Sonderbedingungen für das Online-Banking und für die elektronische Kommunikation

Version 1.0
Stand: 07.04.2026

A. Bedingungen für das Online-Banking

1. Leistungsangebot

1.1 Der Teilnehmer und dessen Bevollmächtigte (im Folgenden „Teilnehmer“ genannt) können bestimmte Bankgeschäfte mittels Online-Banking in dem von der Bank[1] angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online-Banking abrufen.

1.2 Des Weiteren ist der Teilnehmer für die Nutzung des Girokontos gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste im Sinne der § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

1.3 Der persönliche Online-Banking-Bereich dient dem Teilnehmer hauptsächlich dazu, seine Konten zu verwalten. Zu den angebotenen Funktionalitäten des Online-Bankings gehört unter anderem die Sperrung des Zugangs oder der Mobiltelefonnummer, die Änderung persönlicher Daten (wie Anschrift und Kontaktdaten) sowie der Erhalt und die Übermittlung von Nachrichten und Informationen durch die Bank. Zum Leistungsangebot gehört darüber hinaus die Möglichkeit des Teilnehmers, weitere Kontoeröffnungsanträge online zu stellen.

1.4 Der Teilnehmer kann im Online-Banking-Bereich den aktuellen Finanzstatus einzusehen. Im Finanzstatus wird eine Liste mit allen Konten des Teilnehmers sowie die dazugehörige Kontonummer, der Status und der Online-Saldo des jeweiligen Produktes angezeigt. Für jedes Konto kann wiederum aus dieser Ansicht in die Umsatzansicht gewechselt werden.

1.5 In der Übersicht für die Einlagenkonten werden darüber hinaus zusätzliche Angaben, wie der Eröffnungstag des Kontos, Laufzeitende, Laufzeit und Zinssatz p.a., angezeigt.

2. Voraussetzungen zur Nutzung des Online-Banking

2.1 Der Teilnehmer kann das Online-Banking nutzen, wenn die Bank ihn authentifiziert hat.

2.2 Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten personalisierten Instruments oder Verfahrens, 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).

[1] Dieses Dokument wird von der CA Consumer Finance S.A., die unter der Marke Crédit Agricole Savings die in diesem Dokument dargestellten Produkte und Dienstleistungen anbietet, zur Verfügung gestellt. Sofern in diesem Dokument die Bezeichnungen „Crédit Agricole Savings“ oder „Bank“ verwendet werden, ist damit jeweils die CA Consumer Finance S.A. gemeint.

2.3 Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (zum Beispiel persönliche Identifikationsnummer (PIN) bzw. Passwort), und
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (zum Beispiel Gerät zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Teilnehmers nachweisen, wie das mobile Endgerät).
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, zum Beispiel Fingerabdruck als biometrisches Merkmal des Teilnehmers).

2.4 Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, und den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt, soweit dies im Einzelfall notwendig ist.

3. Zugang zum Online-Banking

3.1 Der Teilnehmer erhält Zugang zum Online-Banking der Bank, wenn

- er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

3.2 Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (zum Beispiel zum Zweck der Änderung der Anschrift des Kunden) sowie für bestimmte Funktionalitäten (zum Beispiel Änderung der PIN) 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).

3.3 Nach Beendigung der jeweiligen Geschäftsbeziehung zwischen dem Teilnehmer und der Bank werden die Funktionalitäten des Online-Bankings für weitere 30 Kalendertagen zur Verfügung gestellt. Nach Ablauf dieser Zeit ist die Bank berechtigt, den Zugang zu allen Funktionalitäten des Online-Bankings zu sperren.

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (wie die Eingabe einer PIN oder die Verwendung biometrischer Merkmale) 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. Bearbeitung von Aufträgen durch die Bank

5.1 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 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 darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

5.2 Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Die weiteren Ausführungsbedingungen 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) aus.

5.3 Liegen die Ausführungsbedingungen nach Nummer 5.2 nicht vor, wird die Bank den Online-Banking-Auftrag nicht ausführen und dem Teilnehmer eine Information 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 zur Verfügung stellen.

6. Information des Teilnehmers über Online-Banking Verfügungen

Die Bank unterrichtet den Teilnehmer mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg, sofern in den gesondert vereinbarten Sonderbedingungen (zum Beispiel Sonderbedingungen für das Einlagengeschäft) nichts Abweichendes geregelt ist.

7. Sorgfaltspflichten des Kunden

7.1 Schutz der Authentifizierungselemente

7.1.1. Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird

(vergleiche Nummern 3 und 4 dieser Bedingungen).

