Depot-/Kontoführung:
FONDSDEPOT BANK
an FNZ company
vermittelt durch:
Allianz

Auftrag zur Freischaltung des InfoManager in Verbindung mit der Freischaltung des Onlineportals Meine Allianz

Der Auftrag kann per **Telefax an +49 (0) 9281 820-2187** oder per Mailanhang jeweils mit Kundenunterschrift an **info-allianz@fondsdepotbank.de** gesendet werden.

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: Mit diesem Formular „Auftrag Freischaltung InfoManager Onlineportal Meine Allianz" ist keine Bevollmächtigung möglich. Eine Freischaltung erfolgt nur, wenn der nachfolgend genannte Bevollmächtigte im Depot bereits im/in o.g. Depot/s/Geldkonto/-konten hinterlegt ist.

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 – eine Marke der FNZ Bank SE

Fondsbanking

Das Fondsbanking ermöglicht die Einsichtnahme von Depotbeständen, Kontoständen, Spar- und Auszahlplänen, Depotumsätzen und persönlichen Daten über das Internet (Leseberechtigung).

Ferner kann der Nutzer Kauf-, Verkaufs- und Tauschaufträge sowie Aufträge zu Spar- und Auszahlplänen über das Internet erteilen, Überweisungsaufträge veranlassen und Daueraufträge einrichten und verwalten (Transaktionsberechtigung).

Für die Nutzung des Fondsbanking gelten die „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 Onlineportals vorzunehmen, ausgeschlossen.

Einrichtung Referenzbankverbindung/Mandatserteilung Depot

Zu meiner/unserer Sicherheit wird die Bank Aufträge zum Kauf oder Verkauf von Anteilen oder Aktien an Investmentvermögen jeglicher Art inkl. Steuererstattungsbeträge [nur Privatvermögen]) nur ausführen, wenn der Gegenwert von der genannten Referenzbankverbindung meines/unseres Depots eingezogen wird oder der Transfer des Verkaufserlöses gemäß meiner/unserer Weisung auf meine/unsere genannte Referenzbankverbindung erfolgen soll.

SEPA-Lastschriftmandat

Gläubiger-Identifikationsnummer der Bank: **DE68ZZZ00000025032**

Die Mandatsreferenz wird Ihnen nach Einrichtung des Mandats separat schriftlich mitgeteilt (z. B. bei erstmaligem Einzug einer Lastschrift).
Ich/Wir ermächtige/n die Bank, Geldbeträge von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise/n ich/wir mein/unser Kreditinstitut an, die von der Bank auf dieses Konto gezogene Lastschrift einzulösen.
Ich/Wir stelle/n sicher, dass eine SEPA-Basislastschrift von der Bankverbindung erfolgen kann und habe/n keine Sparkonten angegeben.

Wichtige Informationen:

- Ich/Wir kann/können innerhalb von 8 Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit dem kontoführenden Kreditinstitut vereinbarten Bedingungen.
- Aufträge zu Käufen und Sparplänen per Lastschrift kann ich/können wir nur auf einem gültigen Formular der Fondsdepot Bank – eine Marke der FNZ Bank SE erteilen.
- Mandatserteilung: Das SEPA-Lastschriftmandat verliert seine Gültigkeit, wenn der Zahlungspflichtige oder Zahlungsempfänger dieses schriftlich widerruft bzw. es nach dem letzten Lastschrifteinzug 36 Monate nicht in Anspruch genommen wurde. In diesen Fällen und bei Änderung des Girokontoinhabers ist die Erteilung eines neuen SEPA-Lastschriftmandates erforderlich.

Referenzbankverbindung

Girokontoinhaber (Name, Vorname/n)

Kreditinstitut (Name, Ort)

BIC

IBAN

Ort, Datum

✗

Unterschrift/en des/der Depot-/Kontoinhaber/s bzw. des/der gesetzlichen Vertreter/s (Vollmachtgeber)

Der Girokontoinhaber muss identisch sein mit dem oder einem der Inhaber bzw. mit dem oder einem der gesetzlichen Vertreter/Bevollmächtigten zu Lebzeiten und über den Tod hinaus.

Bitte zurücksenden an: Fondsdepot Bank – eine Marke der FNZ Bank SE, 95025 Hof

InfoManager

Der InfoManager ist ein elektronisches Postfach, in dem bestimmte Dokumente, die im Rahmen der Depot-/Kontoführung produziert werden (z. B. Depot-/Kontoabrechnung, Ausschüttungsmitteilungen, Kosteninformation) zum Download hinterlegt werden.

Für die Nutzung des InfoManager gelten die „Besonderen Bedingungen für die Nutzung des Fondsbanking und des InfoManager".

Ich/Wir beauftrage/n die Bank zur Freischaltung des InfoManager und veranlassen Sie die Freischaltung für o. g. Depot/s/ Geldkonto/-konten.

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

B. Das Onlineportal Meine Allianz bei der Allianz Deutschland AG

Meine Allianz ist ein Onlineportal, mit dem der/die Depot-/Geldkontoinhaber bzw. der/die gesetzliche/n Vertreter seine/ihre Verträge und Depots/Geldkonten 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 das Onlineportal Meine Allianz".

Hinweis: Durch die Freischaltung von „Meine Allianz" erhalten Sie den Zugang zu allen Leistungsmöglichkeiten des Onlineportals Meine Allianz. In diesem Zusammenhang können Sie u. a. die hinterlegte Adresse online ändern, möglicherweise bestehende Lebensversicherungsverträge einsehen sowie das Onlineportal nutzen. Lesen Sie deshalb bitte die „Nutzungsbedingungen für das Onlineportal 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 Onlineportals Meine Allianz vorzunehmen, ausgeschlossen.

