Depot-/Kontoführung:

FONDSDEPOT BANK

Online Service: Meine Allianz

Allianz

Auftrag zur Freischaltung des InfoManager in Verbindung mit der Freischaltung des Online Services Meine Allianz

An die
Fondsdepot Bank GmbH
95025 Hof

Depot/Konto-Nr. _____

Dieser Auftrag soll außerdem für folgende/s Depots/Konto gelten:

Nr. _____

Nr. _____

Depot-/Kontoinhaber 1 bzw. gesetzlicher Vertreter 1

Name, Vorname _____ Geburtsdatum _____

Straße, Hausnummer _____

PLZ, Ort _____ _____

wohnhaft in **Deutschland** oder _____ **Mobilfunknummer** _____

E-Mail _____

Depot-/Kontoinhaber 2 bzw. gesetzlicher Vertreter 2

Name, Vorname _____ Geburtsdatum _____

Straße, Hausnummer _____

PLZ, Ort _____ _____

wohnhaft in **Deutschland** oder _____ **Mobilfunknummer** _____

E-Mail _____

Bevollmächtigter

Hinweis: Bedingung für die Freischaltung des Bevollmächtigten ist eine entsprechend separat beauftragte und bei der Bank vermerkte Depotvollmacht. Zusätzlich ist die Zustimmung aller Depot-/Kontoinhaber mittels Unterschrift auf diesem Formular zwingend erforderlich.

Name, Vorname _____ Geburtsdatum _____

Straße, Hausnummer _____

PLZ, Ort _____ _____

wohnhaft in **Deutschland** oder _____ **Mobilfunknummer** _____

E-Mail _____

_____ **Pflichtfelder**

A. Freischaltung für das Fondsbanking und den InfoManager bei der Fondsdepot Bank GmbH

Fondsbanking

Das Fondsbanking bietet dessen Nutzer die Möglichkeit Depotbestände, Kontostände, Spar- und Auszahlpläne, Depotumsätze und persönliche Daten (z. B. Adresse und Freibeträge) über das Internet einzusehen (Leseberechtigung). Ferner kann der Nutzer Kauf-, Verkaufs- und Tauschaufträge, im Falle eines ggf. neu zu eröffnenden Geldkontos Überweisungsaufträge veranlassen und Aufträge zu Spar- und Auszahlplänen über das Internet erteilen (Transaktionsberechtigung). Für die Nutzung des Fondsbanking gelten die in den Eröffnungsunterlagen abgedruckten Besonderen Bedingungen für die Nutzung des Fondsbanking und des InfoManager. Produkte der Bank, für die Besondere Bedingungen/besondere Produktbedingungen gelten (z. B. Allianz AufbauPlan, Allianz VL-SparPlan), sind von der Möglichkeit Transaktionen im Rahmen des Online-Fondsbanking vorzunehmen, ausgeschlossen.

InfoManager

Der InfoManager ist ein elektronisches Postfach, in dem für den/die Depot-/Geldkontoinhaber bestimmte Dokumente, die im Rahmen der Depot-/Kontoführung produziert werden (z. B. Depot-/Kontoabrechnungen, Kosteninformation), zum Download hinterlegt werden. Für die Nutzung des InfoManager gelten die in den Eröffnungsunterlagen abgedruckten Besonderen Bedingungen für die Nutzung des Fondsbanking und des InfoManager.

Entscheidung des/der Depot-/Kontoinhaber/s

☒ **Ich/Wir beauftrage/n die Bank, das/die mit diesem Antrag neu zu eröffnende/n Depot/s und das ggf. neu zu eröffnende Geldkonto für den InfoManager freizuschalten.**

Der Zugriff erfolgt dabei über „Meine Allianz", für das eine separate Freischaltung benötigt wird; ergänzend gelten die im Vertragsteil „Meine Allianz" genannten Regelungen. Die Freischaltung für das Fondsbanking mit Leseberechtigung bzw. mit Transaktionsberechtigung im Bereich „Meine Allianz" erfolgt aus rechtlichen Gründen separat nach der Einrichtung des Zuganges zu „Meine Allianz".

B. Der Online Service Meine Allianz bei der Allianz Deutschland AG

Meine Allianz ist ein Online-Dienst, mit dem der/die Depot-/Geldkontoinhaber bzw. der/die gesetzliche/n Vertreter seine/ihre Verträge und Depots unter www.allianz.de online verwalten kann/können.

Für die Nutzung von Meine Allianz und des InfoManager gelten die mit diesen Unterlagen zur Verfügung gestellten Nutzungsbedingungen für den Online Service Meine Allianz.

Hinweis: Durch die Freischaltung von Meine Allianz erhalten Sie den Zugang zu allen Leistungsmöglichkeiten des Online Services Meine Allianz. In diesem Zusammenhang können Sie u. a. die hinterlegte Adresse online ändern, möglicherweise bestehende Lebensversicherungsverträge einsehen sowie das Online-Fondsbanking nutzen. Lesen Sie deshalb bitte die Nutzungsbedingungen für den Online Service Meine Allianz gründlich.

