Sparda-Bank

Einführung der Echtzeitüberweisung ab dem 15.07.2025

Die Nutzung der Echtzeitüberweisung steht Ihnen ab dem 15.07.2025 zur Verfügung. Wir führen zukünftig diese sekundenschnelle Echtzeitüberweisung innerhalb von maximal 10 Sekunden aus.

Aufgrund der gesetzlichen Vorgaben der Europäischen Union beträgt ab dem 9. Januar 2025 das Entgelt für die in Euro ausgeführte Echtzeitüberweisung auf die derzeitige Entgelthöhe der entsprechenden „Standard"-Überweisungen, also 0,00 Euro. Dies betrifft Echtzeitüberweisungen innerhalb der Bank oder an einen anderen Zahlungsdienstleister innerhalb Deutschlands und in andere Staaten des Europäischen Wirtschaftsraums (EWR).

Das monatliche Entgelt für Ihr Kontomodell bleibt unverändert. Alternativ zur „Standard"- Überweisung steht Ihnen aufgrund der gesetzlichen Vorgaben ab 15.07.2025 auch die Nutzung der Echtzeitüberweisung in Ihrem Kontomodell entsprechend zur Verfügung.

Bei Echtzeitüberweisungen handelt es sich um ein europaweites Überweisungsverfahren, das Ihnen rund um die Uhr zur Verfügung steht. Überweisungen in Euro werden von Ihrem Girokonto (Zahlungskonto) innerhalb weniger Sekunden ausgeführt. Echtzeitüberweisungen können Sie derzeit bis zu einem Betrag in Höhe von 100.000 Euro pro Überweisungsauftrag durchführen.

Sie haben selbstverständlich weiterhin wie gewohnt die Möglichkeit, mit der „Standard"- Überweisung Gelder in Euro innerhalb des Europäischen Wirtschaftsraums (EWR) zu überweisen.

Wichtig

Gleichzeitig mit der Annahme der Sonderbedingungen für die Ausführung von Echtzeit-Überweisungen gilt Ihre Zustimmung zur Einführung der Echtzeit-Überweisung mit Verweis auf Nummer 1 Absatz 2 unserer Allgemeinen Geschäftsbedingungen als erteilt, wenn Sie uns Ihre Ablehnung nicht vor dem 15.07.2025 anzeigen. Sie können den jeweiligen von diesen Änderungen betroffenen Zahlungsdiensterahmenvertrag (also zum Beispiel den Girokontovertrag) auch kostenfrei und fristlos vor dem 15.07.2025 kündigen.

Für Fragen stehen wir Ihnen sehr gerne telefonisch unter 0911 6000 8000 oder in unseren Filialen zur Verfügung.

Sparda-Bank

Kundeninformation

Sonderbedingungen für das Online-Banking, die Nutzung zentraler Authentifizierungsdienste im Online-Banking, die Nutzung von Multibanking-Zusatzdiensten im Online-Banking, die Nutzung des elektronischen Postfachs und die Ausführung von Echtzeit-Überweisungen

gültig ab 14. Juli 2025

Inhaltsverzeichnis

Sonderbedingungen für das Online-Banking

Fassung: September 2019

1 Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online-Banking abrufen.

Des Weiteren sind sie gemäß § 675f Abs. 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Abs. 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden einheitlich als „Teilnehmer", Konto und Depot einheitlich als „Konto" bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

(3) Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

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 Zahlungsinstrumentes, 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
- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer [PIN] oder der Nutzungscode für die elektronische Signatur) und
- 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, sowie
- 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 Wissenselement, 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 der Bank, wenn
- er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder 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.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Abs. 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 Abs. 26 Satz 2 ZAG).

4 Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder elektronische Signatur als Nachweis des Besitzelements) zu verwenden, sofern mit der Bank nichts anderes vereinbart wurde. 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 (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

5 Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der 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 Arbeitslaufs. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis" angegebenen 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.

(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 (z. B. Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen 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 (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 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 Kunden über Online-Banking-Verfügungen

Die Bank unterrichtet den Kunden 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 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 (vgl. Nummern 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
(a) Wissenselemente, 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) weitergegeben 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) weitergegeben 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) Seinselemente, 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 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 (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. 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 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Bank, 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 (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). 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

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) 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 eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle 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 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 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

(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.

(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 Besitzelements

(1) Eine Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in den Absätzen 1 und 2 genannten Besitzelemente 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.

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden 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 Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg 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 Kunden unverzüglich.

10 Haftung

10.1 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 (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kunden 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 abhandengekommenen 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 Kunde 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 Sorgfaltspflichten nach

- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 4,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

dieser Bedingungen 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 Abs. 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 dieser Bedingungen).

(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 Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 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.

(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 Absätzen 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.

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

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z. B. Wertpapiertransaktionen) 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 Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung 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.

10.2.4 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 Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis" näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.

Sonderbedingungen für die Nutzung zentraler Authentifizierungsdienste im Online-Banking

Fassung: Januar 2021

1 Leistungsangebot

(1) Die Bank stellt dem Teilnehmer einen zentralen Authentifizierungsdienst (nachfolgend: „CAS“ (Central Authentication Services) genannt) zur sicheren Identifizierung gegenüber Dritten als weitere Funktionalität ihres Online-Banking-Angebots zur Verfügung. Der CAS ermöglicht es dem Teilnehmer, sich bei bestimmten Drittanbietern, die Onlineangebote über Websites, Apps und andere digitale Kanäle bereitstellen, mit seinem Zugang für das Online-Banking anzumelden und seine bei der Bank gespeicherten Daten zur Identifizierung zu nutzen.

