Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager (gültig ab 2. Januar 2017)

1. Leistungsangebot/Widerruf der Fondsbankingvereinbarung und Definitionen

(1) Der Kunde kann Bankgeschäfte mittels Fondsbanking in dem von der Fondsdepot Bank GmbH (im Nachfolgenden „Bank" genannt) angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels Fondsbanking bzw. den InfoManager abrufen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Nachfolgenden als Nutzer bezeichnet.

(3) Für das Fondsbanking sind nur natürliche Personen nutzungsberechtigt. Sofern der Nutzer eine juristische Person ist und das Fondsbanking nutzen möchte, muss er eine oder mehrere nutzungsberechtigte natürliche Personen als Nutzer benennen.

(4) Der Nutzer ist berechtigt, seine Einwilligung zur Nutzung des Fondsbanking jederzeit zu widerrufen. Im Fall des Widerrufs der Einwilligung zur Nutzung des Fondsbanking durch den Kunden entfällt die Nutzungsberechtigung auch für alle von ihm bevollmächtigten Nutzer, es sei denn der Widerruf ist ausdrücklich auf den widerrufenden Kunden beschränkt. Widerruft ein Kunde eines Gemeinschaftsdepots mit Einzelverfügungsberechtigung seine Einwilligung zur Nutzung des Fondsbanking, so entfällt die Nutzungsberechtigung auch für alle anderen Kunden sowie für alle bezüglich dieses Depots/Kontos bevollmächtigten Nutzer, es sei denn, der Widerruf ist ausdrücklich auf den widerrufenden Kunden beschränkt.

(5) Personalisierte Sicherheitsmerkmale sind:

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

(6) Das Authentifizierungsinstrument ist die von der Bank zur Verfügung gestellte Transaktionsnummern-Liste.

2. Leseberechtigung/Transaktionsberechtigung

Der Nutzer kann Depotbestände, Kontostände, Spar- und Auszahlpläne, Depotumsätze und persönliche Daten (z. B. Adresse und Freibeträge) über Internet einsehen (Leseberechtigung). Ferner kann der Nutzer Fondsbanking-Aufträge im jeweils von der Bank angebotenen Leistungsumfang erteilen, z. B. Kauf-, Verkaufs- und Tauschaufträge oder Einrichtung von Spar- und Auszahlplänen (Transaktionsberechtigung).

Je nach Wunsch kann der Nutzer beim Fondsbanking entweder sowohl eine Lese- als auch eine Transaktionsberechtigung erhalten oder aber seine Zugriffsmöglichkeiten auf die Leseberechtigung beschränken. Für Minderjährige ist lediglich die Einräumung einer Leseberechtigung möglich. Produkte der Bank, für die Besondere Bedingungen gelten (z. B. VL-Depots), sind von der Transaktionsberechtigung ausgeschlossen.

3. Zugangsberechtigung

Für die gewünschte Lese- bzw. Transaktionsberechtigung erteilt die Bank dem Nutzer brieflich eine Zugangskennung und eine persönliche Identifikationsnummer (PIN). Daneben sendet die Bank mit gesonderter Post eine Liste mit Transaktionsnummern zu. Die PIN muss beim ersten Zugang geändert werden. Jede Transaktionsnummer kann nur einmal verwendet werden. Bei Bedarf erhält der Nutzer eine neue Liste mit Transaktionsnummern. Bei Gemeinschaftsdepots mit Einzelverfügungsberechtigung muss der Auftrag für die Freischaltung zum Fondsbanking von allen Kunden unterschrieben werden. Jeder Kunde, der das Fondsbanking nutzen will, erhält einen eigenen Zugang mit eigener Zugangskennung, eigener PIN und eigenen Transaktionsnummern. Für Gemeinschaftsdepots mit gemeinschaftlicher Verfügungsberechtigung ist eine Nutzung des Fondsbanking nicht möglich. Sofern der Nutzer des Fondsbanking nicht mit dem/den Kunden identisch ist (z. B. Bevollmächtigter), so ist der Auftrag für die Freischaltung zum Fondsbanking ebenfalls von dem/den Kunden zu unterschreiben.

