Deutsche Bank
Aktiengesellschaft

Formular zurücksetzen

Vollmacht zur Nachlassabwicklung

Filialnr. | Kundennummer

Filialnr. | Kundennummer

Filialnr. | Kundennummer

Erblasser (Kontoinhaber)

Angaben zum Bevollmächtigten

Vorname/n

Nachname

Geburtsname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Telefon

Familienstand

Alle Staatsangehörigkeiten (1. und ggf. weitere)

Angaben zum Steuerumgehungsbekämpfungsgesetz (StUmgBG)

☐ Ich bin in Deutschland steuerlich ansässig.

Deutsche (Steuer-) Identifikationsnummer (IdNr.)

☐ Ich bin nicht in Deutschland steuerlich ansässig.

Hinweis: Nach der AO müssen Banken für jeden Kontoinhaber, Verfügungsberechtigten und wirtschaftlich Berechtigten die IdNr., die W-IdNr. oder ersatzweise bei nicht-nat. Personen die Steuernummer, nach FKAustG die st. Ansässigkeit erheben. Auch im Falle einer nicht steuerlichen Ansässigkeit in Deutschland können Sie eine deutsche Steuer ID besitzen. Bei Nichtangabe der Steuerkennziffern erfolgt ein Abruf beim, ggf. eine Meldung an das BZSt.

Ich/Wir bevollmächtige/n hiermit die oben genannte Person, mich/uns gegenüber der Deutsche Bank AG für die Nachlassabwicklung des oben genannten Erblassers zu vertreten:

1. Umfang der Vollmacht
Der Bevollmächtigte ist berechtigt, über die bei der Bank bestehenden Kontoguthaben und Depots des Verstorbenen zu verfügen. Die Vollmacht erstreckt sich auch auf Schrankfächer und Verwahrstücke.

Diese Vollmacht gilt auch für Unterkonten und/oder Unterdepots. Die Verfügungen des Bevollmächtigten sind der Bank gegenüber auch dann uneingeschränkt wirksam, wenn der Bevollmächtigte zu eigenen Gunsten oder zu Gunsten Dritter verfügt. Dementsprechend darf der Bevollmächtigte der Bank Weisungen und Aufträge jeder Art – vor allem zum An- und Verkauf von Wertpapieren – erteilen und Kontoauszüge, Depotaufstellungen, Abrechnungen und sonstige Schriftstücke für mich/uns entgegen nehmen, prüfen und anerkennen.

2. Auflösung von Konten und Depots
Der Bevollmächtigte ist zur Auflösung der Konten und Depots berechtigt.

3. Geltungsdauer
Diese Vollmacht erlischt nicht mit meinem/unserem Tode.

4. Widerruf
Diese Vollmacht kann von mir/uns oder meinen/unseren Erben gegenüber der Bank widerrufen werden. Bei einem Widerruf ist die Bank unverzüglich und aus Beweisgründen schriftlich zu unterrichten.

Der Widerruf eines oder mehrerer Vollmachtgeber oder eines von mehreren Erben bringt die Vollmacht nur für den Widerrufenden zum Erlöschen. Der Bevollmächtigte kann dann von der Vollmacht nur noch gemeinsam mit dem Widerrufenden Gebrauch machen. Die Bank kann verlangen, dass sich der Widerrufende als Erbe ausweist.

Anmeldung der Filial-Kundennummer/n für das Online-Banking

☐ Hiermit melde ich/wir das/die Konto/Konten, Depot/-s unter der/den oben genannten Filial-/Kundennummer/n für das Online-Banking an.

Für Online Überweisungen wird ein Verfügungsrahmen von 2.500 Euro pro Tag beantragt, wenn nachstehend kein abweichender Rahmen beantragt wird.

Abweichend beantragter Verfügungsrahmen:

EUR

Damit kann der Bevollmächtigte in dem von der Bank angebotenem Umfang das Online-Banking nutzen (z.B. Kontoumsätze einsehen, In- und Auslandsüberweisungen tätigen, Depotumsätze einsehen und Wertpapieraufträge erteilen).

Ausstattung mit Zugangsdaten

Sofern der Bevollmächtigte bereits über persönliche Zugangsdaten für das Online-Banking verfügt, gelten diese auch für die oben genannte Filial-/Kundennummer/n. Andernfalls werden diese an die Adresse des Bevollmächtigten gesandt.