Freischaltung des Depots/Geldkontos für das Onlineportal 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 Onlineportals 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 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.

Die Allianz Deutschland AG weist darauf hin, dass im Rahmen dieses Onlineportals auch die „Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager" der Fondsdepot Bank – eine Marke der FNZ Bank SE gelten.

C. Schlusserklärungen

C.1 Schlusserklärung für die Freischaltung für das Fondsbanking und den InfoManager bei der Fondsdepot Bank – eine Marke der FNZ Bank SE

Es gelten die mit diesen Unterlagen zur Verfügung gestellten „Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager".

C.2 Schlusserklärung für das Onlineportal Meine Allianz bei der Allianz Deutschland AG

Es gelten die mit diesen Unterlagen zur Verfügung gestellten „Nutzungsbedingungen für das Onlineportal Meine Allianz".

Ort, Datum

✗ Unterschrift Depot-/Geldkontoinhaber 1 bzw. Gesetzlicher Vertreter 1

✗ Unterschrift Depot-/Geldkontoinhaber 2 bzw. Gesetzlicher Vertreter 2

✗ Unterschrift Bevollmächtigter

Bitte zurücksenden an: Fondsdepot Bank – eine Marke der FNZ Bank SE, 95025 Hof

Inhalt

Folgende Bestandteile sind in diesen Unterlagen enthalten:

FONDSDEPOT BANK
an FNZ company

Geschäftsbedingungen der Fondsdepot Bank – eine Marke der FNZ Bank SE

- Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager

Besondere Bedingungen für die Nutzung des Fondsbanking und des InfoManager (Stand 1. Dezember 2024)

Anbieter: Fondsdepot Bank – eine Marke der FNZ Bank SE

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 Online Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Online Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem

mobilen Endgerät, das für das Online Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (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 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 Abrechnungen im InfoManager zur Verfügung, soweit nicht ausdrücklich Schriftform vorgeschrieben ist oder ein Wahlrecht zum Erhalt in schriftlicher Form besteht. 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/Konto in den InfoManager eingestellten Dokumente.

(3) Die Bank behält sich vor, Dokumente postalisch bzw. auf andere Weise dem Teilnehmer 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, soweit der Bank eine aktuelle E-Mail-Adresse des Teilnehmers vorliegt. 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 Teilnehmer 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 dem Teilnehmer 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.

Vertragsbedingungen der Allianz Deutschland AG

- Nutzungsbedingungen für das Onlineportal Meine Allianz

Nutzungsbedingungen für das Onlineportal Meine Allianz (gültig ab 11.01.2022)

1. Gegenstand und Geltungsbereich der Nutzungsbedingungen; Nutzungsberechtigte Personen; Kontaktdaten der Allianz

1.1 Willkommen beim Onlineportal Meine Allianz („**Meine Allianz**"), abrufbar unter https://allianz.de/meine-allianz („**Plattform**") der Allianz Deutschland AG, Königinstr. 28, 80802 München („**Allianz**").
1.2 Die Allianz bietet auf der Plattform registrierten natürlichen Personen, die das 18. Lebensjahr vollendet haben, ggf. deren gesetzlichen Vertretern bzw. Bevollmächtigten („**Privatnutzer**") und juristischen Personen sowie Personengesellschaften („**Firmennutzer**", Privatnutzer und Firmennutzer insgesamt „**Nutzer**") die Möglichkeit, die Plattform und die darauf abrufbaren Dienste auf Grundlage und gemäß den Vorgaben dieser Nutzungsbedingungen („**diese Bedingungen**") für private oder kommerzielle Zwecke, d. h. zu Zwecken der gewerblichen oder selbstständigen beruflichen Tätigkeit des Nutzers, zu nutzen. Der Nutzer erklärt sich durch das Anklicken des entsprechenden Feldes bei seiner Registrierung (vgl. Ziffer 3) mit der ausschließlichen und verbindlichen Geltung dieser Bedingungen einverstanden.
1.3 Kontaktdaten der Allianz:
Tel.: 0 800.4 52 01 04
E-Mail Privatnutzer: online-service@allianz.de
E-Mail Firmennutzer: support-firmenportal@allianz.de

2. Abrufbare Dienste; Unentgeltlichkeit

2.1 Auf der Plattform sind insbesondere folgende Dienste abrufbar:
(a) Profilverwaltung;
(b) Digitale Kommunikation;
(c) Informationen zu ausgewählten Verträgen sowie
(d) verschiedene digitale Services.
Nähere Informationen zu den in Meine Allianz einsehbaren Verträgen und verfügbaren Diensten und Services sind in den Erläuterungen auf der Internetseite https://allianz. de/service/meine-allianz („**FAQ**") abrufbar.
2.2 Die Nutzung der Plattform und der Dienste ist unentgeltlich; etwaige anfallende Kosten für die (mobile) Internetnutzung richten sich nach den Tarifen des jeweiligen Telekommunikationsanbieters.

