Retail Energy Code Company Ltd
27 Old Gloucester Street
London, WC1N 3AX

Retail Energy Code Company
info@retailenergycode.co.uk
www.retailenergycode.co.uk

By email only: digitalisation@ofgem.gov.uk

4 October 2024

RECCo response to: Consumer Consent Solution Consultation

We welcome the opportunity to respond to this consultation, Consumer Consent Solution. Our non-confidential response represents the views of the Retail Energy Code Company Ltd (RECCo) and is based on our role as operator of the Retail Energy Code (REC) and potentially of the Centralised Registration Service (CRS).

RECCo is a not-for-profit, corporate vehicle ensuring the proper, effective, and efficient implementation and ongoing management of the REC arrangements. We seek to promote trust, innovation and competition, whilst maintaining focus on positive consumer outcomes. Through the REC, the services we manage, and the programmes we run, we are dedicated to building a more effective and efficient energy market for the future. We are committed to ensuring that RECCo is an "*intelligent customer*", ensuring efficacy and value-for-money of the services we procure and manage on behalf of REC Parties, including those which constitute the REC Code Manager.

RECCo has been engaged with Ofgem over the past two years on the Consumer Consent project. Our response is based on a detailed understanding of the intent of the project, its requirements and an informed analysis of the options.

Summary of the key points discussed in our consultation response:

- A hybrid model that considers, on a case-by-case basis, the most effective approach to delivering each of the required functions of the solution will deliver the optimum outcome.
- Detailed aspects of the design should be considered through consultation led by the Delivery Body, once the selection process for the Delivery Body is complete;
- We broadly agree with Ofgem's assessment of the delivery bodies but believe that it its conclusion could be reinforced by highlighting RECCo's unique position as manager of a consumer-orientated code that protects customers' data and already incorporates key elements of governance that will be required by the Consumer Consent solution;
- The REC's governance processes can obviate the requirement to establish new oversight mechanisms and potentially alleviate the need for new licence conditions.

We are happy to discuss any of the points raised in this response.

Yours sincerely,

Jon Dixon
Director, Strategy and Development

Appendix 1: RECCo response to consultation questions

Q1: Do you agree with the proposed Design Principles? Would you recommend any additional Design Principles?

We support the proposed principles, though we see opportunities to refine the definitions. Refinement will provide greater clarity of needs and expectations as well as ensure that Ofgem (and by extension consumers) have more robust controls over the consent mechanism (governance, service and technology). This will ensure the best outcomes are achieved through this work. Below we provide comments about each principle:

a) Simple and Low Friction

We think it is culturally important to enshrine that the overriding priority of this work is to explicitly serve consumers' best interests. The Simple and Low Friction principle seems to be suitable for this and so we recommend that part of its definition states unambiguously that the Consent Solution and work of the Delivery Body are to be consumer focused. This will provide important messaging to the Delivery Body and other stakeholders and may contribute to building trust with consumers in a Consent Solution. While we know serving consumers' interests is Ofgem's overriding intent, we think it is worth including this principle to make this absolutely clear to all.

As well as being "simple and low friction", we suggest that the service needs to be "consistent", as this will allow consumers to become familiar with it over time and steadily increase their trust in it. In other respects, this principle might be well described as a subset of the Inclusive by Design principle. This is because ensuring that a service is simple to use and that its user experience is 'low friction' and does not present unnecessary barriers to engagement could be considered to be aspects of what it means to be 'inclusive-by-design'; however, we think Ofgem's defining this theme as a dedicated principle will create the emphasis needed to ensure that the solutions created prioritise simplicity and low-friction services.

One way we believe Ofgem can gain assurance that simplicity of design and low-friction services are being achieved (see paragraph 3.6) is by having the Delivery Body adopt the 'presumed open' stance to the information that describes the design of the solution architecture (i.e. borrowing from Data Best Practice guidance). This will lead to maximised responsible opening of data, software scripts and data models wherever practical and value for money to do so. The benefit of this will be to promote service transparency, trust and accountability, making it easy for all market actors to scrutinise and form opinions over whether in practice there is simplicity of design on a continuing basis.

RECCo is set up to support this way of working. REC expects Data Best Practice Principles to be followed as part of its 'Data Access Principles' and we would apply this to a Consent Solution as a new service[1].

b) Interoperable

In this section of the consultation (see paragraph 3.7) Ofgem describes its expectations of the approach to be taken for creating a Minimum Viable Product (MVP) service before maturing to Live operations. We support this approach. Ofgem has also described its vision for a mature solution, which implies the creation of a highly advanced service capability and sophisticated user experience. This vision is demanding, but achievable and would be of great value to consumers. We therefore propose an agile approach to delivery with full

[1] https://digital-navigator.azurewebsites.net/codes-schedules/2/5.2

consultation with industry parties to achieve full interoperability and the meeting of the other Design Principles.

It will be important for the Delivery Body to coordinate with the other digitalisation-related initiatives taking place in the sector, such as the Smart Secure Electricity Systems (SSES), Data Sharing Infrastructure (DSI) and Flexibility Market Asset Registration (FMAR) programmes.

We anticipate that the Delivery Body will need to keep cross-sector usage of personal data in-scope of its work, even though it should be led first by the needs of energy consumers. In the long-term some of the largest benefits to consumers gained from giving permission for their personal data to be processed will be realised through the integration of personal data held by different organisations operating in different vertical markets, who today, are unable to create integrated insights for people.

We therefore think consumers' overall needs will be best served if their energy consent service includes explicit expectations on its Delivery Body to promote cross-market interoperability, while still positioning the energy market as its overriding priority. We think this expectation should stop short of requiring the Delivery Body to be responsible for creating cross-market interoperability (as this goes beyond the Delivery Body's and regulator's control), but that it does expect the Delivery Body to lower barriers to cross-market interoperability, wherever practical.

c) Agile, Flexible, and Scalable

Agility, flexibility and scalability are key topics. Common pitfalls for complex initiatives are that programmes achieve early success but then struggle to scale to meet wider market needs, or that programmes are too strongly wedded to initial assumptions. This results in them building services that mismatch against what users really expect and require because they have not adapted plans or anticipated this possibility and so have not built in project flexibility to accommodate the risk of user needs driving changes to requirements over time.

If RECCo is appointed as the Delivery Body, we would manage delivery through our proposed approach of continuously integrating features into an initial (limited in scope) Live service (see our response to the Interoperability principle, above). This approach creates an ongoing focus on design and integrates flexibility and enduring opportunities to adapt 'by-design' of the delivery approach; this will create long-term dividends and low-risk delivery of services.

Our approach achieves agility, flexibility and scalability of programme delivery and services because it leads to a modularisation of service features. This provides a fine-grain control over decisions and so leads to:

- the agility to course-correct the design of services as we continually learn needs from real consumers
- flexibility to reconfigure, modify, add and remove service modules for a dynamic solution
- scalability through controllability granting access to sophisticated automated testing that will sustain design and process transparency as complexity grows over time and so ensure that stakeholders responsible for governance (security, privacy, performance, etc.) retain trust in the service design

We support the Ofgem suggestion of working in partnership with Citizens Advice and/or organisations like them. We think this will be enhanced through a broader collaboration that engages all types of stakeholders and service providers in the testing and development process. Accordingly (given Ofgem's positioning RECCo as its preferred option as the Delivery Body) we have begun discussion with Citizens Advice and other market stakeholders to investigate this approach further, with a view to working through Local Citizen Advice (LCA) offices and equivalent services provided by other consumer bodies/charities.

We think this approach has the potential to simultaneously meet a complex collection of needs. It will:

- provide important early benefits to a cohort of consumers who already know and trust community service providers (like Citizens Advice and the Money Advice Trust) and who tend to be facing vulnerabilities that can be overcome through consented use of personal data;
- enables service providers, like supplier licensees and personalised service providers with innovative business ideas to engage with a prototype service and so share feedback and learn practical requirements that will help their business prepare for consent services;
- opens the door to longer-term more strategic market support, such as working with Citizens Advice across their whole portfolio of consumer customers so that deeper insights can be (permissively) gained about how to tackle vulnerability and develop new personalised consent-based market services;
- allow for testing and understanding of front-end service needs: Citizens Advice will have need for consent data dashboard interfaces;
- refine back-end service needs and API integration requirements that can be abstracted for any organisation to use when developing its own front-end user services.

Another aspect of the Consent Solution that requires agility, flexibility and scalability is its financial arrangements and overall commercial suitability. We would expect conscious choices to be made by stakeholders over designs and solution delivery that balance the trilemma of needs that characterise any project: cost, time and quality. This should be included in stakeholder engagement discussions and be subject to ongoing review to allow for preferences to evolve over time; this will help the delivery programme stay honest with its stakeholders as it makes its programme decisions.

d) Transparent and Informative

A cornerstone of ensuring consumers can trust the service is in it always being absolutely clear to them which organisations are accessing their data and the purposes of this access.

It will drive better outcomes if the Delivery Body is required to maximise the transparency of its work. This would gain stakeholder engagement and provide greater accountability and assurance about progress made. To enhance delivery against this principle Ofgem may wish to mandate compliance with the Data Best Practice guidance; it may also be prudent to expect the Delivery Body to produce planning information that, among other information, includes following the principles of the Digitalisation Strategy & Action Plan guidance.

It is our expectation that many features of the Consent Solution and its delivery programme can be made transparent in ‘near real-time'. Examples include: programme information such as roadmaps, work packages, service visions, existing descriptions as well as (de-sensitised) stakeholder feedback and how this is being acted on and data architecture (data tables, data models, data processing algorithms). This can all be subjected to the Ofgem ‘Open Data Triage’ process to maximise transparency. The REC is comparable in this sense: RECCo already runs its processes openly, which contributes to creating positive experiences for our users. Our 2023

Annual Satisfaction Survey shows satisfaction across RECCo services and a view that our services are continuing to improve.[2]

We have begun working openly for our preparatory work; this demonstrates the spirit of how we would continue to work if we should be appointed the Delivery Body for the Consent Solution. We expect that continuous testing and validation will be required to strike the right balance between delivery and making the service transparent and informative. Through applying a test-driven approach to all parts of the service delivery and its associated transparency information, the Delivery Body will be able to continually adapt its work to respond to the needs of consumers and the market. Additionally, to ensure work of the Delivery Body is informative for end-users of the service it could seek the Crystal Mark from the Plain English campaign.[3]

e) Inclusive by Design

For this inclusive design principle to fully meet the expectations of all consumers, we recommend additional specificity in its description to ensure that all aspects of inclusivity are accounted for. We recommend that Ofgem's explanation of the principle includes mention of the standards that are to be adhered to and that the standards and guidance we have included in our answer to Q4 are considered for this.