BestSign

Für das Online-Banking der Deutsehe Bank wird neben den Zugangsdaten (ID und Passwort) ein BestSign-Sicherheitsverfahren benötigt.

Falls BestSign bereits in einem bestehenden Online-Zugang genutzt wird, kann dieses ebenfalls für die oben genannte/n Filial-/Kundennummer/n verwendet werden.

Falls nicht, benötigt der Bevollmächtigte die Deutsche Bank App auf einem Smartphone oder ein separates BestSign-Gerät.

Die Deutsche Bank App wird kostenfrei im Google PlayStore (für Android) und im App Store (für iOS) angeboten.

Alle Informationen und Anleitungen zu BestSign sind unter www.deutsche-bank.de/bestsign zufinden.

Einbeziehung der Geschäftsbedingungen

Es gelten die Allgemeinen Geschäftsbedingungen der Bank. Ergänzend gelten die Bedingungen für den Zugang zur Bank über elektronische Medien, die Bedingungen für den Electronic Bronking Service (EBS), die Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking, die Sonderbedingungen zur Nutzung der Deutsche Bank InfoServices und die Bedingungen für Zahlungen mittels paydirekt.

Der Wortlaut der einzelnen Regelungen kann in den Geschaftsräumen der Bank oder unter www.deutsche-bank.de eingeschen werden. Sie werden auf Wursch ausgehändigt oder zugesandt.

Deutsche Bank
Aktiengesellschaft

Vollmacht zur Nachlassabwicklung

Filialnr.	Kundennummer	
Filialnr.	Kundennummer	
Filialnr.	Kundennummer	

Erblasser (Kontoinhaber)

Besondere Hinweise zur sofortigen Vertragsausführung

☐ Ich/Wir erkläre/-n mich/uns ausdrücklich damit einverstanden, dass die Bank nach Annahme meines Vertragsantrages auf Abschluss des Vertrages, aber noch vor Ablauf der Widerrufsfrist mit der Ausführung dieses Vertrages beginnt.

Datenschutzrechtlicher Hinweis

Datenschutzrechtliche Hinweise zu AO, GwG, StUmgBG, FKAustG und FATCA
Personenbezogene Daten in Bezug auf den/die Konteninhaber, Verfügungsberechtigte und wirtschaftlich Berechtigte i. S. d. GwG müssen von der Bank nach den o. g. rechtlichen Rahmenbedingungen erhoben werden. Die hier erhobenen personenbezogenen Daten (z. B. Name, Anschrift, Ansässigkeit, Steuerkennziffern, Jahresendsaldo/-wert, Gesamtbruttobetrag der Zinsen, Dividenden, Verkaufserlöse und im Falle von jur. Personen Informationen über Anteilsbesitz oder Stimmrecht/Kontrollmöglichkeiten) werden dabei auch für bereits bestehende und künftige Geschäftsbeziehungen genutzt, soweit gesetzliche Vorgaben eine entsprechende Datenverarbeitung auch für diese Zwecke erforderlich machen. Sollten Sie Ihrer Mitwirkungspflicht, z. B. im Rahmen der Eröffnung einer neuen Kundenverbindung, nicht innerhalb von 14 Tagen nachkommen und können wir die steuerlichen Informationen auch nicht aus anderem Anlass rechtmäßig erfassen, werden wir maschinell die relevanten steuerlichen Informationen beim BZSt erfragen. Sofern die gesetzlich vorgeschriebenen zu erhebenden Daten aufgrund unzureichender Mitwirkung nicht ermittelt werden konnten, sind wir verpflichtet, dies dem BZSt mitzuteilen. Konten mit Auslandsbezug werden ggf. für CRS/FATCA -Zwecke über das BZSt ausländischen Steuerbehörden gemeldet.

Datum	Ort

Unterschrift — Unterschrift des Bevollmächtigten[1]
X

Unterschrift — 1. Unterschrift des Vollmachtgebers
X

Unterschrift — 2. Unterschrift des Vollmachtgebers
X

Unterschrift — 3. Unterschrift des Vollmachtgebers
X

[1] Diese Unterschrift hinterlegt die Bank als Unterschriftsprobe.