3. Registrierung; Nutzerkonto; Zulassung; Nutzungsvereinbarung

3.1 Die Nutzung der Plattform setzt eine einmalige Registrierung des Nutzers und eine Zulassung (vgl. Ziffer 3.7) des Nutzers voraus. Ein Anspruch auf Zulassung besteht nicht; die Allianz ist berechtigt, die Zulassung ohne Angabe von Gründen zu verweigern.
3.2 Inhaber eines Nutzerzugangs zur Plattform („**Nutzerkonto**") kann ausschließlich ein einzelner Nutzer sein. Der Zugang zur Plattform und den Diensten über ein fremdes Nutzerkonto ist nicht gestattet. Das Nutzerkonto ist nicht übertragbar.
3.3 Sämtliche im Rahmen der Registrierung erfragten Daten und sonstigen Angaben sind vollständig und korrekt anzugeben. Die Allianz wird diese ggf. auf Vollständigkeit und Plausibilität überprüfen und kann zur Verifizierung der Identität und Berechtigung des Nutzers weitere Schritte vorsehen (z. B. die Eingabe von Sicherheits-Codes).
3.4 Die Registrierung eines Privatnutzers hat unter Angabe des Namens des Nutzers, seiner privaten E-Mail-Adresse und seiner Mobilfunknummer zu erfolgen.
3.5 Die Registrierung eines Firmennutzers hat durch eine vertretungsberechtigte natürliche Person unter Angabe des Namens des Firmennutzers, der Firmen-E-Mail-Adresse und der Mobilfunknummer der vertretungsberechtigten natürlichen Person zu erfolgen.
3.6 Der Nutzer hat seinen Benutzernamen und sein persönliches Passwort zu wählen. Im Nachhinein erhält er seine Zugangsnummer von der Allianz. Zugangsnummer, Benutzername und Passwort bilden zusammen die „**Login Daten**". Die Allianz behält sich vor, dem Nutzer darüber hinaus alternative Wege zur Registrierung zur Verfügung zu stellen.
3.7 Sobald die Allianz die erfragten Daten und sonstigen Angaben überprüft hat und aus ihrer Sicht keine Bedenken gegen eine Zulassung bestehen, schaltet sie den Zugang zur Plattform frei und benachrichtigt den Nutzer hierüber per E-Mail. Diese E-Mail gilt als Annahme des Antrags des Nutzers auf Zulassung auf die Plattform („**Zulassung**"); es kommt zwischen der Allianz und dem Nutzer auf Grundlage dieser Bedingungen zum Abschluss eines Vertrages über die Nutzung der Plattform und der Dienste („**Nutzungsvereinbarung**").
3.8 Ab Abschluss der Nutzungsvereinbarung und der Identifizierung ist der Nutzer zur vollumfänglichen Nutzung der Plattform und der Dienste gemäß den Vorgaben dieser Bedingungen berechtigt.

4. Änderungsvorbehalt

Im Hinblick auf den technologischen Fortschritt, die Optimierung und Weiterentwicklung der Plattform und der Dienste behält sich die Allianz vor, diese Bedingungen zu ändern, soweit dies dem Nutzer zumutbar ist. Die Allianz wird den Nutzer vorab über solche Änderungen in Textform informieren. Sofern der Nutzer einer solchen Änderung nicht innerhalb von zwei (2) Monaten nach der Information in Textform (z. B. per E-Mail an die in Ziffer 1.3 bezeichnete E-Mail-Adresse) widerspricht, gilt diese als vom Nutzer akzeptiert; die Allianz wird den Nutzer in der Information auf diesen Umstand hinweisen. Im Falle des Widerspruchs wird die Nutzungsvereinbarung (vgl. Ziffer

3.7) zu den bestehenden Bedingungen fortgesetzt. Der Allianz bleibt jedoch unbenommen, die Nutzungsvereinbarung zu kündigen, wobei ein die Allianz zur außerordentlichen Kündigung berechtigender wichtiger Grund insbesondere dann anzunehmen ist, wenn eine Fortsetzung der Nutzungsvereinbarung zu den bestehenden Bedingungen technisch nicht möglich ist.
Diese Ziffer 4 gilt nicht für Änderungen der vertraglichen Hauptleistungspflichten und nicht für wesentliche Vertragsänderungen.

5. Wechsel des Vertragspartners

5. Die Allianz ist berechtigt, die Nutzungsvereinbarung und alle ihre Rechte und Pflichten aus der Nutzungsvereinbarung auf (1.) die Allianz Kunde und Markt GmbH, Königinstraße 28, 80802 München, oder (2.) eine andere Gesellschaft des Allianz Konzerns, d.h. die Allianz SE, Königinstraße 28, 80802 München, sowie alle mit der Allianz SE gem. §§ 15. ff AktG verbundenen Unternehmen (die vorbezeichneten Unternehmen gemeinsam „**Allianz Konzernunternehmen**“) zu übertragen. Die Allianz Kunde und Markt GmbH oder das andere Allianz Konzernunternehmen tritt in diesem Fall als Vertragspartner anstelle der Allianz Deutschland AG in die Nutzungsvereinbarung ein. Die Allianz wird den Nutzer über einen Vertragspartnerwechsel mindestens zwei Monate vor dem Wirksamwerden des Wechsels informieren. Für den Fall, dass die Allianz von ihrem vorbeschriebenen Recht Gebrauch macht, steht dem Nutzer das Recht zu, die Nutzungsvereinbarung mit sofortiger Wirkung zu kündigen.

