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.	Architecture diagram has been submitted.

#	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?	Yes Youtility makes use of a number of third party services in order to deliver a complete and robust feature set.
1.2.1	Please provide a list of all subcontractors, third parties or service providers, including what activity they are performing.	Youtility's APIs orchestrate data between multiple systems. - Youtility's service infrastructure is hosted in Microsoft Azure as PaaS. All Youtility infrastructure is hosted in deployment zones within the UK. Youtility use Kubernetes and Docker to create a scalable virtualised environment built on Linux VMs. There is a separate virtualised environment for each enterprise partner in order to ensure scaling efficiency and separation of data/domains. - Workflow data is stored in Azure based SQL Server instances with rolling backups within multiple zones (all within the UK) for redundancy. All data identified as PII stored in this manner is stored with an extra layer of encryption to make it unreadable at rest in the Youtility database. After the workflow is completed the encryption key is destroyed

		so data at rest in the database can not be deciphered and data backups containing encrypted PII cannot be decrypted. - Quote data is stored within Microsoft Azure Redis on demand service with a session timeout of 1 hour. This means quote data is only held in memory for 1 hour. - Datadog is used for log aggregation and monitoring. Datadog is a secure cloud-based log aggregation and indexing service. Youtility uses this service to track and trace potential issues/unusual behaviour and to fix potential issues. Datadog is also used for debugging purposes. No user data is transmitted in this way and logs only contain information regarding internal Youtility orchestration services. - Youtility currently uses Energylinx and GBG to source address/postcode data, MPAN/ MPRN data, live tariff and pricing data - although this is only in the short term and will be removed in Q1 2022. - Youtility use an in-house developed monitoring system to monitor service status and metrics. This is built on top of Youtility's Kubernetes environment using Prometheus Server and Grafana.

#	Item to be assessed	Your Response

1.3	How will you be accessing the data for the REC Service you have requested?	Youtility will be accessing data through direct API integration.
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?	- Youtility maintains a comprehensive risk register that is reviewed at least twice a year. This register tracks and assesses any risks resulting from technology or operational processes. A copy of this register has been provided - Youtility also employs a robust risk assessment process for any third party provider that has contact with user information. This includes reviewing their internal documentation and policies, whether they have had any security or privacy breaches and assessing their track record and who their clients are. Before selecting a technology partner Youtility undertakes a thorough comparison process whereby the technical and business requirements that are needed to ensure the quality, reliability and security of the functionality on offer are documented. Youtility then engages with several other market leading providers to understand the details of their technology offering and internal processes including support, compliance, privacy and security. The providers are then compared and scored based on the criteria identified. This process provides a way to ensure that Youtility is only engaging with partners who have a proven

		track record, technology offering and well documented processes including a well documented GDPR compliance posture. Once a provider is selected, further due diligence is performed and the details of their policies on privacy, security, GDPR and business continuity are thoroughly documented and checked. Youtility uses an Outsourcing Checklist document to track the details of the partner's policies and highlight any operational risks and their mitigations. This checklist is regularly reviewed and updated. - Youtility maintains an IT Security Policy (supplied) that adheres to ISO/SEC 27001. This policy is reviewed and internal processes are checked for compliance with this policy twice a year. - Youtility Operates a robust Data Handling and Backup policy (supplied) which ensures that any PII data is only held for the time needed to process a comparison or switch, and is destroyed afterwards.

#	Item to be assessed	Your Response
1.5	What information security accreditation do you hold to mitigate the applicable risks to your organisation?	Youtility does not hold any security accreditation. Youtility policies are compatible with ISO/SEC 27001 and internally audited. Additionally, Youtility undertakes external security testing by a CREST certified provider, including penetration testing at least once a year.

