MERCK FINCK
A QUINTET PRIVATE BANK

Bedingungen für das Online-Banking

1. Online-Banking/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 Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 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-Bankings gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

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
-Wissenselemente, 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 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 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. Aufträge

4.1 Auftragserteilung
Der Teilnehmer muss einem Auftrag (zum Beispiel Überweisung) zu dessen 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-Bankings erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit 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 (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" 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 darauf folgenden 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 (zum Beispiel 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 (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. Sie wird den Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

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. An-sonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 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-Bankings 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, Au-thentifizierungs-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-Bankings 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) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-Banking nur dann als Authentifizierungselement ver-wendet 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 (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 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 (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (zum Beispiel 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.

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 dreimal in Folge der Nutzungscode für die elektronische Signatur 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 Absätzen 1 und 2 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-Bankings 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 (zum Beispiel 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 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 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 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 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 Absatz 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 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.

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 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.

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. Postkorb/Leistungsangebot
(1) Der Teilnehmer stimmt der Einrichtung des Postkorbs zu, in dem die Bank Dokumente und Informationen (z.B. Kontoauszüge, Rechnungsabschlüsse usw.) online zur Verfügung stellt. Der Teilnehmer kann diese Unterlagen nach erfolgreicher Registrierung des Postkorbs im Online-Banking aufrufen.
(2) Der Postkorb bietet zudem dem Teilnehmer die Möglichkeit, der Bank Kundenaufträge (möglich sind nur die im Postkorb aufgeführten Auftragsarten) zu erteilen.
(3) Der Teilnehmer kann die empfangenen und gesendeten Dokumente online ansehen, herunterladen und/ oder ausdrucken.

11.1 Voraussetzungen zur Nutzung des Postkorbs
(1) Die Nutzung des Postkorbs ist ausschließlich dem Teilnehmer selbst und den von ihm hierzu bevollmächtigten Personen vorbehalten. Sind Gemeinschaftskonten betroffen, müssen alle Gemeinschaftskonteninhaber die Nutzung des Postkorbs vereinbaren.
(2) Die Dokumentenauswahl kann von der Bank jederzeit erweitert oder verringert werden. Der aktuelle Umfang der in den Postkorb eingestellten Dokumente kann jederzeit auf unserer Internetseite unter www.merckfinck.de „Online Banking“ eingesehen werden.

11.2 Zugang
(1) Entscheidet sich der Teilnehmer für die Nutzung des Postkorbs, gehen ihm die in den Postkorb eingestellten Dokumente ausschließlich in digitaler Form zu. Der Teilnehmer wird mit einer gesonderten an die in der Teilnahmevereinbarung/Vollmacht für die Nutzung des Online-Bankings angegebenen E-Mail-Adresse oder auf sonstige mit ihm vereinbarte Weise darüber informiert, dass im Postkorb neue Dokumente/Informationen vorhanden und verfügbar sind.
(2) Die im Postkorb eingestellten Dokumente/Informationen gehen dem Teilnehmer in dem Zeitpunkt zu, in dem (i) es der Postkorb dem Teilnehmer ermöglicht, die an ihn persönlich gerichteten Dokumente/Informationen derart zu speichern, dass er sie in der Folge für eine angemessene Dauer einsehen kann und ihm die unveränderte Wiedergabe der gespeicherten Dokumente/Informationen möglich ist, ohne dass ihr Inhalt durch die Bank oder einen Administrator einseitig geändert werden kann und (ii) dem Teilnehmer die Benachrichtigung über die Zurverfügungstellung der Dokumente/Informationen im Postkorb in der nach Absatz 1, Satz 2 vereinbarten Weise zugeht.
(3) Im Übrigen ist maßgeblich der Zugang der Dokumente in Papierform.

11.3 Mitwirkungspflichten des Teilnehmers
(1) Der Teilnehmer verpflichtet sich, den Postkorb regelmäßig auf neu eingestellte Dokumente zu kontrollieren und deren Inhalt zu überprüfen. Etwaige Einwendungen hat er unverzüglich zu erheben. Soweit der Teilnehmer eine Benachrichtigung über den Eingang neuer Dokumente z. B. per E-Mail oder per SMS erhält, entbindet ihn das nicht von der Überprüfung des Postkorbs.
(2) Falls vom Teilnehmer erwartete Mitteilungen und Rückmeldungen auf Aufträge nicht innerhalb einer angemessenen Frist im Postkorb eingestellt werden, hat er die Bank unverzüglich zu benachrichtigen.

11.4 Unveränderbarkeit der Daten
(1) Die Bank stellt die Unveränderbarkeit der in den Postkorb eingestellten Dokumente sicher, sofern diese innerhalb des Postkorbs gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb des Postkorbs gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die Bank hierfür keine Haftung.
(2) Zu beachten ist, dass aufgrund der individuellen Hard- oder Softwareeinstellung das Format eines Ausdrucks nicht immer mit der Darstellung am Bildschirm übereinstimmen muss.