6. Login; Sicherheitsmerkmale; 2FA; Meine Allianz App

6.1 Der Nutzer muss sich für jede Nutzung der Plattform mit seinen Login Daten anmelden („**Login**“). Die Allianz behält sich vor, dem Nutzer darüber hinaus alternative Wege zum Login zur Verfügung zu stellen.
6.2 Die Allianz fordert den Nutzer auf, ausgewählte Aktionen durch die Eingabe eines Sicherheitsmerkmals, wie beispielsweise einer Transaktionsnummer (TAN), eines Sicherheits-Codes oder Ähnlichem („**Sicherheitsmerkmale**“), zu genehmigen.
6.3 Die Allianz empfiehlt, sofern verfügbar, zur Absicherung des Login-Vorgangs die Aktivierung einer Zwei-Faktor-Authentifizierung („**2FA**“), da dieses Verfahren ein zusätzliches Sicherheitsniveau bietet. Nutzer, die die 2FA aktiviert haben, müssen zusätzlich zu den Login-Daten ein weiteres Sicherheitsmerkmal (z. B. TAN) verwenden, um Zugang zur Plattform zu erhalten.
Um bestimmte Funktionen nutzen zu können (z. B. Anzeige von Inhalten mit Gesundheitsdaten), kann es notwendig sein, 2FA zu aktivieren.
6.4 Meine Allianz App
Die Allianz stellt Privatnutzern für den optimierten Zugang zur Plattform über mobile Endgeräte die Applikation „Meine Allianz App“ („**App**“) zur Verfügung. Weitere Informationen zur App (z. B. zu technischen Voraussetzungen) sind in den FAQ auf der Internetseite https://allianz.de/service/meine-allianz und im jeweiligen App Store abrufbar. Download, Installation und Nutzung der App sind ausschließlich auf Grundlage und nach Maßgabe dieser Nutzungsbedingungen gestattet. Mit Start des Downloads der App im App Store akzeptiert der Nutzer die ausschließliche und verbindliche Geltung dieser Nutzungsbedingungen; es kommt zwischen dem Nutzer und der Allianz zu einem Nutzungsverhältnis über die App auf Grundlage dieser Nutzungsbedingungen.
Wenn der Nutzer bereitgestellte Sicherheitsupdates, verbesserte Funktionalitäten oder Updates zur Fehlerbeseitigung nicht installiert, kann es zu Beeinträchtigungen der Funktionstauglichkeit der App kommen.
Die App verwendet Open Source-Komponenten, die eigenen Open Source-Bedingungen unterliegen. Die betreffenden Open Source-Komponenten und -Bedingungen sind in der App abrufbar. Die App verwendet überdies Dritt-Dienste, die eigenen Dritt-Bedingungen unterliegen. Die betreffenden Dritt-Dienste und -Bedingungen sind in der App abrufbar. Die Nutzer haben die vorgenannten Open Source- und Dritt-Bedingungen zur Kenntnis zu nehmen und akzeptieren diese. Im Falle von Widersprüchen haben die Open Source- und Dritt-Bedingungen Vorrang zu den Regelungen dieser Bedingungen. Die App steht Firmennutzern derzeit nicht zur Verfügung. Sollte die App zu einem späteren Zeitpunkt verfügbar sein, wird die Allianz dies in den FAQ klarstellen. Sollte die App für Firmennutzer verfügbar sein, gilt Ziffer 6.4 [...] entsprechend.

7. Sorgfaltspflichten und Verantwortlichkeit des Nutzers

7.1 Der Nutzer ist verpflichtet, seine im Rahmen der Registrierung angegebenen Daten (einschließlich Kontaktdaten) und sonstigen Angaben aktuell zu halten. Ändern sich diese, hat der Nutzer diese unverzüglich zu aktualisieren.
7.2 Die Allianz ergreift angemessene Maßnahmen zum Schutz der Nutzer. Dennoch haben auch die Nutzer Vorkehrungen zu treffen, um sicherzustellen, dass der Prozess, durch den sie auf die Plattform zugreifen, sie nicht dem Risiko von Viren, Schadsoftware oder sonstigen Beeinträchtigungen ihrer Computersysteme und Geräte aussetzt. Für den Zugriff auf die Plattform muss der Nutzer insbesondere (a) ausschließlich private/vertrauenswürdige Endgeräte verwenden, (b) Betriebssystem und Browser des Endgerätes auf dem neusten Stand halten und (c) Vorkehrungen zum Schutz vor Schadsoftware treffen.
7.3 Der Nutzer hat seine Login Daten und seine Sicherheitsmerkmale (zusammen „**Authentifizierungselemente**“) geheim zu halten und vor dem Zugriff Dritter zu sichern. Insbesondere ist Folgendes zum Schutz der Authentifizierungselemente zu beachten:
a) Authentifizierungselemente dürfen nicht ungesichert elektronisch gespeichert werden (zum Beispiel in dem zum TAN-Verfahren genutzten Endgerät).
b) Bei Eingabe eines Authentifizierungselements ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
c) Authentifizierungselemente dürfen nicht auf dritten Internetseiten (z. B. Online-Händler) eingegeben werden.
d) Authentifizierungselemente dürfen nicht außerhalb der Plattform weitergegeben werden, also beispielsweise nicht per E-Mail oder SMS.

BO1--000220 (25V) PDF.11.21

e) Einzelne Authentifizierungselemente dürfen nicht zusammen verwahrt werden.
7.4 Wenn der Nutzer ein mobiles Endgerät verwendet, um auf die Plattform zuzugreifen oder ein Sicherheitsmerkmal zu generieren (z. B. mTAN), hat er zusätzlich zu den in Ziffer 7.3 bezeichneten Pflichten insbesondere
a) durch geeignete Sicherheitsmaßnahmen sicherzustellen, dass das Risiko eines unbefugten Zugriffs durch einen Dritten minimiert wird (z. B. durch das Einrichten einer Display-Sperre und die Nutzung von Fingerabdruck, Gesichtserkennung oder möglichst komplexer Passwörter, Entsperrmuster und PINs zum Entsperren mit Gerätesicherheit);
b) das Betriebssystem auf seinem mobilen Endgerät auf dem neusten Stand zu halten;
c) es bei Verwendung des mTAN-Verfahrens zu unterlassen, das mobile Endgerät, auf dem er die mTAN generiert hat, gleichzeitig auch für den Zugriff auf die Plattform zu nutzen.
Der Nutzer ist für sämtliche Handlungen verantwortlich, die mithilfe seiner Authentifizierungselemente und/oder seines Nutzerkontos auf der Plattform vorgenommen werden, selbst wenn die betreffenden Handlungen nicht von ihm genehmigt oder beabsichtigt waren. Der Nutzer haftet allein für Schäden, die durch die Benutzung der Authentifizierungselemente und/oder seines Nutzerkontos durch ihn selbst oder Dritte entstehen, es sei denn, er hat die schadenverursachende Handlung nicht zu vertreten.