(2) Die vorliegenden Sonderbedingungen ergänzen die geltenden Sonderbedingungen für das Online-Banking sowie die Vereinbarung über die Nutzung des Online-Banking und gehen diesen im Falle eines Widerspruchs vor.

(3) Der Teilnehmer kann den CAS im Rahmen des von der Bank bereitgestellten Funktionsumfangs und ausschließlich gegenüber solchen Drittanbietern nutzen, die direkt oder über sogenannte zentrale Vermittlungsdienste, wie z. B. YES.com, am CAS teilnehmen (sogenannte „Akzeptanzstellen“), sowie gegenüber Vertrauensdienstanbietern.

2 Voraussetzungen für die Nutzung des CAS

Die Nutzung des CAS setzt voraus, dass der Teilnehmer Zugang zum Online-Banking der Bank erhält und im Wege eines Online-Banking-Auftrags nach Nr. 4.1 der Sonderbedingungen für das Online-Banking die vorliegenden Sonderbedingungen akzeptiert.

3 Funktionsumfang des CAS

3.1 Sichere Identifikation als Vertragspartner

(1) Mit dem CAS kann sich der Teilnehmer gegenüber einer oder mehreren Akzeptanzstellen als Vertragspartner sicher identifizieren. Voraussetzung dafür ist, dass die Akzeptanzstelle dem Teilnehmer die Nutzung des CAS anbietet und der Teilnehmer sich mit seinen Zugangsdaten nach Ziffer 3 der Sonderbedingungen für das Online-Banking in seinem Online-Banking anmeldet sowie die jeweilige Akzeptanzstelle im Wege eines Online-Banking-Auftrags nach Nr. 4.1 der Sonderbedingungen für das Online-Banking freischaltet.

(2) Vor der Freischaltung werden dem Teilnehmer die zum Zwecke der Identifizierung erforderlichen Daten („Identifizierungsdaten“) zur Bestätigung angezeigt, soweit sie sich unmittelbar auf seine Person beziehen. Die Bank wird nach Freischaltung durch den Teilnehmer der Akzeptanzstelle die Identifizierungsdaten sowie eine dem Teilnehmer zugeordnete, eindeutige CAS-ID („CAS-ID“) übermitteln. Mit der Freischaltung entbindet der Teilnehmer die Bank für die Zwecke der Übermittlung der Identifizierungsdaten und der CAS-ID an die Akzeptanzstelle vom Bankgeheimnis. Die Bank übermittelt der freigeschalteten Akzeptanzstelle die Identifizierungsdaten, die sie im Rahmen der bestehenden Vertragsbeziehung vom Teilnehmer erhoben und gespeichert hat. Die Bank übernimmt keine Gewähr für die Aktualität und Richtigkeit der übermittelten Identifizierungsdaten.

(3) Eine Freischaltung bleibt grundsätzlich gültig, soweit und solange sich die Kategorien und der Zweck der Identifizierungsdaten nicht ändern und der Teilnehmer die Freischaltung nicht aufhebt.

(4) In einer Übersicht im Online-Banking kann der Teilnehmer die von ihm vorgenommenen Freischaltungen einsehen, verwalten sowie für die Zukunft aufheben.

(5) Ist eine Freischaltung bereits erfolgt, übermittelt die Bank bei weiterer Nutzung des CAS durch den angemeldeten Teilnehmer gegenüber der freigeschalteten Akzeptanzstelle dieser zur Identifikation des Teilnehmers primär die CAS-ID. Die Identifizierungsdaten werden erneut übermittelt, soweit die Akzeptanzstelle diese zur Identifikation oder zur Aktualisierung der bei ihr gespeicherten Daten des Teilnehmers anfordert.

(6) Die Akzeptanzstelle identifiziert den Teilnehmer mithilfe der Identifizierungsdaten sowie der CAS-ID und ermöglicht ihm so die Anmeldung für die von ihr angebotenen Dienste. Die Anmeldung, ebenso wie die Inanspruchnahme der angebotenen Dienste, erfolgt gemäß den Bedingungen der Akzeptanzstelle. Die Bank ist an diesem Vertragsverhältnis nicht beteiligt. Insbesondere ist die Bank weder Vertreter noch Erfüllungsgehilfe der Akzeptanzstelle.

(7) Die Bank übermittelt die Identifizierungsdaten sowie die CAS-ID ausschließlich zum Zweck der Identifizierung des Teilnehmers für den Zugang zu Onlineangeboten der Akzeptanzstelle. Die Verwendung der Identifizierungsdaten sowie der CAS-ID durch die Akzeptanzstelle für andere Zwecke richtet sich ausschließlich nach den geltenden datenschutzrechtlichen Bestimmungen.

3.2 Identifikation nach dem Geldwäschegesetz

(1) Soll die Authentifizierung des Teilnehmers nach Nummer 3.1 zur Identifizierung nach dem Geldwäschegesetz (GwG) erfolgen, überprüft die Bank zusätzlich, ob die bei ihr gespeicherten Daten noch innerhalb der zulässigen Frist erhoben wurden und vollständig sind. Eine darüberhinausgehende Prüfung auf Richtigkeit und Aktualität übernimmt die Bank nicht.