It might be appropriate, for example, to make explicit mention of WCAG2.2 compliance as part of this principle; that the solution should be multi-lingual from the outset; and that non-digital service channels will need to be included and integrated into the overall service. It may also be suitable to set expectations on the user research approach, such as ensuring demonstration of securing a diverse demographic’s engagement with the research.

If RECCo is appointed as the Delivery Body it would be our plan to engage with end-consumers directly throughout our research and for these users to be selected to ensure representation across user types, demographics and geographies. We would conduct this research in multiple ways, including focus groups and through research and testing we intend to carry out in partnerships with consumer bodies who provide support services to end-consumers. This will ensure our understanding (and therefore development requirements) reflect actual user needs and that the service design will be inclusive for all consumers.

f) Secure by Design

We agree that this is an important principle, and we recommend that it is extended to also include privacy-by-design. We have provided additional standards and working practices that should be considered by Ofgem and the Delivery Body to ensure this principle is met (see our answer to Q3). Working with the NCSC and ICO for security and privacy considerations, respectively, will be vital to success. The Delivery Body will have to develop ways of working that are compatible with the operating models of these two organisations. For example, these organisations do not necessarily take on a direct role of ‘signing-off’ approvals of designs and solutions, meaning the Delivery Body will need to take on the responsibility of learning and understanding expectations and interpreting these into designs, working practices and policies for the development and

[2] https://www.retailenergycode.co.uk/fs/wp-content/uploads/2024/04/RECCo-Annual-Satisfaction-Survey-Results-2023-24.pdf

[3] See https://www.plainenglish.co.uk/

operation of the solution. This carries risk for the Delivery Body and so should be the subject of scrutiny and discussion among stakeholders in advance of costly investments being made.

Q2.Do you have a preference between the centralised, decentralised or hybrid models? Please elaborate.

We prefer a hybrid approach.

We do not view there to be a singular dichotomy between centralisation and decentralisation. There are many features to a Consent Solution and often these features can have independent decisions made over the extent to which their services are designed to be centralised or decentralised. We prefer that design decisions are made with consumer outcomes more directly in mind.

We recognise that centralisation/decentralisation is a recurring theme during market discussions and that there are legitimate concerns among stakeholders that need to be heard, thought through and aligned. For example, it is the normal practice of the UK government to leave energy markets to their own devices except where compelling evidence justifies a market intervention and a characteristic of decentralisation is that it tends to enable more actors to operate autonomously, i.e. as a free market. Decentralisation is often, therefore, viewed as preferrable to centralisation of services by default, with centralisation then being expected to require justification ahead of adoption.

However, we advocate for framing design option decisions around the best practice methodologies that are well-established in workplaces, i.e. presenting design decisions in terms of their propensity to deliver the best positive outcomes for consumers with this including a lineage of evidence (requirements, risks, capabilities, etc).

Important nuances to inform the centralisation versus decentralisation discussion:

- **They are relative terms**. We might centralise by storing consent data in one organisation or decentralise by storing consent data among suppliers or other companies. But we could go further in both cases, by centralising consent data in a single database or decentralising further by storing consent data in individual wallets for each consumer. It tends not to be the case that something is centralised or decentralised, but rather to what extent it is.
- **Multiple definitions of centralisation/decentralisation can be relevant at once**. Selection of a single cloud native platform to provide a Consent Service would simultaneously centralise technology choices but decentralise data centre storage locations. Depending on the frame of reference used, this as a design option would centralise and decentralise services. It does both at once.
- **Governance and technology options are generally independent of each other**. Decision-making over the data architecture design of a Consent Solution might, for example, be made centrally but this would not constrain the choice over whether to have a single solution implement this architecture for market reuse or whether to have market participants each individually implement a version of this architecture into their own systems.
- **Each model offers unique advantages/disadvantages and it is these that we should focus on.** For any design decision it is what centralisation/decentralisation provide as services or as risks that really matter. These consequences should be the focus, rather than seeking an overarching principle: what is the propensity for scalability? How complex is security? How responsive is the solution to meeting changes to consumers' needs?

Other prominent technical considerations:

- **Accreditation services**: these are not new and, related to this work, they have been successfully implemented in Open Banking. In the case of Open Banking banks and third parties are accredited as approved providers: this lowers barriers to consent provision for consumers at the point of their use of consent-based services. The Open Banking approach has a mix of decentralised features (actual consent-gathering services) and centralised features (accreditation register and associated services).
- **Monitoring services**: these can help improve the quality of the service by reducing instances of erroneous use of personal data and incorrect holding of permissions for using personal data. Operational monitoring can conduct validation tests of marketplace actors' understandings of their permissions to work with personal data in order to proactively catch errors and manage practical issues, such as the potential for a desynchronisation of the status of permissions. This will ensure consumers expectations are met when interacting with services.
- **Giving consent and related authentication services**: there are a range of design options for these services; they feature varying centralisation/decentralisation and typically include use of tokens either held in highly federated Digital Wallets or by the Delivery Body or by data providers. Each method has advantages and disadvantages and this requires more detailed investigation and consultation before a preferred approach is selected. There is scope to reuse/expand on existing methods.
- **Obtaining data:** personal data storage and transfer also includes design options. It is unlikely to be a good solution for the Delivery Body itself to handle the personal data being shared; however, there are options with regard to whether data is passed on from data holders to third-parties or whether more sophisticated information sharing techniques are employed, such as through having data providers share 'answers to questions', rather than 'data about which questions can be asked'. Rather than address these topics through theory, we believe they are better tackled in the context of specific use cases with practical requirements.
- **Coordination:** The Consent Service is not the only industry initiative taking place at present that is investing in digitalising services and aiming to support consumers in vulnerable circumstances. Other prominent regulatory/policy examples include Data Sharing Infrastructure, the Smarter Regulation consultation, and the Vulnerability Strategy. The industry itself has already invested in many services that can be borrowed from and taken advantage of through reuse. Development of this service will need to coordinate its investments with these industry and policy initiatives. The Consent Service itself will also require coordination across industry as it is likely in any realistic scenario that many organisations will need to provide stages of the service journey for consumers to be motivated and to actually gain the intended benefits. We support the Delivery Body taking on the role of leading on this coordination work and, if RECCo is appointed as the Delivery Body, we would use the established REC processes to facilitate this.

Q3: Do you consider the security measures referenced in this section, including the access control measures, will meet the requirements of a consent solution holding consumer data? Which additional protections would you recommend?

The security measures that have been proposed, including access controls, are essential for managing sensitive consumer data. Our view is that the Delivery Body should work with the NCSC from the outset and do so continually along with other key stakeholders. Doing this would establish and maintain an agreed approach to security that should, among other activities, agree the specific set of security standards to be complied with.

In addition to those proposed by Ofgem, we suggest that a broader set of security standards and protocols are considered with stakeholders for use both for guiding the solution itself and for the delivery programme through which the solution is created. We have provided a list of additional security standards and practices to consider at the end of our answer to this question (note that a cloud deployment has been assumed).

We consider it essential that policies and practices are established by the Delivery Body and its programme of work, such that:

- it is ensured that security standards are always considered and integrated into the setting of requirements for all programme and solution design, development and operations tasks;
- the programme continually measures compliance with security standards as part of its quality assurance testing of each task and that it takes remediating action based on findings;
- there are robust security processes for software integration and deployment for all releases and updates to the solution;
- portfolio-level monitoring and evaluation of programme and solution security is carried out effectively.

Additional security and privacy standards to consider:

1. **NCSC certifications –** The UK's National Cyber Security Centre (NCSC) provides a certification scheme to ensure protection against common cyber threats. These include **Cyber Essentials and Cyber Essential Plus**, which may be sensible certifications for the Delivery Body to ensure developers of Consent Solution services are validated against;
2. **GDPR** – Compliance with GDPR may seem self-evident in the case of this Consent Solution, but it is best practice to explicitly state all standards to be followed;
3. **PCI-DSS (Payment Card Industry Data Security Standard) –** The applicability of whether the service needs to be designed to meet this standard will depend on the service design and architecture; the standard is specific to payment data. PCI-DSS's encryption and security practices could be adopted for consumer data protection;
4. **FIDO2 Standards –** This is an emerging standard that the service might need to align to if a highly decentralised solution architecture is adopted; for example, it is relevant in the case of digital wallets. Implementing Fast Identity Online (FIDO2) enables secure, passwordless authentication and reduces the risk of credential theft;

Practices to consider:

5. **NCSC guidance** – As well as providing the Cyber Essentials standards, NCSC provide guidance for how services are best delivered with respect to security. Any service development should follow the **14 Cloud Security Principles** and the **10 Steps to Cyber Security**;
6. **'Zero-Trust' Architecture approach**: This is a common working methodology among architects. It achieves high security standards through designing each technology component within a solution to require verification, authentication, and authorisation from other components before any access requests can take place between them. This 'zero-trust' model helps minimise the risk of insider threats and also hardens services against external attacks;
7. **CIS Critical Security Controls** – These are a collection of recommended actions for mitigating cyber attacks, including advanced threat protection and access controls. They include hardening guidance and methods for securing enterprise systems;
8. **Create a Security Operations Centre (SOC)** – the Consent Solution should be subject to active monitoring of its systems in real-time. This might be achieved by deploying a **Security Information and Event Management (SIEM)** solution to proactively detect and respond to anomalies and threats; this

methodology can be thought of as akin to applying agile working techniques to delivery, only in this case the context is security management;

9. **Multi-Factor Authentication (MFA)**: Enforce MFA for all users accessing the consent solution to enhance security beyond simple password protection;
10. **Penetration Testing and Audits**: Regular third-party penetration testing and security audits should be conducted to identify vulnerabilities and ensure compliance with the agreed security standards;
11. **Incident Response Planning –** Establish a detailed incident response plan, ensuring that stakeholders are prepared for quick and effective actions in case of a data breach or other security incident;
12. **Detailed Logging and Monitoring**: Maintain comprehensive logs of all access attempts, changes to consent records, and system activities. These logs should be regularly reviewed to ensure compliance and detect any irregularities. They should provide audit, such as for ensuring accountability, and should support forensic investigations in case of incidents.