8. Informations- und Anzeigepflichten; Sperranzeige

8.1 Sofern der Nutzer den Verdacht hat, dass ein Dritter eines seiner Authentifizierungselemente kennt und/oder sein Nutzerkonto unberechtigt nutzt, ist er verpflichtet, seine Login Daten unverzüglich zu ändern und die Allianz unverzüglich (z. B. per E-Mail an die in Ziffer 1.3 genannten E-Mail-Adressen) über den Verdacht zu informieren („**Sperranzeige**").
8.2 Der Nutzer hat jeden Diebstahl oder Missbrauch seiner Authentifizierungselemente und/oder die unberechtigte Nutzung seines Nutzerkontos unverzüglich bei der Polizei zur Anzeige zu bringen.

9. Nutzungssperre; Löschung des Nutzerkontos

9.1 Die Allianz ist berechtigt und auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Ziffer 8.1, verpflichtet, das Nutzerkonto bzw. die Authentifizierungselemente des Nutzers zu sperren („**Nutzungssperre**") bzw. zu löschen. Die Allianz ist zu einer solchen Nutzungssperre bzw. zur Löschung des Nutzerkontos darüber hinaus berechtigt, wenn (a) die Nutzungsvereinbarung von ihr aus wichtigem Grund gekündigt werden kann, (b) sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente, dem sicheren Betrieb der Plattform selbst oder des einzelnen Nutzerkontos dies rechtfertigen, (c) der betreffende Nutzer bei der Registrierung falsche Angaben gemacht bzw. seine Angaben bei einer Änderung nicht gemäß Ziffer 7.1 aktualisiert hat, (d) sein Nutzerkonto übertragen oder anderen Personen Zugang zu diesem verschafft hat, (e) er bei der Nutzung der Plattform gegen geltende Gesetze, Verordnungen, behördliche Vorschriften, Richtlinien und Bekanntmachungen, die guten Sitten oder die Bestimmungen dieser Bedingungen verstößt oder Rechte Dritter verletzt. Ein Nutzer mit einem gesperrten oder gelöschten Nutzerkonto darf die Plattform nicht über ein anderes bestehendes oder neues Nutzerkonto nutzen (vgl. auch Ziffer 3.2).
9.2 Die Allianz wird den Nutzer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch nach der Nutzungssperre bzw. der Löschung des Nutzerkontos unterrichten.
9.3 Die Allianz wird eine Nutzungssperre aufheben oder die Authentifizierungselemente austauschen, wenn die Gründe für die Nutzungssperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Nutzer.

10. Verantwortlichkeit für Nutzerinhalte; Anforderungen an Nutzerinhalte; Meldemöglichkeit; Zusicherung

10.1 Der Nutzer ist berechtigt, bestimmte Inhalte (zum Beispiel: Bilder, Dokumente) auf der Plattform hochzuladen („**Nutzerinhalte**"). Nutzerinhalte sind ausschließlich solche des betreffenden Nutzers und stellen weder die Meinung noch eine Willenserklärung der Allianz dar.
10.2 Das Einstellen von Nutzerinhalten, die gegen geltende Gesetze, Verordnungen, behördliche Vorschriften, Richtlinien und Bekanntmachungen oder die guten Sitten verstoßen, Rechte Dritter verletzen oder bei denen es sich sonst um verbotene Inhalte im Sinne der nachfolgenden Auflistung handelt, ist den Nutzern untersagt. „**Verbotene Inhalte**" sind Nutzerinhalte, die (a) geistige Eigentumsrechte oder sonstige Rechte Dritter (Urheber-/Leistungsschutzrechte, Werktitel, Designs, Patente, Marken, Unternehmenskennzeichen etc.) verletzen, (b) gegen Datenschutz- oder Persönlichkeitsrechte verstoßen, (c) schädliche Codes (Viren, Trojaner, Würmer etc.) oder andere Programme enthalten, die Systeme, Programme, Daten etc. beschädigen oder beeinträchtigen können, (d) diffamierend bzw. verunglimpfend sind, (e) irreführend bzw. täuschend sind oder (f) in sonstiger Weise inakzeptabel sind. Die Allianz behält sich vor, verbotene Inhalte jederzeit ohne Angabe von Gründen zu löschen, soweit sie von diesen Kenntnis erlangt.
10.3 Der Nutzer sichert zu, dass er (a) die Plattform und die Dienste ausschließlich nach Maßgabe und im Rahmen dieser Bedingungen nutzen wird, (b) über sämtliche geistigen Eigentumsrechte und ggf. sonstige Rechte, Zustimmungen und/oder Erlaubnisse an seinen Nutzerinhalten verfügt, die nach Maßgabe dieser Bedingungen und/oder für die ordnungsgemäße Nutzung der Plattform und der Dienste erforderlich sind, (c) nicht in die Integrität, Verfügbarkeit und Leistungsfähigkeit der Plattform und/oder der Dienste (oder jeweils Teilen davon) eingreifen oder diese beeinträchtigen wird und (d) es sich bei seinen Nutzerinhalten nicht um verbotene Inhalte gemäß Ziffer 10.2 handelt.
10.4 Der Nutzer hat für die sichere Aufbewahrung der Originale der Nutzerinhalte Sorge zu tragen und ggf. eigene Kopien vorzuhalten. Die Allianz ist nicht verpflichtet, Nutzerinhalte über etwaige gesetzliche Aufbewahrungspflichten hinausgehend aufzubewahren.

