

# Sonderbedingungen für die Security-App

Gültig ab 01.09.2020

Um die Lesbarkeit dieser Geschäftsbedingungen zu erleichtern, wurde auf das Gendern verzichtet. Alle personenbezogenen Formulierungen sind geschlechtsneutral zu verstehen.

## 1. Allgemeines

Die Security-App stellt ein Sicherheitsverfahren der Ford Bank GmbH (nachfolgend „Bank“ genannt) im Online-Banking dar. Hierbei kann der Kunde, eine von ihm bevollmächtigte Person oder ein durch das Gesetz bestimmter Vertreter (nachfolgend „Teilnehmer“ genannt), der sich für die Security-App registriert hat, die für die Erteilung eines Auftrags erforderliche Freigabe mittels der Security-App generieren. Für die Security-App gelten die Allgemeinen Geschäftsbedingungen für Einlageprodukte, die Sonderbedingungen für das Online-Banking sowie die nachfolgenden Sonderbedingungen für die Security-App.

## 2. Personalisiertes Sicherheitsmerkmal und Authentifizierungsinstrument

Bei dem personalisierten Sicherheitsmerkmal handelt es sich um den Aktivierungscode, der dem Teilnehmer in einem Aktivierungsbrief zur Verfügung gestellt wird, damit er sich in der Security-App registrieren kann.

Die Freigabe eines Auftrags kann der Teilnehmer über ein mobiles oder stationäres Endgerät (z. B. Smartphone, Tablet oder Desktop-Computer) mit installierter Security-App erteilen („Authentifizierungsinstrument“).

## 3. Geheimhaltung des personalisierten Sicherheitsmerkmals und sichere Aufbewahrung des Authentifizierungsinstruments

Zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments ist der Teilnehmer verpflichtet, diese geheim zu halten und vor dem Zugriff anderer Personen sicher zu verwahren.

Die Security-App ist ausschließlich direkt von der Bank oder von einem von der Bank genannten Anbieter zu beziehen.

## 4. Vergleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank wird dem Teilnehmer die Daten aus seinem Online-Banking-Auftrag in der Security-App anzeigen und eine Autorisierung durch eine entsprechende Bestätigung verlangen. Der Teilnehmer ist verpflichtet, vor der Autorisierung die Übereinstimmung der im Online-Banking angezeigten Daten mit den in seinem Authentifizierungsinstrument dargestellten Daten (Betrag, IBAN des Zahlungsempfängers) zu prüfen. Eine Autorisierung des Auftrags durch

den Teilnehmer darf nur erfolgen, wenn die Daten im Online-Banking und im Authentifizierungsinstrument übereinstimmen.

## 5. Sperranzeige durch den Teilnehmer

Stellt der Teilnehmer den Verlust oder den Diebstahl des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten („Sperranzeige“).

## 6. Sperrung auf Veranlassung der Bank

Die Bank darf die Zulassung des Authentifizierungsinstruments zurückziehen und dieses für die Security-App sperren, wenn:

- Anzeichen für eine missbräuchliche Nutzung des Authentifizierungsinstruments vorliegen,
- das Authentifizierungsinstrument abhanden gekommen ist oder
- sonstige Sicherheitserfordernisse die Sperre gebieten.

## 7. Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach den Sonderbedingungen für das Online-Banking vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang.

Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn:

- er den Verlust oder Diebstahl des Authentifizierungsinstruments oder des zugehörigen Gerätes (z. B. Smartphone mit installierter Security-App) oder des Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er davon Kenntnis erlangt hat,
- er die Security-App der Bank nicht direkt von der Bank oder einem von der Bank benannten Anbieter bezieht oder
- die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft oder trotz fehlender Übereinstimmung der Daten die entsprechende Transaktion freigibt.