

Externe datahosting vereisten voor derden

Aan de volgende voorwaarden moet worden voldaan als BT-gegevens worden

- Gehost in een externe omgeving (Niet-BT-datacentrum)
- Overgebracht tussen datacentra (DC) (Niet-BT-datacentrum)
- Overgebracht tussen datacentra en back-upvoorzieningen. (Niet-BT-datacentrum)

Dit is van toepassing op alle BT-gegevens "In vertrouwen", BT-gegevens "In het striktste vertrouwen" en BT-persoonsgegevens. Zie de Informatieclassificatie en behandelingsspecificatie voor derden op <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm> voor de gebruikte definities. Er zijn aanvullende controles voor gevoelige persoonsgegevens.

Ref	Controle	Reden
EDH20	Er moet een proces zijn geïmplementeerd voor het geval dat de externe hosting is gecompromitteerd en BT-gegevens zijn gestolen of gewijzigd om te garanderen dat BT geïnformeerd wordt conform het contract, op het detailniveau beschreven in de minimale veiligheidsvereisten van BT en de conditie genaamd "bescherming van persoonsgegevens" waar persoonlijke gegevens worden verwerkt.	Om te garanderen dat BT snel op de hoogte wordt gesteld van een eventueel incident/gegevensdiefstal.
EDH30	Het datacentrum moet beschikken over een geldig ISO 27001-certificaat voor veiligheidsmanagement (of een of meer certificaten die gelijkwaardige controles garanderen, ondersteund door een onafhankelijk auditor-rapport)	ISO 27001 garandeert dat een operationeel informatie-risicomanagementkader voor controles is geïmplementeerd.
EDH60	Het beheer van cryptografische sleutels moet voldoen aan de vereisten van de cryptografiernorm in de informatieclassificatie en behandeling specificatie voor derden http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Best practice cryptografie
EDH70	Logische gebruikerstoegang voor administratieve doeleinden moet functiespecifiek zijn en voldoen aan een 2-factor-authenticatie conform de industriernorm, bijvoorbeeld eenmalige wachtwoordtokens of certificaten verstrekt door erkende basiscertificering autoriteiten. De namen en dossiers van erkende basiscertificeringinstanties kunnen worden gevonden op: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Onvoldoende toegangscontrole kan leiden tot ongeoorloofde toegang.
EDH90	De administratie van extern gehoste applicaties of gegevens moet plaatsvinden via een beveiligde (gecodeerde) verbinding en met behulp van 2-factor-authenticatie, zoals vermeld in EDH70.	Om te garanderen dat de toegangscontrole op afstand net zo veilig is als plaatselijke toegang.
EDH100	Alle directe toegang op afstand tot gegevens waar BT-gegevens worden verwerkt of zijn gearchiveerd/opgeslagen moet plaatsvinden vanuit hetzelfde land als waarin het datacentrum is gevestigd of vanuit een land of gebied waar een adequaat niveau van bescherming van BT-gegevens is geïmplementeerd. <u>Externe opslag moet plaatsvinden binnen hetzelfde land als waarin het datacentrum is gevestigd of binnen een land of gebied dat een adequaat niveau van bescherming garandeert voor de BT-gegevens</u>	Om het risico te minimaliseren dat niet wordt voldaan aan de wetten voor gegevensbescherming of "In vertrouwen" gegevens die worden verwerkt in regio's die van belang zijn voor BT.
EDH110	Enige toegang (fysiek of logisch) voor wijzigingscontrole of storingsonderzoek/hersteldoeleinden wordt verkregen middels een wijzigingsverzoek of storingsticket. Dergelijke toegang wordt alleen toegestaan voor de duur van de wijziging/storing en wordt naderhand ingetrokken.	Om het risico dat ongeautoriseerde wijzigingen worden aangebracht te minimaliseren.

EDH130	Back-up gegevensopslag moet op medianiveau worden gecodeerd, bijvoorbeeld op tape, discs, enz. volgende de coderingsstandaard opgenomen in de informatieclassificatie en behandeling specificatie voor derden http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Om BT-gegevens te beschermen en het risico dat niet wordt voldaan aan de wetten voor gegevensbescherming van het land te minimaliseren
---------------	--	--