



Bedingungen zur Nutzung eines mobilen EBICS-Zugangs mit der Deutschen Bank im Rahmen der Datenfernübertragung (DFÜ)

Die nachfolgenden Bedingungen für die Datenfernübertragung (DFÜ) gelten für Kunden der DB Privat- und Firmenkundenbank AG (nachfolgend einheitlich Bank genannt).

1. Allgemeines

Der Kunde und die Bank haben eine Vereinbarung zur Durchführung der Datenfernübertragung abgeschlossen, nach welcher die Bank dem Kunden bestimmte elektronische Bankdienstleistungen bereitstellt („DFÜ-Vereinbarung“). Der mobile EBICS-Zugang bei der Bank ermöglicht es, Bankgeschäfte im Rahmen des EBICS-Standards abzuwickeln.

2. Geltung der Bedingungen für die Datenfernübertragung

Die Bedingungen für die Datenfernübertragung gelten grundsätzlich auch für die Nutzung des mobilen EBICS-Zugangs bei der Bank, allerdings mit nachfolgenden Modifizierungen:

a) Legitimations- und Sicherungsmedium

Das Smartphone oder der Tablet-Computer, über welche der mobile EBICS-Zugang erfolgt, stellt ein Legitimations- und Sicherungsmedium im Sinne von § 1 Abs. 5 Zahlungsdiensteaufsichtsgesetz dar.

b) Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags

Abweichend zu Klausel 4 der Bedingungen für die Datenfernübertragung gilt Folgendes:

- Die den Teilnehmer legitimierenden Daten müssen verschlüsselt in einem geschützten Bereich der Software für die Nutzung des mobilen EBICS-Zugangs gespeichert werden.
- Eine Datensicherung (z. B. in der Form des iTunes Backup) ist nur zulässig, wenn die den Teilnehmer legitimierenden Daten hierbei verschlüsselt sind.
- Die Entnahme des Legitimationsmediums nach Beendigung der DFÜ-Nutzung (z. B. Entnahme der Chipkarte aus dem Chipkartenlesegerät) ist im Rahmen des mobilen Verfahrens nicht möglich und daher nicht erforderlich.

c) Verhaltens- und Sorgfaltspflichten im Umgang mit Sicherungsmedien für den Datenaustausch

Abweichend zu Klausel 5 der Bedingungen für die Datenfernübertragung gilt Folgendes:

- Als Sicherungsmedium gilt das Schlüsselmateriale innerhalb der „EBICS mobile“-App.
- Der Kunde und jeder Teilnehmer ist verpflichtet, das Sicherungsmedium durch geeignete Maßnahmen (z. B. PIN-Zugriff) gegen unautorisierten Zugriff auf das Legitimationsmedium (Smartphone oder Tablet-Computer) zu schützen.

d) Sicherheitsanforderungen an das EBICS-Kundensystem

In Ergänzung zur Anlage 1c der Bedingungen für die Datenfernübertragung gilt Folgendes:

- Mobile Endgeräte sowie die Software für die Nutzung des mobilen EBICS-Zugangs müssen durch ein Passwort vor dem unbefugten Zugriff Dritter geschützt werden.
- Es wird empfohlen, die mobilen Endgeräte mit einem aktuellen Virens scanner, einer Anti-Malware-Software und der aktuellen Betriebssystemsoftware zu nutzen.
- Es wird dringend empfohlen, bei Nutzung des mobilen EBICS-Zugangs – speziell im WLAN – dieses durch eine Firewall abzusichern.
- Es ist sicherzustellen, dass die mobilen Endgeräte nur mit den standardmäßigen Rechten genutzt werden. Es ist nicht erlaubt, die vom Hersteller für bestimmte Funktionen serienmäßig vorgesehenen Nutzungsbeschränkungen zu umgehen, zu entfernen (z. B. sog. Jailbreak) oder ähnliche unautorisierte Handlungen vorzunehmen.