7.1.2. Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(i) Wissenselemente, wie zum Beispiel die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (zum Beispiel telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Online-Banking in Textform (zum Beispiel per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (zum Beispiel 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 (zum Beispiel mobiles Endgerät) oder zur Prüfung des Seinselements (zum Beispiel mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

(ii) Besitzelemente, wie zum Beispiel das mobile Endgerät, sind vor Missbrauch zu schützen, insbesondere

- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (zum Beispiel Mobiltelefon) nicht zugreifen können, und
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät befindliche Anwendung für das Online-Banking (zum Beispiel Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online-Banking (zum Beispiel Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (zum Beispiel durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (zum Beispiel TAN) nicht außerhalb des Online-Banking mündlich (zum Beispiel per Telefon) oder in Textform (zum Beispiel per E-Mail, Messenger-Dienst) weitergegeben werden und.
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (zum Beispiel 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.

(iii) Seinselemente, wie zum Beispiel 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 Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online-Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das

Online-Banking das von der Bank ausgegebene Wissenselement (zum Beispiel PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

7.1.3. Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

7.1.4. Die für das mobile-TAN-Verfahren hinterlegte Referenzmobiltelefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Online-Banking nicht mehr nutzt.

7.1.5. Ungeachtet der Schutzpflichten nach den Nummern 7.1.1 bis 7.1.3 darf der Teilnehmer seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1.2 Sätze 2 und 3 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel mittels mobilen Endgerätes).

Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

8.1.1. Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Referenzmobiltelefons, oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest,

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

8.1.2. Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

8.1.3. 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 dieser Bedingungen,

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

9.2 Sperre auf Veranlassung der Bank

9.2.1. 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 des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

9.2.2. Die Bank wird den Teilnehmer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre 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 Teilnehmer unverzüglich.

9.4 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Teilnehmers verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Teilnehmer über eine solche Zugangsverweigerung unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

10. Haftung

10.1 Haftung der Bank bei nicht autorisierten oder fehlerhaft ausgeführten Änderungen kundenspezifischer Informationen

Die Bank haftet bei einer nicht autorisierten Änderung, oder einer nicht, fehlerhaft oder verspätet ausgeführten Änderung der kundenspezifischen Informationen (wie zum Beispiel Änderung der Kontaktdaten, Änderung der PIN) für den hieraus entstandenen Schaden.

10.2 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

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

10.3 Haftung des Teilnehmers bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.3.1. Haftung des Teilnehmers bei nicht autorisiertem Zugriff und Änderung der kundenspezifischen Informationen vor der Sperranzeige

(i) Beruht ein nicht autorisierter Zugriff und eine Änderung kundenspezifischer Informationen vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Teilnehmer für den der Bank hierdurch entstehenden Schaden, sofern der Verlust, das Abhandenkommen oder die sonstige missbräuchliche Verwendung des Authentifizierungselements auf einer fahrlässigen oder schuldhaften Handlung des Teilnehmers beruht.

(ii) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz (i) 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 Zugriff und der Änderung 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.

10.3.2. Haftung des Teilnehmers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(i) 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 Teilnehmer 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.

(ii) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz (i) 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.

10.3.3. Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen oder einem nicht autorisierten Zugriff und einer Änderung kundenspezifischer Informationen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Teilnehmer abweichend von Absatz (ii) der Nummern 10.3.1 und 10.3.2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 7.1.2 oder
- Nummer 7.1.3 Satz 2 oder
- Nummer 7.3 oder
- Nummer 8.1.1

dieser Bedingungen verletzt hat.

10.3.4. Abweichend von den Absätzen (i) der Nummern 10.3.1 und 10.3.2 und von der Nummer 10.3.3 ist der Teilnehmer nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen und Besitz oder Sein (siehe Nummer 2.3 dieser Bedingungen).

10.3.5. Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

10.3.6. Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz (i) der Nummern 10.3.1 und 10.3.2 und Nummer 10.3.3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

10.3.7. Die Absätze (ii) der Nummern 10.3.1 und 10.3.2 und die Nummern 10.3.4 bis 10.3.6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.4 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (zum Beispiel Verfügungen über Einlagen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Teilnehmer und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.5 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 oder Änderungen entstehenden Schäden.

Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.6 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.

B. Bedingungen für die elektronische Kommunikation

1. Einleitung

1.1 Die Kommunikation zwischen der Bank und dem Kunden erfolgt grundsätzlich elektronisch über das Online-Banking. Die Bank und der Kunde vereinbaren, dass die Bank das Online-Banking für die Kommunikation mit dem Kunden und insbesondere für die Bereitstellung von Dokumenten und Informationen an den Kunden (z. B. Kontoauszüge) nutzen darf.

1.2 Der Kunde kann insbesondere die Online-Banking-Funktion nutzen, um die von der Bank bereitgestellten Dokumente abzurufen, online einzusehen, herunterzuladen, auszudrucken und zu archivieren.