BO1--0002Z0 (25V) PDF.11.21

11. Nutzungsrechte

11.1 Der Nutzer behält sämtliche Rechte an seinen Nutzerinhalten. Unbeschadet dessen ist es z. B. für die Durchführung des Versicherungsvertragsverhältnisses wie z. B. der Schadenregulierung erforderlich, dass der Nutzer der Allianz und den Allianz Konzernunternehmen, mit denen der Nutzer den betreffenden Versicherungsvertrag geschlossen hat, die nachfolgenden eingeschränkten Nutzungsrechte einräumt.

11.2 Mit ihrem Einstellen auf der Plattform räumt der Nutzer der Allianz und den Allianz Konzernunternehmen, mit denen der Nutzer den betreffenden Versicherungsvertrag geschlossen hat, an seinen Nutzerinhalten das einfache, unentgeltliche, sublizensierbare Recht ein, diese räumlich unbeschränkt ausschließlich im Rahmen und zu den Zwecken der Durchführung des Versicherungsvertragsverhältnisses zu nutzen.

11.3 Die Allianz ist Inhaberin bzw. Lizenznehmerin des gesamten geistigen Eigentums an der Plattform, der App und den Diensten, einschließlich etwaiger Inhalte, die die Allianz im Zusammenhang mit der Plattform bereitstellt („**Allianz Inhalte**"), der der Plattform und der App zugrunde liegenden Software, den Systemen, der Texte, Grafiken, Icons sowie des Audio- und Videomaterials.

11.4 Dem Nutzer ist es nur gestattet, die Plattform, die App und die Dienste, einschließlich der Allianz Inhalte, (oder jeweils Teile davon) auf der Plattform oder in der App selbst und entsprechend den dortigen Funktionalitäten im Rahmen und gemäß den Vorgaben dieser Bedingungen zu nutzen. Insoweit räumt die Allianz ein jederzeit widerrufliches, auf die Dauer des Nutzungsverhältnisses beschränktes, einfaches und nicht-übertragbares Nutzungsrecht ein. Vorbehaltlich einer Erlaubnis durch unabdingbare gesetzliche Bestimmungen oder diese Bedingungen, ist es dem Nutzer ohne vorherige schriftliche Zustimmung der Allianz insbesondere nicht gestattet, (a) den Programm- oder Quellcode der Plattform, der App oder der Dienste (oder jeweils Teile davon) zu bearbeiten, umzugestalten, zu adaptieren, zu übersetzen, zu vervielfältigen, anzugleichen, zu veröffentlichen, zu dekompilieren, zu zerlegen oder zurückzuentwickeln (sog. Reverse Engineering) oder den Quellcode auf andere Weise festzustellen sowie abgeleitete Werke hiervon zu erstellen, (b) Allianz Inhalte über den bestimmungsgemäßen Gebrauch auf der Plattform oder App hinaus zu speichern (z. B. auf Datenträgern und Abspielgeräten), zu vervielfältigen und an Dritte weiterzugeben oder solche Handlungen zu unterstützen, (c) technische Beschränkungen zu umgehen, (d) Allianz Inhalte systematisch zu Zwecken der Wiederverwendung zu extrahieren (z. B. durch Data Mining, Robots und/oder ähnliche Datensammel- und Extraktionsprogramme), (e) die Plattform, die App oder die Dienste in einer Weise zu nutzen, die mit dem Geschäftsmodell der Plattform im Wettbewerb steht, oder (f) Urhebervermerke, Logos und sonstige Kennzeichen oder Schutzvermerke zu entfernen, zu ändern oder unkenntlich zu machen. Die Bestimmungen der §§ 69d, 69e UrhG bleiben unberührt.

12. Digitale Kommunikation; E-Mail statt Brief

12.1 Die Allianz stellt dem Nutzer auf der Plattform unter anderem ein elektronisches Postfach zur Verfügung („**Postfach**"). Das Postfach dient der digitalen Kommunikation im Zusammenhang mit Vertragsverhältnissen des Nutzers mit Allianz Konzernunternehmen. Die Allianz benachrichtigt den Nutzer per E-Mail, wenn ein neues Dokument in sein Postfach eingestellt wurde.
Ein Anspruch des Nutzers 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.

12.2 Falls der Privatnutzer am Programm „**E-Mail statt Brief**" teilnimmt, gilt Folgendes: Der Nutzer erklärt sich damit einverstanden,
dass er (a) Unterlagen (z. B. Rechnungen) zu allen aktuellen und künftigen Verträgen mit Allianz Konzernunternehmen nicht mehr per Post erhält; ausgewählte Dokumente wie zum Beispiel solche, die dem Gesetz nach schriftlich vorliegen müssen, versendet die Allianz weiterhin per Post; und (b) seine Unterlagen per E-Mail erhält.
Zusätzlich werden die Unterlagen in sein Postfach auf der Plattform eingestellt.
Die Allianz verwendet für den E-Mail-Versand 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 hiermit 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.
„E-Mail statt Brief" steht Firmennutzern derzeit nicht zur Verfügung. Sollte dies zu einem späteren Zeitpunkt möglich sein, wird die Allianz dies in den FAQ klarstellen. Falls die Teilnahme von Firmennutzern am Programm „E-Mail statt Brief" möglich ist und ein Firmennutzer teilnimmt, gilt Ziffer 12.2 Absätze [1–4] entsprechend.