4. Verfahren

(1) Der Nutzer hat mittels Fondsbanking Zugang zum Konto/Depot, wenn er zuvor seine Kundennummer sowie seine PIN eingegeben hat, die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Nutzers ergeben hat und keine Sperre des Zugangs vorliegt. Nach Gewährung des Zugangs zum Fondsbanking kann der Nutzer Informationen abrufen oder Aufträge erteilen.

(2) Zur Freigabe einer Verfügung hat der Nutzer zusätzlich eine Transaktionsnummer einzugeben. Die erforderlichen Transaktionsnummern werden dem Nutzer auf einer Liste zur Verfügung gestellt, die einmal verwendbare Transaktionsnummern enthalten.

5. Fondsbanking-Aufträge

5.1 Auftragserteilung und Autorisierung

Der Nutzer muss Fondsbanking-Aufträge (z. B. eine Kauf- oder Verkaufsorder) zu deren Wirksamkeit mit einer Transaktionsnummer autorisieren und der Bank mittels Fondsbanking übermitteln. Die Bank bestätigt mittels Fondsbanking den Eingang des Auftrags.

5.2 Widerruf von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Fondsbanking-Verfahrens erfolgen. Die Bank kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihr diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist.

6. Bearbeitung von Fondsbanking-Aufträgen durch die Bank/Verfügbarkeit des Fondsbanking

(1) Die Bearbeitung der Fondsbanking-Aufträge erfolgt an den im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem im Preis- und Leistungsverzeichnis bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Preis- und Leistungsverzeichnis der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, sofern der Nutzer sich mit seinem personalisierten Sicherheitsmerkmal legitimiert hat.

(3) Sollte der Bank die Ausführung des Auftrags unmöglich sein, wird sie den Nutzer über die Nichtausführung und soweit möglich über deren Gründe schriftlich informieren. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt.

(4) Der Nutzer nimmt zur Kenntnis, dass die Verfügbarkeit des Fondsbanking aufgrund von Störungen von Netzwerk- oder Telekommunikationsverbindungen, höhere Gewalt, aufgrund von für den reibungslosen Betriebsablauf erforderlichen Wartungsarbeiten oder sonstiger Umstände eingeschränkt oder zeitweise ausgeschlossen sein kann. Eine Haftung der Bank aus diesem Grund ist ausgeschlossen.

7. Fondsbanking-Bankverbindung/Geldkonto/Betragsgrenze für Onlineaufträge

(1) Für die Bearbeitung von Fondsbanking-Aufträgen ist es erforderlich, dass zum Depot mindestens eine hinterlegte Kundenbankverbindung (Geldkonto bei der Bank oder externe Bankverbindung), für welche hiermit ein/e Einzugsermächtigung/Mandat erteilt wird, besteht. Die Bank wird per Fondsbanking erteilte Aufträge nur ausführen, wenn der Gegenwert von der im Fondsbanking Kauf-Auftrag ausgewählten Kundenbankverbindung eingezogen werden soll. Erlöse aus Verkäufen von Anteilen oder Aktien an Investmentvermögen werden ausschließlich zu Gunsten der im Fondsbanking Verkaufs-Auftrag ausgewählten Kundenbankverbindung überwiesen. Eine Änderung der Kundenbankverbindungen ist der Bank bekannt zu geben.

(2) Unterhält der Nutzer kein Geldkonto oder ist das Geldkonto nicht das Fondsbanking-Referenzkonto und erteilt der Nutzer Kaufaufträge zu Gunsten eines Depots der Bank per Fondsbanking, so wird die Bank den Kaufauftrag nur dann ohne vorhergehenden Geldeingang ausführen, wenn das Ordervolumen 50.000,00 EUR nicht übersteigt.

(3) Unterhält der Nutzer bei der Bank ein Geldkonto, so darf der Nutzer Verfügungen zu Lasten des Geldkontos nur im Rahmen des Kontoguthabens oder eines zuvor eingeräumten Kredites vornehmen. Auch wenn der Nutzer diese Nutzungsgrenzen bei seinen Verfügungen nicht einhält, ist die Bank berechtigt aber nicht verpflichtet, die erteilte Fondsbankingorder auszuführen. Im Falle der Ausführung liegt eine geduldete Kontoüberziehung vor; die Bank ist berechtigt, in diesem Fall den für geduldete Kontoüberziehungen geltenden Zinssatz zu verlangen.