2. Einrichtung und Nutzungsmöglichkeiten

2.1 Die Bank richtet für den Kunden im Online-Banking-Bereich einen speziellen Bereich für die elektronische Kommunikation ein („**Postfach**“). Die Bank kann das Postfach jederzeit umbenennen oder technisch ändern, ohne dass dies Auswirkungen auf seine Funktion als vereinbarter Kanal für die elektronische Kommunikation hat.

2.2 Sobald die Funktion verfügbar ist, kann der Kunde außerdem die Nachrichtenfunktion innerhalb des Online-Banking-Bereichs nutzen, um Nachrichten an die Bank zu senden (wie z. B. Fragen zum Konto, Rückrufbitten oder Aktualisierungen von Kontaktdaten). Das Senden von Dokumenten oder Grafiken vom Kunden an die Bank über diese Funktion ist ausgeschlossen, sofern dies nicht ausdrücklich von der Bank freigegeben wurde.

2.3 Kommt das Geschäftsverhältnis nicht zu Stande oder wird es nachträglich beseitigt, (zum Beispiel durch Ausübung eines gesetzlichen Widerrufsrechts) kann die Bank die Online-Banking-Funktion, einschließlich des Postfachs unverzüglich deaktivieren und wenn notwendig den Inhalt löschen.

2.4 Die Bank ist jederzeit berechtigt, den Zugang zur Online-Banking-Funktion, einschließlich des Postfachs teilweise oder ganz zu sperren oder zu beschränken, wenn Umstände die Vermutung rechtfertigen, dass die Sicherheit des Zugriffs beeinträchtigt, ein nicht autorisierter oder betrügerischer Zugriff möglich sein kann oder die Bank berechtigt ist, die Geschäftsbeziehung zu dem Kunden aus wichtigem Grund zu kündigen.

3. Einstellen von Dokumenten und Verzicht des Kunden auf sonstige Zustellung

3.1 Der Kunde erklärt sein Einverständnis dazu, dass die Bank alle Dokumente im Zusammenhang mit der Geschäftsbeziehung des Kunden zu der Bank verschlüsselt und rechtsverbindlich im Postfach bereitstellt, soweit nicht die Schriftform mit dem Kunden ausdrücklich vereinbart wurde oder gesetzlich erforderlich ist.

3.2 Der Kunde nimmt zur Kenntnis und erklärt sein Einverständnis dazu, dass ihm solche Dokumente nicht auf anderem Weg bereitgestellt werden müssen. Der Kunde verzichtet insbesondere auf den postalischen Versand dieser Dokumente.

3.3 Die Bank ist jedoch weiterhin berechtigt, dem Kunden Informationen und Dokumente auf andere geeignete Weise bereitzustellen, wenn dies gesetzlich erforderlich ist oder wenn es

aufgrund anderer Umstände angemessen ist (z. B. bei einer vorübergehenden Störung der Online-Banking-Funktion).

3.4 Ungeachtet dessen ist die Bank berechtigt, dem Kunden einzelne oder bei technischen Problemen alle Dokumente, auf dem Postweg oder in sonstiger Weise an den Kunden zuzusenden, wenn sie dies unter Berücksichtigung des Kundeninteresses als zweckmäßig erachtet.

4. Zugangszeitpunkt

4.1 Die von der Bank im Postfach eingestellten Dokumente gehen zu, wenn der Kunde von der Bank über die Einstellung und Möglichkeit des Abrufs über das Postfach informiert wurde und üblicherweise mit der Kenntnisnahme durch den Kunden gerechnet werden kann, d.h. spätestens an dem Geschäftstag, der auf die Information der Bank folgt. Falls der Kunde die Dokumente bereits vorher tatsächlich abgerufen hat, gehen sie bereits zu diesem Zeitpunkt zu.

4.2 Ab dem Zeitpunkt des Zugangs des jeweiligen Dokuments nach Ziffer 4.1 beginnt der Lauf der an diesen Zugang anknüpfenden Fristen (zum Beispiel eine Widerrufsfrist).

5. Integrität der Dokumente innerhalb des Postfachs

5.1 Die Bank stellt die Unveränderbarkeit der Dokumente innerhalb des Postfachs sicher.

5.2 Diese Pflicht gilt nicht, soweit die Dokumente außerhalb des Postfachs gespeichert oder aufbewahrt werden. Sobald diese durch den Kunden außerhalb des Postfachs gespeichert oder genutzt werden (zum Beispiel nach dem Herunterladen) übernimmt die Bank keine Verantwortung für die Integrität der Dokumente sowie deren Inhalt.

