Exigences relatives à l'hébergement externe de données par des tiers

Les conditions suivantes doivent être remplies lorsque les données de BT sont :

- Hébergées dans un environnement externe (centre de données autre que BT)
- Transférées entre des centres de données (autres que des centres de données de BT)
- Transférées entre des centres de données et des installations de secours (centre de données autre que BT).

Ces exigences s'appliquent à l'ensemble des données confidentielles de BT, des données strictement confidentielles de BT et des données personnelles de BT. Pour en savoir plus sur les définitions, se reporter au document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement) disponible à l'adresse http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm. Des contrôles supplémentaires s'appliquent aux données personnelles sensibles.

Réf.	Contrôle	Motif
EDH20	Si l'hébergement externe est compromis et que les données de BT sont volées ou modifiées, une procédure doit être en place afin d'en assurer la notification à BT, conformément aux dispositions du contrat. Cette notification doit fournir un degré suffisant de détail, conformément aux exigences minimales de BT en matière de sécurité et à la condition intitulée « Protection des données personnelles » aux fins du traitement des données personnelles.	Assurer que BT est rapidement informé d'un incident potentiel ou d'un éventuel vol des données.
EDH30	Le centre de données doit être titulaire d'un certificat ISO 27001 valide pour la gestion de la sécurité de l'information (ou de certificats attestant de l'application de contrôles équivalents, appuyés par un rapport d'audit indépendant).	La norme ISO 27001 indique qu'un cadre de contrôle utilisant les meilleures pratiques est en place pour la gestion des risques liés à l'information.
EDH60	La gestion des clés cryptographiques doit respecter les exigences en matière de cryptographie du document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement) http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Application des meilleures pratiques pour la cryptographie
EDH70	L'accès logique des utilisateurs à des fins administratives doit être fondé sur les rôles attribués et utiliser l'authentification forte en usage dans le secteur (par ex., systèmes de mot de passe à usage unique ou certificats racines approuvés délivrés par des autorités de certification reconnues). Des fichiers et des listes des autorités de certification racine approuvée sont disponibles à l'adresse suivante - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Un contrôle insuffisant de l'accès comporte des risques d'accès non autorisé.
EDH90	L'administration de données ou d'applications hébergées à l'extérieur doit passer par une connexion (cryptée) sécurisée et recourir à l'authentification forte, conformément à l'exigence EDH70.	Garantir que la sécurité de l'accès à distance est aussi élevée que celle de l'accès local.
EDH100	Tout accès distant direct aux données, qu'il s'agisse de données de BT en transit ou stockées, doit se faire depuis le pays dans lequel le centre de données se situe ou dans un pays ou un territoire assurant un niveau de sécurité adéquat pour les données de BT. Le stockage hors site doit avoir lieu dans le pays dans lequel le centre de données se situe ou dans un pays ou un territoire assurant un niveau de sécurité adéquat pour les données de BT.	Minimiser le risque de non-respect des lois nationales sur la protection des données ou le risque de traitement des données confidentielles dans des régions préoccupantes pour BT.

EDH110	Tout accès (physique ou logique) visant à contrôler des modifications ou à rechercher/corriger des défaillances doit faire l'objet d'une demande de modification ou d'un rapport pour correction de défaillance. Cet accès doit uniquement être accordé pour la durée de la modification/défaillance avant d'être retiré.	Minimiser le risque de modifications non autorisées.
EDH130	Le stockage de données de sauvegarde doit être crypté au niveau même des supports (par ex., bandes, disques, etc.), conformément aux exigences en matière de chiffrement du document « 3rd Party Information Classification and Handling Specification » (Classification des informations échangées avec des tiers et spécifications relatives à leur traitement) http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Protéger les données de BT et minimiser le risque de non-respect des lois nationales sur la protection des données.