1.6	How do you ensure that you have appropriate risk, security and control arrangements in place that are reviewed on a regular basis?	Youtility maintains a comprehensive set of policies that detail the processes and procedures in place to ensure Youtility systems function in a robust and secure manner, and ensure that data is handled in compliance with legislation and internal security policies. Youtility's Compliance related Policies and Procedures are split into the following documents, all provided with our response submission: - Business Continuity Policy - Confidentiality Policy - Data Protection Policy - Data Handling and Backup Policy - GDPR API Policy - GDPR Data Request Policy - IT Security Policy - Risk register (Template provided) - Outsourcing Policy and checklist Youtility policies are reviewed on a quarterly or semi-annual basis, depending on the policy. The review processes ensure policies are kept up to date and reflect the current state of systems and procedures. Youtility staff have refresher training on company policies on an annual basis and are encouraged to review policy documents after each update. Training consists of presentations and interactive workshops held by the management team. As an FCA regulated company, Youtility is additionally required to submit quarterly operational and security risk assessments (REP018).

#	**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?	- Youtility follows the provided IT Security policy which all staff are required to read and understand. Periodic refresher training is also provided to staff to ensure a consistent understanding of policies. This policy is reviewed twice a year to ensure it is up to date. - Youtility maintains, reviews, and enforces a comprehensive Information security policy that covers all aspects of information security. - Youtility runs an internal audit to ensure compliance with all policies at least once a year. - As is evident by the Data Handling and Backup Policy, information security and privacy are built into Youtility development processes from project inception to implementation. All new developments must comply with security and privacy requirements as set out in Youtility policies. These requirements are used as part of the acceptance criteria for any new build or change to the system and are tested as part of the QA process.
1.8	How has your business taken steps to ensure appropriate information security and control procedures are in place?	- Youtility embeds information security requirements into any project or development that is undertaken. - All new developments must comply with security and privacy requirements as set out in Youtility policies. These requirements are used as part of the acceptance criteria for any new build or change to the system and are tested as part of the QA process and embedded into the release process. - All Youtility technical build activities must be in compliance with the Data Handling and Backup Policy and more widely compliant with Youtility's Information Security Policy. All technology releases must be compliant with Youtility policies which are measured during the testing process as non-functional requirements.

#	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?	- Youtility operates a remote working policy and all access controls are detailed within the IT Security Policy. - All Youtility production systems are deployed in Microsoft Azure and access is controlled via Active Directory. No data is held in on premises deployments, as such no physical access controls are needed. - The physical security policies for Microsoft Azure can be found here: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
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?	- Youtility uses Microsoft Azure Active Directory system and Google Workspaces federated authentication system to limit staff access to only the resources they require to perform their duties, and this access is regularly reviewed. Youtility also employs two factor authentication to log into Active Directory accounts that have access to production systems. - Youtility uses AI driven active monitoring within the Microsoft Azure environment. Any security event are immediately escalated via email to ley personnel such as the Head of engineering and Lead developers. When an alert is received it is immediately verified, and if a breach is detected Youtility's breach procedures are implemented as described in the provided Information Security Policy and breach procedure documents. Youtility staff work remotely and always have access to laptops and communication devices so processes can be followed at any time.

		- Youtility's Google Workspace systems include active monitoring and automatically flag up any unusual access or access attempt to the management team. All alerts are immediately investigated.

#	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.	- Youtility API services follow security best practice by using OAuth 2.1 to secure the API, with IDServerV4 acting as the repository for credentials and issuing access tokens. All tokens expire over time and require refreshing to avoid man in the middle attacks. - A limited set of employees responsible for developing and maintaining API authentication have access to the IDServer. This access is granted on a per need basis as defined in the IT Security Policy and access is revoked when the employee no longer requires it. - Secret key information is only used to encrypt and decrypt PII data and handled as described in the Data Handling and Backup Policy. - Credentials to internal company systems and tools used to perform various functions are held in an enterprise grade password vault, with individual

