Sicherheitsprinzipien

License12 ist eine Dienstleistungsplattform mit hohen Sicherheitsanforderungen. Um dem Anspruch einer hohen Datensicherheit und Serviceverfügbarkeit zu entsprechen, werden folgende Prinzipien den jeweils neuesten Erkenntnissen nach technisch umgesetzt:

1. Schutz des Anwenders
   Der Nutzer von L12 wird bei der Registrierung und Anmeldung vor Verwechselung und dem Missbrauch seiner Identität, geschützt. Dazu benötigt er eine persönliche SMS-fähige Telefonnummer, bzw. einen Ansagedienst im jeweiligen Land. Er wählt ein sicheres Passwort welches er vor fremdem Zugriff schützt.
2. Schutz der Vertragsdaten
   Der Master-User (Registrierer) des Kunden hat die Möglichkeit, Zugriffsgruppen zu definieren, um bestimmte Vertragsdaten nur einem eingeschränkten Nutzerkreis zugänglich zu machen. Der Master-User wird auf Anforderung in der Ausübung dieser administrativen Aufgabe geschult. Scheidet ein Nutzer aus, so werden seine Zugriffsdaten umgehend nach der Information seines Ausscheidens gelöscht, soweit es noch andere Nutzer gibt, die auf die entsprechenden Daten Zugriff haben.
3. Schutz des Rechenzentrums
   Das Rechenzentrum verfügt über einen Grundschutz zur Abwehr unberechtigter Zugriffe. Dieser besteht aus einem Zutrittskontrollsystem mit ID-Karten, einer Einbruchsmeldeanlage, einem Videoüberwachungssystem, sowie der Gebäudekontrolle durch einen Sicherheitsdienst.
4. Schutz der Server
   Die Server werden täglich mit Programmupdates versorgt, soweit diese sicherheitstechnisch relevant sein können. Zusätzlich werden die Server nach Bedarf durch dedizierte Schutz-mechanismen, Hardware- bzw. Software-gestützt, vor unzulässigen Zugriffen geschützt.
5. Schutz der Anwendung
   Die Anwendung wird regelmäßig einem Sicherheitsaudit unterzogen. Dabei werden die neuesten Erkenntnisse über den letzten Stand der cyber-Kriminalität zugrunde gelegt. Hierbei zutage tretende neue Sicherheitsfragen werden durch entsprechende Auf- und Nachrüstung in Architektur und Software adressiert.
6. Schutz der Datenbank
   Die Datenbank wird täglich gesichert und sekündlich gespiegelt. Davon unabhängig wird der Datenbestand dem Anwender in Office-Format zum Download zur Verfügung gestellt. Der Anwender kann somit jederzeit über seinen aktuellen Datenbestand verfügen.
7. Schutz der Zahldaten
   Die Abwicklung der Zahlungsvorgänge erfolgen durch einen PCI-DSS zertifizierten Provider, wie er auch im Bankensektor zum Schutz von Online-Transaktionen implementiert ist.