(2) Sind die von der Bank gespeicherten Daten des Teilnehmers unvollständig oder veraltet, gilt Folgendes: Der Teilnehmer erhält die Möglichkeit, sich mit den von der Bank angebotenen Identifizierungsverfahren (z. B. Videolegitimation, POSTIDENT, Identifizierung in der Filiale) erneut gegenüber der Bank zu identifizieren. Bei der Identifizierung durch Drittanbieter im Auftrag der Bank gelten ergänzend deren Bestimmungen. Nach erfolgreicher Durchführung der Identifizierung speichert die Bank die aktualisierten und vervollständigten Daten des Teilnehmers.

(3) Anschließend stellt die Bank der Akzeptanzstelle die bei ihr gespeicherten Daten zur geldwäscherechtskonformen Identifikation zur Verfügung. Auf Anforderung der Akzeptanzstelle stellt die Bank dieser Kopien der für die Identifizierung erforderlichen Dokumente zur Verfügung.

3.3 Unterschrift in elektronischer Form

(1) Der Teilnehmer kann den CAS nach Maßgabe der folgenden ergänzenden Regelungen auch zur Vorbereitung der Abgabe einer elektronischen Unterschrift mittels einer sogenannten qualifizierten elektronischen Signatur nutzen.

(2) Entscheidet sich der Teilnehmer dafür, eine rechtsverbindliche Erklärung in elektronischer Form gegenüber einer Akzeptanzstelle abzugeben, so hat er nach Auswahl seiner Bank die Möglichkeit, sich in das Online-Banking seiner Bank einzuloggen. Dort kann der Teilnehmer einen mit der Bank kooperierenden Vertrauensdienstanbieter mit der Erstellung einer elektronischen Signatur beauftragen. Der Teilnehmer beauftragt unmittelbar den Vertrauensdienstanbieter und es gelten dessen Nutzungsbedingungen. Die Bank ist an dem Vertragsverhältnis zwischen dem Teilnehmer und dem Vertrauensdienstanbieter bzw. dem Vertragsverhältnis zwischen dem Teilnehmer und der Akzeptanzstelle nicht beteiligt, auch nicht als Vertreter oder Erfüllungsgehilfe.

(3) Die Bank wird die vom Vertrauensdienst angeforderten Identifizierungsdaten entsprechend Nummer 3.1 an den Vertrauensdienstanbieter nach dessen Beauftragung durch den Teilnehmer übermitteln. Voraussetzung hierfür ist, dass ein vollständiger und hinreichend aktueller Datensatz bei der Bank vorliegt; Nummer 3.2 gilt entsprechend.

(4) Der Vertrauensdienstanbieter generiert mithilfe der von der Bank übermittelten Identifizierungsdaten ein Zertifikat. Dieses Zertifikat kann

der Teilnehmer nutzen, um das gewünschte Dokument bei der Akzeptanzstelle mit einer qualifizierten elektronischen Signatur zu versehen.

4 Sperrung

Ergänzend zu Nr. 9 der Sonderbedingungen für das Online-Banking kann die Bank Akzeptanzstellen und Vertrauensdienstanbietern die Nutzung des CAS verweigern, wenn sachliche Gründe im Zusammenhang mit einer nicht autorisierten oder betrügerischen Nutzung vom CAS durch die Akzeptanzstelle oder den Vertrauensdienstanbieter es rechtfertigen.

5 Ergänzende Sorgfalts- und sonstige Mitwirkungspflichten des Teilnehmers

(1) Zur Vermeidung von Missbrauch im Zusammenhang mit den CAS-Diensten kommt der Einhaltung der geltenden Sorgfalts- und sonstigen Mitwirkungspflichten des Teilnehmers insbesondere nach Nr. 11 der AGB der Bank sowie Nrn. 7 und 8 der Sonderbedingungen für das Online-Banking besondere Bedeutung zu. Denn insbesondere wenn der Teilnehmer nicht alle zumutbaren Vorkehrungen trifft, um seine Authentifizierungselemente vor unbefugtem Zugriff zu schützen, besteht die Gefahr, dass das Online-Banking im Zusammenhang mit dem CAS missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird, um Identifizierungsdaten an Dritte und Vertrauensdienstanbieter zu übertragen.

(2) Ergänzend zu Nr. 7.3 der Sonderbedingungen für das Online-Banking gilt Folgendes: Soweit die Bank ihm die Identifizierungsdaten im Rahmen der Freischaltung zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die angezeigten Identifizierungsdaten zu prüfen und bei Feststellungen von Abweichungen den Vorgang abzubrechen.

(3) Unbeschadet der vorstehenden Absätze gilt ergänzend zu Nr. 11 Absatz 1 der AGB der Bank Folgendes: Zur ordnungsgemäßen Abwicklung des Geschäftsverkehrs im Rahmen der CAS-Dienste ist es zudem erforderlich, dass der Teilnehmer der Bank Änderungen, die seine Identifizierungsdaten betreffen, unverzüglich mitteilt.

6 Ergänzende Haftungsregelungen

(1) Kommt es zu Fehlern bei der Übermittlung von Identifizierungsdaten, da der Teilnehmer seine Pflichten verletzt hat, insbesondere, wenn er trotz Abweichungen im Sinne von Nummer 5 Absatz 2 den Vorgang nicht abgebrochen oder entgegen Nummer 5 Absatz 3 Änderungen, die seine Identifizierungsdaten betreffen, nicht unverzüglich mitgeteilt hat, trägt der Teilnehmer den der Bank hierdurch entstandenen Schaden, es sei denn, er hat die Pflichtverletzung nicht zu vertreten.