		employees granted access to the systems that they require to perform their duties. - All key production systems and tooling are protected using 2FA authentication for added security.
1.12	What steps has your business taken in relation to human resource security, such as appropriate screening and relevant training?	As part of Youtility's recruitment process the Company undertakes a standard interview procedure, which includes a technical test (subject to role) and a minimum of 2 interviews, conducted by at least 2 distinct and separate individuals undertaking the interviews and external referencing routines and references from previous employment for the past 5 years as standard. During the interview, Youtility discuss and review a candidate's CV and prior experience and/or educational achievements (educational aspects are key where no prior work history exists) to ensure they have the requisite and tangible skills to perform the role. Youtility also discusses the role requirements with the individual in the interview process and asks questions to test their knowledge and expertise and their suitability for the role, including integrity and ethical behaviour and their ability to perform the role at the standards required.

		Using the output from the interviews conducted, the direct line manager compares and contrasts the output, and there may be further meetings to gain a consensus on the candidate's suitability and capabilities for the role under consideration and we make a similar comparison to other candidates for the role being recruited for. Youtility always interviews at least 2, but as many quality candidates as possible within the boundaries of timeframes, to ensure selection of the best candidate for the role in question. The interview and recruitment attributes include: - A clear bullet point job description is provided to the candidate prior to interview; - During the interview, an assessment of the candidate's previous experience in meeting the role specific standards, is done as an assessment against the job description; - The interviewer makes an objective assessment of the candidate's demonstrated skills and experience or attributes discussed; - Competency based questions are used to assess the candidates general experience and approach; - Youtility then shortlists candidates for the role and undertake further interviews by the wider team if required, or at this stage go to a decision and hire procedure; - Any gaps in competence that are identified during recruitment are documented; - Youtility ensure that this procedure and assessment against standards are applied consistently (to both internal and external candidates);

		- There is no consideration given to any candidate based on their sex, race, age, religion and sexual orientation or other such attributes; Youtility maintain a strictly non-discriminatory approach and policy; - Youtility do ensure appropriate referencing and fitness & proprietary checks are done and positively affirmed; and - Appropriate records are maintained & Youtility transform any gaps into the successful candidate's initial Continuing Professional Development plan CPD. As part of our onboarding process for new joiners, Youtility require all employees to read and retain both the IT Security Policy and Business Continuity Policy. Training is given on a regular basis when required to ensure key information is understood and is delivered to employees and access levels to the systems. When joining Youtility all staff members are given access to all the necessary internal documentation and are given time in the first weeks to review and analyse all documents. The Head of engineering and Founders discuss with all new joiners any questions and key items associated with the documentation to ensure the new joiner fully understands the company wide requirements and role specific responsibilities.

#	**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?	- Youtility uses AI driven active monitoring within the Microsoft Azure environment. Any security event are immediately escalated via email to ley personnel such as the Head of engineering and Lead developers. When an alert is received it is immediately verified, and if a breach is detected Youtility's breach procedures are implemented as described in the provided Information Security Policy and breach procedure documents. Youtility staff work remotely and always have access to laptops and communication devices so processes can be followed at any time. - Youtility’s Google Workspace systems include active monitoring and automatically flag up any unusual access or access attempt to the management team. All alerts are immediately investigated. - Additionally, all mission critical systems such as Microsoft Azure and developer tools are protected with two factor authentication.
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?	- All new development activity follows strict coding and architectural standards to ensure the security and robustness of the systems being built. Youtility follows SOLID architecture principles which ensure the development of high quality, secure, enterprise grade code. - Code quality and automated vulnerability scanning tools are used as a standard part of Youtility’s build process, which identifies code defects and configuration issues that could affect security. Any identified issues are fixed. - Youtility undertakes independent third-party security and penetration testing at a minimum once a year using a CREST certified provider. Any identified vulnerabilities are patched. Additionally, any time there are significant changes to

		the architecture or infrastructure of Youtility systems, testing is carried out again to ensure no vulnerabilities have been introduced.