In the context of practical technical design, we consider that a token-based approach is a strong candidate for providing the service capabilities that the Consent Solution will require. This method preserves opportunities for a decentralised design for other aspects of the service (such as the ability of consumers and third parties to autonomously engage with the services and therefore for consumers to only have to directly engage with organisations that they trust.). Meanwhile, this design approach also has attributes that position it well to meet the expectations of security and privacy; key examples here are that tokens are well-suited to efficiently enforcing all of the GDPR minimum requirements, such as for the expiry of consent permissions and revocation of permission given.

Certain topics will raise complex questions relating to security and privacy. For example, a known but unresolved challenge in the sector is the need to manage risks to personal identification in households where there are multiple people, only one person is the bill payer and that bill payer may be a landlord and not a resident. We have sought legal advice on this subject, which has advised that there is room for early progress to be made through starting with limited services that treat bill payers as the people entitled to manage consent permissions. However, we recognise that this will not be suitable for all situations. This is an important subject that will require ongoing stakeholder engagement, especially as service provision and complexity increases over time.

To manage this, we will grow the scope of the service incrementally over time to minimise risk. We can also use the research and testing we conduct with consumers to create and share a body of knowledge on this topic that can in turn aid legal processes in better defining best practice and the law. Ultimately, the solution needs to be fit for purpose, while keeping consumer data secure and ensuring value for money. If selected as Delivery Body, we would at each stage consult with stakeholders through established REC processes (which allow us to engage both with REC Parties and non-REC Parties) to determine how this can best be achieved.

Q4: Do you consider these standards are sufficient parameters to ensure inclusivity, accessibility and interoperability for the consent solution? Which standards would you recommend?

The proposed standards cover many important aspects of making the consent solution accessible and inclusive. We recommend that additional standards and approaches are considered to ensure that everyone, particularly people who are not comfortable using digital systems, can easily use and benefit from the solution.

There will be people who need human help, such as through receiving support from community support hubs like charities (local Citizens Advice branches, Money Advice Trust helplines, local government community centres and many more) and through companies' call centres, where trained staff can assist them with consent management. This brings additional challenges, such as ensuring that those people who play roles helping others to use the service can do so securely and with appropriate well-evidenced permission.

While the listed standards address many aspects of inclusivity and accessibility, additional considerations for human-assisted access and delegated authentication will be essential. We expect that multiple authentication and verification methods will be required for a fully inclusive service. Standards like WCAG 2.1, ISO 9241-171, and ETSI EN 301 549, combined with non-digital support mechanisms, will ensure that the consent solution is universally inclusive and accessible to all, regardless of digital literacy.

Below we provide a long-list of accessibility-related standards and practices for consideration throughout delivery of a consent solution. It may not be appropriate to follow all of these and even if followed, it may be that some are only introduced during delivery, such as post-MVP launch. This all needs to be subject to detailed stakeholder consultation by the Delivery Body.

If RECCo is appointed as the Delivery Body then we suggest making use of our existing REC Schedule 6 to provide governance over decisions relating to accessibility standards and working practices.

Additional accessibility standards to consider:

1. **WCAG 2.1 Level AA (Web Content Accessibility Guidelines)** – ensures digital interfaces are accessible to people with disabilities, addressing visual, auditory, cognitive, and physical limitations;
2. **ISO/IEC 40500:2012** – the international standard equivalent of WCAG 2.0, ensures web content is usable by diverse individuals;
3. **ETSI EN 301 549** – European standard for accessibility of ICT products and services, including requirements for public procurement;
4. **WAI-ARIA (Accessible Rich Internet Applications)** – Defines ways to make web content and applications more accessible to people with disabilities, especially those who rely on assistive technologies;
5. **ISO 9241-171** – A standard for ensuring accessibility in human-system interaction. Particularly useful for designing user interfaces that cater to diverse user needs;
6. **BS 8878** – A British Standard that guides web accessibility, especially useful for ensuring that web products and services meet accessibility requirements from the design phase onward;

Considerations for Non-Digital Access:

7. **Human Support via Call Centres**: Provisions will need to be made for human-assisted access through call centres or other support services for individuals who are not digitally native or lack access to the internet. In such cases, customer service agents may need to access the system on behalf of the individual;

8. **Delegated Authentication**: This introduces the need for a system that supports delegated authentication. Standards such as OAuth 2.0 could enable temporary access to consumer data, with explicit consent from the individual;
9. **Multi-Factor Authentication (MFA) for Delegates**: Additional layers of security, such as MFA, may be needed to ensure that only authorised agents can access the system on behalf of consumers. The system should track and log delegated access events for auditing and accountability purposes;
10. **Consent Logging**: Each time a delegate accesses the system, clear logs and audit trails must be created to ensure that the individual's consent is respected and the delegation process is transparent.

Additional suggestions:

11. **Multilingual Support**: The system should support multiple languages to ensure inclusivity across different demographics, particularly in regions with diverse populations; incorporating this from the outset will promote inclusivity and will save money in the long run;
12. **Non-Digital Access:** Non-digital means, such as phone call or postal methods, may need to be available for managing consent, which will require secure ways for individuals to provide and revoke consent via human agents;
13. **User Testing Across Demographics**: to ensure the system meets diverse needs, user testing should be conducted with individuals from various backgrounds, including those with disabilities, older adults, and those without digital skills;
14. **User-Centered Design**: the interface, both digital and human-assisted, should be designed with a focus on simplicity and clarity, making it easy for consumers to understand what they are consenting to and how their data is being used;
15. **Delegated Consent Standards**: Develop clear policies and procedures for delegation, including creating secure access tokens for customer service agents to act on behalf of consumers while ensuring accountability.

Ultimately, we will seek to apply the standards and approaches necessary in order to ensure that the solution delivers on its intended purpose and represents value for money. We are committed to informing our consideration of the issues discussed above through consultation with stakeholders.

In relation to interoperability and the related topic of integration, we note that there are six legal bases for processing personal data and that consent is only one of these. We believe that this mechanism should at the outset be limited to the basis of consent; however, ultimately extending it to the other bases for processing personal data can be considered if consultation with consumers and industry indicates that this will be beneficial. For example, providers of the Priority Services Register have been advised to make use of legitimate interest as the basis for PSR data sharing. Without careful design, consumers could face complexity and confusion over who is seeing their data and why that reduces the inclusiveness and effectiveness of services. This is a risk that must be managed throughout delivery.

The consultation proposes that the supervision of accreditation and membership of the Usage Governance Mechanism would be under the aegis of the Delivery Body as part of the requirements set by Ofgem.

The REC has an established Performance Assurance Framework, which is known and understood by industry, and could be extended to support these requirements further. We believe that performance assurance should be used to facilitate continuous monitoring of the data providers and the third-party app providers. High performance levels will be integral to gaining and sustaining consumers' trust in the solution. It is essential in this respect to learn the lessons from open banking, which used ongoing performance monitoring to enhance the reliability of the service.

In establishing requirements on the Delivery Body, Ofgem should be given further comfort by the proposed licensing of RECCo under the code governance reform programme. This will enhance the regulator’s ability to ensure that the anticipated standards are being met through the governance mechanism, if RECCo is chosen.

Q5. Do you agree with the options assessment conducted by Ofgem? If not, why?

We agree with the assessment conducted by Ofgem. However, we would emphasise a few points as we believe that, even where the various options may have the same RAG rating, it is important to be mindful of the distinctions between these options:

- In terms of our "Company Overview", we note that RECCo is an independent, not-for-profit organisation that owns and manages a consumer-orientated code. Ensuring that customers' interests and data are protected in the operation of the REC is part of our core objectives, as stated in the REC code[4]. Furthermore, under Ofgem's code reform proposals, we will, as indicated in the consultation, become a licensed entity; we believe that this will offer clear benefits to Ofgem in its oversight of the consumer consent programme.

- The "Implementation and Governance" element of the assessment might note that RECCo already operates with a performance assurance framework and a change process with which industry are familiar. These components and the procedures by which they are underpinned are set out transparently in the REC and all parties must adhere to them. RECCo can reuse these governance instruments, which will significantly reduce the cost to industry and risks of delivery, weighed against the need to establish these or comparable elements under a different Delivery Body.

- The REC also provides us with most of the guardrails and processes that we would require for us to co-design a Consent Solution with the sector and wider stakeholders; this provides the required opportunities for engagement that will ensure that all features of such a programme of work benefit from stakeholder input (consumer research, market research, funding model, coordination and collaborations, and technical design).

- In terms of "Independence", in addition to our being a not-for-profit organisation the consultation rightly notes that RECCo does not have any products or services for sale in the retail energy market, nor does it implement agreements enabling the use of data for its own commercial gain.

- Under "Operational Capabilities", Ofgem notes that RECCo has been working on consumer consent for two years. As part of this, we have proactively sought to inform the development of thinking on this issue; this has included producing the paper, *Consumer Consent: Consumer Focused Findings*. More generally, owing to our part in fulfilling interventions such as the Market Stabilisation Charge and Prepayment Levelisation, we have a demonstrable track record of successfully delivering regulatory projects, often on relatively short timescales. This positions us well to act as Delivery Body, if selected, for consumer consent.

- Relating to "Engagement" and "Implementation and Governance": we are committed to further improving our transparency as an organisation and so for a new service such as a Consumer Consent Solution would be, we commit to voluntarily complying with the Ofgem Data Best Practice guidance.

The assessment, as described in the consultation document, appears to primarily focus on the as-is capabilities of the assessed organisations, but Ofgem rightly pointed out its duty to also serve the needs of future consumers. We think the assessment would be enhanced by also considering the propensity for the candidate organisations to sustain their capabilities into the future, such as by examining whether organisational design controls exist that will ensure an organisation remains suitable to the Delivery Body role over time.

[4] https://digital-navigator.azurewebsites.net/codes-schedules/2/5.2

The not-for-profit status of RECCo ensures that we face fewer diverging incentives than other organisations must manage, meaning we are organisationally less inclined to ever deviate from the core mission associated with the Delivery Body role. Similarly, the governance provided by the REC that controls our work programmes would require robust and transparent market engagement and therefore by design will ensure our continued alignment to the Delivery Body's required work. Finally, through Ofgem's Code Reform proposals, RECCo is to be a licenced entity and therefore its overall operating model can be expected to be resilient and subject to ongoing regulatory scrutiny and direct oversight into the future.

