



Bedingungen für das Online Banking (Stand: 31.03.2020)

1. Leistungsangebot

- (1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können der Kunde und dessen Bevollmächtigte Informationen der Bank mittels Online Banking abrufen. Zudem sind sie gemäß §675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdienststeuergesetz (ZAG) zu nutzen, insofern die Verwendung von Unterschriftsmappen ausgeschlossen ist (im Folgenden: „U-Mappen“). Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.
- (2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.
- (3) Zur Nutzung des Online Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimits. Eine Änderung dieser Limits kann der Teilnehmer mit seiner Bank gesondert vereinbaren. Dieser Absatz 3 greift nicht im Falle der Verwendung von U-Mappen.

2. Voraussetzungen zur Nutzung des Online Banking

- (1) Der Teilnehmer kann das Online Banking nutzen, wenn die Bank ihn authentifiziert hat.
- (2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).
- (3) Authentifizierungselemente sind
 - Wissensselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer (PIN)),
 - Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
 - Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).
- (4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

3. Zugang zum Online Banking

- (1) Der Teilnehmer erhält Zugang zum Online Banking, wenn
 - er seine individuelle Teilnehmerkennung (z.B. Kontonummer, Anmeldename) angibt und
 - er sich unter Verwendung der von der Bank angeforderten Authentifizierungselemente ausweist und
 - keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.Nach Gewährung des Zugangs zum Online Banking kann der Teilnehmer Informationen abrufen oder Aufträge (siehe Nummer 4) erteilen.
- (2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z.B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

4. Online Banking-Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines 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 Online Banking erfolgen, es sei denn, die Bank, sieht eine Widerrufsmöglichkeit im Online Banking ausdrücklich vor.

5. Auftragsbearbeitung durch die Bank

- (1) Die Bearbeitung der -Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. 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 Online Banking-Seite der Bank oder „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 den Auftrag autorisiert (vgl. Nummer 4.1);
 - die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder oder Überweisungsauftrag) liegt vor;
 - das Online-Banking-Datenformat ist eingehalten;
 - das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3). Diese Regelung greift nicht im Falle der Verwendung von U-Mappen;
 - 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 Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
- (3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und dem Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

- (1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4).
- (2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
 - a) Wissensselemente, wie z.B. die PIN, sind geheim zu halten; sie dürfen insbesondere
 - nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
 - nicht außerhalb des Online Banking in Textform (z.B. per E-Mail, Messenger-Dienst) weiter gegeben werden,
 - nicht ungesichert elektronisch gespeichert (z.B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
 - nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.
 - b) Besitzelemente, wie z.B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
 - sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z.B. Mobiltelefon) nicht zugreifen können,
 - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
 - ist die Anwendung für das Online Banking (z.B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
 - dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
 - muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit Anwendung für das Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.
- c) Seinsselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinsselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinsselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissensselement (z.B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinsselement.
- (3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.
- (4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online Banking nicht mehr nutzt.
- (5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

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.

7.3 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zum Beispiel Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

- (1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. mobiles Endgerät, Signaturkarte) oder
 - die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungselements fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.
- (2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.
- (3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

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

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

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

- den Online Banking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online Banking.

9.2 Sperre auf Veranlassung der Bank

- (1) Die Bank darf den Online-Banking-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
 - sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente dies rechtfertigen oder
 - der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.
- (2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

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

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstrumentes

- (1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.
- (2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscode erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.
- (3) Ein TAN-Verfahren sperrt sich selbst, wenn fünfmal in Folge die TAN falsch eingegeben wird.
- (4) Die in Absätzen 1, 2 und 3 genannten Authentifizierungsinstrumente können dann nicht mehr für das Online Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online Banking wiederherzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht oder fehlerhaft ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung seiner Authentifizierungselemente

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 Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.
- (2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn
- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
 - der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.
- (3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltpflichten nach
- Nummer 7.1 Absatz 2,
 - Nummer 7.1 Absatz 4,
 - Nummer 7.3 oder
 - Nummer 8.1 Absatz 1 verletzt hat.
- (4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3).
- (5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

- (6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer 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.
- (7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.
- (8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:
 - Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
 - Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

1022 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhend nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen, welche keine Anwendung bei der Verwendung von U-Mappen finden) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des eines Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

1023 Haftung der Bank ab der Sperranzeige

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.

1024 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.

11. Multibanking

Die von der Bank angebotene Multibankingfunktion ist eine vom Kunden optional nutzbare Möglichkeit der Einbindung von Konten, Kreditkarten und Depots von inländischen Drittanbietern. Der jeweilige Drittanbieter muss hierzu die Möglichkeit eines Datenaustausches über eine entsprechende Schnittstelle bereitstellen. Beim Drittanbieter muss der Teilnehmer ebenfalls am Online Banking mit einem PIN/TAN-Verfahren teilnehmen oder dessen Online Angebot mit einem vergleichbaren, vom Anbieter unterstützten Sicherungsverfahren nutzen. Die Bank hat Zugriff auf die Kontoinformationen und Transaktionen des Kunden, und verarbeitet diese fortlaufend und regelmäßig zur Erbringung ihrer Leistungen im Rahmen der Multibankingfunktion und um diese in ausgewählten Beratungsprozessen einzusetzen und um dem Kunden individuelle Angebote zu unterbreiten. Personenbezogene Daten übermittelt die Bank nur dann an Dritte, wenn hierzu eine gesetzliche Verpflichtung besteht oder der Teilnehmer der Bank hierzu seine Einwilligung erteilt hat.

Die über die Multibankingfunktion im Online Banking der Bank angezeigten Daten zu den bei Drittanbietern geführten Konten, Kreditkarten und Depots werden über entsprechende Schnittstellen bei den Drittanbietern abgefragt. Die Bank übernimmt keine Haftung für die Genauigkeit und Vollständigkeit der von den Drittanbietern über Ihre Schnittstellen bereitgestellten Daten. Die Bank haftet nicht für eine Verfügbarkeit der Multibankingfunktion. Die Bank stellt die Funktionalität in der jeweils aktuellen Form bereit und behält sich das Recht vor, diese jederzeit und ohne vorherige Ankündigung weiterzuentwickeln, einzuschränken oder zu beenden. Für Schäden aus deren Ausfall haftet sie nur, wenn sie diesen vorsätzlich oder grob fahrlässig verschuldet hat.