Mehr als ein Versprechen

Datenschutz und Datensicherheit bei FinTecSystems (FTS)

Zwei starke Partner

FinTecSystems (FTS) liefert für Agicap als technischer Infrastrukturanbieter mit BaFin-Erlaubnis über seine Open Banking-Plattform eine universelle Banking-Schnittstelle.

Diese deckt rund 6.000 Banken und mehr als 500 Millionen Konten in Europa ab. Die Integration von Online-Konten fügt sich dabei nahtlos in die SaaS-Lösung von Agicap ein und garantiert damit ein perfektes Kundenerlebnis: Durch die technische Anbindung können Unternehmen ihre Konten direkt mit Agicap verbinden und ein- und ausgehende Zahlungen werden automatisch abgeglichen – etwa 99,5 Prozent aller Banken in Europa sind so angebunden.

Mit FTS hat Agicap einen Partner an Bord, der höchste Sicherheitsstandards bietet und zertifiziert ist.

FTS mit BaFin-Erlaubnis als Konto-informations- und Zahlungsauslösedienst

Der Erlaubnis ging ein intensiver Antrags- und Prüfungsprozess voraus. Die BaFin legt als "Bankenaufsicht" hohe Maßstäbe an Datensicherheit und Datenschutz, die zum Großteil über die europäischen Vorgaben hinausgehen. FinTecSystems erfüllt bei seinen technisch-organisatorischen Maßnahmen zur Datensicherheit die strengen Maßgaben des Banken-IT-Standards BAIT ("Bankaufsichtliche Anforderungen an die IT") der BaFin. Darüber hinaus unterliegt FinTecSystems natürlich den Anforderungen des Bundesdatenschutzgesetzes (BDSG) sowie der Datenschutzgrundverordnung der Europäischen Union (DSG-VO).

Als eines der ersten Finanztechnologie-Unternehmen in Deutschland erhielt FinTecSystems im April 2019 von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Erlaubnis, als Zahlungsauslöse- und Kontoinformationsdienst am Markt zu agieren.

Das BAIT: FTS erfüllt die Standards der Bankenbranche

Das BAIT fußt auf mehreren Säulen, die die Datensicherheit und damit den Datenschutz gewährleisten sollen und hat hohe Anforderungen, die FTS erfüllt und regelmäßig überprüft. Dazu gehören beispielsweise:

- Die IT-Prozesse bei FTS stellen zu jeder Zeit die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicher.
- FTS nutzt im Bereich Benutzerberechtigung ausschließlich sichere Authentifizierungsverfahren (wie zum Beispiel 2FA) und setzt bei der Übertragung und Speicherung von Daten auf starke Verschlüsselung.
- Es erfolgt eine permanente Protokollierung der Systemaktivität, der Systemzugriffe und es existieren Audit Logs und sichere Programmierstandards.
- Regelmäßige Sensibilisierungs- und Schulungsmaßnahmen der Mitarbeiter sowie ein Notfallkonzept (Incident Response Plan) manifestieren den hohen Stellenwert des Datenschutzes innerhalb des Unternehmens.

Die Kundendaten bei FTS: maximaler Schutz im deutschen Rechenzentrum

Alle Kundendaten, die gesetzlich vorgeschrieben 30 Tage gespeichert werden müssen, liegen in einem deutschen Tier 3-Rechenzentrum, das alle Anforderungen an moderne Sicherheitsstandards (zum Beispiel detektierte Zaunanlage, Videoüberwachung und biometrisches Zutrittssystem) erfüllt. Das Rechenzentrum hält die Zertifizierungen ISO 27001, PCI-DSS und ISAE 3402 und alle Daten werden ausschließlich auf dedizierter Hardware verarbeitet.

Das TÜV-Siegel Geprüfter Datenschutz: FTS geht über die Vorgaben hinaus

Im Sinne der Dokumentation seiner eigenen hohen Ansprüche an den Datenschutz lässt sich FTS regelmäßig für das Zertifikat Geprüfter Datenschutz des TÜV Saarland auditieren.

Prüfgrundlagen sind unter anderem das Bundesdatenschutzgesetz (BDSG), ausgewählte Aspekte des BSI-Grundschutzes, relevante Elemente der ISO 27001 sowie der internationalen Norm für Managementsysteme für die Informationssicherheit (ISO/IEC 27000). Geprüft werden unter anderem Datenschutzmanagement sowie bauliche, organisatorische und technische Anforderungen. Diese umfassen beispielsweise Verschlüsselung, Zuständigkeitsregelungen, Zugriffsregelung, Passwortmanagement, Datenverarbeitungsprozesse, Outsourcing und Kontrollmechanismen sowie regelmäßige Schulungen der Mitarbeiter.