Unterschrift — 4. Unterschrift des Vollmachtgebers
X

Unterschrift — 5. Unterschrift des Vollmachtgebers
X

Unterschrift — 6. Unterschrift des Vollmachtgebers
X

Empfangsbestätigung

Ich/Wir bestätige/n den Erhalt der folgenden Unterlagen:
— Bedingungen für den Zugang zur Bank über elektronische Medien,
— Bedingungen für den Electronic Broking Service (EBS),
— Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking.

Unterschrift — Unterschrift des Bevollmächtigten
X

Unterschrift — 1. Unterschrift des Vollmachtgebers
X

Unterschrift — 2. Unterschrift des Vollmachtgebers
X

Unterschrift — 3. Unterschrift des Vollmachtgebers
X

Unterschrift — 4. Unterschrift des Vollmachtgebers
X

Unterschrift — 5. Unterschrift des Vollmachtgebers
X

Unterschrift — 6. Unterschrift des Vollmachtgebers
X

Deutsche Bank
Aktiengesellschaft

Vollmacht zur Nachlassabwicklung

Filialnr. | Kundennummer |

Filialnr. | Kundennummer |

Filialnr. | Kundennummer |

Erblasser (Kontoinhaber)

Angaben zu den Vollmachtgebern

Zu 1

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Zu 2

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Zu 3

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Zu 4

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Zu 5

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Zu 6

Vorname/n

Nachname

Geburtsdatum | Geburtsort

Straße | Haus-Nr.

PLZ | Ort

Deutsche Bank
Aktiengesellschaft

Vollmacht zur Nachlassabwicklung

Filialnr. | Kundennummer

Filialnr. | Kundennummer

Filialnr. | Kundennummer

Erblasser (Kontoinhaber)

Wird von der Bank ausgefüllt

Vorgelegter Ausweis des Bevollmächtigten

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Vorgelegter Ausweis der Vollmachtgeber

Zu 1

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Zu 2

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Zu 3

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Zu 4

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Zu 5

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Zu 6

Art der Urkunde

Ausstellungsdatum | Nr./Aktenzeichen

Ausstellende Behörde

Die Unterschriften der Vollmachtgeber und des Bevollmächtigten wurden überprüft

Datum | Ort

Unterschrift R

Unterschrift GZ

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

Stand: 09/2019

1. Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels elektronischer Zugangsmedien, im Einzelnen Online-Banking und Telefon-Banking (jeweils einzeln „Online-Banking" bzw. „Telefon-Banking" sowie gemeinsam „Zugangsmedien" bzw. „elektronische Medien"), in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online- und Telefon-Banking abrufen. Im Rahmen des Online-Bankings sind sie gemäß § 675f Absatz 3 BGB zusätzlich berechtigt, Zahlungsauslösedienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen sorgfältig ausgewählte sonstige Drittdienste nutzen. Hinweis: Im Rahmen von maxblue bietet die Bank keine Anlageberatung an.

(2) Kunde und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet.

(3) Für die Nutzung der Zugangsmedien gelten die mit der Bank gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der elektronischen Medien

(1) Der Teilnehmer kann Bankgeschäfte über elektronische Medien abwickeln, 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 bestimmten 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[1] erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind

— Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. die persönliche Identifikationsnummer [PIN] oder das persönliche Passwort),
— Besitzelemente, also etwas, was nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder Empfang von einmal verwendbaren Transaktionsnummern [TAN], 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 das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

(5) Je nach Authentifizierungsverfahren und -instrument benötigt der Teilnehmer hierfür gegebenenfalls geeignete Hard- und Software. Über das Angebot der bankeigenen Anwendungen hinaus bleibt der Teilnehmer selbst für die Beschaffung, Installation und Pflege dieser Hard- und Software verantwortlich.

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

(6) Bei einer Nutzung einer Hard- bzw. Software von Drittanbietern durch den Teilnehmer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

3. Zugang über elektronische Medien

(1) Der Teilnehmer erhält Zugang zu Online- und Telefon-Banking der Bank, wenn

— dieser die Kontonummer oder seinen individuellen Benutzernamen angibt und
— er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
— keine Sperre des Zugangs (siehe Nummer 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online- und Telefon-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge[1] 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 Authentifizierungselementes 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 Daten (§ 1 Absatz 26 Satz 2 ZAG).

