

Market Entry

Information Security and
Data Protection
Assessment

RETAIL
ENERGY
CODE





This section applies to all applicants, except those applying to only access the Green Deal Central Charging Database.

Once you have completed your response, please upload the completed form, along with the required supporting material into the REC Portal. To upload files into the REC Portal, please navigate to Party Operations, then Performance Assurance, and click 'Your Files'. As you will have multiple files to upload, please zip your files relating to this application, naming each file with the reference number relating to the question below where relevant.

#	Item to be assessed	Your Response
1.1	Please specify the architecture of your in-scope systems.	



#	Item to be assessed	Your Response
1.2	Are you making use of any subcontractors, third parties or service providers to provide the operation of the service or develop and manage any of the technical solution?	
1.2.1	Please provide a list of all subcontractors, third parties or service providers, including what activity they are performing.	





#	Item to be assessed	Your Response
1.3	How will you be accessing the data for the REC Service you have requested?	
1.4	How do you ensure that you have identified and appropriately assessed all information security and data protection risks relating to your business operations?	





#	Item to be assessed	Your Response
1.5	What information security accreditation do you hold to mitigate the applicable risks to your organisation?	
1.6	How do you ensure that you have appropriate risk, security and control arrangements in place that are reviewed on a regular basis?	





#	Item to be assessed	Your Response
1.7	How do you ensure there is appropriate governance, oversight and right tone from the top in relation to Information Security?	
1.8	How has your business taken steps to ensure appropriate information security and control procedures are in place?	





#	Item to be assessed	Your Response
1.9	How has your business taken steps to ensure appropriate physical security and environmental control procedures are in place?	
1.10	How has your business taken steps to ensure appropriate user access security and control procedures have been developed with respect to your service to guard against unauthorised logical access to data and programs?	





#	Item to be assessed	Your Response
1.11	How has your business taken steps to ensure that credentials used to access services are held in a secure manner, and any relevant secret key material is secured throughout its lifecycle.	
1.12	What steps has your business taken in relation to human resource security, such as appropriate screening and relevant training?	





#	Item to be assessed	Your Response
1.13	How does your business ensure that any unauthorised activity within your relevant systems is monitored and if detected is appropriately prevented and/or rectified?	
1.14	How does your business monitor and identify any vulnerabilities on your relevant systems and, if identified, what steps are taken to mitigate or remediate the vulnerabilities?	





#	Item to be assessed	Your Response
1.15	What processes does your business have in place in relation to incident management?	
1.16	How do you ensure your data is held in a secure manner, retained for only the necessary time required and deleted appropriately?	





#	Item to be assessed	Your Response
1.17	How do you ensure data is only accessed for the purposes for which it is required?	
1.18	Please provide a completed up-to-date and relevant ICO checklist.	





#	Item to be assessed	Your Response
1.19	Please provide your Data Protection Registration number and registration.	
1.20	Have you reported any data breaches to the ICO in the last year and what action did you take to remedy these?	





Name	
Title	
Company	
Date	
Signature	





To find out more please contact:

enquiries@recmanager.co.uk

**RETAIL
ENERGY
CODE**