(2) Beruhen nicht autorisierte Nutzungen des CAS außerhalb der Ausführung nicht autorisierter Zahlungsvorgänge (z. B. Identitätsmissbrauch beim Abschluss von Verträgen mit Akzeptanzstellen) vor der Sperranzeige gemäß Nr. 8.1 der Sonderbedingungen für das Online-Banking auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf sonstiger missbräuchlicher Nutzung eines Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens. Nrn. 10.2.2, 10.2.3 und 10.2.4 der Sonderbedingungen für das Online-Banking gelten entsprechend. Die Haftung der Bank für Schäden des Kunden richtet sich nach Nr. 3 der AGB der Bank.

Sonderbedingungen für die Nutzung von Multibanking-Zusatzdiensten im Online-Banking

Fassung: Februar 2020

1 Leistungsangebot

(1) Die Bank stellt dem Teilnehmer in Ergänzung ihres Online-Banking-Angebots eine Multibanking-Funktion (Multibanking) und darauf aufbauende Zusatzdienste (Multibanking-Zusatzdienste) als weitere Funktionalitäten zur Verfügung. Die vorliegenden Sonderbedingungen ergänzen die geltenden Sonderbedingungen für das Online-Banking sowie die Vereinbarung über die Nutzung des Online-Banking und gehen diesen im Fall eines Widerspruchs vor.

(2) Dem Teilnehmer stehen das Multibanking sowie die Multibanking-Zusatzdienste über die gleichen Zugangswege zur Verfügung wie auch das Online-Banking. Möglich sind im Rahmen des Angebots insbesondere der Abruf via PC oder mobilem Endgerät, wie Smartphone und Tablet. Letzteres kann die Installation einer Bank-Applikation erfordern, für die besondere Nutzungsbedingungen gelten.

(3) Die Multibanking-Funktion ermöglicht die Einbindung von weiteren Konten des Teilnehmers (Fremdbankkonten) bei anderen Kreditinstituten bzw. Zahlungsdienstleistern (Fremdbanken) in einer Kontoübersicht im Online-Banking der Bank. Eingebunden werden können Zahlungskonten sowie weitere Konten, wie z. B. Sparkonten, Depotkonten, Kreditkartenkonten und sonstige Konten, sofern die Bank dies zulässt. Darüber hinaus kann der Teilnehmer weitere Zusatzdienste in dem von der Bank angebotenen Umfang auswählen.

(4) Voraussetzung für die Einbindung eines Fremdbankkontos ist, dass der Teilnehmer am Online-Banking der Fremdbank teilnimmt, diese den Abruf der Kontoinformationen über eine Schnittstelle zulässt und der Teilnehmer dem Abruf von Kontoinformationen bei der Fremdbank durch Auswahl des betreffenden Kontos zur Anzeige gemäß Ziffer 2.1 Absätze 2 und 3 dieser Sonderbedingungen ausdrücklich zugestimmt hat.

(5) Der Abruf der Kontoinformationen erfolgt durch die Bank im Auftrag des Teilnehmers. Die Bank geht kein Vertragsverhältnis zur kontoführenden Fremdbank ein. Der Teilnehmer ist allein verantwortlich für die Einhaltung der Nutzungsbedingungen der Fremdbank.

(6) Ist der Teilnehmer Mitinhaber oder Kontobevollmächtigter aufgrund einer Vollmacht, so ist er zur Nutzung der Multibanking-Zusatzdienste nur berechtigt, wenn der Mitinhaber bzw. der Vollmachtgeber ihn hierzu ermächtigt hat. Der Teilnehmer nutzt diese Dienste insoweit als Vertreter des Kontoinhabers bzw. Mitkontoinhabers. Der Kontobevollmächtigte ist dennoch auch im eigenen Namen verpflichtet, die in diesen Bedingungen enthaltenen Regelungen als Teilnehmer einzuhalten.

(7) Zur Nutzung der Multibanking-Zusatzdienste muss sich der Teilnehmer gegenüber der Fremdbank als berechtigter Kontoinhaber oder Bevollmächtigter authentifizieren. Die Authentifizierung erfolgt gemäß der Vereinbarung zwischen Teilnehmer und Fremdbank.

2 Funktionsumfang der Multibanking-Zusatzdienste

2.1 Anzeige Konto- und Umsatzübersicht

(1) Im Online-Banking der Bank werden dem Teilnehmer in der Konto- und Umsatzübersicht die Konten der Bank sowie die jeweils eingebundenen Fremdbankkonten angezeigt.

(2) Zur Einbindung der Fremdbankkonten wählt der Teilnehmer die kontoführende Fremdbank mittels Namen, BIC oder Bankleitzahl aus. Anschließend gibt er seine individuelle Teilnehmerkennung (z. B. Kontonummer, Anmeldename) für das Online-Banking der Fremdbank an und weist sich unter Verwendung des oder der von der Fremdbank angeforderten Authentifizierungselemente(s) aus. Der Teilnehmer wählt aus den der betreffenden Teilnehmerkennung zugeordneten Fremdbankkonten diejenigen Konten aus, die in die Konto- und Umsatzübersicht übernommen werden sollen.

(3) Der Teilnehmer erteilt seine ausdrückliche Zustimmung dazu, dass die Bank auf die Kontoinformationen der ausgewählten Konten zum Zwecke der Einbindung in die Konto- und Umsatzübersicht zugreifen und diese speichern und nutzen darf. Davon umfasst sind bspw. der aktuelle Kontostand sowie die für einen von der Fremdbank bestimmten Zeitraum abrufbaren Umsatzinformationen, in der Regel Betrag, Empfänger, Verwendungszweck und Datum.

