Public	Information intended for unrestricted access, such as published news articles and press releases.

Reference	RECPAB_26_1027_01_A
Status	Appendix
Pages	3

Draft ISDP Questions

This appendix sets out the proposed questions to be included in the ISDP assessment:

Question	Criteria
Section 1: Company information	
1.1	Company name and number
1.2	Provide your Information Commissioner's Office (ICO) registration number
1.3	Registered Address
Section 2: Understanding how you will use the CCS	
2.1	Please indicate the expected maximum number of unique data access records your organisation plans to hold or access through the CCS within a 12-month period. This refers to the number of individual consumers for whom your organisation will either manage consent or facilitate data transfer. *For maintenance of qualification, please also identify any material change in the scale or frequency of data access since the previous assessment.*
2.2	How will your organisation access the REC Service (e.g. API integration, system-to-system connection, manual access through a portal)?
2.3	Which systems or applications within your organisation will access or process REC Data? Please include a description or diagram of how REC data flows through your systems, including any integration points (e.g. Application Programming Interfaces (APIs), third parties, or external platforms).
2.4	Will REC data obtained be stored within your systems, or processed only temporarily? If so, where will this data be stored or processed (including by any hosting provider)? Please identify the country or countries involved.
2.5	Have you reported any personal data breaches to the ICO in the past 12 months? If yes, provide a brief description and actions taken.
2.6	Confirm that the systems used to access or process REC data are within the scope of a current Cyber Essentials Plus or ISO27001 certification. Please provide the certification date, scope and Statement of Applicability (SoA).
Section 3: Data handling and protection	
3.1	For what specific business purpose(s) will your organisation use the REC data? This purpose must directly align with the consent obtained from the consumer.
3.2	How do you ensure REC data is only accessed by staff or systems that require it for their role?
3.3	What is your data retention policy specifically for REC data, and how is data securely deleted when no longer required or when consent is revoked?

©2026 Retail Energy Code Company Ltd. Company No. 10989875

This email/document and its contents have been classified as 'Public' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

3.4	Please provide a redacted copy of your Data Protection Impact Assessment (DPIA)for this data processing. This should detail the key data protection risks identified, and the measures implemented to mitigate those risks. It should also detail how you ensure data accessed under REC services is only used in line with the authorised purpose and consumer consent provided, and describe the controls in place to prevent unauthorised or inappropriate use of such data.
3.5	How do you ensure that only the minimum necessary REC data is requested and processed, strictly in line with the consumer's consent and stated purpose?
3.6	Do you have a documented process in place to handle data subject rights requests (e.g., access, rectification, erasure, portability, object and restriction) for the personal data you hold? Please describe how this process ensures responses are provided without undue delay.
3.7	If REC data is transferred internationally (outside the UK), how do you ensure that data subjects' rights and the level of data protection are maintained in accordance with UK GDPR requirements (e.g., mechanisms including the use of a transfer risk assessment, reference to adequacy decisions, Standard Contractual Clauses (SCCs), or other appropriate safeguards)?
3.8	What controls are in place to prevent secondary use, profiling, or onward sharing of data accessed under REC services beyond the stated purpose and consent provided?
3.9	Describe your process for handling requests from consumers to withdraw their consent for data sharing, ensuring all relevant data is managed appropriately (in accordance with data retention policies) to enable notification to be provided to CCS in accordance with REC requirements.
Section 4: Security Controls & Assurance	
4.1	How is personal data accessed via the CCS or enquiry services (as applicable) protected in transit (e.g. when transmitted from the Energy Data Holder to your systems, or between your internal systems) and at rest (when stored within your systems)? Please describe the encryption standards and methods employed, as well as any other security controls.
4.2	How is personal data accessed via the CCS protected against unauthorised access, loss or disclosure once it is stored, processed or accessed within your organisation's environment, including where it is stored, processed or accessed through servers, databases, cloud services or end-user devices? Please describe relevant controls, including where applicable encryption, data loss prevention, monitoring and other measures not already evidenced through your Cyber Essentials Plus or ISO 27001 certification.
4.3	How does your data classification scheme inform and dictate the security controls applied to different types of consumer/customer energy data you process?
Section 5: Security Governance (not required for organisations with applicable ISO27001 certification)	
5.1	Please describe your organisation's data governance framework, including the roles, responsibilities, and meetings involved, specifically concerning REC data.
5.2	Who within your organisation is responsible for information security and data protection?
5.3	How does your organisation identify and manage information security risks related to the processing of REC data accessed via the CCS?
5.4	What training do staff receive specifically on handling REC data, and adhering to consent requirements?
Section 6: Security Incident Management	
6.1	What process does your organisation follow to detect and respond to security incidents affecting REC data or services?
6.2	In line with REC obligations, how would your organisation notify RECCo (and the Information Commissioner's Office, where required) of a security incident, data breach or vulnerability affecting REC data or REC services, including the expected timeframe for notification?
Section 7 - Regulatory Compliance	
7.1	Confirm that your organisation complies with applicable UK data protection legislation (UK GDPR and Data Protection Act 2018) when processing REC data.
Section 8: Third party and operational controls	

©2026 Retail Energy Code Company Ltd. Company No. 10989875

This email/document and its contents have been classified as 'Public' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

8.1	Do any subcontractors or service providers support the systems used to access or process REC data? If yes, please list them and briefly describe their role.
8.2	Do you share REC data with any third parties or service providers? If yes, please provide a list of the third parties used and describe the purpose of this sharing for each party
8.3	Please describe the mechanisms in place to ensure consistent and robust data security and protection throughout the entire data processing chain? How do you gain assurance over these third parties by assessing and monitoring them to ensure they comply with the consumer's consent and data protection requirements?
8.4	What physical or hosting environment protections exist for the systems processing REC data (e.g. office controls, secure hosting provider)?

©2026 Retail Energy Code Company Ltd. Company No. 10989875

This email/document and its contents have been classified as 'Public' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.