Produkte der Bank, für die Besondere Bedingungen/besondere Produktbedingungen gelten (z. B. Allianz AufbauPlan, Allianz VL-SparPlan), sind von der Möglichkeit Transaktionen im Rahmen des Online Services Meine Allianz vorzunehmen, ausgeschlossen.

Freischaltung des Depots/Geldkontos für den Online Service Meine Allianz

☒ **Ich/Wir beauftrage/n hiermit die Allianz Deutschland AG, das/die o. g. Depot/s und ggf. das o. g. Geldkonto für die Nutzung des Online Services Meine Allianz, im Rahmen der Freischaltung des InfoManager, freizuschalten. Die Freischaltung für das Fondsbanking mit Leseberechtigung bzw. mit Transaktionsberechtigung im Bereich „Meine Allianz" erfolgt aus rechtlichen Gründen separat nach der Einrichtung des Zuganges zu „Meine Allianz".**

Bei Gemeinschaftsdepots/-konten bzw. bei mehreren gesetzlichen Vertretern werden alle Depot-/Geldkontoinhaber bzw. alle gesetzlichen Vertreter freigeschaltet. In diesem Fall ist die Freischaltung, für nur einen Depot-/Geldkontoinhaber bzw. gesetzlichen Vertreter, nicht möglich

Für jeden Depot-/Geldkontoinhaber, gesetzlichen Vertreter sowie Bevollmächtigten wird ein separater Zugang freigeschaltet. Dazu erhält jeder Teilnehmer, soweit nicht bereits ein Zugang für Meine Allianz besteht, per E-Mail ein Link zur Registrierung für Meine Allianz für das/die auf Seite 1 genannte/n Depot/s und ggf. Geldkonto/-konten. Bitte beachten: Ohne die Registrierung für Meine Allianz ist kein Zugriff auf die Depot-/Geldkonto relevanten Dokumente möglich.

Produkte der Bank, für die Besondere Bedingungen/besondere Produktbedingungen gelten (z. B. Allianz AufbauPlan, Allianz VL-SparPlan), sind von der Möglichkeit Transaktionen im Rahmen des Online Services Meine Allianz vorzunehmen, ausgeschlossen.

Die Allianz Deutschland AG weist darauf hin, dass im Rahmen dieses Online-Services auch die Bedingungen des Infomanagers und Fondsbankings der Fondsdepotbank GmbH gelten.

Die mit diesen Unterlagen zur Verfügung gestellten „Nutzungsbedingungen für den Online Service Meine Allianz" habe/n ich/wir gelesen und erkenne/n ich/wir unverändert an.

C. Schlusserklärungen

C.1 Schlusserklärungen für die Freischaltung für das Fondsbanking und den InfoManager bei der Fondsdepot Bank GmbH

Die mit diesen Unterlagen zur Verfügung gestellten Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager habe/n ich/wir gelesen und erkenne/n ich/wir unverändert an.

C.2 Schlusserklärungen für den Online Service Meine Allianz bei der Allianz Deutschland AG

Die mit diesen Unterlagen zur Verfügung gestellten Nutzungsbedingungen für den Online Service Meine Allianz habe/n ich/wir gelesen und erkenne/n ich/wir unverändert an.

Ort, Datum

✗	✗	✗
Unterschrift Depot-/Geldkontoinhaber 1 bzw. gesetzlicher Vertreter 1	Unterschrift Depot-/Geldkontoinhaber 2 bzw. gesetzlicher Vertreter 2	Unterschrift Bevollmächtigter

Dieses Formular muss im Original an die Bank übermittelt werden (kein Telefax, keine Kopie).

Fondsdepot Bank GmbH, 95025 Hof, Telefon +49 (0) 9281 820-2000

Inhalt

Folgende Bestandteile sind in diesen Unterlagen enthalten:

FONDSDEPOT BANK

Vertragsbedingungen der Fondsdepot Bank GmbH

- Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager

Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager (Stand 1. Juli 2020)

Im Nachfolgenden wird der Begriff Fondsbanking durch Online Banking ersetzt.

Teil A: Online Banking

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 zusätzlich sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absatz 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 Banking 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 Banking 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 Arbeitslaufes. 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. Ansonsten 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 Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist die Anwendung für das Online Banking (z. B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das On-

line 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 (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 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 Authentifizierungslemente 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 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 (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 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 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 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.

Teil B: InfoManager

1. Hinterlegung von Dokumenten, Verzicht auf postalischen Versand

(1) Die Bank stellt dem Teilnehmer 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 Teilnehmer kann die im InfoManager hinterlegten Dokumente ansehen, ausdrucken und herunterladen.