#	Item to be assessed	Your Response
1.15	What processes does your business have in place in relation to incident management?	Youtility has standard service SLAs that apply to all commercial services. The SLAs define severity levels as: 1. Critical: The service is unavailable or unable to complete core functionality. 2. Serious: The service is intermittently unavailable for stretches of more than 15 minutes at a time and core functionality can be started/completed but not consistently 3. Moderate: A core element of the service is impaired, but the impairment does not constitute a serious issue (such as malformed error messages or minor issues with edge cases) and the functionality can be completed 4. Minor: Core functionality is intact with minor non-functional issues, such as spelling mistakes in copy Notification of any issues with Youtility services is by web chat (usually Slack) or email. Upon receipt of notification a confirmation is relayed back from Youtility with indicative timings and next actions. Youtility will update progress periodically and

		alert via web chat or email when the issue has been resolved. These issue classifications and communication processes apply to Youtility's client facing APIs. Youtility employs an agile process for identifying and addressing technical issues. Issues are detected when we encounter an issue during our standard development, during QA, or as reported by a user. When we identify a suspected issue, it is raised by the development team to the product owner. The product owner is then responsible for discussing the issue with the Head of engineering and senior engineering team. This discussion includes how much impact the issue is likely to have on the system and our users, and what information we already have about the issue. This allows the team to triage the issue and the product owner logs it in JIRA as a bug. If further research is required to investigate and understand the issue, an investigation task will also be created in Jira. After the bug is logged in Jira it is prioritised in the bug backlog based on impact and business urgency. Once it is in the backlog the development team picks it up and it progresses through our development pipeline from development, to testing by QA, to our staging environment for further user testing. Finally, it will be deployed to production and that bug ticket will be marked as closed in Jira. This enables us to have an agile, fluid process while also maintaining traceability. Any incident that results in a service outage or has a severe impact to the Youtility platform or API is recorded in an incident register. Additionally, any security breaches or fraud are also recorded in the incident register. Any breaches that expose private information are immediately reported to the FCA. To date Youtility has had no major incidents.

1.16	How do you ensure your data is held in a secure manner, retained for only the necessary time required and deleted appropriately?	Please refer to the Data Handling and Backup policy for a detailed explanation. All data at rest is held in Youtility's SQL Server database infrastructure. These databases are encrypted by default as are all backups. Any sensitive data held within these databases has an additional layer of 256 bit AES encryption with the encryption key stored in a secure vault. When the data is no longer needed (a switch has been processed or workflow expired), the encryption key is deleted and the data is rendered unreadable. Encrypted data is cleared from the database once a week for additional security. Access to production databases is limited to the minimum number of staff needed to maintain and improve the functionality encapsulated within. Access to the secure vault is limited to the Head of engineering and Lead developers. Youtility uses Microsoft Azure Active Directory system to limit staff access to only the resources they require to perform their duties and this access is regularly reviewed. Youtility also employs two factor authentication to log into Active Directory accounts.

#	Item to be assessed	Your Response

1.17	How do you ensure data is only accessed for the purposes for which it is required?	Data access only occurs through Youtility APIs and automated systems built to power those APIs. As such no human intervention is needed to collect, read, or utilise the data. This ensures that the data is handled in accordance with the Data Handling and Backup policy provided.
1.18	Please provide a completed up-to-date and relevant ICO checklist.	Processor checklist according to the ICO site included. There's a webpage where you answer what you've implemented.

#	Item to be assessed	Your Response

1.19	Please provide your Data Protection Registration number and registration.	Youtility is registered with the ICO as a data controller (ZA255938).
1.20	Have you reported any data breaches to the ICO in the last year and what action did you take to remedy these?	No. Youtility has not had any data breaches.

Name	Charlie Quigley
Title	Co-founder
Company	Youtility Limited
Date	11th October 2021
Signature	Charlie Quigley

To find out more please contact:

enquiries@recmanager.co.uk

RETAIL
ENERGY
CODE