Requisiti per l'hosting di dati esterno di terze parti

Le seguenti condizioni devono essere soddisfatte quando i dati BT:

- sono ospitati in un ambiente esterno (Centro dati non-BT)
- vengono trasferiti tra Centri dati (Centro dati non-BT)
- vengono trasferiti tra Centri dati e strutture di back up. (Centro dati non-BT)

Si applicano a tutti i dati BT 'confidenziali' (In Confidence, IC), ai dati BT 'strettamente confidenziali' (In Strictest Confidence, ISC) e ai dati BT personali. Per le definizioni, consultare le Specifiche per la classificazione e la gestione delle informazioni di terze parti http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm. I Dati personali sensibili richiedono controlli supplementari.

Rif.	Verifica	Motivo
EDH20	Se l'hosting esterno è compromesso e i dati BT vengono sottratti o modificati, va messa in atto una procedura volta a garantire che BT sia informata, come da contratto, con un grado sufficiente di particolari, come previsto dai Requisiti minimi di sicurezza di BT e, in caso di elaborazione di dati personali, dalla condizione indicata nella sezione sulla "protezione dei dati personali".	Garantire che BT venga informata tempestivamente di potenziali incidenti/sottrazioni di dati.
EDH30	Il Centro dati deve essere in possesso di una norma ISO 27001 valida per la gestione della sicurezza (o di una o più norme che dimostrino il possesso di procedure di verifica equivalenti, supportate dalla relazione di revisori indipendenti)	Lo standard ISO 27001 dimostra l'esistenza di un sistema di verifiche, basato sulle migliori prassi, per la gestione dei rischi relativi alle informazioni.
EDH60	La gestione delle chiavi crittografiche deve ottemperare ai requisiti dello standard di crittografia indicati nelle Specifiche per la classificazione e la gestione delle informazioni di terze parti http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Migliori prassi in materia di crittografia
EDH70	L'accesso logico degli utenti a scopo amministrativo deve avvenire in base al ruolo e utilizzare l'autenticazione a 2 fattori standard del settore. Ad esempio, token o certificati con password monouso rilasciati da organismi di certificazione di base affidabili e riconosciuti. Elenchi e file degli organismi di certificazione di base affidabili sono disponibili su: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Un controllo degli accessi carente potrebbe dare luogo ad accessi non autorizzati.
EDH90	L'amministrazione delle applicazioni o dei dati ospitati esternamente deve essere effettuata utilizzando una connessione sicura (crittografata) e l'autenticazione a due fattori, come indicato in EDH70.	Verificare che il supporto all'accesso remoto abbia lo stesso livello di sicurezza dell'accesso locale.
EDH100	Qualunque accesso diretto remoto ai dati, quando i dati BT sono in transito o archiviati, deve avvenire dall'interno dello stesso paese in cui si trova il Centro dati, oppure in un paese o territorio che garantisca un livello di protezione adeguato ai dati BT. L'archiviazione off-site deve avvenire all'interno dello stesso paese in cui si trova il Centro dati, oppure in un paese o territorio che garantisca un livello di protezione adeguato ai dati BT.	Ridurre al minimo il rischio di non ottemperare alla legislazione nazionale in tema di protezione dei dati o il rischio che i dati confidenziali vengano elaborati in regioni che BT ritiene problematiche.
EDH110	Qualunque accesso (fisico o logico) volto al controllo delle modifiche o alla ricerca/riparazione di guasti, deve essere accompagnato da una richiesta di modifica o da un'attestazione di guasto. Tale accesso deve essere concesso solo per la durata della modifica o del guasto e poi essere rimosso.	Limitare al massimo il rischio che vengano apportate modifiche non autorizzate.

EDH130	L'archiviazione dei dati di back-up deve essere crittografata a livello dei mezzi di supporto (ad esempio, su nastro, dischi, ecc.), come previsto dallo standard di crittografia indicato nelle Specifiche per la classificazione e la gestione delle informazioni di terze parti http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Proteggere i dati BT e ridurre al massimo il rischio di non conformità alle leggi nazionali di protezione dei dati.