(2) Der Teilnehmer 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 Teilnehmern 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.

2. Kontrollpflicht, Information des Teilnehmers

(1) Der Teilnehmer 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 Teilnehmer bei Einstellung eines neuen Dokuments per E-Mail hierüber informieren. Diese E-Mail dient jedoch lediglich der Information und entbindet den Teilnehmer nicht von seiner Kontrollpflicht.

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

3. Verfügbarkeit, Unveränderbarkeit von Dokumenten, Haftung

(1) Der Teilnehmer 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 Teilnehmer 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.

(3) 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 Teilnehmer.

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 Teilnehmer aus dem InfoManager entfernen.

5. Kündigung, Beendigung der Geschäftsbeziehungen

(1) Der Teilnehmer kann ohne Angabe von Gründen die Nutzung des InfoManager jederzeit kündigen. Ab Zugang der Kündigung zuzüglich einer angemessenen Bearbeitungszeit werden alle Dokumente entgeltpflichtig per Post an die vom Teilnehmern 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 Allgemeine Geschäftsbedingungen und den Sonderbedingungen der Fondsdepot Bank GmbH dem Teilnehmern postalisch zugesandt.

(3) Der Teilnehmer 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.

Teil C: Schlussbestimmungen

1. Kommunikation und technische Anforderungen

(1) Zur Durchführung von Bankgeschäften über das Online Banking Portal benötigt der Teilnehmer eine eigene Zugangskennung und eine Zugangs-PIN. Nach Eingabe seiner Transaktionsdaten erhält der Teilnehmer bei Nutzung des sogenannten Push TAN Verfahrens eine TAN via APP angezeigt, welche zur Authentifizierung seiner Transaktion gültig ist. Für die Generierung und Anzeige einer einmaligen TAN wird die Fondsdepot Bank Push TAN APP benötigt. Diese kann der Teilnehmer auf einem Android oder IOS betriebenen Gerät installieren. Die Freischaltung der APP für seine Konten muss der Teilnehmer mit dem per Post zugesandten Aktivierungscode veranlassen. Für jede Zugangskennung kann nur ein mobiles Gerät registriert werden.

(2) Im Falle vermuteten oder tatsächlichen Betrugs oder bei Sicherheitsrisiken wird die Bank den Teilnehmer per Post unterrichten.

2. Änderungen der Besondere Bedingungen

Für Änderungen dieser Besondere Bedingungen gilt Ziffer 1.2 der AGB.

Allianz

Vertragsbedingungen der Allianz Deutschland AG

- Nutzungsbedingungen für den Online Service Meine Allianz

Der Online Service Meine Allianz

Der Online Service Meine Allianz (im Folgenden „Meine Allianz" genannt) ist ein Angebot der Allianz Deutschland AG (im Folgenden „Allianz" genannt). Die Nutzungsbedingungen gelten auch im Verhältnis zu anderen Unternehmen der Allianz Gruppe mit Sitz in Deutschland, die ihre Online Dienste im Rahmen von Meine Allianz anbieten und mit denen der Kunde in einer Vertragsbeziehung steht (im Nachfolgenden insgesamt „Allianz Unternehmen" genannt).

Bitte lesen Sie diese Nutzungsbedingungen gründlich durch, bevor Sie sich mit Ihnen einverstanden erklären.

Nutzungsbedingungen für den Online Service Meine Allianz (gültig ab 01.01.2019)

A. Allgemeine Nutzungsbedingungen

1. Angebotene Dienste

Meine Allianz bietet privaten Nutzern die Möglichkeit, unter der Adresse meine.allianz.de die in Meine Allianz angebotenen Dienste der Allianz und der Allianz Unternehmen für ihre privaten Versicherungsgeschäfte zu nutzen. Die Dienste erstrecken sich nicht auf Versicherungsgeschäfte, die im Zusammenhang mit der gewerblichen oder selbständigen beruflichen Tätigkeit stehen. Personengesellschaften oder juristischen Personen stehen die Dienste nicht zur Verfügung.

2. Nutzungsberechtigte Personen

2.1 Nutzungsberechtigung

Die Nutzungsberechtigung für Meine Allianz wird nur an natürliche Personen vergeben, die entweder bereits einen Versicherungsvertrag mit der Allianz oder einem Allianz Unternehmen abgeschlossen haben (Kunden), die an einem Vertragsabschluss über Meine Allianz interessiert sind (Interessenten) oder die von einem Kunden der Allianz unter den Voraussetzungen nach Ziffer 3 zur Verwaltung seiner Verträge bevollmächtigt sind (Bevollmächtigte). Wenn im Folgenden die Bezeichnung „Nutzer" verwendet wird, sind sämtliche nutzungsberechtigte Personen gemeint.

