3rd Party External data hosting requirements

The following conditions must be met when BT data is

- Hosted in an external environment (Non BT Data Centre)
- Transferred between Data Centre's (DC) (Non BT Data Centre)
- Transferred between Data Centre's and back up facilities. (Non BT Data Centre)

It applies to all BT 'In Confidence (IC) data, BT 'In Strictest Confidence' (ISC) data and BT Personal data. See the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm for definitions. There are additional controls for Sensitive Personal Data.

Ref	Control	Reason
EDH20	If the external hosting is compromised and BT data is stolen or modified, a process must be in place to ensure BT is notified as per the contract, with sufficient level of detail as per BT's Minimum Security Requirements and the condition headed "protection of Personal Data" where processing personal data.	To make sure BT is quickly made aware of a potential incident /data theft.
EDH30	The Data Centre should hold a valid ISO 27001 certificate for security management (or certification(s) that demonstrate equivalent controls, supported by independent auditors report)	ISO27001 demonstrates that a best practice information risk management framework of controls is in place.
EDH60	Management of cryptographic keys must meet the requirements of the Cryptography Standard in the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Cryptography best practice
EDH70	Logical user access for Administration purposes must be role based and use industry standard 2-factor authentication e.g. one time password tokens or certificates issued by recognised trusted root certification authorities. Lists and files of trusted root certification authorities can be found at - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Weak access control could result in unauthorised access.
EDH90	Administration of externally hosted applications or data must be via a secure (encrypted) connection and use 2 factor authentication as per EDH70.	To make sure remote access support is as secure as local access.
EDH100	Any remote direct access to data where, BT data is in transit or at rest must be from within the same country as the Data Centre or in a country or territory that ensures an adequate level of protection for the BT data. Off-site storage must be within the same country as the Data Centre or in a country or territory that ensures an adequate level of protection for the BT data	To minimise the risk of not meeting country data protection laws or In Confidence data being processed in regions of concern to BT.
EDH110	Any access (physical or logical) for change control or fault investigation/remediation purposes must have a change request or fault ticket. Such access must only be granted for the duration of the change/fault and removed afterwards.	To minimise the risk of unauthorised changes being made.
EDH130	Back-up data storage must be encrypted at the media level, e.g. tape, disks etc. as per the Encryption standard in the 3rd Party Information Classification and Handling Specification http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	To protect BT data and minimise the risk of not meeting country data protection laws