Q6. Do you agree with Ofgem's minded-to position that RECCo should be selected as the Delivery body for the consent solution? If not, which of the three proposed organisations should be selected as the Delivery Body for the consent solution, and why?

Yes. RECCo would welcome the opportunity to take on the responsibility of being the Delivery Body for an energy sector Consent Solution. We consider the Delivery Body responsibility to align to our mission, which is to facilitate the efficient and effective running of the retail energy market, including its systems and processes through promoting innovation, competition and delivering positive consumer outcomes. It also aligns to the objective of the REC itself to protect consumer data.

Key features of our organisation that position us to be best suited to taking on the responsibility of delivering the Consent Solution on behalf of the energy sector and for the benefit of consumers are that we:

- are a not-for-profit organisation created for the sector specifically to manage its shared needs for the retail market. We do not face the tensions of trading-off between customer and shareholder needs in the way a profit-seeking company does;
- have a proven ability to adapt services and so evolve and change over time; recent evidence of this is our making improvements to the Green Deal Central Charging database, which saved £640k through our approach of continually reviewing and adapting services to optimise them to meet consumers' needs as efficiently as possible[5];
- can provide a mature and effective set of governance processes for stakeholders to enable effective design and delivery of a Consent Solution;
- have a strong relationship with stakeholders across the sector, including consumer interest bodies, and the licenced supplier community;
- are voluntarily adopting the Ofgem Data Best Practice guidance to ensure our ways of working live up to the high standards that consumers and industry expect of us;
- are motivated to overcome this challenge, as evidenced by the actions we have listed, below.

Accordingly, since the initial work of the Energy Data Taskforce and the subsequent recommendations made by the Energy Digitalisation Taskforce, we have already made a series of investments to discover and learn about needs and requirements in relation to consumer consent data. This includes our work:

- voluntarily publishing a Data & Digitalisation Strategy;
- publishing open data;
- researching and creating personas of consumers that characterise stances towards consumer consent;
- helping define how FMAR responsibilities better sit with the Market Facilitator and not RECCo;
- supporting the NESO in taking on the development of a Digital Spine (Data Sharing Infrastructure)

Q7: Do you hold any views as to how the proposed solution should be funded? Please consider the points regarding fairness raised in paragraph 4.12 – 4.14, and Ofgem's duty to consumers when providing your answer.

The views we give here about how funding should take place are specific to the scenario in which Ofgem decides that RECCo should take on the role of being the Delivery Body and the costs specific to that function. The incorporation of the governance arrangements into the REC would be facilitated through the REC Change Process and any associated costs would be funded and recovered from REC funding entities in accordance with the REC Charging Regime.

[5] https://www.retailenergycode.co.uk/how-we-saved-over-640k-for-our-stakeholders-by-migrating-the-green-deal-central-charging-database/

Our view is that the most appropriate route for covering the costs of the Consent Solution will evolve over time and so the funding mechanism needs to be designed to accommodate this. We think the funding of a consent solution should be fair, equitable and non-discriminatory, meaning those who gain the benefits of the service should be responsible for its cost, as far as is practical and reasonably measurable. As RECCo is a non-profit making entity it is crucial that any funding mechanism does not increase its credit risk exposure or create a cross-subsidy arrangement with allowable REC charges.

The types of benefits that we assume will be gained by organisations and their customers are:

- access to new services that require use of personal data that lower the cost / improve the quality of energy services;
- better protections for customers facing vulnerable circumstances;
- better knowledge for business planning, such as through better demand/supply forecasting and credit rating improvements about customer portfolios;
- better strategic planning opportunities, such as through being able to gain deeper insights about what events and interventions drive people into and out of vulnerable circumstances.

With this in mind, we anticipate that a Consent Solution service is likely to need to increasingly cover its costs from the organisations that make use of and benefit from its services.

We think the REC charging methodology arrangements, with the caveat regarding credit risk and cross-subsidy, could be utilised for managing funding arrangements. It includes provisions for its licenced energy entities (primarily energy suppliers but also in limited instances, electricity network operators) to meet the majority of REC costs while allowing for the creation of "user pays" arrangements through the Charging Methodology, for example TPIs who use our existing Enquiry Service. This could be extended for a Consent Solution service.

This way of gaining funding will both take advantage of the successful funding approach that has been proven by the open banking community where funding first came from banks and increasingly over time has been met by third parties. This is analogous with funding initially being provided by energy suppliers and subsequently moving to service beneficiaries paying on a "user pays" basis.

As noted above, RECCo is a non-profit making organisation and it would not be appropriate for that financial risk profile to be materially changed. This could happen in the form of a cashflow and credit risk if funding arrangements are not appropriately planned. For the former, were RECCo to incur costs for operating Consent Solution services and be awaiting payment from a marketplace of parties who used the service, this would create a cashflow risk while non-payment of charges would create a 'bad debt' and therefore a credit risk. That 'bad debt' could not be cross subsidised through other REC charges or REC funding parties. The cashflow risk can be mitigated through using the REC process to define payment methods that meet the needs of all parties and the credit risk would need to be mitigated through either a bad debt allowance within charges or outsourcing of the debt.

While the above describes our current best view for funding arrangements, we regard this as a topic that requires thoughtful discussion with stakeholders and we have already begun this process. This will allow us to hear additional ideas for how best to fund costs, test and validate known options for funding and to continue to validate funding approaches as the solution evolves and matures over time.

Funding should be equitable across demographics, geography and across time, transparent; in particular, it should be designed to avoid disproportionately impacting consumers, especially vulnerable groups. In 2024, RECCo commissioned and economic consultancy to review the existing charging regimes and to recommend an economic charging regime for 'user pays' access to and use of the Enquiry Services which is fair, cost-reflective, transparent and non-discriminatory. The report recommended some minor changes to our charging regime to achieve these outcomes. These have been fully implemented.

We think these following themes will serve as useful guides for when deciding over detailed funding matters:

- The Beneficiary Pays Principle:
    - Organisations that stand to benefit the most from access to consumer data (e.g., energy suppliers and third-party service providers) should be the main contributors to the funding.
- Banding of usage:
    - Allow organisations to select from a range of cost and service provision bands that allow larger/smaller entities to gain access to a service suited to their needs
    - This banding will ensure no economic barriers to entry for smaller companies and new entrants and this will encourage innovation and competition.
- Cost Control and Transparency:
    - Establish strict cost control measures and require regular financial reporting to ensure funds are used efficiently.
    - Any cost savings should be passed on to consumers where possible.

We also expect that Ofgem will wish to gain assurance over the budgeting process to ensure that the Delivery Body strikes the right balance between cost, time and quality as it delivers on behalf of energy consumers. We expect Ofgem (and other stakeholders) to have transparency regarding budgeting and costs and that it would be appropriate for this data to be subjected to the Data Best Practice 'Open Data Triage' process to therefore maximise responsible visibility of financial information to all stakeholders. Should Ofgem decide to assign RECCo the responsibility of being the Delivery Body, we commit to providing this transparency.

Q8. Do you agree with our position to make sharing consent data with consumers (via the consent solution) an obligation for licensees?

The crux of this question appears to be extent to which the proposed Consumer Consent solution should take precedence over alternative arrangements, with the trade-off between simplicity and interoperability on the one hand, versus the risk of stymying innovation and imposing inefficient costs on the other.

On balance, yes we believe that obligation through the licence is appropriate in ensuring consent data is shared with consumers. This would be consistent with and a natural extension of the consumers right to be informed of how their data is being used, and may be critical in gaining and maintain consumer trust. However, the opening paragraphs of Chapter 5 of the consultation referred to a iwder range of potential obligations; we have set out below our understanding of the proposals and our view against each.

A) Use of the Consumer Consent solution being an **obligation on organisations seeking to access consumers data**

We note that the potential users of the MVP and certainly those of the wider use cases for a consumer consent solution would extend beyond licensees. Whilst that may militate against access being effectively assured through the licence, though this could be done through code or, albeit less efficiently, through bilateral data access and sharing agreements.

Should RECCo be chosen to be the Delivery Body, we anticipate that our REC governance processes will be effective at overcoming most solution design and delivery challenges, including the access to data, without need for enforcement of licence obligations. Ways in which this might be achieved include the option of using the processes associated with the Performance Assurance Framework within the REC, which are currently used successfully for controlling access to the consumer data held in the gas and electricity enquiry services.

B) An **obligation for supply licensee to report where consent has been obtained in the consent solution**

Under the UK GDPR the consumer has the right to be informed about the collection and use of their personal data, and our understanding is that this would include details their energy consumption. While the legislation is clear about what is required, this would not extend to prescribing any particular solution and we recognise that suppliers may already have a number of ways in which this information is provided to the consumer. However, while the requirements of the MVP are stated as including an consumer-facing interface, it is likely that a wider range of participants will require visibility of which properties are half-hourly read and have provided, or have the potential to provide consent to access that data.

Although it may be possible to build upon rather than supersede suppliers' existing mechanisms for obtaining consumer consent and subsequently keeping their consumers informed about the use of data, it may not be practicable or desirable for third parties to interface with potentially dozens of different solutions. Therefore, whilst we recognise the potential disadvantages of prescription, we consider that as a minimum there should be expectation that any relevant systems that sit outside of the consumer consent solution are are able to integrate with it, facilitating the provision of a single point of reference.

C) Not proposing to require **supply licensees to use the consumer consent solution to obtain consent from consumers**

This area seem to focus on the costs of compliance and we consider that it may be helpful to make a distinction between the *what* and the *how.*

The concept of consumer consent already exists within the gas and electricity supply licences. In particular, and of relevance to the proposed MVP, Standard Condition 47 of the electricity supply sets out the circumstances under which a supplier is allowed to obtain electricity consumption data relating to a period of less than one month, and what they are permitted to use that data for. This includes rules about getting consent from customers to obtain and use their consumption data.

