

# Schwäbische Bank

## Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN

### 1. Leistungsangebot

Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Sofern die Bank für Verfügungen mittels Online-Banking eine Betragsbegrenzung im System vorsieht, informiert sie ihn hierüber.

### 2. Nutzungsberechtigte und Zugangsmedien

Zur Abwicklung von Bankgeschäften mittels Online-Banking unter Verwendung von PIN und TAN erhalten der Konto-/Depotinhaber und etwaige Bevollmächtigte von der Bank jeweils eine persönliche Identifikationsnummer (PIN) sowie gegebenenfalls Transaktionsnummern (TAN). Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

### 3. Verfahren

- (1) Der Nutzer hat mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor seinen Namen sowie seine PIN eingegeben hat.
- (2) In den von der Bank im Einzelnen angegebenen Fällen hat der Nutzer jeweils zusätzlich eine TAN einzugeben. Zur Erläuterung der Nutzungsmöglichkeiten stellt die Bank eine Verfahrensanleitung zur Verfügung.
- (3) Der Nutzer ist verpflichtet, die technische Verbindung zum Online-Banking-Angebot der Bank nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen.
- (4) Der Nutzer ist für die Sicherung seiner Hard- und Software (z.B. Virenschutz, Schutz vor Ausspähen der Systeme) selbst verantwortlich.

### 4. Nachrichtenfregabe/Verwendung der TAN/TAN per SMS

- (1) Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungsaufträge) sind abgegeben, wenn sie abschließend zur Übermittlung an die Bank freigegeben sind. Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z. B. Überweisungsauftrag), ist die Freigabe der TAN maßgebend. Eine TAN kann nicht mehr verwendet werden, sobald sie zur Übermittlung an das Institut freigegeben worden ist.
- (2) Für das mobile TAN-Verfahren wird der Telekommunikationsanschluss des Nutzers registriert. Auf das registrierte Mobiltelefon wird dem Nutzer von der Bank bei Bedarf eine TAN durch eine Textmeldung (SMS) übermittelt. Stellt der Nutzer den Verlust seines Mobiltelefons oder der SIM-Karte fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer verpflichtet die Bank unverzüglich zu benachrichtigen.

### 5. Bearbeiten von Aufträgen im Online-Banking

Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags. Mittels Online-Banking erteilte Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.

- (1) Die Bearbeitung der Online-Banking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
- (2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
  - Der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert.
  - Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
  - Das Online-Banking-Datenformat ist eingehalten.
  - Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
  - Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Online-Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
- (3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online-Banking eine Information zur Verfügung stellen.

### 6. Finanzielle Nutzungsgrenze

Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredites vornehmen. Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung; die Bank ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

### 7. Geheimhaltung der PIN und der TAN

- (1) Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und der TAN erlangt. Jede Person, die die PIN und - falls erforderlich - eine TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen.

Sie kann z. B. Aufträge zu Lasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;
  - die dem Nutzer zur Verfügung gestellte TAN-Liste ist sicher zu verwahren;
  - bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.
  - beim mobile TAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.
- (2) Stellt der Nutzer fest, dass eine andere Person von seiner PIN oder von einer TAN oder von beidem Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er die Bank unverzüglich zu unterrichten. In diesem Fall wird die Bank den Online-Banking-Zugang zum Konto/Depot sperren. Die Bank haftet ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.
- (3) Der Teilnehmer muß die Sicherheitshinweise auf der Internetseite der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

## **8. Änderung der PIN**

Der Nutzer ist berechtigt, seine PIN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

## **9. Sperre des Online-Banking-Angebotes**

- (1) Wird dreimal hintereinander eine falsche PIN eingegeben, so sperrt die Bank den Online-Banking-Zugang zum Konto/Depot.
- (2) Werden dreimal hintereinander falsche TAN eingegeben, so wird der Zugang gesperrt. In diesem Falle sollte sich der Nutzer mit der Bank in Verbindung setzen.
- (3) Die Bank wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über den Online-Banking-Zugang besteht. Sie wird den Kontoinhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann mittels Online-Banking nicht aufgehoben werden.
- (4) Die Bank wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch des Kontoinhabers sperren. Auch diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

## **10. Rückruf oder Änderung von Aufträgen**

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, die Bank sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Die Bank kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihr diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

## **11. Haftung**

- (1) Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)
- (2) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.
- (3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.
- (4) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- (5) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.2 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
- (6) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 7.2),
  - das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat
  - das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde
  - das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat
- (7) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.
- (8) Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- (9) Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

## **12. Anwendbares Recht**

Auf die Geschäftsbeziehung zwischen dem Konto-/Depotinhaber und der Bank findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.