12.3 Der Nutzer ist verpflichtet, sein Postfach regelmäßig auf den Eingang neuer Nachrichten und Dokumente zu kontrollieren und diese eventuell auszudrucken oder abzuspeichern. Die Kontrolle ist insbesondere dann vorzunehmen, wenn aufgrund eines zuvor erteilten Auftrags mit der Einstellung neuer Dokumente zu rechnen ist oder der Nutzer über das Einstellen eines neuen Dokuments benachrichtigt wurde. Eine Verpflichtung zum nachträglichen unentgeltlichen Versand von Dokumenten nach Beendigung dieser Nutzungsvereinbarung besteht nicht, sofern dazu keine gesetzliche oder vertragliche Verpflichtung besteht.

BO1--0002Z0 (25V) PDF.11.21

12.4 Die im Postfach eingestellten Dokumente werden den Nutzern im PDF-Format zur Verfügung gestellt. Die Allianz garantiert die Unveränderbarkeit der Daten, sofern die Daten im Postfach gespeichert oder aufbewahrt werden. Werden Dokumente außerhalb des Postfachs gespeichert, aufbewahrt oder in veränderter Form in Umlauf gebracht, übernimmt die Allianz hierfür keine Haftung.
12.5 Im Postfach werden die Informationen für einen Zeitraum von mindestens 24 Monaten nach deren Einstellung vorgehalten. Nach 24 Monaten kann die Allianz die Informationen auch ohne vorherige Mitteilung an den Nutzer aus dem elektronischen Postfach entfernen.
12.6 Der Privatnutzer wird über wichtige Bearbeitungsschritte seiner Anliegen per E-Mail und/oder per SMS informiert. Der Nutzer kann die Benachrichtigungsfunktion jederzeit ändern oder deaktivieren.
12.7 Die Benachrichtigungsfunktion steht Firmennutzern derzeit nicht zur Verfügung. Sollte dies zu einem späteren Zeitpunkt möglich sein, wird die Allianz dies in den FAQ klarstellen. Falls die Benachrichtigungsfunktion für Firmennutzer zur Verfügung steht, gilt Ziffer 12.6 entsprechend.

13. Gewährleistung

13.1 Der Nutzer nimmt zur Kenntnis und akzeptiert, dass der Zugriff auf die Plattform von Unterbrechungen, Fehlern oder Verzögerungen betroffen sein kann. Diese können u. a. auf notwendigen Instandsetzungs- oder Wartungsarbeiten zum Zweck des korrekten Ablaufs oder der Verbesserung, Optimierung und/oder Weiterentwicklung der Plattform, auf technischen Problemen bei der Ausführung oder dem Betrieb der Plattform oder auf technischen Problemen oder hohem Datenaufkommen im Internet oder Infrastrukturausfällen beruhen.
13.2 Bei einer Datenübertragung über das Internet kann keine vollständige Sicherheit garantiert werden. Die Allianz bemüht sich um einen angemessenen Schutz, kann jedoch die Sicherheit der vom Nutzer an die Allianz übermittelten Inhalte/Daten nicht gewährleisten. Vielmehr erfolgt jede Übermittlung von Inhalten/Daten an die Allianz auf eigenes Risiko des Nutzers. Die Haftungsregelungen gemäß Ziffer 14 bleiben unberührt.

14. Haftung

14.1 Die Allianz haftet
a) im Umfang einer übernommenen Garantie sowie
b) nach den Vorschriften des Produkthaftungsgesetzes.
14.2 Im Übrigen haftet die Allianz im Rahmen der unentgeltlichen Nutzung der Plattform und der Dienste
a) für Sach- oder Rechtsmängel, soweit die Allianz den jeweiligen Mangel arglistig verschwiegen hat, sowie
b) für sonstige Pflichtverletzungen bei Vorsatz und grober Fahrlässigkeit.
In allen übrigen Fällen ist eine Haftung der Allianz – gleich, aus welchem Rechtsgrund – ausgeschlossen.
14.3 Die Regelungen dieser Ziffer 14 gelten auch zugunsten der gesetzlichen Vertreter, Erfüllungs- und Verrichtungsgehilfen der Allianz.

15. Haftungsfreistellung

15.1 Der Nutzer ist verpflichtet, die Allianz von sämtlichen Ansprüchen Dritter und hierdurch entstehenden Anwalts- und Gerichtskosten in angemessener Höhe freizustellen, sofern diese auf einer der nachfolgend aufgeführten Vertrags- oder Rechtsverletzungen des Nutzers beruhen:
(a) der Verletzung jeglicher Bestimmung dieser Bedingungen durch den Nutzer;
(b) der Beanstandung Dritter, dass die vom Nutzer eingestellten Nutzerinhalte geistige Eigentumsrechte (Urheber-/Leistungsschutzrechte, Patente, Marken, Unternehmenskennzeichen, Werktitel, Designs etc.) oder sonstige Rechte anderer (Persönlichkeitsrechte, einschließlich Rechte am eigenen Bild etc.) verletzen.
15.2 Für den Fall einer Drittinanspruchnahme der Allianz gemäß Ziffer 15.1 ist der Nutzer verpflichtet, der Allianz auf Anfrage unverzüglich, wahrheitsgemäß und vollständig sämtliche Informationen bereitzustellen, die für die Prüfung der Drittansprüche und eine etwaige Rechtsverteidigung erforderlich sind.
15.3 Eine über diese Ziffer 15 hinausgehende Haftung des Nutzers bleibt unberührt.