We therefore agree that supply licensees will already have effective processes in place for obtaining certain consent from their consumers. However, the current obligations are focused on the licensee gaining access to the consumer's granular consumption data, and are silent on the subsequent sharing of that data with third parties. Any existing consent may therefore need to be extended in order to fulfil the intent of the MVP. If that is the case, costs will be imposed by any new obligation to share half-hourly smart data, even if there is no prescription on *how* that is to be done. In order to avoid any double counting, it may be appropriate to identify the cost of complying with the new requirements in the absence of a consumer consent solution

Conclusion

Licensees and other companies can and should be free to adopt policies, processes and technology that suit their individual needs, and this could apply to many if not the majority of the features of an effective design for a consent solution. However, in some cases a degree of standardisation is necessary and proportionate. Robust governance covering the establishment, maintenance and compliance with standards may ensure the best outcomes for consumers.

Q9. Do you consider SLC 0 an appropriate route for implementing these changes, or should Ofgem create a bespoke licence condition?

While it may not be necessary to create a bespoke licence condition to capture the policy intent for the consumer consent arrangements, we consider that the relevant touchpoints are broader than the scope of SLC0.[6] As a minimum, we suggest that the arrangements should extend to non-domestic consumers as SLC0 applies only to Domestic Consumers. This could be achieved through a general duplication of any additional requirements being set out in both SLC0 and SLC0A. However, we consider that other licence schedules may need to be updated to ensure the best outcomes are achieved.

We have a general preference for a principles-based approach in licencing and we think this is likely sufficient for changes to SLC0 and SLC0A. However, it may be helpful to include more explicit requirements on some topics, particularly with respect to expectations on suppliers when consumers are transferring to another supplier company (SLC14A). We recommend that other licence conditions are considered too. SLC26, SLC41 and SLC47 each could play a role in facilitating an environment within which consumers can be inclusively supported in adopting services that rely on their consent.

The electricity supply licence conditions include several provisions that are directly or indirectly relevant to consumer consent, particularly in relation to data privacy, the use of smart meter data, and communication with consumers. The most relevant licence conditions are those that deal with data access, consumer rights, privacy, and marketing practices.

Whilst recognising that Ofgem has proposed to pursue a phased approach (developing a Minimum Viable Product and allowing suppliers to engage when they are ready) it would future proof the arrangement if there is a clear expectation that details of the status of consent be shared amongst relevant industry parties, particularly upon a customer transfer.

Historically, concerns over compliance with General Data Protection Regulation (GDPR) has hindered effective data sharing within the energy industry. Energy suppliers are bound by GDPR to ensure that they obtain explicit consent for processing personal data, particularly when it involves detailed or sensitive information such as half-hourly consumption data. Suppliers must already be transparent about the data they collect, how it is used, and the rights of consumers to access, correct, or delete their data.

We consider that the introduction of a consumer Consent Solution provides an opportunity to provide a clear and unambiguous legal basis (where it is consented to) not only for capturing and processing consumer data, but also for sharing with other industry parties for legitimate purposes. The development of licence conditions should therefore be seen not only as the means of giving effect to the arrangements, but as means of providing assurance to consumers and retaining their trust.

- ***SLC 0: Treating Domestic Customers Fairly***

The Consent Solution will relate to non-Domestic consumer as well as Domestic consumers. It would therefore need to be set out in both SLC0 and SLC0A: Treating Non-Domestic Customers Fairly. The industry has traditionally found it difficult to accurately distinguish between domestic and non-domestic consumers, relying on segmentation based on installed meter types or profile classes rather than the unreliable Domestic Premises Indicator flag. Applying the same principles to both domestic and non-domestic consumers would future-proof the applicability of the solution to further use case and avoid potential operational issues.

[6] We focus here on changes to the Electricity Supply Licence but recognise that in due course changes to the Gas Supply Licence will also need to be considered.

We agree that the Consumer Consent arrangement should appropriately be referenced in SLC0 (and in SLC0A) insofar as it coves the suppliers dealings with the consumer, but we do not consider that this condition alone would suitably cover all of the necessary touchpoints, including the sharing of data with other licensees and third parties as is likely required by a Consent Solution. We set out additional touchpoints below.

SLC 14A: Customer Transfer

We consider that the obligation in this condition to improve systems and the general obligation to cooperate could appropriately extend to the recording, maintenance and in due course sharing of relevant information about the status of consumer consent upon a customer transfer. While the incoming supplier would have the opportunity to engage with the consumer and confirm any previous consents that may have been given, this should not be necessitated by all such consents having been lost or prevented from transfer upon a switch. This will be detrimental to the consumer experience and create potential friction in the switching process, which could deter the consumer and hamper competition.

There may be a role here for a more prescriptive obligation on suppliers to help consumers continue to gain the benefits of services that rely on personal data processing consent at the point of them switching supplier.

SLC 26: Priority Services Register (PSR)

This condition indirectly relates to consumer consent, as suppliers must ensure that vulnerable customers fully understand their rights regarding data sharing and can provide or withdraw consent freely. Special care must be taken to ensure that consent processes are accessible and clear to vulnerable groups. Suppliers have been encouraged (not through licencing) to use the basis of Legitimate Interest to share PSR data; there is a risk of confusion for consumers and suppliers that could be helped through consideration of this condition.

SLC26.3 includes a duty to share but is caveated "*In so far as permitted by any laws relating to data protection and/or privacy, the licensee must share the Minimum Details using the Relevant Industry Mechanisms*". In practice this limits the amount of data that is shared, resulting in much of the value-add data being lost if a consumer switches supplier. It would further facilitate the "tell me once principle" and the Share Once Support Register if suppliers were not just permitted but expected to share all relevant permissions data that describes what the consumer has consented to be shared (and what is being shared using other legal bases).

SLC 41: Smart Metering Installation and Installation Code of Practice – Domestic Consumers

While these provisions were originally intended as consumer protections and to overcome potential resistance to a home visit, they may be hindering the efficacy of the smart roll-out, insofar as they are limiting an opportunity to educate the consumer on the benefits of smart metering. This will be an increasingly important issue as consumers will need to be made aware of innovations such as time-of-use tariffs and make an informed choice about whether to adopt them.

There is an argument for loosening the requirements of this license condition to make it easier for certain types of engagement and communication with consumers to take place. This may help with consumer education and understanding. Care would need to be taken to ensure this does not lead to sales transactions and marketing during such visits, but there may be a middle ground. Management of the day-to-day needs of this licence condition fall under the REC and so there are opportunities to ensure good practices are followed.

SLC 47: Smart Metering – Matters Relating to Obtaining and Using Consumption Data

Suppliers must ensure that consumers are informed about how their energy consumption data will be used, and consent must be obtained before accessing detailed energy usage data (e.g., half-hourly or daily data).

Suppliers must make consumers aware of their ability to withdraw consent at any time. This licence condition may also be suitable for adaptation that helps with education and understanding.

Appendix 2: Annex of our initial stakeholder research

We have begun learning stakeholders' expectations and needs regarding a Consent Solution to accelerate industry progress at delivery. In addition to our prior research, we have used this consultation process to run a series of comprehensive stakeholder interviews starting with 12 organisations from across the energy sector.

These interviews provide valuable insights from a diverse range of perspectives, including energy suppliers, consumer advocacy groups, digital service providers, and sector bodies. Here we summarise the feedback we have received. While we respect the preference of many stakeholders to remain anonymous, the findings offer a broad and representative view of the sector's priorities and concerns.

In addition to the stakeholder interviews, our analysis also incorporates valuable information from the responses to the public consultation conducted by Ofgem, enriching our understanding of the broader industry sentiment on data sharing, consumer consent, and regulatory challenges.

Below we include a summary of preliminary research findings, based on our engagement to date.

Key findings from the Stakeholder engagement

Broad Consensus on Security and Transparency

There is agreement across stakeholder categories, particularly Energy Suppliers, Consumer Advocacy, and Sector Bodies, on the need for robust security, transparency, and GDPR compliance. Stakeholders emphasise that without clear data-sharing practices and security protocols, consumer trust could not be maintained. A hybrid model (blending centralised and decentralised elements) was seen as a practical way to balance these concerns.

Concerns Around Funding and Complexity'

Stakeholders including Energy Suppliers and Service Providers have worries about the distribution of costs and timeline pressures. Small suppliers and vulnerable consumers are flagged as potential groups who could be disproportionately affected by rising costs or complex systems. There was a call from some Retail Suppliers for careful consideration of the cost-sharing model to ensure fair distribution of financial responsibility across the ecosystem.

Support for Hybrid Model:

Multiple groups, including Energy Suppliers and Sector Bodies, support the idea of a hybrid delivery model to balance central governance with flexibility. This approach could distribute responsibilities more evenly, easing pressure on a single delivery body, while also ensuring cross-sector integration.

Trust and Consumer Transparency as Central Themes

Many stakeholders stress that trust and transparency are critical for consumer engagement. If consumers don't understand how their data is used, participation in the consent system may be limited. This is especially important to Consumer Advocacy groups, who advocated for clear communication channels and transparency measures to drive user confidence in the system.

Security and Token-Based Consent

Security concerns are central, particularly around third-party misuse of consumer data. Energy Suppliers support token-based systems for managing consent access securely. This approach is seen as a way to protect against misuse while ensuring consumers can track who is accessing their data and when.

Inclusivity and Digital Exclusion:

Consumer Advocacy groups and some Energy Suppliers raise concerns about digital exclusion. There is broad support for the inclusion of non-digital methods (e.g., phone or community services) to ensure that less digitally able customers, especially vulnerable consumers will benefit from the changes.

Themes analysis

We have organised our research findings into a database so that granular research information can be easily navigated and summarised up for consumption, this approach will also ensure that we can continue to manage the growing volume of research findings over time.

The themes analysis that follows draws from that database of information. It provides insights gathered from both the public responses to Ofgem's consultation on Data Sharing in a Digital Future and the recent 12 stakeholder engagement sessions run by RECCo, focusing on key areas of concern across different organisation types.

The table, immediately below, is a key that explains the colours used in our summary heatmap, shown on the next page. The heatmap provides a visual summary of themes arose throughout our research and the colour coding represents the impact that theme might have on organisations, i.e. darker colours represent more significant areas of concern.