(4) Die Kontoinformationen werden gespeichert und dem Teilnehmer bei jeder Anmeldung zum Online-Banking angezeigt.

(5) Die Teilnehmerkennung und Authentifizierungselemente zum eingebundenen Fremdkonto werden nur gespeichert, wenn der Teilnehmer die Aktualisierungsfunktion auswählt. In diesem Fall beauftragt der Teilnehmer die Bank, die Kontoinformationen regelmäßig mithilfe der Teilnehmerkennung und Authentifizierungselemente unabhängig von der Anmeldung des Teilnehmers im Online-Banking der Bank automatisiert abzurufen und die abgerufenen Kontoinformationen in die Konto- und Umsatzübersicht zu übernehmen. Der Teilnehmer kann die aktualisierten Kontoinformationen bei der nächsten Anmeldung zum Online-Banking in der Konto- und Umsatzübersicht einsehen. Der Zeitpunkt der jeweiligen Aktualisierung ist in der Kontoübersicht angegeben. Nach dem letzten Aktualisierungszeitraum liegende Umsätze sind in der Konto- und Umsatzanzeige nicht berücksichtigt.

(6) Wählt der Teilnehmer die automatische Aktualisierung nicht aus, werden die Teilnehmerkennung und Authentifizierungselemente zum Fremdkonto nicht gespeichert. Der Teilnehmer kann dann die Kontoinformationen manuell aktualisieren. Für eine manuelle Aktualisierung sind die Teilnehmerkennung und Authentifizierungselemente zum Fremdbankkonto zum Abruf der Kontoinformationen erneut einzugeben.

(7) Die Speicherung der Teilnehmerkennung und der Authentifizierungselemente zum Zwecke der automatischen Aktualisierung der Kontoinformationen bedarf gegebenenfalls einer periodischen Erneuerung der Einwilligung des Teilnehmers. Die Bank wird den Teilnehmer hierauf hinweisen. Bei Änderungen der Teilnehmerkennung und Authentifizierungselemente zum Fremdbankkonto sind die Zugangsdaten ebenfalls im Onlinebereich der Bank zu ändern, da andernfalls eine Aktualisierung nicht möglich ist.

(8) Der Teilnehmer kann jederzeit Fremdbankkonten aus der Konto- und Umsatzübersicht entfernen. In diesem Fall werden sämtliche bei der Bank gespeicherten Daten zu diesen Konten automatisch gelöscht, es sei denn, zwingende gesetzliche Regelungen oder die weiteren vom Teilnehmer gewählten Funktionen verlangen eine weitere Speicherung.

2.2 Weitere Zusatzdienste

(1) Darüber hinaus bietet die Bank weitere Multibanking-Zusatzdienste an, die der Teilnehmer einzeln durch Betätigung eines entsprechenden Aktivierungsbuttons auswählen und jederzeit abwählen kann. Der Teilnehmer erteilt seine ausdrückliche Zustimmung dazu, dass die Bank auf die Kontoinformationen zu Zwecken des aktivierten Zusatzdienstes zugreifen und diese speichern und nutzen darf.

(2) Der Zusatzdienst „frei verfügbares Geld“ bietet dem Teilnehmer eine Prognose des frei verfügbaren Geldes bis zum nächsten Gehaltseingang. Die Prognose basiert auf einer finanzmathematischen Analyse der zurückliegenden Ein- und Ausgänge auf sämtlichen eingebundenen Zahlungskonten einschließlich der Zahlungskonten bei der Bank und soll dem Teilnehmer eine Einschätzung der Entwicklung seiner Liquidität ermöglichen. Nicht berücksichtigt wird die auf sonstigen Konten (z. B. Geldmarktkonten, Sparkonten) vorhandene Liquidität. Die Aussagekraft der Prognose ist unter anderem davon abhängig, dass es sich bei den eingebundenen Zahlungskonten um solche des Teilnehmers handelt, die Ein- und Ausgaben des Teilnehmers im Wesentlichen über diese Zahlungskonten

abgewickelt werden und eine regelmäßige Aktualisierung der über die Konten vorgenommenen Umsätze im Multibanking erfolgt.

(3) Der Zusatzdienst „Umsatzanalyse“ ordnet die Umsätze bestimmten vorgegebenen Kategorien zu und ermöglicht so dem Teilnehmer einen Überblick über die Gesamteinnahmen oder -ausgaben je Kategorie. Der Teilnehmer hat die Möglichkeit, Daten manuell einzugeben und selbst Umsätze bestimmten Kategorien zuzuordnen. Die Kategorien und die Zuordnung der Umsätze sind unverbindliche Vorschläge der Bank auf der Grundlage einer Analyse der Umsatzdaten. Der Teilnehmer kann die Kategorien jederzeit ändern und eigene Kategorien erstellen.

(4) Der Zusatzdienst „Vertragsübersicht“ eröffnet dem Teilnehmer die Möglichkeit, Verträge in einer Anwendung gebündelt zu verwalten. Die Übersicht erfasst sowohl Finanzdienstleistungen als auch Verträge bei Nicht-Finanzdienstleistern, wie z. B. Energieversorgern und Telekommunikationsanbietern. Die Vertragsinformationen werden auf Grundlage einer Analyse der Kontoinformationen erhoben, wie sie sich aus den Kontoumsätzen bei der Bank und den über die Schnittstelle der Fremdbank abgerufenen Kontoumsätzen ergeben. Der Teilnehmer kann die Daten manuell ergänzen und bearbeiten. Dem Teilnehmer werden zudem Verlängerungs- und Kündigungsoptionen sowie gegebenenfalls Vertragsalternativen angezeigt.

