


Leistungsbeschreibung Sunetplus Cloud - Operativer Bereich und Security

Operativ	Information
Umfang neue Lösung	Die Applikation Sunetplus muss nicht mehr lokal installiert werden. Neu wird Sunetplus in einer Citrix-Cloud-Umgebung betrieben. Die Sicherung der Datenbank sowie das Update der Software und Cloud-Infrastruktur wird von BBT übernommen.
Ort der Datenresidenz	Die Daten werden in einer virtualisierten Umgebung des Betriebspartners der BBT in Zürich gehostet.
Betriebspartner der BBT	Der Betriebspartner ist CONVOTIS Schweiz AG. BBT hat mit dem Betriebspartner einen Unterauftragsbearbeitungsvertrag unterzeichnet zwecks Einhaltung der schweizerischen Datenschutzgesetzgebung. Weder BBT noch der Betriebspartner unterliegen dem CLOUD-Act.
Beschreibung der Systemumgebungen	<div style="text-align: center;">  <pre> graph LR A[Development (dev)] --> B[Staging (stage)] B --> C[Production (prod)] </pre> </div> <p>BBT setzt drei Umgebungen ein:</p> <ul style="list-style-type: none"> • Development: Testen neuer Funktionen • Staging: Testen der Einbindung der Schnittstellen • Production: Produktivsystem <p>Die Development-Umgebung enthält reine Beispieldaten (keine produktiven Daten). Die Verwendung von produktiven oder produktivnahen Daten (z.B. Konfigurationen) erfolgt nur auf den Umgebungen Staging und Production. Die Umgebungen sind dementsprechend geschützt. Dem Kunden steht ausschliesslich die Production-Umgebung zur Verfügung.</p>
Backup	Es erfolgt eine regelmässige Sicherung der Datenbanken und des Laufwerkspeichers. Das Backup wird an einem anderen Standort innerhalb der Schweiz aufbewahrt.
Einsicht Kundendaten	Wenn in einem Support-Fall, insbesondere im Rahmen der Datenmigration, eine Bearbeitung durch die Support-Organisation erforderlich ist, geschieht dies ausschliesslich mit ausdrücklichem Einverständnis des Kunden. Sämtliche Zugriffe werden protokolliert.
Prozess Onboarding	Für das Onboarding erhält der Kunde einen Upload-Link, über welchen er die Sunetplus-Datenbank (Microsoft Access, SQLite oder ein Backup der Microsoft SQL-Datenbank) an BBT übermitteln kann. BBT führt die Migration durch und informiert den Kunden, sobald alle Daten übertragen wurden und das System bereitsteht.

Benutzerverwaltung	BBT stellt dem Kunden die Zugangsdaten zum Verwaltungsbereich zur Verfügung. Anschliessend ist der Kunde zuständig und verantwortlich für die Benutzerverwaltung.
Datentransfer bei Kündigung	Im Falle einer Vertragsauflösung durch Kündigung wird dem Kunden ein Download-Link bereitgestellt, mit welchem er seine Daten (Datenbank-Backup und Laufwerkdaten) herunterladen kann. Danach werden alle Daten inkl. Backup von der Cloud-Umgebung unwiderruflich gelöscht.
Security	Information
Zertifizierungen / internes Kontrollsystem	BBT sowie der Betriebspartner CONVOTIS Schweiz AG sind ISO/IEC 27001 zertifiziert. BBT betreibt zudem ein angemessenes und wirksames internes Kontrollsystem. Die Angemessenheit und Wirksamkeit wird jährlich durch eine externe Prüfgesellschaft beurteilt. Der Bericht wird auf Anfrage und gegen Entgelt dem Kunden zur Verfügung gestellt.
Technische und organisatorische Schutzmassnahmen	<ul style="list-style-type: none"> • Zugriff nach dem Least Privilege Prinzip • Die Benutzeranmeldung erfolgt über eine Zweifaktor-Authentifizierung mittels OTP (One-Time-Password) • Die Daten werden nur in verschlüsselter Form übertragen (SFTP, TLS, HTTPS) [in transit] • Die Datenbank und das Datenbank-Backup sind mittels TDE (Transparent Data Encryption) verschlüsselt [at rest] • Dateiübertragungen werden mittels Virens Scanner geprüft • Ein aktives, automatisiertes Monitoring überwacht laufend den Systemzustand • Firewall-Überwachung des Datenverkehrs • Regelmässig durchgeführte Kontrollen zwecks Sicherstellung und Erhöhung der Sicherheit
Sicherstellung der Verfügbarkeit	Die Cloud-Lösung wird in einem Tier-4-Datacenter betrieben. Jeder physische Server hat zwei Stromanschlüsse. Ein redundantes Failover-System ist im Einsatz.
Trennung Kundendaten	Jeder Kunde erhält eine vollwertige, von anderen Kunden abgekoppelte und isolierte Datenablage.
Einbindung eigener Identity Server (z.B. Active Directory, Microsoft Entra ID, Okta, usw.)	Die Einbindung externer Identity Server ist im Standardpaket nicht enthalten. Grundsätzlich ist diese Option möglich und wird gerne auf Anfrage individuell geprüft.

Der vorliegende Leistungsbeschrieb kann durch BBT jederzeit geändert werden. Es gilt jeweils die aktuell, gültige Version.