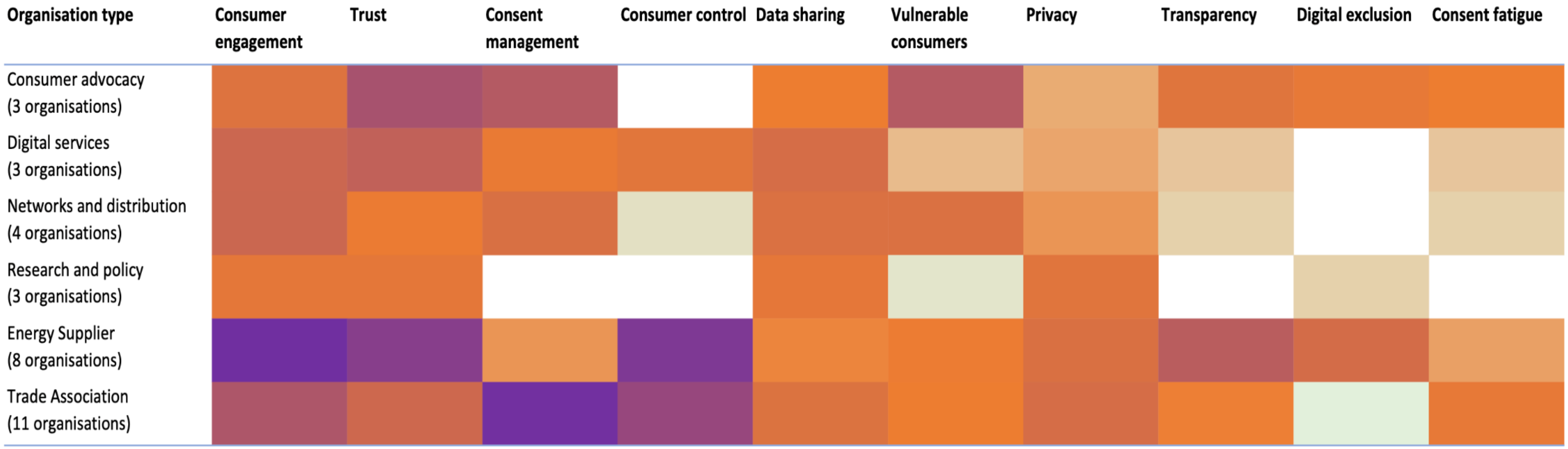
Impact and colour code explanation for the heatmap

Purple (100+)	These squares represent high impact topics for those organisations, meaning they raised significant concerns about these themes, either because they affect many people or vulnerable consumers
Dark Orange (50 - 100)	These squares show moderate impact, indicating considerable interest and concern, though not as widespread or critical as the purple areas
Light Orange (10 - 50)	These represent a lower level of concern for the organisations, showing that while the issue was raised, it has less impact
Beige (1 - 10)	Indicates minimal concern or interest in these themes by the organisations, affecting fewer people or not being as critical
White (No score)	Blank squares indicate that the organisations did not address or raise concerns about these specific themes

An impact score is assigned to each granule of research finding information and this score has been based on two factors: the number of people affected by the issues raised and whether the issues have a greater effect on the more vulnerable groups. Higher scores indicate either a broader impact (affecting more people) or a greater focus on the vulnerable. Lower scores mean fewer people were affected, or the issue is less of a priority for that organisation type.

Heatmap showing the top 10 Themes by Organisation Type

The heatmap chart provides a visual representation of organisational engagement and concern on various themes, helping highlight the key areas of focus for different organisation types.



Themes detail

The table below is our sharing of explanations about each of the themes from the heatmap. The themes are listed in order of priority across stakeholders:

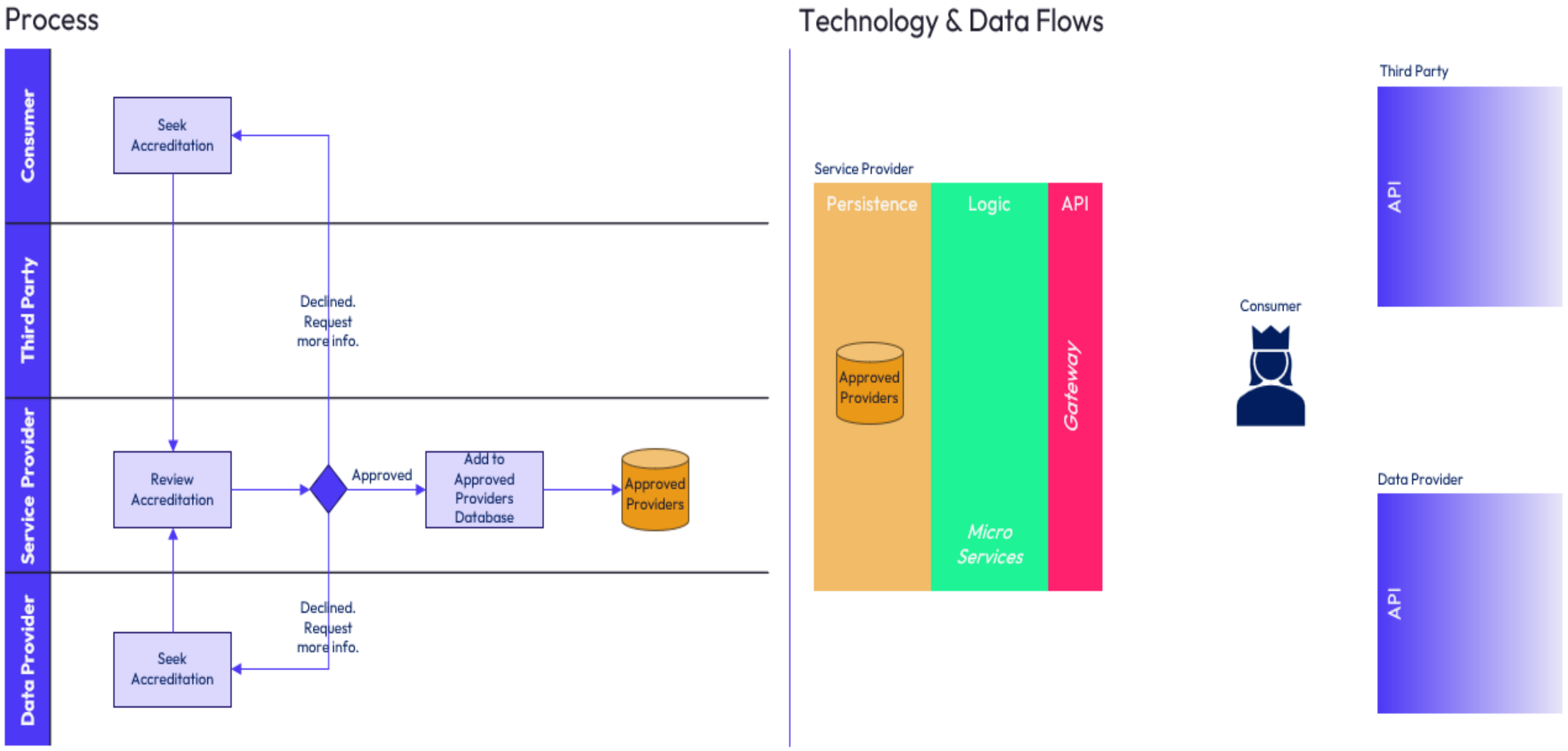
Themes	Insights
Consumer engagement	A top priority across all groups, with a strong focus from Consumer Advocacy and Energy Suppliers. Simplicity in engagement tools is vital, particularly for vulnerable consumers.
Trust	Fundamental to fostering participation, especially among Energy Suppliers and Consumer Advocacy groups. Transparent communication about data use is key to building trust.
Consent management	Digital Services and Energy Suppliers emphasise the need for streamlined consent processes that are easy for consumers to manage, allowing them to view, modify, and revoke permissions with ease.
Consumer control	Focused on empowering consumers to manage their data, but without adding complexity. Ensuring vulnerable consumers can exercise control is a shared concern across many groups.
Data sharing	A high priority for Sector Bodies and Service Providers, who emphasise the need for smooth and secure data transfers. Keeping consumers informed about who is sharing their data is a concern.
Vulnerable Consumers	Protecting vulnerable groups is emphasised by Consumer Advocacy and Consumer Groups. Systems need to be designed to ensure accessibility and inclusivity, particularly for those with limited digital access.
Privacy	Robust privacy frameworks and clear communication to consumers about how their data is used and stored are seen as crucial.
Transparency	Consumers need to understand who has access to their data and for what purpose, which is essential for building trust.
Digital exclusion	Agreement that non-digital pathways need to be provided to prevent vulnerable groups from being left out. Consumer Advocacy and Energy Suppliers mentioned the risks of excluding those without digital access.
Consent fatigue	Frequent consent requests could lead to disengagement, and both Energy Suppliers and Consumer Advocacy groups urge for a streamlined approach to consent management to avoid overwhelming consumers.
Innovation	Sector bodies and Digital services highlight the need for the system to support ongoing innovation in smart energy data and flexible services. Ensuring the solution can adapt to emerging technologies is a priority.
Consumer education	Many groups stress the need for strong consumer education, ensuring people understand how their data is used. Consumer Advocacy groups are particularly focused on clear and accessible information for less digitally aware consumers.

Smart Tech	Digital services and Innovation groups emphasise that smart tech integration needs to be seamless and intuitive. They advocate for systems that support smart appliances and smart meter data to improve user engagement.
Simplicity	Consumer Advocacy and Energy Suppliers urge for simplicity in the design of consent systems. Avoiding overly complex interfaces or processes is seen as essential to drive engagement, particularly for vulnerable consumers.
Data Security	Digital services and Service Providers call for rigorous data security measures to protect consumer data, while Consumer Advocacy groups emphasise the need for clear communication to consumers about how their data is protected.
Stakeholder Engagement	Sector bodies and Energy Suppliers call for continuous stakeholder engagement to ensure the system aligns with industry needs and consumer expectations. Collaborative efforts are seen as key to successful implementation.
Communication barriers	Consumer Advocacy groups have concerns about potential communication barriers, especially for vulnerable consumers, and state the need for clear and accessible language, avoiding technical jargon.
Switch Providers	Energy Suppliers and Consumer Advocacy groups referenced switching providers, and the need to ensure consumer data and consent can be easily transferred without disrupting service or trust.
Consumer Rights	Protecting consumer rights is a core focus for Consumer Advocacy groups, ensuring that consumers remain in control of their data and that their rights are clearly communicated and upheld throughout the process.
Consumer comfort	Consumer Advocacy and Energy Suppliers emphasise that consumer comfort with the system is crucial. This includes making interactions easy and intuitive, to ensure widespread adoption.
Fuel Poverty	Consumer Advocacy groups highlight the need to consider the impact of fuel poverty, ensuring that any data-sharing initiatives do not inadvertently disadvantage those already struggling with energy costs.
Energy efficiency	Innovation and Digital services groups advocate for solutions that drive energy efficiency. They support using data to help consumers manage and reduce energy consumption, benefiting both consumers and the environment.