2.2 Nutzungsvereinbarung

Die Nutzungsberechtigung für Meine Allianz setzt den Abschluss einer Nutzungsvereinbarung zwischen der Allianz und dem Nutzer voraus, für die ein Antrag des Kunden oder Interessenten auf Freischaltung von Meine Allianz oder die Mitteilung der Bevollmächtigung einer Person gem. Ziffer 3 gegenüber der Allianz erforderlich ist. Sämtliche im Rahmen der Anmeldung erfragten Daten und sonstigen Angaben sind vollständig und korrekt anzugeben. Die Nutzungsvereinbarung kommt mit der Freischaltung für Meine Allianz zustande.

3. Bevollmächtigung

Ein Kunde kann einen oder mehrere Familienangehörige in beschränktem Umfang zur Verwaltung seiner mit der Allianz Versicherungs-AG geschlossenen Versicherungsverträge mittels eines von der Allianz zur Verfügung gestellten Formulars bevollmächtigen. Dies gilt nicht für mit der Allianz Lebensversicherungs-AG oder Allianz Private Krankenversicherungs-AG geschlossene Versicherungsverträge. Den bevollmächtigten Personen wird in diesem Fall eine eigene Nutzungsberechtigung erteilt. Der Kunde kann die Bevollmächtigung ohne Angabe von Gründen jederzeit gegenüber der Allianz widerrufen.

4. Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind:
- die persönliche Zugangsnummer,
- der Benutzername, den der Nutzer als Alternative zur Zugangsnummer frei wählen kann,
- das persönliche Passwort,
- die einmal verwendbaren mobilen Transaktionsnummern (mTAN), die dem Nutzer per SMS an die von ihm hinterlegte Mobilfunknummer kurzfristig auf ein mobiles Endgerät zur Verfügung gestellt werden,
- die einmal verwendbaren indizierten Transaktionsnummern (iTAN), die ausschließlich gemäß Ziffer 3 Bevollmächtigten auf einer Liste zur Verfügung gestellt werden
- die einmal verwendbaren Freischaltcodes, die per Post zur Verfügung gestellt werden und
- das dienste- und kartenspezifische Kennzeichen des neuen Personalausweises (DKK) (zusammen: personalisierte Sicherheitsmerkmale).

Alle Nutzer, die über eine validierte E-Mail-Adresse und über eine validierte Mobilfunknummer verfügen, werden automatisch zur Nutzung von mTAN freigeschaltet.

5. Zugang zu Meine Allianz

5.1 Zugangsvoraussetzungen

Der Nutzer erhält Zugang zu Meine Allianz und den darin angebotenen Diensten, wenn
- er seine individuelle Zugangskennung (persönliche(r) Zugangsnummer/Benutzername und persönliches Passwort) übermittelt hat,
- die Prüfung der Zugangsberechtigung erfolgreich war und
- keine Sperre des Zugangs vorliegt.

Nutzer, die die Zwei-Faktor-Authentifizierung (2FA) aktiviert haben, müssen zusätzlich zur Zugangskennung eine mTAN eingeben, um Zugang zu Meine Allianz zu erhalten. Die Allianz empfiehlt die Aktivierung von 2FA, da dieses Verfahren ein zusätzliches Sicherheitsniveau bietet.

Nach erfolgreicher Prüfung der Zugangsdaten kann der Nutzer die in Meine Allianz angebotenen Dienste der Allianz nutzen.

5.2 Nutzung des neuen Personalausweises

Wenn der Nutzer die Online Ausweisfunktion seines Personalausweises für den Zugang zu Meine Allianz nutzen will, muss der Personalausweis einmalig mittels persönlicher(n) Zugangsnummer/ Benutzernamens, persönlichen Passworts, bzw. im Fall von vergessenen Zugangsdaten mittels mTAN, und iTAN bzw. Freischaltcode für die Nutzung registriert werden. Die nachfolgenden Anmeldungen bei Meine Allianz können dann vom Nutzer durch die Nutzung des neuen Personalausweises durchgeführt werden. Die Übermittlung von Zugangsnummer und Passwort erfolgt dann durch die Online Ausweisfunktion.

6. Verfügbarkeit von Meine Allianz

Der Nutzer nimmt zur Kenntnis, dass die Verfügbarkeit von Meine Allianz aufgrund von Störungen von Netzwerk oder Telekommunikationsverbindungen, aufgrund höherer Gewalt, aufgrund von für den reibungslosen Betriebsablauf erforderlichen Wartungsarbeiten oder sonstigen Umständen eingeschränkt oder zeitweise ausgeschlossen sein kann.

7. Sorgfaltspflichten des Nutzers

7.1 Technische Verbindung zu Meine Allianz

Der Nutzer ist verpflichtet, die technische Verbindung zu Meine Allianz nur über von der Allianz und den Allianz Unternehmen mitgeteilte Zugangskanäle herzustellen.

