Colo 2.0

JSE IaaS Service

Data Protection - Cloud Computing Checklist -Colo 2.0

No.	Question	Answer
1	Identify the categories of personal information that will be processed by the cloud service provider	The Colo 2.0 service needs to store user email addresses for the sole purposes of notifying users when orders have completed, and of allowing users to receive password reset emails in the event that they forget their password.
2	Has the cloud service provider provided the JSE with a security assessment conducted by a third party?	the Colo 2.0 solution in partnership with its service provider, utilises a competent 3rd party organisation (CHECK + CREST Certified) to conduct annual penetration tests of its internal infrastructure and web applications. All findings are addressed inline with the Vulnerability Management & Penetration Testing Policy.
3	Does the cloud service provider comply with the requirements of an appropriate industry code of practice or other quality standard (for example, an ISO standard)?	The Colo 2.0 service is ISO 27001 certified audited annually by a UKAS accredited provider.
4	Are all communications between the JSE, the cloud service provider and users encrypted? Is the data encrypted at rest? Is the data encrypted in transit? Are appropriate key management procedures in place (in line with the JSE's Cryptographic standard? Who will manage the encryption key?	All communication between JSE end users and the Colo 2.0 portal are encrypted using TLS encryption, secured by a 2048 bit RSA key. Older encryption protocols are disabled. Encrypted data at rest is not enabled however end clients can utilise any compatible encryption software they might require
5	How much time does the cloud service provider require to delete data and for what period will the cloud service provider retain data? Does the cloud service provider destroy end-of-life data and/or storage mediums?	End users manage the data that resides on the Colo 2.0 service
6	Will the cloud service provider destroy the JSE's data securely upon the termination of the relationship between the JSE and the cloud service provider (for any reason), if so elected by the JSE?	Yes
7	Will the cloud service provider provide the JSE's data to any third parties or will the JSE data be shared across any other services that may be offered by the cloud service provider (including for billing purposes)?	No
8	Does the cloud service provider have adequate user access privilege controls in order to restrict access to the JSE's data and audit trails in place for the JSE to monitor the identity of person's accessing the JSE's data?	All user types and data access privelege is managed by the end user.

9	Is the JSE able to request data from the cloud service provider in a usable format (or in a common format that is usable by the data subject)?	Only end users have access to their data that resides on the Colo 2.0 servers
10	In the event of a major data loss, how long would the cloud service provider require to restore the JSE's data (without alteration) from a backup?	Data backup is not part of the standard offering
11	Will the quality of service received by the JSE be impacted by the actions of the other customers of the cloud service provider?	No
12	Will the data hosted by the cloud service provider always be accessible when required by the JSE?	JSE would not be expected to access their clients data hosted on exchange cloud
13	If the cloud service provider suffered a major outage, how would this impact the JSE? What is the process that the cloud service provider will follow in the event of a major outage?	The infrastructured is housed in the JSE data centre and in the case of an outage the JSE crisis management procedure will be followed.
14	How will the cloud service provider communicate changes to its services that may impact the JSE?	Change management processes have been agreed with JSE and it's provider. Any client facing changes will be communicated with 2 weeks prior notice.
15	In which countries will the cloud service provider process the data provided to it by the JSE and what information is available relating to the safeguards in place that those locations? Are You able to ensure that the rights of data subject's will be adequately protected at these locations (i.e. requirements which are substantially similar to the requirements of POPIA itself)?	JSE's service provider's headquarters is in the UK so some JSE data (eg support contact info) will be processed in the UK with a copy of the client email address also stored in New York.
16	In which circumstances will the cloud service provider transfer the JSE's data to another country?	Client trading data is not stored by JSE's service provider
17	Does the cloud service provider have the technical capability to limit the processing of JSE data to a single country (or to countries designated by the JSE)?	Support related data would be processed in the UK only with an email address stored in the New York provisioning system of the JSE's service provider.