11.5 Speicherung der Dokumente
(1) Im Postkorb aufrufbare Dokumente werden während der Laufzeit der Nutzungsvereinbarung dem Teilnehmer für einen Zeitraum von drei Jahren zur Verfügung gestellt. Nach Ablauf dieses Zeitraums ist die Bank berechtigt, diese zu entfernen.
(2) Nach Ablauf der dreijährigen Frist erhält der Teilnehmer keine gesonderte Nachricht. Zur dauerhaften Aufbewahrung von Dokumenten können diese ausgedruckt oder direkt auf einem eigenen Datenträger gespeichert werden.
(3) Die Bank stellt dem Teilnehmer auf Anforderung Zweitausfertigungen papierhaft gegen Kostenersatz zur Verfügung. Die Höhe der vom Teilnehmer zu tragenden Kosten ergibt sich aus dem jeweils gültigen Preis-/Leistungsverzeichnis der Bank.

11.6 Kündigung durch den Teilnehmer/ die Bank
(1) Der Teilnehmer kann die Nutzung des Postkorbs ohne Angabe von Gründen jederzeit kündigen. Die Kündigung erfolgt in Textform.
(2) Die Bank wird dem Teilnehmer die für den Postkorb vorgesehenen Mitteilungen nach Wirksamwerden der Kündigung wieder ausschließlich auf dem Postwege zukommen lassen.
(3) Ab Wirksamwerden der Kündigung sperrt die Bank die Mitteilungen im Postkorb.
(4) Die Bank kann die Nutzung des Postkorbs jederzeit mit einer Frist von sechs Wochen kündigen. Im Falle eines wichtigen Grundes, der die Bank zu einer außerordentlichen Kündigung berechtigt, kann die Bank ohne Einhaltung einer Frist oder mit Einhaltung einer geringeren als der sechswöchigen Frist kündigen; sie wird hierbei die berechtigten Interessen des Teilnehmers berücksichtigen. Ein wichtiger Grund liegt insbesondere dann vor, wenn es der Bank auch unter angemessener Berücksichtigung der Belange des Teilnehmers unzumutbar erscheint, die Nutzung des Postkorbs fortzusetzen. In diesem Fall wird die Bank dem Teilnehmer nach Wirksamwerden der Kündigung die für den Postkorb vorgesehenen Mitteilungen wieder auf dem Postwege zukommen lassen. Auch im Falle einer fristlosen Kündigung ermöglicht die Bank dem Teilnehmer die anderweitige Speicherung oder den Ausdruck der sich aktuell im Postkorb befindenden Dokumente für einen angemessenen Zeitraum.
(5) Ab Wirksamwerden der Kündigung obliegt es dem Teilnehmer, zuvor die Mitteilungen im Postkorb auf einem eigenen Datenträger zu speichern oder in Papierform auszudrucken.

11.7 Einstellung der Nutzung des Postkorbs
(1) Unbeschadet der Kündigungsfrist nach Ziff. 2.5 kann die Bank die Nutzung des Postkorbs teilweise oder ganz einstellen. Dem Teilnehmer obliegt es, zuvor die Mitteilungen im Postkorb auf einem eigenen Datenträger zu speichern oder in Papierform auszudrucken.
(2) Eine Verpflichtung der Bank zur Aufrechterhaltung des Postkorbs besteht nicht. Die Bank wird den Teilnehmer über die Einstellung rechtzeitig informieren und ihm die Kundendokumente in elektronischer Form zusenden.

11.8 Haftung
(1) Für Störungen des elektronischen Versandwegs, insbesondere für die nicht ordnungsgemäße Datenübermittlung sowie dafür, dass der Zugang zum Postkorb vorübergehend nicht möglich ist, haftet die Bank nur bei grobem Verschulden.
(2) Die Bank übernimmt keine Garantie für die Richtigkeit, Rechtzeitigkeit und Vollständigkeit der übermittelten Daten. Soweit fehlerhafte, unvollständige oder verzögerte Übertragung auf einem Verschulden der Bank, ihrer gesetzlichen Vertreter oder Erfüllungsgehilfen beruht, haftet die Bank nur bei Vorsatz und grober Fahrlässigkeit.
(3) 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.

11.9 Einwilligung zur Datenverarbeitung
Mit der Annahme dieser Teilnahmevereinbarung erklärt sich der Kunde damit einverstanden, dass die Bank ausschließlich für die Verarbeitung und Abwicklung der Aufträge des Teilnehmers relevanten personenbezogenen Daten an das Rechenzentrum Bank-Verlag GmbH weitergibt.

11.10 Anerkennung durch Finanzbehörden
(1) Der elektronische Kontoauszug bzw. Rechnungsabschluss erfüllt nach Auffassung der Finanzverwaltung weder die Anforderungen der steuerlichen Aufbewahrungspflicht nach § 147 AO noch die einer Rechnung im Sinne des Umsatzsteuergesetzes. Es wird daher nur im Privatkundenbereich und damit für Kontoinhaber anerkannt, die nicht buchführungs- und aufzeichnungspflichtig im Sinne der §§ 145 ff. AO ist.
(2) Die Bank gewährleistet nicht, dass die Finanzbehörden die im Posteingang gespeicherten Informationen anerkennen. Der Teilnehmer sollte sich darüber vorher bei dem für ihn zuständigen Finanzamt informieren.

11.11 Geltung der Allgemeinen Geschäftsbedingungen und Sonderbedingungen /Datenschutzerklärung

(1) Ergänzend gelten die Allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank, die in den Geschäftsräumen der Bank oder unter www.merckfinck.de „AGB“ eingesehen werden können und dem Kunden auf Wunsch auch auf dem Postweg zugesandt werden.

(2) Unsere Datenschutzhinweise finden Sie unter www.merckfinck.de „Datenschutz“.