7.2 Sicherheit des Kundensystems

Der Nutzer muss die Sicherheitshinweise auf der Internetseite der Allianz und der Allianz Unternehmen, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Geheimhaltung und Aufbewahrung der personalisierten Sicherheitsmerkmale

Der Nutzer hat seine personalisierten Sicherheitsmerkmale geheim zu halten und insbesondere die per SMS übermittelte mTAN, die iTAN-Liste und den Freischaltcode vor dem Zugriff anderer Personen sicher zu verwahren. Denn jede andere Person, die im Besitz von personalisierten Sicherheitsmerkmalen ist, kann Meine Allianz missbräuchlich nutzen.

Insbesondere ist Folgendes zum Schutz der personalisierten Sicherheitsmerkmale zu beachten:
- Personalisierte Sicherheitsmerkmale dürfen nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem und dem zum mTAN-Verfahren genutzten Endgerät).
- Bei Eingabe eines Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Personalisierte Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online Händlerseiten).
- Personalisierte Sicherheitsmerkmale dürfen nicht außerhalb von Meine Allianz weitergegeben werden, also beispielsweise nicht per E-Mail oder SMS.
- Das Passwort darf nicht zusammen mit der iTAN-Liste oder einem Freischaltcode verwahrt werden.
- Der Nutzer darf zur Autorisierung nicht mehr als eine iTAN, einen Freischaltcode oder eine mTAN verwenden.

7.4 Verwendung und Absicherung des mobilen Endgeräts bei Verwendung von mTAN

Bei der Verwendung von mTAN hat der Nutzer
- durch geeignete Sicherheitsmaßnahmen sicherzustellen, dass das Risiko eines unbefugten Zugriffs durch einen Dritten minimiert wird (z. B. durch das Einrichten einer Display-Sperre).
- das Betriebssystem auf seinem mobilen Endgerät auf dem neusten Stand zu halten.
- den Inhalt der empfangenen SMS mit der zu genehmigenden Transaktion abzugleichen.
- es zu unterlassen, das mobile Endgerät, auf dem er die mTAN empfangen hat, auch für den Zugriff auf Meine Allianz zu nutzen.

8. Anzeige und Unterrichtungspflichten

8.1 Verpflichtung des Nutzers zur Sperranzeige gegenüber der Allianz

Stellt der Nutzer
- den Verlust oder den Diebstahl seiner iTAN-Liste, seines Freischaltcodes oder des im Rahmen des mTAN-Verfahrens genutzten Endgeräts,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seiner personalisierten Sicherheitsmerkmale fest, ist er verpflichtet, die Allianz hierüber zu unterrichten (Sperranzeige).

Der Nutzer ist ebenfalls verpflichtet, eine Sperranzeige zu erstatten, wenn er den Verdacht hat, dass eine andere Person unberechtigt
- in den Besitz seiner iTAN-Liste, seines Freischaltcodes oder des im Rahmen des

mTAN-Verfahrens genutzten Endgeräts gelangt ist,
– Kenntnis seiner übrigen personalisierten Sicherheitsmerkmale erlangt hat oder
– seine personalisierten Sicherheitsmerkmale verwendet.

8.2 Verpflichtung des Nutzers zur Anzeige bei der Polizei

Der Nutzer hat jeden Diebstahl oder Missbrauch personalisierter Sicherheitsmerkmale unverzüglich bei der Polizei zur Anzeige zu bringen.

8.3 Verpflichtung des Nutzers zur Unterrichtung der Allianz

Der Nutzer hat die Allianz unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags über den Sachverhalt zu unterrichten.

9. Nutzungssperre

9.1 Voraussetzungen für eine Sperrung des Online Zugangs oder der personalisierten Sicherheitsmerkmale des Nutzers

Die Allianz ist auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Ziffer 8.1, berechtigt und verpflichtet, den Online Zugang bzw. die personalisierten Sicherheitsmerkmale des Nutzers zu sperren. Die Allianz ist zu einer solchen Sperrung darüber hinaus berechtigt, wenn
– die Nutzungsvereinbarung von ihr aus wichtigem Grund gekündigt werden kann,
– Gründe im Zusammenhang mit der Sicherheit der personalisierten Sicherheitsmerkmale dies rechtfertigen oder
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der personalisierten Sicherheitsmerkmale besteht.

9.2 Information des Nutzers über eine Sperre

Die Allianz wird den Nutzer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Allianz wird eine Sperre aufheben oder die personalisierten Sicherheitsmerkmale austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Nutzer unverzüglich.

10. Hochladen von Dokumenten in Meine Allianz

10.1 Hochladen von Dokumenten

Der Nutzer kann Dokumente zu Versicherungsverträgen, die er mit Allianz Unternehmen oder mit anderen Versicherungsunternehmen abgeschlossen hat, in Meine Allianz hochladen. Als Speicherplatz steht dem Nutzer insgesamt 200 MB zur Verfügung, die maximale Größe eines Dokumentes darf 10 MB nicht überschreiten.