Conceptual technical designs

We have not made any design decisions about the Consent Solution and our doing so will involve extensive stakeholder engagement. However, we have begun to think about design options so that they can be evaluated, we included these design concepts in our interviews with stakeholders and we will use them as informative starting points should we be appointed to take on the role of the Delivery Body.

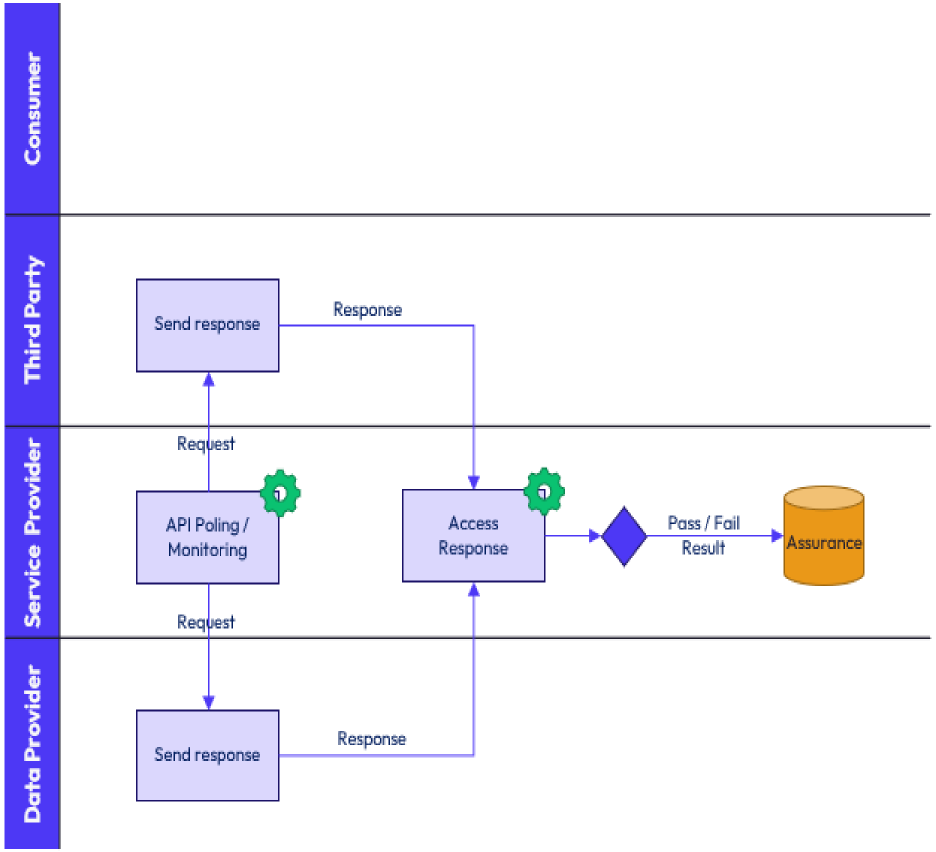
Accreditation – To build trust Third Party and Data Providers must by Accredited for use


Process

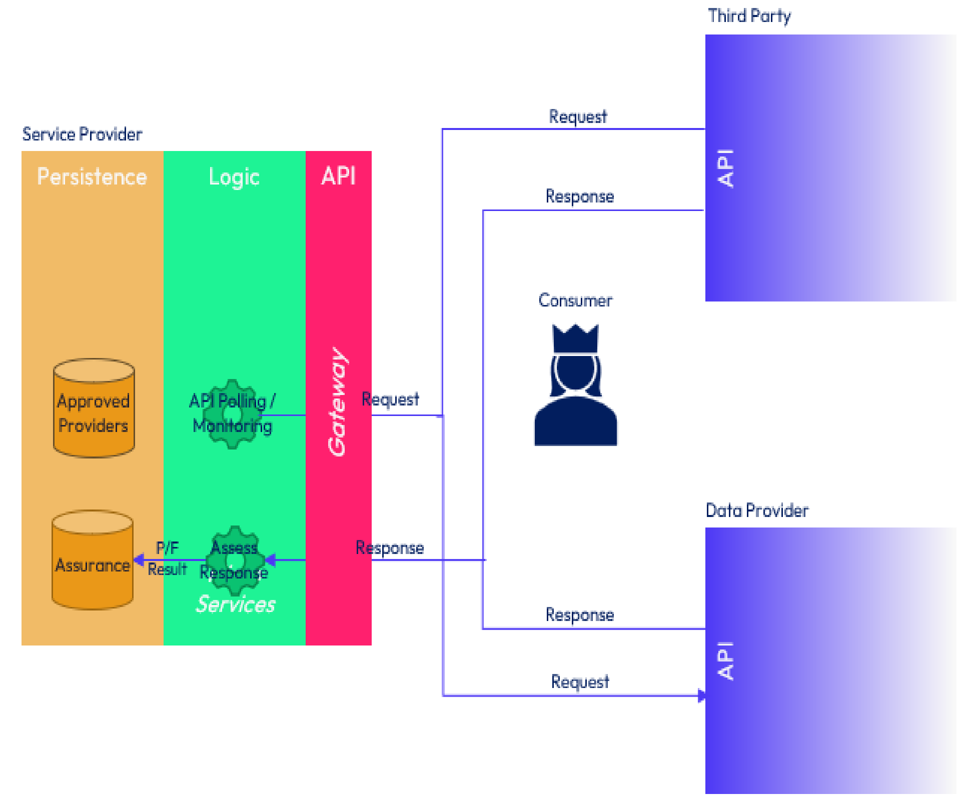
Technology & Data Flows

Monitor – Performance Assurance of Third Parties & Data Providers, Increases consumer Trust

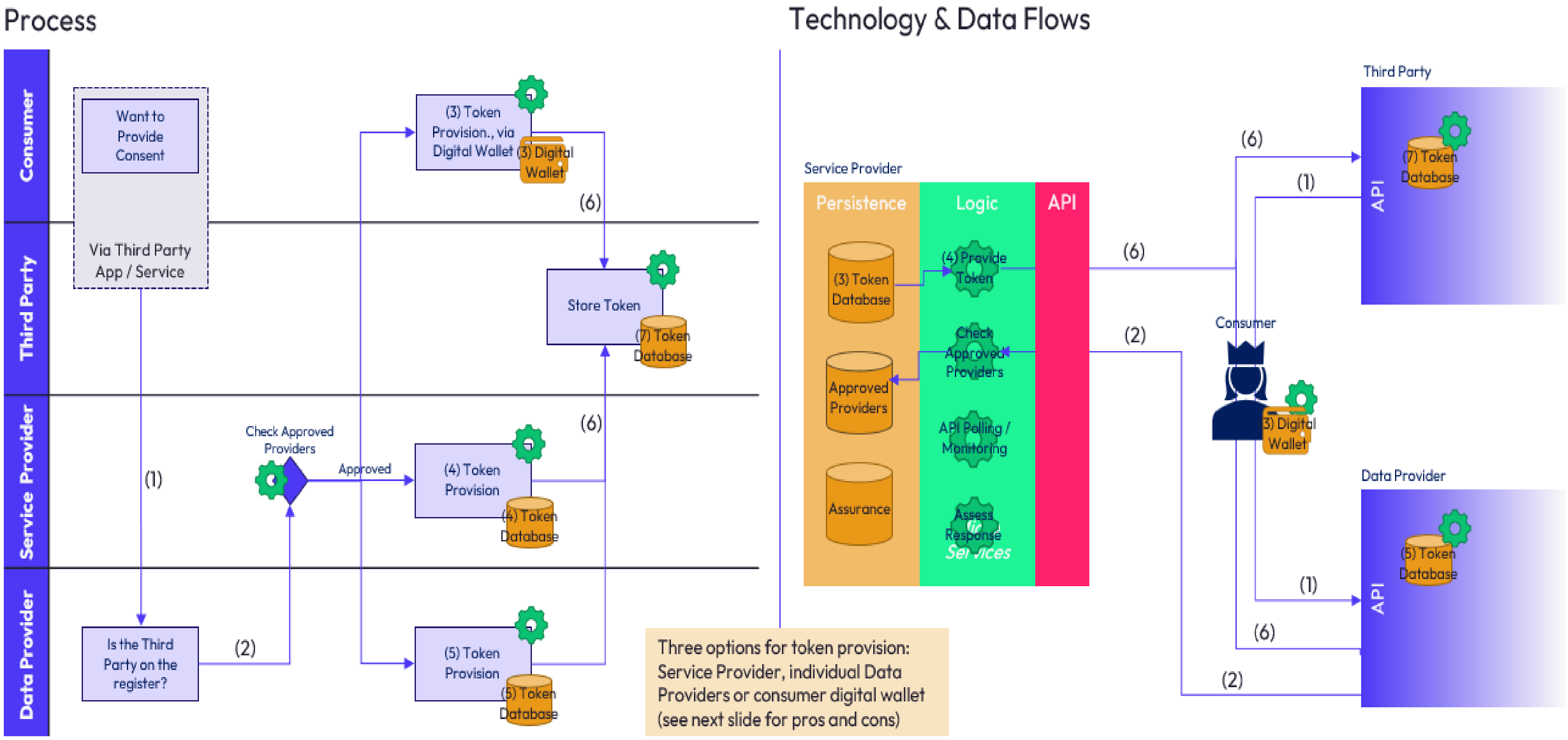
Process



Technology & Data Flows



Authentication & Consent – Multiple Options provide varying Pros and Cons



Process

Consumer

Third Party

Service Provider

Data Provider

Want to Provide Consent

Via Third Party App / Service

(1)

Is the Third Party on the register?