8. Sorgfaltspflichten des Nutzers

8.1 Technische Verbindung zum Fondsbanking

Der Nutzer ist verpflichtet, die technische Verbindung zum Fondsbanking nur über die von der Bank für das Online-Banking bereitgestellten Internetdienste oder Applikationen herzustellen.

8.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Nutzer hat

– seine personalisierten Sicherheitsmerkmale [siehe Nr. 1 Absatz (5)] geheim zu halten sowie
– sein Authentifizierungsinstrument [siehe Nr. 1 Absatz (6)] vor dem Zugriff anderer Personen sicher zu verwahren.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

– Das personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. auf dem Computersystem des Kunden).
– Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
– Das personalisierte Sicherheitsmerkmal darf nicht außerhalb der Internetseiten der Bank eingegeben werden. Die Internetseite der Bank ist hierzu direkt oder über einen von der Bank zur Verfügung gestellten Link aufzurufen.
– Das personalisierte Sicherheitsmerkmal darf nicht außerhalb
  - der Internetseite der Bank
  - der von der Bank zur Verfügung gestellten Applikationen

  eingegeben werden.
– Der Nutzer darf zur Autorisierung z. B. eines Auftrags nicht mehr als eine Transaktionsnummer verwenden.

8.3 Sicherheit des Kundensystems

Der Nutzer muss die Sicherheitshinweise auf der Internetseite der Bank zum Fondsbanking beachten (insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software des Computersystems des Nutzers).

8.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Nutzer Daten aus seinem Fondsbanking-Auftrag (z. B. Betrag, IBAN des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem zur Bestätigung anzeigt, ist der Nutzer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Nutzer den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals fest, muss der Nutzer die Bank hierüber unverzüglich unterrichten (Sperranzeige).

Der Nutzer hat folgende Möglichkeiten, eine Sperranzeige gegenüber der Bank abzugeben:

- über das Fondsbanking,
- während der Service-Zeiten über die telefonische Kundenbetreuung,
- über die 24-Stunden-Hotline außerhalb der Service-Zeiten.

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

(3) Hat der Nutzer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.

9.2 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.

10. Nutzungssperre

10.1 Sperre auf Veranlassung des Nutzers

Die Bank sperrt auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Nr. 9.1,

- den Fondsbanking-Zugang für ihn oder alle Nutzer oder
- sein Authentifizierungsinstrument.

10.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Fondsbanking-Zugang für einen Nutzer sperren, wenn

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

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

10.3 Aufhebung der Sperre

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

11. Haftung

11.1 Haftung des Kunden bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

11.1.1 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 Authentifizierungsinstruments, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 EUR, ohne dass es darauf ankommt, ob den Nutzer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhandengekommen ist, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 EUR, wenn der Nutzer seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Der Kunde ist nicht zum Ersatz des Schadens nach den Nummern 11.1.1 Absatz (1) und 11.1.1 Absatz (2) verpflichtet, wenn der Nutzer die Sperranzeige nach Nr. 9.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Nutzer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Nutzers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nr. 8.1),
- das personalisierte Sicherheitsmerkmal in seinem Computersystem gespeichert hat [siehe Nr. 8.2 Absatz (2), 1. Punkt],
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt oder das Authentifizierungsinstrument einem Dritten zugänglich gemacht hat und der Missbrauch dadurch verursacht wurde [siehe Nr. 8.2 Absatz (1), 2. Punkt],
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat [siehe Nr. 8.2 Absatz (2), 3. Punkt],
- das personalisierte Sicherheitsmerkmal außerhalb des Fondsbanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat [siehe Nr. 8.2 Absatz (2), 4. Punkt],
- die PIN auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat,
- mehr als eine Transaktionsnummer zur Autorisierung eines Auftrags verwendet hat [siehe Nr. 8.2 Absatz (2), 5. Punkt].

11.1.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.1.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Nutzers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Fondsbanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Nutzer in betrügerischer Absicht gehandelt hat.

11.1.4 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.

12. InfoManager

12.1 Hinterlegung von Dokumenten, Verzicht auf postalischen Versand

(1) Die Bank stellt dem Kunden alle Dokumente, Mitteilungen und Erklärungen (im Nachfolgenden „Dokumente“ genannt) wie z. B. AGB-Änderungen, Mitteilungen über Zinssatzänderungen und Depotabrechnungen im InfoManager zur Verfügung, soweit nicht ausdrücklich Schriftform vorgeschrieben ist. Der Kunde kann die im InfoManager hinterlegten Dokumente ansehen, ausdrucken und herunterladen.