10.2 Kein Hochladen von Dokumenten mit unerlaubten Inhalt

Der Nutzer ist nicht berechtigt, Dokumente mit unerlaubten Inhalt in Meine Allianz hochzuladen. Zu unerlaubten Inhalten gehören Dokumente, die die Rechte Dritter verletzen (wie z.B. copyright-geschützte Filme oder Musikdateien) und Dokumente mit pornographischen, rassistischen oder schadhaften Inhalten (Viren, Trojaner etc.). Der Nutzer erklärt und gewährleistet gegenüber der Allianz, dass er der alleinige Inhaber sämtlicher Rechte an den von Ihnen hochgeladenen Dokumenten ist oder anderweitig berechtigt ist (z.B. durch wirksame Erlaubnis des Rechteinhabers), die betreffenden Dokumente hochzuladen.

10.3 Aufbewahrung der Originaldokumente, Zugriff auf Dateien

Der Nutzer hat für die sichere Aufbewahrung der Originale der hochgeladenen Dokumente Sorge zu tragen und lokale Kopien vorzuhalten. Die Allianz garantiert keinen permanenten Zugriff auf Dateien, s. hierzu Ziffer 6.

10.4 Löschung

Der Nutzer kann die von ihm hochgeladenen Dokumente selbst in Meine Allianz ändern oder löschen. Eine physikalische Löschung der Dokumente ist technisch bedingt erst nach 24 Stunden sichergestellt. Die vom Nutzer zu Verträgen mit Allianz Unternehmen hochgeladenen Dokumente werden mindestens für die Dauer der Vertragsbeziehung vorgehalten. Nach Beendigung des zugrundeliegenden Versicherungsvertrags können die Dokumente ohne eine gesonderte Benachrichtigung gelöscht werden. Bei Kündigung des Meine Allianz-Zugangs werden alle hochgeladenen Dokumente physikalisch gelöscht (vgl. Ziffer 13.5).

10.5 Verschlüsselung

Die Dokumente werden beim Hochladen automatisch mit einer 256bit AES-Verschlüsselung gesichert und verschlüsselt abgelegt. Mitarbeiter der Allianz haben keinen Zugriff auf die Daten.

10.6 Haftung

Sollte dem Nutzer durch die Nutzung des unentgeltlichen Services ein Schaden entstehen, haftet die Allianz nur bei Vorsatz (einschließlich Arglist) oder grober Fahrlässigkeit.

11. Digitale Kommunikation

11.1 Elektronisches Postfach

Die Allianz stellt dem Nutzer in Meine Allianz ein Postfach zur Verfügung. In dieses Postfach können die Allianz und die Allianz Unternehmen dem Nutzer Nachrichten und Dokumente zu seinen Verträgen und Produkten sowie allgemeine Informationen einstellen.

Die Allianz benachrichtigt den Nutzer per E-Mail, wenn ein neues Dokument in sein Postfach eingestellt wurde.

Ein Anspruch des Kunden auf die elektronische Bereitstellung bestimmter Dokumente bzw. der elektronischen Zustellung aller Dokumente zu einem bestimmten Vertrag/ Produkt besteht nur, wenn dies im Versicherungsvertrag ausdrücklich vorgesehen ist.

11.2 E-Mail statt Brief

Falls der Nutzer am Programm „E-Mail statt Brief" teilnimmt, gilt Folgendes: Der Nutzer erklärt sich damit einverstanden, dass er
– Unterlagen (z.B. Rechnungen) zu allen aktuellen und künftigen Allianz Verträgen nicht mehr per Post erhält. Ausgewählte Dokumente wie zum Beispiel solche, die dem Gesetz nach schriftlich vorliegen müssen, versendet die Allianz weiterhin per Post;
– seine Unterlagen per E-Mail erhält.

Zusätzlich werden die Unterlagen in sein elektronisches Postfach in Meine Allianz eingestellt. Unterlagen, die Angaben zur Gesundheit des Nutzers enthalten, werden nicht per E-Mail versandt, sondern in das elektronische Postfach in Meine Allianz eingestellt bzw. per Post versandt. Die Allianz verwendet für den E-Mailversand eine Transportverschlüsselung (derzeit die sog. Transport Layer Security, kurz: TLS), welche eine abgesicherte und zuverlässige Datenübertragung zwischen der Allianz und dem E-Mail-Provider des Nutzers ermöglicht. Für den seltenen Ausnahmefall, dass der E-Mail-Provider des Nutzers eine Transportverschlüsselung nicht unterstützen sollte, macht die Allianz den Nutzer darauf aufmerksam, dass die E-Mail Kommunikation unverschlüsselt erfolgen kann. Die Transportverschlüsselung verhindert den Zugriff Unberechtigter während des Transports, verhindert aber nicht Zugriffe auf den E-Mail Inhalt nach Posteingang im E-Mail Account des Nutzers. Hier sollte der Nutzer gegebenenfalls selbst Sicherungsmaßnahmen treffen (z. B. Löschung im E-Mail Account). Der Nutzer kann seine Teilnahme an E-Mail statt Brief jederzeit widerrufen.