(2)

Check Approved Providers

Approved

(3) Token Provision., via Digital Wallet

(3) Digital Wallet

(6)

Store Token

(7) Token Database

(4) Token Provision

(4) Token Database

(6)

(5) Token Provision

(5) Token Database

Technology & Data Flows

Service Provider

Persistence

Logic

API

(3) Token Database

Approved Providers

Assurance

(4) Provide Token

Check Approved Providers

API Polling / Monitoring

Assess Response

Services

(6)

(2)

Third Party

API

(7) Token Database

(6)

(1)

Consumer

(3) Digital Wallet

Data Provider

API

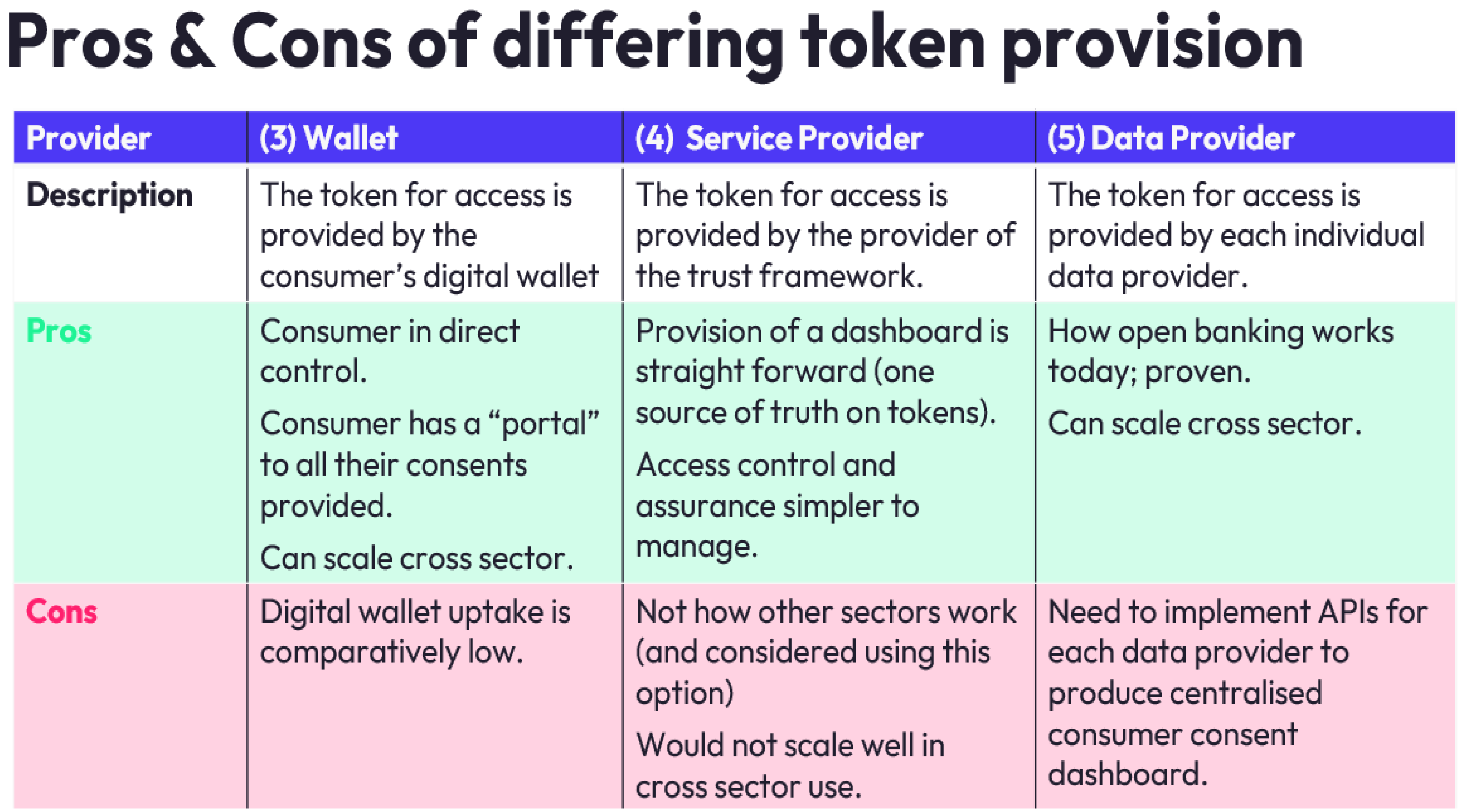
(5) Token Database

(1)

(6)

(2)

Three options for token provision: Service Provider, individual Data Providers or consumer digital wallet (see next slide for pros and cons)

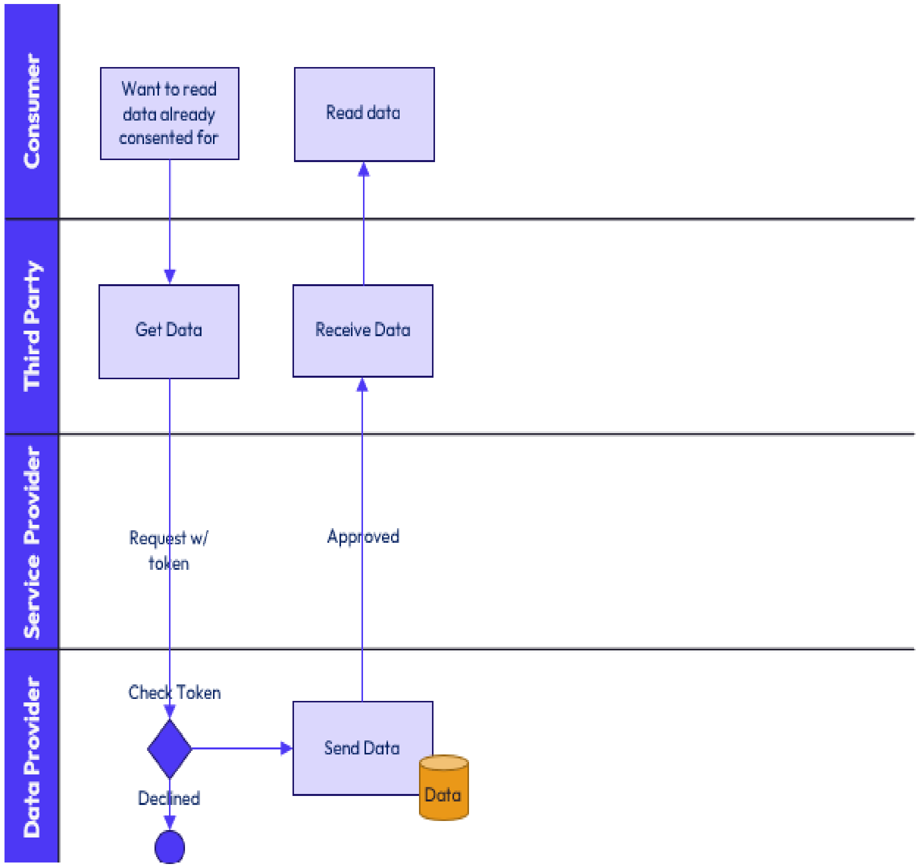


Pros & Cons of differing token provision

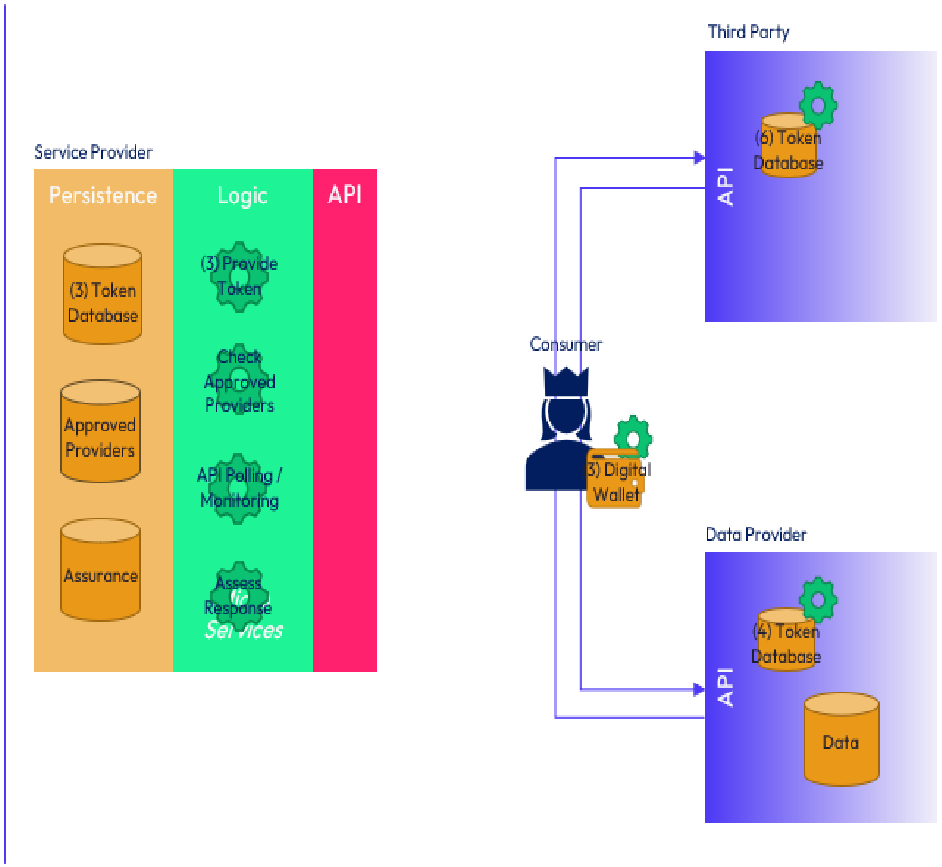
Provider	(3) Wallet	(4) Service Provider	(5) Data Provider
Description	The token for access is provided by the consumer's digital wallet	The token for access is provided by the provider of the trust framework.	The token for access is provided by each individual data provider.
Pros	Consumer in direct control. Consumer has a "portal" to all their consents provided. Can scale cross sector.	Provision of a dashboard is straight forward (one source of truth on tokens). Access control and assurance simpler to manage.	How open banking works today; proven. Can scale cross sector.
Cons	Digital wallet uptake is comparatively low.	Not how other sectors work (and considered using this option) Would not scale well in cross sector use.	Need to implement APIs for each data provider to produce centralised consumer consent dashboard.

Obtain Data – The Data Transfer does not go through the data provider

Process



Technology & Data Flows


Third Party
API
(6) Token Database
Service Provider
Persistence
Logic
API
(3) Token Database
Approved Providers
Assurance
(3) Provide Token
Check Approved Providers
API Polling / Monitoring
Assess Response
Services
Consumer
(3) Digital Wallet
Data Provider
API
(4) Token Database
Data