

Anforderungen an externes Datenhosting durch Dritte

Die folgenden Bedingungen müssen erfüllt sein, wenn BT-Daten

- In einer externen Umgebung gehostet werden (Non-BT-Rechenzentrum)
- Zwischen Rechenzentren (RZ) übertragen werden (Non-BT-Rechenzentrum)
- Zwischen Rechenzentren und Backup-Einrichtungen übertragen werden. (Non-BT-Rechenzentrum)

Dies gilt für alle BT-Daten mit den Merkmalen „In Confidence“ (IC) und „In Strictest Confidence“ (ISC) und für persönliche Daten bei BT. Definitionen finden Sie in der Informationsklassifikation und den Handhabungsspezifikationen für Dritte <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>. Für sensible persönliche Daten bestehen weitere Kontrollen.

Ref.	Kontrolle	Grund
EDH20	Wenn das externe Hosting beeinträchtigt wurde und BT-Daten gestohlen oder modifiziert wurden, muss ein Prozess vorhanden sein, mit dem sichergestellt wird, dass BT vertragsgemäß benachrichtigt wird, dabei ausreichend Details gemäß den Mindestsicherheitsanforderungen von BT erhält und die Angelegenheit mit „Schutz persönlicher Daten“ überschrieben wird, wenn es um die Verarbeitung persönlicher Daten geht.	Sicherstellen, dass BT rasch auf potenzielle Zwischenfälle/Datendiebstähle aufmerksam gemacht wird.
EDH30	Das Rechenzentrum muss über ein gültiges Zertifikat nach ISO 27001 für Sicherheitsmanagement verfügen (oder (ein) Zertifikat/e, mit dem/denen dementsprechende Kontrollen nachgewiesen werden, unterstützt durch einen unabhängigen Auditbericht)	ISO 27001 zeigt an, dass Kontroll-Rahmenbedingungen für das Risikomanagement gemäß den Best Practices bestehen.
EDH60	Das Management kryptografischer Schlüssel muss die Anforderungen des Kryptografiestandards gemäß der Informationsklassifikation und den Handhabungsspezifikationen für Dritte erfüllen http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Best Practices der Kryptografie
EDH70	Logische Benutzerzugänge für Administrationszwecke müssen rollenbasiert sein und die Zwei-Faktor-Authentifizierung nach Branchenstandard nutzen, z. B. einmalige Passwort-Token oder Zertifikate, die von anerkannten und vertrauenswürdigen Root-Zertifizierungsstellen ausgestellt werden. Listen und Dateien von vertrauenswürdigen Root-Zertifizierungsstellen finden Sie unter - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Schwache Zugriffskontrollen können zu unberechtigtem Zugriff führen.
EDH90	Die Administration extern gehosteter Anwendungen oder Daten muss über eine sichere (verschlüsselte) Verbindung erfolgen und die Zwei-Faktor-Authentifizierung gemäß EDD7H70 nutzen.	Sicherstellung, dass Remote-Zugänge so sicher sind wie lokale Zugänge.
EDH100	Jeglicher direkte Remote-Zugriff auf Daten, bei dem BT-Daten übertragen oder aufgerufen werden, muss von innerhalb des Landes erfolgen, in dem sich das Rechenzentrum befindet, oder von einem Land oder Gebiet aus, in dem ausreichender Schutz für BT-Daten gewährleistet ist. Externe Speicherung muss innerhalb des Landes erfolgen, in dem sich das Rechenzentrum befindet, oder in einem Land oder Gebiet, in dem ausreichender Schutz für BT-Daten gewährleistet ist.	Zur Minimierung des Risikos, dass Datenschutzgesetze des Landes nicht eingehalten oder „In Confidence“-Daten in für BT bedenklichen Regionen verarbeitet werden.
EDH110	Jeglicher Zugriff (physisch oder logisch) für Änderungskontrollen oder zur Untersuchung/Behebung von Fehlern muss über eine Änderungsanforderung oder ein Fehlerticket verfügen. Derartige Zugriffe dürfen nur für die Dauer der Veränderung/des Fehler gewährt werden und sind danach zu löschen.	Zur Minimierung des Risikos von nicht autorisierten Veränderungen.

ÖFFENTLICHES DOKUMENT

EDH130	Backup-Datenspeicherung muss auf Niveau des Mediums verschlüsselt sein, z. B. Band, Disks usw., gemäß dem Verschlüsselungsstandard in der Informationsklassifikation und den Handhabungsspezifikationen für Dritte http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Schutz von BT-Daten und zur Minimierung des Risikos, Datenschutzgesetze des Landes nicht einzuhalten
---------------	--	--