# Bedingungen Onlinebanking

akf bank
der finanzpartner

**Bedingungen für das Onlinebanking**

**1. Leistungsangebot**

**(1)** Der Kunde kann Bankgeschäfte über sein Konto mittels Onlinebanking in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Onlinebanking abrufen.

**(2)** Zur Nutzung des Onlinebanking gelten die mit der Bank ggf. gesondert vereinbarten Verfügungslimite.

**2. Voraussetzungen zur Nutzung des Onlinebanking**

Der Kunde benötigt für die Abwicklung von Bankgeschäften mittels Onlinebanking die mit der Bank vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als zum Onlinebanking berechtigter Kunde auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Ein SMS-fähiges Mobiltelefon, Smartphone oder alternativ ein spezielles Lesegerät sind für das Onlinebanking erforderlich.

**2.1 Personalisierte Sicherheitsmerkmale**

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

– die persönliche Identifikationsnummer (PIN),
– einmal verwendbare Transaktionsnummern (TAN)

**2.2 Authentifizierungsinstrumente**

Die TAN können dem Kunden auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

– mittels App auf dem Smartphone zur Generierung von TAN per QR-Grafik (activeTAN)
– mittels Lesegerät zur Generierung von TAN per QR-Grafik (activeTAN)
– mittels eines mobilen Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN)

**2.3 Besondere Regelungen für das activeTAN-Verfahren**

Für die Nutzung von activeTAN ist ein TAN-Generator notwendig. Als TAN-Generator kann eine Smartphone-App oder alternativ ein spezielles Lesegerät der Bank verwendet werden.

Vor der ersten Verwendung ist die Aktivierung des TAN-Generators notwendig, um das Gerät mit dem Onlinebanking-Zugang des Kunden zu verknüpfen. Für die Aktivierung der App ist einmalig eine Internetverbindung notwendig.

Zur Anmeldung und zur Durchführung einer Transaktion im Onlinebanking wird dem Kunden eine QR-Grafik im Onlinebanking-Bereich angezeigt. Diese ist mit dem TAN-Generator zu scannen, der daraufhin eine TAN anzeigt. Dieser Prozess erfolgt offline.

Der Kunde hat im Onlinebanking-Bereich die Möglichkeit, bis zu zwei TAN-Generatoren zu verwalten. Ein bereits aktivierter TAN-Generator kann wieder deaktiviert werden.

**2.4 Besondere Regelungen für das mobileTAN-Verfahren**

Für die Teilnahme am mobileTAN-Verfahren ist ein Mobiltelefon mit deutscher SIM-Karte erforderlich. Beim mobileTAN-Verfahren wird die mobile Rufnummer des Kunden bei der Bank hinterlegt. Zur Anmeldung und zur Durchführung von Transaktionen im Onlinebanking-Bereich erhält der Kunde von der Bank auf Anforderung durch eine Online-Anwendung für jede Transaktion eine Textmeldung (SMS) mit einer TAN auf das Mobiltelefon. Die in der SMS angegebene TAN ist nur für die Transaktion gültig, für die sie angefordert wurde. Stellt der Kunde den Verlust seines Mobiltelefons oder der SIM-Karte fest oder besteht der Verdacht einer mißbräuchlichen Nutzung, ist der Kunde verpflichtet, die Bank unverzüglich zu benachrichtigen. Zusätzlich ist er verpflichtet, die SIM-Karte beim jeweiligen Telekommunikationsnetzbetreiber sperren zu lassen.

**3. Zugang zum Onlinebanking**

Der Kunde erhält Zugang zum Onlinebanking, wenn

– dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN übermittelt hat,
– er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(n) ausweist,
– die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Kunden ergeben hat und
– keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Onlinebanking kann der Kunde Informationen abrufen oder Aufträge erteilen.

**4. Onlinebanking-Aufträge**

**4.1 Auftragserteilung und Autorisierung**

Der Kunde muss Onlinebanking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal (TAN) autorisieren und der Bank im Onlinebanking-Bereich übermitteln. Die Bank bestätigt im Onlinebanking-Bereich den Eingang des Auftrags.

**4.2 Widerruf von Aufträgen**

Die Widerrufbarkeit eines Onlinebanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Onlinebanking-Bereiches erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Onlinebanking ausdrücklich vor.

**5. Bearbeitung von Onlinebanking-Aufträgen durch die Bank**

**(1)** Die Bearbeitung der Onlinebanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Onlinebanking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nicht an einem Geschäftstag gemäß Preis- und Leistungsverzeichnis der Bank zu, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen.



akf bank GmbH & Co KG
Servicecenter
Postfach 1242
85312 Freising
T +49 202 25727-2121
F +49 202 25727-2122

Sitz der Gesellschaft:
Am Diek 50, 42277 Wuppertal

www.akf24.de
service@akf24.de

Geschäftsführer:
Dr. Frank Henes (Vorsitzender),
Bernhard Ismann, Daniel Eschbach

Zuständige Aufsichtsbehörde:
Bundesanstalt für Finanzdienstleistungsaufsicht

**(2)** Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- der Kunde hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Kunden für die jeweilige Auftragsart liegt vor;
- das Onlinebanking-Datenformat ist eingehalten;
- das gesondert vereinbarte Onlinebanking-Verfügungslimit ist nicht überschritten;
- die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Onlinebanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr) aus.