16. Laufzeit und Beendigung der Nutzungsvereinbarung

16.1 Die Nutzungsvereinbarung läuft auf unbestimmte Zeit.
16.2 Der Nutzer kann die Nutzungsvereinbarung jederzeit ohne Einhaltung einer Kündigungsfrist kündigen. Die Allianz kann die Nutzungsvereinbarung jederzeit mit einer Kündigungsfrist von sechs Wochen kündigen.
16.3 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.
16.4 Kündigungen bedürfen der Textform (bei einer Kündigung des Nutzers z. B. per E-Mail an die in Ziffer 1.3 bezeichnete E-Mail-Adressen). Die Allianz behält sich vor, dem Nutzer darüber hinaus alternative Wege zur Kündigung zur Verfügung zu stellen.
16.5 Im Falle einer ordentlichen Kündigung durch den Nutzer räumt die Allianz dem Nutzer die Möglichkeit ein, die Plattform für einen Übergangszeitraum von sechs Wochen („**Übergangszeitraum**“) weiter zu nutzen, insbesondere um Dokumente u.a. zu sichern. Macht der Nutzer von dieser Möglichkeit Gebrauch, gelten diese Bedingungen auch für den Übergangszeitraum.
16.6 Die Allianz behält sich vor, die Logindaten des betreffenden Nutzers nach Wirksamwerden der Kündigung bzw. im Falle von Ziffer 16.5 nach Ablauf des Übergangszeitraums zu sperren und das Nutzerkonto inklusive aller dort hinterlegten Daten (Dokumente, etc.) zu löschen. Die Allianz wird den Nutzer darauf hinweisen. Der Nutzer erhält von der Allianz eine Bestätigungs-E-Mail, sobald das Nutzerkonto gelöscht ist. Das Recht der Allianz zur Nutzungssperre und Löschung des Nutzerkontos gemäß Ziffer 9 bleibt hiervon unberührt.
16.7 Kündigt der Nutzer die Nutzungsvereinbarung, endet mit Zugang der Kündigung eine etwaige Teilnahme des Nutzers an „E-Mail statt Brief“ (Ziffer 12.2). Kündigt die Allianz die Nutzungsvereinbarung, endet eine etwaige Teilnahme des Nutzers an „E-Mail statt Brief“ zum Zeit-

BO1--0002Z0 (25V) PDF.11.21

punkt der Beendigung der Nutzungsvereinbarung.
16.8 Ist der Nutzer aus einem Versicherungsvertrag mit der Allianz oder einem Allianz Konzernunternehmen verpflichtet, die Plattform zu nutzen, gelten im Falle einer Kündigung die Regelungen des jeweiligen Versicherungsvertrages.

17. Datenschutz

Der Schutz der Daten des Nutzers ist für die Allianz sehr wichtig. Informationen zur Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Plattform finden sich in den Datenschutzhinweisen zum Onlineportal Meine Allianz.

18. Links auf externe Webseiten

Die Plattform enthält Verknüpfungen („**Links**“) zu externen Webseiten Dritter („**externe Webseiten**“). Die externen Webseiten unterliegen der Haftung ihrer jeweiligen Betreiber. Die Allianz hat bei der erstmaligen Verknüpfung der externen Webseiten deren Gestaltung und fremde Inhalte („**Fremdinhalte**“) auf bestehende Rechtsverstöße überprüft. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Die Allianz hat keinerlei Einfluss auf die aktuelle und zukünftige Gestaltung der externen Webseiten und deren Fremdinhalte. Das Setzen von Links bedeutet nicht, dass sich die Allianz die hinter den Links liegenden Fremdinhalte zu eigen macht; eine ständige Kontrolle dieser Fremdinhalte ist für die Allianz ohne konkrete Hinweise auf Rechtsverstöße nicht zumutbar. Bei Kenntnis von Rechtsverstößen wird die Allianz die betreffenden Links jedoch unverzüglich löschen. Die Nutzer werden gebeten, jegliche (auch nur möglicherweise) bestehenden Rechtsverstöße, die sie auf den externen Webseiten sehen, der Allianz zu melden. Dies kann z. B. per E-Mail an die in Ziffer 1.3 genannte E-Mail-Adresse erfolgen.
19. Anwendbares Recht; Gerichtsstand; salvatorische Klausel
19.1 Es gilt ausschließlich deutsches Recht unter Ausschluss des UN-Kaufrechts.
19.2 Im Geschäftsverkehr mit Vollkaufleuten, juristischen Personen des öffentlichen Rechts und öffentlich-rechtlichen Sondervermögen gilt das Landgericht München I als ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesen Bedingungen und/oder der Nutzungsvereinbarung.
19.3 Die Allianz nimmt nicht an Streitbeilegungsverfahren vor Verbraucherschlichtungsstellen teil.
19.4 Sollte eine Bestimmung dieser Bedingungen unwirksam sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Allianz und der Nutzer sind in einem solchen Fall verpflichtet, an der Schaffung von Bestimmungen mitzuwirken, durch die ein der unwirksamen Bestimmung wirtschaftlich möglichst nahekommendes Ergebnis rechtswirksam erzielt wird. Das Vorstehende gilt für die Schließung etwaiger Vertragslücken entsprechend.

BO1--0002Z0 (25V) PDF.11.21