(2) Der Kunde verzichtet ausdrücklich auf den postalischen Versand der für das Depot in den InfoManager eingestellten Dokumente.

(3) Die Bank behält sich vor, Dokumente postalisch bzw. auf andere Weise dem Kunden zur Verfügung zu stellen, wenn dies gesetzliche Vorgaben erforderlich machen oder es aufgrund anderer Umstände unter Berücksichtigung der Anlegerinteressen zweckmäßig erscheint, weil z. B. der InfoManager zeitweise nicht zur Verfügung steht. Die Bank behält sich vor, die Auswahl der in den InfoManager einzustellenden Dokumente zu ändern.

12.2 Kontrollpflicht, Information des Kunden

(1) Der Kunde ist verpflichtet, den InfoManager auf den Eingang neuer Dokumente zu kontrollieren, die hinterlegten Dokumente abzurufen sowie deren Inhalt zu überprüfen. Die Kontrolle ist regelmäßig und zeitnah, insbesondere jedoch dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrages mit der Einstellung neuer Dokumente zu rechnen ist. Eventuelle Unstimmigkeiten sind der Bank unverzüglich anzuzeigen.

(2) Die Bank wird den Kunden bei Einstellung eines neuen Dokuments per E-Mail hierüber informieren. Diese E-Mail dient jedoch lediglich der Information und entbindet den Kunden nicht von seiner Kontrollpflicht.

(3) Dokumente, die dem Kunden im InfoManager hinterlegt werden, gelten mit Einstellung und der Möglichkeit des Abrufs als zugegangen.

12.3 Verfügbarkeit, Unveränderbarkeit von Dokumenten, Haftung

(1) Der Kunde nimmt zur Kenntnis, dass die Verfügbarkeit des InfoManager aufgrund von Störungen von Netzwerk oder Telekommunikationsverbindungen, höherer Gewalt, aufgrund von für den reibungslosen Betriebsablauf erforderlichen Wartungsarbeiten oder sonstiger Umstände eingeschränkt oder zeitweise ausgeschlossen sein kann.

(2) Die in den InfoManager eingestellten Dokumente werden dem Kunden im PDF-Format zur Verfügung gestellt. Die Bank garantiert die Unveränderbarkeit der Daten, sofern die Daten im InfoManager gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb des InfoManager gespeichert, aufbewahrt

oder in veränderter Form in Umlauf gebracht, wird die Bank hierfür keine Haftung übernehmen.

Die Anerkennung der im InfoManager gespeicherten Dokumente durch Steuer- oder Finanzbehörden kann durch die Bank nicht gewährleistet werden. Eine vorherige Erkundigung beim zuständigen Finanzamt obliegt dem Kunden.

12.4 Dauer der Hinterlegung

Im InfoManager werden die Dokumente des laufenden sowie des vorherigen Kalenderjahres vorgehalten. Jeweils zum Kalenderjahreswechsel wird die Bank die Dokumente des vorvergangenen Jahres automatisch und ohne zusätzliche Mitteilung an den Kunden aus dem InfoManager entfernen.

12.5 Kündigung, Beendigung der Geschäftsbeziehungen

(1) Der Kunde kann ohne Angabe von Gründen die Nutzung des InfoManager jederzeit kündigen. Ab Zugang der Kündigung zuzüglich einer angemessenen Bearbeitungszeit werden alle Dokumente per Post an die vom Kunden angegebene Adresse versendet.

(2) Die Bank kann die Nutzung des InfoManager mit einer Frist von zwei Monaten kündigen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt hiervon unberührt. Sämtliche nach Wirksamwerden der Kündigung erstellten Dokumente werden gemäß den AGB dem Kunden postalisch zugesandt.

(3) Der Kunde verpflichtet sich, bis zum Wirksamwerden der Kündigung bzw. zur Beendigung der Geschäftsbeziehung alle im InfoManager gespeicherten Dokumente zu kontrollieren und diese eventuell auszudrucken oder abzuspeichern. Eine Verpflichtung zum nachträglichen unentgeltlichen Versand von den zu diesem Zeitpunkt in den InfoManager eingestellten Dokumenten besteht nicht.