11.3 E-Mail-/SMS-Benachrichtigungen über den Bearbeitungsstand

Der Nutzer wird über wichtige Bearbeitungsschritte seiner Anliegen per E-Mail und /oder per SMS informiert – zum Beispiel bei Schadenfällen oder bei eingereichten Rechnungen zur Krankenversicherung.

11.4 Mitwirkungs- und Kontrollpflichten des Nutzers

11.4.1 Aktualisierung von E-Mail-Adresse und Mobilfunknummer

Der Nutzer ist verpflichtet, Änderungen der hinterlegten E-Mail-Adresse und seiner hinterlegten Mobilfunknummer unverzüglich in Meine Allianz vorzunehmen.

11.4.2 Kontrolle des elektronischen Postfachs

Der Kunde ist verpflichtet, sein elektronisches Postfach regelmäßig auf den Eingang neuer Nachrichten zu kontrollieren. Die Kontrolle ist regelmäßig, insbesondere jedoch dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrages mit der Einstellung neuer Dokumente zu rechnen ist oder der Nutzer über das Einstellen eines neuen Dokuments benachrichtigt wurde.

11.5 Unveränderbarkeit von Informationen und Haftung

Die im elektronischen Postfach eingestellten Dokumente werden dem Kunden im PDF-Format zur Verfügung gestellt. Die Allianz garantiert die Unveränderbarkeit der Daten, sofern die Daten im elektronischen Postfach gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb des elektronischen Postfachs gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die Allianz hierfür keine Haftung.

11.6 Dauer der elektronischen Bereitstellung von Dokumenten

Im elektronischen Postfach werden die Informationen für einen Zeitraum von mindestens 24 Monaten nach deren Einstellung vorgehalten. Nach Ablauf dieses Zeitraums kann die Allianz die Informationen auch ohne vorherige Mitteilung an den Nutzer aus dem elektronischen Postfach entfernen.

11.7 Ende der Bereitstellungspflicht

Die Pflicht zur Bereitstellung von Informationen über das elektronische Postfach endet mit Wirksamwerden der Kündigung der Nutzungsvereinbarung, spätestens aber mit der Beendigung der zugrunde liegenden Geschäftsverbindung.

11.8 Pflichten des Kunden

Der Kunde verpflichtet sich, bis zum Wirksamwerden der Kündigung bzw. zur Beendigung der Geschäftsbeziehung alle im elektronischen Postfach eingestellten Nachrichten und Dokumente zu kontrollieren und diese eventuell auszudrucken oder abzuspeichern. Eine Verpflichtung zum nachträglichen unentgeltlichen Versand von bis zu diesem Zeitpunkt in das elektronische Postfach eingestellten Dokumenten besteht nicht.

12. Änderungen der Nutzungsbedingungen

Änderungen dieser Nutzungsbedingungen werden dem Nutzer spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Die Zustimmung des Nutzers zu den Änderungen der Nutzungsbedingungen gilt als erteilt, wenn er seine Ablehnung nicht vor dem angekündigten Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat. Auf diese Genehmigungswirkung wird ihn die Allianz in ihrem Angebot besonders hinweisen.

13. Kündigungsrechte

13.1 Kündigung durch den Nutzer

Der Nutzer kann die Nutzungsvereinbarung für Meine Allianz jederzeit ohne Einhaltung einer Kündigungsfrist in Textform (z. B. per Brief, E-Mail oder durch Meldung über Meine Allianz) kündigen. Ist der Nutzer aus einem Versicherungsvertrag mit der Allianz verpflichtet, Meine Allianz zu nutzen, ist die Allianz im Falle einer Kündigung der Nutzungsvereinbarung durch den Nutzer nach den Vorschriften des Versicherungsvertrages ggf. berechtigt, den Tarif des Nutzers umzustellen. Insoweit gelten die Regelungen des Versicherungsvertrages.

13.2 Übergangszeitraum

Im Falle einer Kündigung durch den Nutzer nach Ziffer 13.1, räumt die Allianz dem Nutzer die Möglichkeit ein, Meine Allianz für einen Übergangszeitraum von 6 Wochen weiter zu nutzen, insbesondere um seine Dokumente und Daten zu sichern. Macht der Nutzer von dieser Möglichkeit Gebrauch, gelten die Nutzungsbedingungen auch in dem Übergangszeitraum bis zur Deaktivierung des Accounts.

13.3 Kündigung durch die Allianz

Die Allianz kann die Nutzungsvereinbarung für Meine Allianz jederzeit mit einer zweimonatigen Kündigungsfrist in Textform kündigen. Dieses Recht steht ihr nicht zu, wenn sie aus einem Versicherungsvertrag mit dem Kunden verpflichtet ist, diesem die Nutzung von Meine Allianz zu gewährleisten.