2.3 Zahlungsauslösedienst

(1) Die Nutzung des von der Bank angebotenen Zahlungsauslösedienstes (ZAD) ermöglicht es dem Teilnehmer, Zahlungen von Fremdkonten auszulösen, die in die Kontoübersicht im Online-Banking der Bank eingebunden wurden. Damit kann der Teilnehmer seine Bankgeschäfte über alle von ihm eingebundenen Fremdkonten, die zugleich Zahlungskonten sind, hinweg im Online-Banking der Bank ausführen.

(2) Mit der Nutzung des ZAD beauftragt der Teilnehmer die Bank, einen Zahlungsauftrag an die Fremdbank zu übermitteln. Die Bank wird sich unter Einhaltung der rechtlichen Vorgaben für die Erbringung von Zahlungsauslösediensten als Übermittler des Auftrags des Teilnehmers gegenüber der Fremdbank identifizieren und der Fremdbank den Zahlungsauftrag über die von dieser zur Verfügung gestellte Schnittstelle übermitteln.

(3) Zur Auslösung einer Zahlung füllt der Teilnehmer das Zahlungsformular unter Angabe u. a. des Empfängers, des Zahlbetrags und des Verwendungszwecks aus und gibt in die dafür vorgesehenen Felder Teilnehmerkennung und Authentifizierungselemente zum Fremdkonto ein. Anschließend autorisiert der Teilnehmer die Auslösung der Zahlung durch Eingabe eines weiteren Authentifizierungselementes (z. B. TAN).

(4) Bis zur Erteilung der Zustimmung zur Auslösung der Zahlung kann dieser den Übermittlungsauftrag durch Erklärung gegenüber der Bank widerrufen.

(5) Die Übermittlung des Zahlungsauftrags erfolgt unverzüglich unter der Voraussetzung, dass die von der Fremdbank zur Verfügung gestellte Schnittstelle die Übermittlung zulässt. Konnte der Zahlungsauftrag nicht innerhalb der üblichen Frist übermittelt werden, bspw. weil die Schnittstelle der Fremdbank nicht erreichbar ist, wird die Bank dem Teilnehmer dies unverzüglich mitteilen.

(6) Die Bank bestätigt dem Teilnehmer die Zahlung unter Angabe der dem Zahlungsvorgang zugeordneten Kennung, des Zahlbetrags und des Datums des Zugangs des Übermittlungsauftrags, sobald sie eine entsprechende Bestätigung durch die Fremdbank erhalten hat. Die Ausführung des Zahlungsauftrags erfolgt dann zu den Bedingungen zwischen Fremdbank und Teilnehmer. Dem Teilnehmer obliegt es, die zwischen ihm und der Fremdbank getroffenen Vereinbarungen, insbesondere zur Nutzung des Online-Bankings im Zusammenhang mit Zahlungsauslösediensten, einzuhalten.

3 Änderungen des Leistungsangebots und dieser Sonderbedingungen

(1) Der Teilnehmer kann die Multibanking-Zusatzdienste in dem Umfang nutzen, wie sie von der Bank aktuell angeboten werden. Die Bank behält sich vor, das Multibanking-Angebot regelmäßig anzupassen und zu verändern, insbesondere weitere Zusatzdienste in das Angebot aufzunehmen und wenig genutzte Funktionen aus dem Angebot zu entfernen.

(2) Für Änderungen dieser Sonderbedingungen gilt Ziff. 1 Abs. 2 der Allgemeinen Geschäftsbedingungen.

4 Hinweise zur Verarbeitung personenbezogener Daten

(1) Zur Erbringung der Leistungen des Multibanking-Angebots verarbeitet die Bank personenbezogene Daten des Teilnehmers (Stammdaten über Konten bei Fremdbanken, Kontoinformationen wie Umsätze, Depotinformationen) auf der Grundlage des Art. 6 Abs. 1 Satz 1 lit. b DSGVO.

(2) Weiterhin verarbeitet die Bank die in Absatz 1 genannten personenbezogenen Daten des Teilnehmers, um ihm passend und zielgenau werbliche Angebote für Produkte der Bank und Mitgliedern der Genossenschaftsgruppe (z. B. Union Investment, R+V Versicherung) unterbreiten zu können. Dies geschieht nur, wenn der Teilnehmer der Bank eine Einwilligung zur Nutzung der Daten für diesen Zweck erteilt hat (Art. 6 Abs. 1 Satz 1 lit. a DSGVO) oder wenn die Bank den Teilnehmer ausdrücklich auf die werbliche Nutzung seiner Daten hingewiesen hat (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Der Teilnehmer kann seine erteilte Einwilligung über einen Widerrufsbutton unter Einstellungen in der Zugriffsverwaltung des Online-Banking der Bank jederzeit widerrufen oder der werblichen Nutzung seiner Daten generell widersprechen.

(3) Die Bank analysiert im Fall einer Verarbeitung gemäß Ziffer 2 keine besonderen Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO (z. B. politische Meinungen, Gesundheit).

(4) 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.

5 Kündigung

(1) Die Sonderbedingungen für die Nutzung von Multibanking-Zusatzdiensten im Online-Banking gelten auf unbestimmte Zeit.