5.3 Aufgrund der individuellen Hard- oder Softwareeinstellung stimmt ein Ausdruck optisch nicht immer mit der Darstellung am Bildschirm überein.

6. Benachrichtigung

6.1 Die Bank wird dem Kunden bei Einstellung eines neuen Dokuments in das Postfach einen Hinweis auf einen Posteingang per E-Mail an die für den Kunden hinterlegte E-Mail-Adresse senden. Der Kunde wird regelmäßig seinen Posteingangs- sowie den Spam-Ordner der von ihm verwendeten E-Mail-Anwendung kontrollieren. Der Kunde erklärt sich damit einverstanden, entsprechende Benachrichtigungen unverschlüsselt per E-Mail zu erhalten.

6.2 Der Kunde ist verpflichtet, die bei Begründung der Geschäftsbeziehung mit der Bank mitgeteilte E-Mail-Adresse für den Empfang von E-Mails bereit zu halten. Der Kunde ist verpflichtet, der Bank eine Änderung der E-Mail-Adresse unverzüglich mitzuteilen.

7. Besondere Mitwirkungspflichten des Kunden

7.1 Der Kunde ist verpflichtet, das Postfach in regelmäßigen, angemessenen Zeitabständen, mindestens jedoch einmal im Monat, und im Falle eines konkreten Anlasses (zum Beispiel nach einer Weisung an die Bank oder nach einer Benachrichtigungs-E-Mail nach Ziffer 6.1 dieser Bedingungen) stets unverzüglich auf Posteingang zu prüfen.

7.2 Der Kunde erklärt hiermit, dass die Bank ihren Übermittlungs- und Benachrichtigungspflichten mit dem Eingang der Dokumente im Postfach

und der entsprechenden Benachrichtigungs-E-Mail an den Kunden nachgekommen ist.

7.3 Der Kunde ist verpflichtet, die von der Bank im Postfach eingestellten Dokumente abzurufen und deren Inhalt hinsichtlich Richtigkeit und Vollständigkeit zu kontrollieren.

7.4 Unbeschadet der Nr. 6 (2) der Allgemeinen Geschäftsbedingungen der Bank hat der Kunde Beanstandungen gegenüber der Bank unverzüglich nach Zugang der Dokumente, mindestens in Textform (zum Beispiel per E-Mail oder durch Nutzung des Postfachs), anzuzeigen.

8. Speicherzeit

Die im Postfach bereitgestellten Dokumente stehen für die gesamte Dauer der jeweiligen Geschäftsbeziehung zwischen dem Kunden und der Bank zur Verfügung. Nach Beendigung der jeweiligen Geschäftsbeziehung zwischen dem Kunden und der Bank werden die im Postfach bereitgestellten Dokumente für weitere 30 Kalendertagen bis zur Sperrung des gesamten Online-Banking Funktion zur Verfügung gestellt. Der Kunde ist für die Speicherung der Dokumente nach Beendigung der Geschäftsbeziehung selbst verantwortlich. Gesetzliche Aufbewahrungspflichten der Bank bleiben unberührt.

9. Anerkennung der Dokumente

Die Bank gewährleistet nicht, dass die im Postfach eingestellten Dokumente von Dritten, insbesondere den zuständigen Behörden und Stellen (wie die Finanzbehörden) anerkannt werden. Der Kunde ist verpflichtet, sich selbst bei der für ihn zuständigen Behörde oder Stelle über die Anerkennung der Dokumente zu informieren.

10. Aufrechterhaltung und Änderung des Services

10.1 Die Bank kann das Postfach in Teilen beschränken, umgestalten, weiterentwickeln oder einstellen und/oder die Nutzung durch den Kunden von Auflagen abhängig machen.

10.2 Über eine solche Änderung und/oder Einstellung des Postfachs wird die Bank den Kunden mit angemessenem, zeitlichem Vorlauf informieren und den Kunden gegebenenfalls über den alternativen Kommunikationsweg in Kenntnis setzen.

10.3 Die Bank gewährleistet nicht die jederzeitige, ununterbrochene Verfügbarkeit des Postfachs oder der darin eingestellten Dokumente. Die Bank kann die Erreichbarkeit des Postfachs insbesondere für Wartungsfenster unterbrechen.

10.4 Die Erreichbarkeit kann auch wegen solcher, nicht im Machtbereich der Bank liegender Umstände (zum Beispiel Ausfall der Internetverbindung) unterbrochen sein.

11. Beendigung der Geschäftsbeziehung

Nach Beendigung der jeweiligen Geschäftsbeziehung zwischen dem Kunden und der Bank werden die Dokumente für weitere 30 Kalendertage im Postfach abrufbar sein. Nach Ablauf dieser Zeit ist die Bank berechtigt, den Zugang zum Postfach zu sperren.