

How does the CCS interact with Elexon's P494 and the Smart Data Repository (SDR)?

CCS provides the consumer consent layer—recording whether a consumer has agreed to share their energy data. At day one, consent capture does not, in itself, grant operational permission; it establishes the authorised basis for data sharing. P494 and the Smart Data Repository (SDR) focus on how data is stored and accessed, while CCS focuses on whether the consumer permits data access. The two are designed to work together, not overlap.

Will CCS be mandatory for parties accessing data under P494, or will parallel routes exist?

Yes – where parties wish to access data via the Elexon SDR and consumer consent is required, use of the CCS will be mandatory. CCS is being designed as the standard mechanism for managing consumer consent under P494. While it is not currently mandated in all scenarios, the clear intention is to avoid parallel or duplicated consent routes, and therefore, access routes requiring consumer consent through SDR will be expected to use CCS.

How will CCS Interoperate with Tariff Interoperability, SDR, DSI, and FMAR over time?

CCS is being designed as the cross-market standard for managing consumer consent. Over time, it is expected to interoperate with SDR, DSI, FMAR and Tariff Interoperability by providing a consistent way to capture, validate and share consent across services. The intention is to avoid multiple consent routes and enable a joined-up approach as these programmes evolve and align.

Will CCS cover both electricity and gas data?

Yes. CCS will cover both electricity and gas data. The solution is being developed in a data source-agnostic way, meaning it is designed to manage consumer consent consistently regardless of whether the underlying data relates to electricity or gas.

What is the difference between an Authorised Third Party (ATP), an Energy Data Provider (EDP), and a CCS User? Who falls into these categories?

- **Authorised Third Party (ATP):** An organisation acting on behalf of a consumer to access or use their energy data (e.g. comparison services, energy apps).
- **Energy Data Provider (EDP):** An organisation that holds, controls, or has access to energy data (e.g. suppliers, network operators, Elexon, SEC, Other Users).
- **CCS User:** A collective term for both ATPs and EDPs that have been accredited to participate in the CCS arrangements.

Who decides how organisations are classified?

Classification is based on what role an organisation plays in data sharing, not who they are. An organisation may act in more than one role in different contexts.

How will microbusinesses be treated compared to domestic consumers?

The scope of the CCS Minimum Marketable Product (MMP) will apply to domestic consumers only. Extending CCS arrangements to cover non-domestic customers (including microbusinesses) will be considered as part of the future roadmap.

How will suppliers be treated under CCS?

Suppliers are not required to become accredited CCS Users as part of the Minimum Marketable Product (MMP). The initial focus is on half-hourly consumption data held or accessible by Elexon and SEC Other Users.

Ofgem's direction included a proposal that existing supplier consents could also be recorded within CCS. This will be considered further during 2026.

How will CCS avoid duplicating onboarding, assurance, and audit requirements already required under SEC, REC, or BSC?

CCS is being designed to reuse and recognise existing assurance and security controls wherever possible. The aim is alignment, not repetition.

Is there a plan to align or recognise existing accreditations across codes?

Yes. CCS is being designed to align with existing accreditation approaches where possible, to avoid unnecessary duplication.

It is proposed that, as a minimum, CCS Users would be required to hold **Cyber Essentials Plus certification**, consistent with the expectations set out in the Ministerial letter on cyber security - GOV.UK.

We also expect to base CCS accreditation requirements on the existing REC approach for Non-Party REC Service Users accessing data through the REC enquiry services.

Will CCS introduce new security requirements?

CCS will set **minimum security standards** to ensure consumer data is protected, including requirements to support secure data exchange.

Where possible, CCS will align with existing industry controls and assurance frameworks to minimise duplication. However, to reduce ambiguity and complexity, CCS will aim to define clear minimum standards rather than relying heavily on “or equivalent” approaches.

Is CCS considering a ‘new consent first’ approach rather than bulk migration?

This is still under consideration. CCS is exploring a “new consent first” approach, prioritising new consents and migrating existing consents only if they are clear, valid, and safe to do so.

Why is CCS cautious about migrating old consents?

Some legacy consents may be unclear, outdated, or poorly evidenced. Migrating these without care could risk consumer harm or legal issues. CCS is prioritising trust and clarity over speed.

How will consumers be informed if an existing consent is migrated?

If consents are migrated, consumers will be clearly informed and given the opportunity to review and manage them.

Who is responsible for identity verification (IDV) within the CCS ecosystem?

The central CCS solution provided by RECCo will be responsible for delivering identity verification (IDV). RECCo is planning to procure one or more specialist service providers to carry out this activity.

What happens if matching fails?

Clear fallback and support processes will be put in place so consumers are not blocked without explanation or help.

How will CCS ensure consent is clear, informed, and not buried in small print?

The **Customer Experience Guidelines** will define how consumers interact with the CCS across the Request, Renew, Review, and Withdraw journeys. To ensure these Guidelines serve all consumers effectively, we have developed four behavioural archetypes. Each archetype surfaces distinct needs that the Guidelines must address.

How easy will it be for consumers to review and revoke consent, and what happens if they see a consent they do not recognise?

CCS is being designed to make it **straightforward for consumers to review and revoke consent.** If a consumer identifies a consent they do not recognise, they will be able to dispute or revoke it.

Appropriate safeguards will also be built in, particularly for **shared properties**, to ensure the correct person is taking these actions. This balance between ease of use and security is being carefully designed.

Is there a published cross-programme governance map covering CCS, SDR, FMAR, and related initiatives, and when will more details be available?

CCS is currently developing a cross-programme governance map to show how decision-making links across CCS, SDR, FMAR, Tariff Interoperability and other related initiatives. This will be published once finalised, and will provide more detail on how governance alignment across codes will work in practice.

Who can I contact for more information?

Whether you have a question, concern, or want to stay informed, our dedicated Consumer Consent Solution team is here to help and collaborate with you. Contact us at: **consumerconsent@retailenergycode.co.uk**