(2) Mit der Beendigung der Vereinbarung über die Nutzung des Online-Bankings endet zugleich auch die Vereinbarung über die Nutzung von Multibanking-Zusatzdiensten im Online-Banking.

(3) Der Teilnehmer kann diese Vereinbarung jederzeit zusammen mit der Vereinbarung über die Nutzung des Online-Bankings kündigen. Die Kündigung kann auch durch Deaktivierung der Multibanking-Funktion im Online-Banking der Bank erfolgen. Darüber hinaus kann der Teilnehmer jederzeit Fremdbankkonten löschen und die Zusatzdienste abwählen.

6 Haftung

(1) Die Bank ruft die Kontoinformationen des Teilnehmers von Fremdkonten über Schnittstellen bei der Fremdbank ab und gibt diese in der Konto- bzw. Umsatzübersicht lediglich wieder. Die Bank übernimmt daher keine Gewähr für die Vollständigkeit, Richtigkeit und Aktualität der angezeigten Kontoinformationen sowie der hierauf beruhenden Anzeigen und Auswertungen.

(2) Die Verfügbarkeit der Multibanking-Zusatzdienste hängt von der Verfügbarkeit der Schnittstellen der Fremdbanken ab. Die Bank übernimmt daher keine Gewähr für die ständige Verfügbarkeit der Multibanking-Zusatzdienste.

(3) Die im Multibanking-Angebot der Bank erstellten Auswertungen und Prognosen dienen der Unterstützung der Finanzplanung des Teilnehmers und werden mit großer Sorgfalt unter Einsatz finanzmathematischer Analysen und unter Berücksichtigung von Erfahrungswerten erstellt. Diese stellen weder eine Handlungsempfehlung der Bank dar noch übernimmt die Bank die Gewähr für den Eintritt des prognostizierten Ereignisses.

(4) Die Haftung der Bank für Schäden des Kunden richtet sich im Übrigen nach Nr. 3 der AGB der Bank.

Sonderbedingungen für die Nutzung des elektronischen Postfachs

Fassung: Juni 2021

1 Bereitstellung und Nutzung eines elektronischen Postfachs

Die Bank stellt dem Kunden auf seinen Wunsch ein elektronisches Postfach zur Verfügung. Die Nutzung des elektronischen Postfachs setzt die Teilnahme des Kunden am Online-Banking-Angebot der Bank voraus. Der Kunde kann das Postfach im bereitgestellten Funktionsumfang nutzen.

Bevollmächtigten ist die Nutzung des elektronischen Postfachs in gleicher Weise wie dem Kontoinhaber bzw. den Kontoinhabern gestattet.

2 Umfang der Postfachkommunikation

Bei Nutzung des elektronischen Postfachs übermittelt die Bank auf diesem Weg für die festgelegten Konten, Depots und sonstigen Vertragsbeziehungen grundsätzlich alle Mitteilungen und Informationen. Dies umfasst beispielsweise

- Konto- und Depotauszüge,
- Rechnungsabschlüsse,
- Kreditkartenabrechnungen,
- Angebote zur Änderung der Allgemeinen Geschäftsbedingungen, Sonderbedingungen oder Entgelten.

Die Übermittlung der Mitteilungen und Informationen erfolgt unter anderem durch Einstellung von Dateien im PDF-Format in das elektronische Postfach des Kunden. Die Bank bleibt dazu berechtigt, dem Kunden Dokumente nicht durch Einstellung einer Datei in das elektronische Postfach, sondern per Post zuzusenden, wenn sie dies unter Berücksichtigung des Kundeninteresses für zweckmäßig hält oder es aus rechtlichen Gründen erforderlich ist.

Kunden, die handels- und steuerrechtlichen Aufbewahrungspflichten unterliegen, sollten sich bei einem Angehörigen der steuerberatenden Berufe informieren, was im Fall des Bezugs von elektronischen Dokumenten (z. B. Kontoauszügen) zur Erfüllung dieser Pflichten zu beachten ist.

3 Beendigung der Nutzung des elektronischen Postfachs

Der Kunde kann die Nutzung des elektronischen Postfachs jederzeit in Textform ohne Einhaltung einer Frist kündigen.

Die Bank kann die Nutzung des Postfachs jederzeit mit einer Frist von zwei Monaten kündigen, es sei denn, es liegt ein wichtiger Grund vor, der sie zu einer außerordentlichen Kündigung berechtigen würde. Ein wichtiger Grund liegt insbesondere dann vor, wenn es der Bank auch unter angemessener Berücksichtigung der Belange des Kunden unzumutbar erscheint, den elektronischen Postfach-Dienst fortzusetzen.

Hat der Kunde mittels seiner girocard (Debitkarte) Zugang zum Kontoauszugdrucker, werden ihm ab dem Wirksamwerden der Kündigung grundsätzlich alle Mitteilungen und Informationen der Bank am Kontoauszugdrucker zur Verfügung gestellt. Andernfalls werden sie ihm per Post zugestellt. Die Bank bleibt in jedem Fall dazu berechtigt, dem Kunden Dokumente per Post zuzusenden, wenn sie dies unter Berücksichtigung des Kundeninteresses für zweckmäßig hält oder es aus rechtlichen Gründen erforderlich ist.

Sonderbedingungen für die Ausführung von Echtzeit-Überweisungen

Fassung: Januar 2021

Für die Ausführung von Überweisungsaufträgen von Kunden im Echtzeit-Überweisungsverfahren gelten die folgenden besonderen Ausführungsbedingungen ergänzend zu den „Sonderbedingungen für den Überweisungsverkehr“, sofern im Folgenden keine anderweitige Vereinbarung getroffen wird. Weitere Regelungen sind Bestandteil des „Preis- und Leistungsverzeichnisses“. Hierzu wird an entsprechenden Stellen auf das „Preis- und Leistungsverzeichnis“ verwiesen.