**(3)** Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Onlinebanking-Auftrag nicht ausführen und dem Kunden über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Onlinebanking eine Information zur Verfügung stellen.

**6. Information des Kunden über Onlinebanking-Verfügungen**

Die Bank unterrichtet den Kunden mindestens einmal monatlich über die mittels Onlinebanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

**7. Sorgfaltspflichten des Kunden**

**7.1 Technische Verbindung zum Onlinebanking**

Der Kunde ist verpflichtet, die technische Verbindung zum Onlinebanking nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

**7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente**

**(1)** Der Kunde hat
- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Onlinebanking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2, 2.3 und 2.4) vor dem Zugriff anderer Personen sicher zu verwahren. Jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal das Onlinebanking-Verfahren missbräuchlich nutzen.

**(2)** Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
- Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das personalisierte Sicherheitsmerkmal darf nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden.
- Die PIN darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Kunde darf zur Autorisierung eines Auftrags, zum Beispiel zur Aufhebung einer Sperre, nicht mehr als eine TAN verwenden.
- Beim activeTAN-Verfahren und beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum Beispiel Smartphone), nicht gleichzeitig für das Onlinebanking genutzt werden.

**7.3 Sicherheit des Kundensystems**

Der Kunde muss die Sicherheitshinweise auf der Internetseite der Bank zum Onlinebanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

**7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten**

Soweit die Bank dem Kunden Daten aus seinem Onlinebanking-Auftrag (zum Beispiel Betrag und IBAN des Zahlungsempfängers) oder über ein Gerät des Kunden (Mobiltelefon, Smartphone oder Lesegerät) zur Bestätigung anzeigt, ist der Kunde verpflichtet, vor der Auftragsbestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

**8. Anzeige- und Unterrichtungspflichten**

**8.1 Sperranzeige**

**(1)** Stellt der Kunde
- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest,

muss der Kunde die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Kunde kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

**(2)** Der Kunde hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

**(3)** Hat der Kunde den Verdacht, dass eine andere Person unberechtigt
- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.



ELG_BOB_Neu_21_11_19

akf bank GmbH & Co KG
Servicecenter
Postfach 1242
85312 Freising
T +49 202 25727-2121
F +49 202 25727-2122

Sitz der Gesellschaft:
Am Diek 50, 42277 Wuppertal

www.akf24.de
service@akf24.de

Geschäftsführer:
Dr. Frank Henes (Vorsitzender),
Bernhard Ismann, Daniel Eschbach

Zuständige Aufsichtsbehörde:
Bundesanstalt für Finanzdienstleistungsaufsicht

**8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge**

Der Kunde hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

**9. Nutzungssperre**

**9.1 Sperre auf Veranlassung des Kunden**

Die Bank sperrt auf Veranlassung des Kunden, insbesondere im Fall der Sperranzeige nach Nummer 8.1

- den Onlinebanking-Zugang für ihn oder alle Kunden oder
- sein Authentifizierungsinstrument.

**9.2 Sperre auf Veranlassung der Bank**

**(1)** Die Bank darf den Onlinebanking-Zugang für einen Kunden sperren, wenn

- sie berechtigt ist, den Onlinebanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

**(2)** Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

**9.3 Aufhebung der Sperre**

Die Bank wird eine Sperre aufheben oder das personalisierte Sicherheitsmerkmal austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

**10. Haftung**

**10.1 Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügung**

Die Haftung der Bank bei einer nicht autorisierten Onlinebanking-Verfügung und einer nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

**10.2 Haftung des Kunden bei missbräuchlicher Nutzung seines Authentifizierungsinstruments**

**10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige**

**(1)** Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, ohne dass es darauf ankommt, ob den Kunden an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

**(2)** 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 Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 EUR, wenn der Kunde seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

**(3)** Ist der Kunde kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 EUR nach Absatz 1 und 2 hinaus, wenn der Kunde fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

**(4)** Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Kunde die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

**(5)** Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Kunde seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Kunden 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 8.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2),
- das personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2),
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Onlinebanking nutzt (siehe Nummer 7.2 Absatz 2).

**(6)** Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.



akf bank GmbH & Co KG
Servicecenter
Postfach 1242
85312 Freising
T +49 202 25727-2121
F +49 202 25727-2122

Sitz der Gesellschaft:
Am Diek 50, 42277 Wuppertal

www.akf24.de
service@akf24.de

Geschäftsführer:
Dr. Frank Henes (Vorsitzender),
Bernhard Ismann, Daniel Eschbach

Zuständige Aufsichtsbehörde:
Bundesanstalt für Finanzdienstleistungsaufsicht

**10.2.2 Haftung der Bank ab der Sperranzeige**

Sobald die Bank eine Sperranzeige eines Kunden erhalten hat, haftet sie für alle danach durch nicht autorisierte Onlinebanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kunde in betrügerischer Absicht gehandelt hat.

**10.3 Haftungsausschluss**

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.



akf bank GmbH & Co KG
Servicecenter
Postfach 1242
85312 Freising
T +49 202 25727-2121
F +49 202 25727-2122

Sitz der Gesellschaft:
Am Diek 50, 42277 Wuppertal

www.akf24.de
service@akf24.de

Geschäftsführer:
Dr. Frank Henes (Vorsitzender),
Bernhard Ismann, Daniel Eschbach

Zuständige Aufsichtsbehörde:
Bundesanstalt für Finanzdienstleistungsaufsicht