13.4 Weitere Kündigungsrechte
Gesetzliche Kündigungsrechte sowie etwaige Kündigungsrechte aus anderen Vereinbarungen mit der Allianz oder einem Allianz Unternehmen bleiben hiervon unberührt.

13.5 Löschung des Meine Allianz-Accounts
Die Allianz ist berechtigt nach einer Kündigung der Nutzungsvereinbarung den Meine Allianz-Account des Nutzers samt aller dort hinterlegten Daten und Dokumente zu löschen. Die Allianz wird den Kunden über eine bevorstehende Löschung unmittelbar nach Kündigung der Nutzungsvereinbarung hinweisen und über die Deaktivierung des Accounts gesondert informieren.

13.6 Beendigung von E-Mail statt Brief
Kündigt der Nutzer die Nutzungsvereinbarung, endet mit Eingang der Kündigung eine etwaige Teilnahme des Nutzers an E-Mail statt Brief (Ziffer 11.2). Kündigt die Allianz die Nutzungsvereinbarung, endet die Teilnahme des Nutzers an E-Mail statt Brief im Zeitpunkt des Wirksamwerdens der Kündigung.

14. Vertragsbedingungen der Allianz und der Allianz Unternehmen

14.1 Ergänzende Geltung der Nutzungsbedingungen
Diese Nutzungsbedingungen gelten ergänzend zu den Vertragsbedingungen der Allianz und der Allianz Unternehmen, mit denen der Kunde in einem Vertragsverhältnis steht.

14.2 Sonderfälle
Diese Nutzungsbedingungen ersetzen die „Bedingungen für die Nutzung des Online Fondsbanking der Allianz Kapitalanlagegesellschaft mbH“ und die „Allgemeinen Bedingungen für die Nutzung von Meine Allianz der Allianz-Lebensversicherungs-AG bzw. der Deutschen Lebensversicherungs-AG (DLVAG)“.

15. Vertraglich vereinbarte Schriftform

Die Allianz und die Allianz Unternehmen werden sich nicht auf die Unwirksamkeit von Willenserklärungen und Mitteilungen berufen, für die vertraglich die Schriftform vereinbart ist, wenn der Nutzer diese Willenserklärungen bzw. Mitteilungen im Rahmen von Meine Allianz abgibt und damit seinerseits auf das vertragliche Schriftformerfordernis verzichtet.

16. Anwendbarkeit deutschen Rechts

Für Streitigkeiten im Zusammenhang mit diesen Nutzungsbedingungen gilt deutsches Recht.

B. Besondere Nutzungsbedingungen für Versicherungen

1. Haftung

Hat der Nutzer durch ein schuldhaftes Verhalten, insbesondere durch eine Verletzung der besonderen Sorgfalts- und Sicherheitspflichten bei der Geheimhaltung von personalisierten Sicherheitsmerkmalen zur Entstehung eines Schadens beigetragen, bestimmt es sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang die Allianz/die Allianz Unternehmen und der Kunde den Schaden zu tragen haben.

2. Keine Beratung, Verantwortung für die Anlageentscheidung

Meine Allianz ermöglicht dem Vertragspartner der Allianz Lebensversicherungs-AG bzw. der Deutschen Lebensversicherungs-AG (DLVAG) den Zugang zum Service Leben dieser Unternehmen. Im Rahmen des Service Leben findet keine Beratung statt. Die Anlageentscheidung bei fondsgebundenen Versicherungen (z. B. Aufteilung der Anlagebeträge ändern oder Anteileinheiten umschichten) trifft der Vertragspartner eigenverantwortlich aufgrund seiner eigenen Informationen und Kenntnisse. Das Risiko und die Verantwortung für seine Anlageentscheidung trägt der Vertragspartner in vollem Umfang selbst.

C. Kontaktdaten Meine Allianz

Allianz Deutschland AG
Allianz Online Service
10900 Berlin
Tel.: 0800 4520104
E-Mail: online-service@allianz.de

Allianz Deutschland AG
Vorsitzender des Aufsichtsrats: Oliver Bäte.
Vorstand: Dr. Klaus-Peter Röhler, Vorsitzender; Fabio De Ferrari, Katja de la Viña, Bernd Heinemann, Andreas Kanning, Nina Klingspor, Frank Sommerfeld, Renate Wagner, Dr. Andreas Wimmer.
Für Umsatzsteuerzwecke: USt-IdNr.: DE 814 580 981
Finanz- und Versicherungsleistungen i.S.d. UStG / MwStSystRL sind von der Umsatzsteuer befreit.
Sitz der Gesellschaft: München
Registergericht: Amtsgericht München HRB 158878

(Stand: 15. Juli 2020)