1 Begriffsbestimmung und wesentliche Merkmale

Der Kunde kann die Bank elektronisch beauftragen, durch eine Echtzeit-Überweisung einen Geldbetrag in Euro innerhalb des Gebiets des einheitlichen Euro-Zahlungsverkehrsraums („Single Euro Payments Area“, SEPA) innerhalb der Ausführungsfrist gemäß Nummer 5 zu übermitteln. Zu SEPA gehören die in der Anlage genannten Staaten und Gebiete. Grundlage bildet das SEPA-Echtzeit-Überweisungsverfahren „SEPA INSTANT CREDIT TRANSFER (SCT INST) Scheme Rulebook“ des European Payments Council (EPC). Die Ausführung der Echtzeit-Überweisung erfolgt nur dann, wenn der Zahlungsdienstleister des Zahlungsempfängers am SEPA-Echtzeit-Überweisungsverfahren teilnimmt und über entsprechende Zahlungssysteme erreichbar ist.[1]

Der Zahlungsdienstleister des Zahlungsempfängers ist gegenüber dem Zahlungsempfänger verpflichtet, ihm den Zahlungsbetrag möglichst innerhalb von Sekunden zur Verfügung zu stellen. Die Bank stellt dem Zahler Informationen über die Ausführung einer Echtzeit-Überweisung in der über das Online-Banking abrufbaren Umsatzliste oder über einen anderen vereinbarten elektronischen Weg sowie nachträglich über den Kontoauszug zur Verfügung. Gleiches gilt, wenn die Überweisung abgelehnt wird oder nicht ausgeführt werden kann.

Erhält die Bank für ein in Euro geführtes Zahlungskonto eine Echtzeit-Überweisung, so wird sie den Überweisungsbetrag annehmen und hierüber den Zahlungsempfänger in der vereinbarten Form sowie über den Kontoauszug informieren.

2 Betragsgrenze

Für Echtzeit-Überweisungsaufträge bestehen Betragsgrenzen, die sich aus dem Preis- und Leistungsverzeichnis der Bank ergeben bzw. bei der jeweiligen Auftragsannahme durch die Bank geprüft und angezeigt werden.

3 Zugang und Widerruf des Auftrags

Die Bank unterhält in Änderung der Nummer 1.4 der Sonderbedingungen für den Überweisungsverkehr sowie Nummer 5 Absatz 1 der Sonderbedingungen für das Online-Banking den für die Ausführung von Echtzeit-Überweisungen erforderlichen Geschäftsbetrieb für die vereinbarten elektronischen Zugangswege ganztägig an allen Kalendertagen eines Jahres. Mit dem Zugang des Auftrags bei der Bank kann der Kunde diesen nicht mehr widerrufen und es beginnt die Ausführungsfrist gemäß der Angaben im Preis- und Leistungsverzeichnis.

4 Ablehnung der Ausführung

Die Bank wird in Ergänzung der Nummer 1.7 der Sonderbedingungen für den Überweisungsverkehr die Ausführung des Auftrags ablehnen, wenn:

- das Belastungskonto nicht für Echtzeit-Überweisungen vereinbart wurde,
- die Kontowährung des Belastungskontos nicht der Euro ist,
- die Prüfung der Ausführungsbedingungen, zum Beispiel die wirksame Autorisierung, die Einhaltung der Vorgaben des Geldwäschegesetzes oder der Embargobestimmungen nicht kurzfristig abschließend möglich ist,
- der Zahlungsdienstleister des Zahlungsempfängers über das von der Bank genutzte Zahlungssystem nicht erreichbar ist, insbesondere weil dieser dieses Verfahren nicht nutzt.

Die Bank wird den Kunden darüber entsprechend der Nummer 1 informieren.

5 Ausführungsfrist

Die Bank ist in Änderung der Nummern 2.2.1, 3.1.2 und 3.2.2 der Sonderbedingungen für den Überweisungsverkehr verpflichtet, sicherzustellen, dass der Geldbetrag einer Echtzeit-Überweisung nach erfolgreicher Prüfung der Ausführungsvoraussetzungen gemäß der im Preis- und Leistungsverzeichnis vereinbarten Ausführungsfrist bei dem Zahlungsdienstleister des Zahlungsempfängers eingeht.

Anlage: Liste der zu SEPA gehörenden Staaten und Gebiete

1 Staaten des Europäischen Wirtschaftsraums (EWR)

1.1 Mitgliedstaaten der Europäischen Union

Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn sowie Zypern.

1.2 Weitere Staaten

Island, Liechtenstein und Norwegen.

2 Sonstige Staaten und Gebiete

Andorra, Monaco, San Marino, Schweiz, Vatikanstadt, Vereinigtes Königreich von Großbritannien und Nordirland sowie Saint-Pierre und Miquelon, Jersey, Guernsey sowie Isle of Man.

1 Siehe hierzu unter www.epc-cep.eu. Die jeweils aktuelle Liste der teilnehmenden Zahlungsdienstleister am Echtzeit-Überweisungsverfahren des EPC (European Payments Council) kann dort abgerufen werden.

Sparda-Bank Nürnberg eG
Eilgutstraße 9 • 90443 Nürnberg

www.sparda-n.de • info@sparda-n.de