Raiffeisen Landesbank Kärnten

Version 001
11.09.2023

# DIENSTLEISTUNGSBESCHREIBUNG

## 1. Backup As A Service - Datenschließfach

### 1.1. Allgemeines:

Während eines aufrechten Vertragsverhältnisses stellt der Auftragnehmer eine Backupumgebung in Klagenfurt zur Verfügung, die über das Internet erreichbar ist. Der Speicherplatz am Backupziel wird laut Beauftragung freigeschalten. Der Auftraggeber ist verantwortlich für die Speicherquelle und deren Strom- und Netzwerkanbindung. Auf der Backupumgebung sind die Daten verschlüsselt abgelegt und der Auftragnehmer hat keinen Zugriff auf die Daten.

### 1.2. Identitätsmanagement:

Für jeden Auftraggeber wird ein eindeutiger Benutzer vom Auftragnehmer angelegt und die Zugangsdaten werden dem Auftraggeber im Zuge der Erst-Installation vom Auftragnehmer übermittelt. Die Passwörter bestehen aus 12 Zeichen, beinhalten Großbuchstaben, Kleinbuchstaben, Nummern und Sonderzeichen und werden maschinell generiert. Die Benutzerdaten werden vom Auftragnehmer entweder persönlich oder telefonisch dem Auftraggeber übergeben.

### 1.3. Sicherung von Informationen:

Die Backupumgebung ist mit einem RAID System ausgestattet um den Ausfall einzelner Festplatten zu kompensieren.
Der Inhalt des Backups wird vom Auftraggeber selbst definiert und die Verantwortung für die zu sichernden Daten liegt beim Auftraggeber. Häufigkeit, Zeitpunkt und Vorhaltezeit der zu sichernden Daten wird vom Auftraggeber konfiguriert.

### 1.4. Kryptografie:

Die Daten werden vor Übertragung vom System des Auftraggebers mit AES 256 verschlüsselt. Jede Backup-Version wird vom System des Auftraggebers mit einem zufällig generierten AES-Schlüssel verschlüsselt, und es wird genau derselbe Schlüssel benötigt, um die Daten zu entschlüsseln. Um den AES-Schlüssel zusätzlich zu schützen, wird er durch einen öffentlichen RSA-2048-Schlüssel weiter verschlüsselt. Somit werden die Daten schon vor der Übertragung an den Auftragnehmer verschlüsselt.
Die Authentifizierung funktioniert über Username und Passwort mit oben genannter Kennwort-Komplexität.
Die Verantwortung für das verwendete SSL-Zertifikat der Webkonsole der Backupumgebung liegt beim Auftragnehmer.

### 1.5. Protokollierung und Überwachung:

Die Protokolle über die Durchführung der Datensicherung sind auf dem System des Auftraggebers ersichtlich und liegen nicht in der Verantwortung des Auftragnehmers. Alle Logdaten die in der Backupumgebung anfallen werden zentral beim Auftragnehmer gesammelt und der Auftraggeber hat keinen Zugriff auf diese Logdaten.

1.6. Schutz der Protokollinformation:

Die Protokolle auf Seite der Backupumgebung werden vom Auftragnehmer für 10 Jahre auf WORM-Medien aufbewahrt. Diese Logdaten werden getrennt von der Backupumgebung beim Auftragnehmer aufbewahrt.

1.7. Datenwiederherstellungsprozess:

Die Datenwiederherstellung liegt in der Verantwortung des Auftraggebers, der Auftragnehmer stellt dafür nur die technische Infrastruktur zur Verfügung. Bei einer Datenwiederherstellung seitens Auftraggeber werden Logdaten in der zentralen Backupumgebung erzeugt. Welche Daten der Wiederherstellungsprozess beinhaltet, ist für den Auftragnehmer nicht ersichtlich.

1.8. Löschung von Daten

Sämtliche Anfragen zum Löschen von Daten werden im Ticketsystem des Auftragnehmers dokumentiert und betreffen das gesamte Backup des Auftraggebers, eine Änderung oder Zugriff auf die Daten ist durch den Auftragnehmer nicht möglich.

1.9. Geographischer Standort von personenbezogenen Daten (pbD):

Die Datenquelle befindet sich beim Auftraggeber vor Ort, die geographisch getrennte Backup-umgebung beim Auftragnehmer in Klagenfurt.



**RAIFFEISENLANDESBANK KÄRNTEN - RECHENZENTRUM UND REVISIONSVERBAND, REGISTRIERTE GENOSSENSCHAFT MIT BESCHRÄNKTER HAFTUNG**
Raiffeisenplatz 1 | 9020 Klagenfurt am Wörthersee | t +43 463 993 00 | info@rbgk.raiffeisen.at | rlb-bank.at
BIC RZKTAT2K | FN 116094b | Landesgericht Klagenfurt | ATU 25330807