

Anhang B zu den AGB SaaS

Allgemeine technische und organisatorische Maßnahmen

1. Zutrittskontrolle

In den Büroräumen der BRODEL GmbH sind keine Datensätze des Kunden vorhanden. Unsere Server stehen im professionellen Rechenzentrum unseres ISP Providers Hetzner Online GmbH unter Beachtung der Grundregeln zum Datenschutz wie Zutrittskontrolle, Zugangskontrolle etc..

2. Zugangskontrolle

Da unsere Mitarbeiter mit der Programmierung und Wartung des Servers betraut sind, müssen sie über das Administrator-Passwort (unter Linux "Root" Passwort genannt) verfügen. Dieses Passwort wird nach dem Grundsatz der Datensparsamkeit nur den Personen bekannt gemacht, die sich mit dem Server bzw. Programm beschäftigen.

Das Root-Passwort muss aus mindestens 16 Zeichen bestehen. Diese Zeichenkette muss mindestens einen großen und einen kleinen Buchstaben, eine Zahl und ein Sonderzeichen enthalten. Die Rücksetzung des Root-Passwortes ist nicht vorgesehen. Alle Passwörter sind in einem Passwortmanager (z.B. Keepass) aufzubewahren, der über eine 2-Faktor Authentifizierung verfügt.

3. Zugriffskontrolle

Server, die wir zur Datenverarbeitung anmieten, sind immer dedizierten Linux Server mit aktuellem Betriebssystem. Die Kommunikation zwischen dem Browser des Anwenders und unserem Server erfolgt ausschließlich verschlüsselt mit dem Verfahren TLS 1.2 / mindestens 256 Bit tief. Weiterhin gelten auch hier die Ausführungen unter "1) Zutrittskontrolle" sinngemäß.

4. Weitergabekontrolle

Die Server sind dedizierte Linux Server mit aktuellem Betriebssystem. Die Kommunikation zwischen dem Browser und unserem Server erfolgt verschlüsselt mit dem Verfahren TLS 1.2 / mind. 256 Bit-Tiefe (SSL).

Das Verschlüsselungsverfahren entspricht dem Standard "Perfect Forward Secrecy"

Der Server steht bei einem deutschen Provider und unterliegt den deutschen Datenschutzrichtlinien.

5. Eingabekontrolle

Alle Produktiv - Server verfügen über ein Login - System, welche alle Logins und Loginversuche abspeichern.

6. Auftragskontrolle

Jegliche Daten werden nach Weisung des Auftraggebers durch den bestehenden Nutzungsvertrag verarbeitet. Eine Datenverarbeitung ohne vorliegender Weisung des Auftraggebers erfolgt nicht.

7. Verfügbarkeitskontrolle

In den Büroräumen der BRODEL GmbH sind keine Datensätze des Kunden vorhanden.

Auf dem Server beim ISP haben wir ein

- Backup-Verfahren eingerichtet
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung über dedizierten Server
- Firewall / DDoS-Schutz

8. Trennungskontrolle

In den Büroräumen der BRODEL GmbH sind keine Datensätze des Kunden vorhanden. Die Trennung der kundenseitigen Daten erfolgt durch ein loggingesteuertes Rechtmanagement auf dem Server beim ISP.