4. Aufträge[1]

4.1 Auftragserteilung

(1) Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN oder Übertragung einer elektronischen Signatur als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

(2) Der Teilnehmer kann Telefon-Banking-Aufträge nur nach erfolgreicher Autorisierung mit von der Bank bereitgestelltem Personalisiertem Sicherheitsmerkmal erteilen. Die Bank bestätigt den Eingang des Auftrags auf dem vom Teilnehmer für den Auftrag gewählten Zugangsweg. Die zwischen der Bank und dem Kontoinhaber übermittelte Telefonkommunikation wird zu Beweiszwecken automatisch aufgezeichnet und gespeichert.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Online- und Telefon-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im Online- und Telefon-Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen[1] durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online- und Telefon-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auf-

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

trag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis" bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß dem „Preis- und Leistungsverzeichnis" der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

— Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
— Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
— Das Online-Banking-Datenformat ist eingehalten.
— Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten.
— Im Telefon-Banking wird die Bank Verfügungen über das Konto, die eine Zahlung[1] an einen Dritten (abweichende Kontonummer) enthalten, bis zu einem Betrag von insgesamt unter 50.000 EUR pro Tag ausführen, sofern nicht ein anderer Verfügungshöchstbetrag mit dem Teilnehmer vereinbart ist. Für Überträge (Überweisungen) innerhalb der gleichen Kundennummer oder An- und Verkäufe von Wertpapieren gilt diese Betragsgrenze nicht.
— Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. 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 (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für Wertpapiergeschäfte) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels Online- bzw. Telefon-Banking oder postalisch informieren.

6. Information des Kunden über Online- und Telefon-Bankingverfügungen[1]

Die Bank unterrichtet den Kunden mindestens einmal monatlich über die mittels Online- und Telefon-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungsinstrumente

(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- und Telefon-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

(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 außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden.
   — nicht ungesichert außerhalb des zugelassenen Authentifizierungsverfahrens elektronisch gespeichert werden (z. B. PIN im Klartext im Computer oder im mobilen Endgerät) und
   — nicht auf einem Gerät notiert sein oder als Abschrift zusammen mit einem Gerät, das als Besitzelement (z. B. mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient, aufbewahrt werden.

b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

   — ist 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 des Mobiltelefons).
   — dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
   — muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Online-Banking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ein 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.

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

(3) Beim mobileTAN-Verfahren darf das mobile Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

(4) Die für das mobileTAN-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 (siehe Nummer 1 Absatz 1 Satz 3 dieser Bedingungen) verwenden. Möchte der Teilnehmer einen sonstigen Drittdienst nutzen (siehe Nummer 1 Absatz 1 Satz 4 dieser Bedingungen), hat er diesen mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

(6) Der Aufforderung per elektronischer Nachricht (z. B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.

(7) Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie PIN, Geheimzahl oder Passwort/TAN gefragt wird, dürfen nicht beantwortet werden. Die Nutzung von Zahlungsauslösediensten bzw. Kontoinformationsdiensten bleibt hiervon unberührt.

(8) Der Teilnehmer hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf dem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete System- und Anwendungssoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Teilnehmer den Internetseiten der Bank entnehmen.

(9) Die Softwareanwendungen der Bank sind ausschließlich direkt von der Bank oder von einem von der Bank benannten Anbieter zu beziehen.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Bank zum Online-Banking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten. Darüber hinaus hat der Kunde in eigener Verantwortung etwaige Sicherheitshinweise der Anbieter der eingesetzten Kundensysteme zu beachten (z. B. Sicherheitsupdates von Systemsoftware mobiler Endgeräte).

7.3 Prüfung durch Abgleich der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Daten (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilem Endgerät oder Lesegerät). Der Teilnehmer ist verpflichtet, vor der Autorisierung (z. B. Eingabe der TAN) die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen. Stimmen die angezeigten Daten nicht überein, ist der Vorgang abzubrechen und die Bank unverzüglich zu informieren.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

— den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät, Signaturkarte) oder
— die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine 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 vom Teilnehmer bezeichneten Banking-Zugang für ihn oder alle Teilnehmer oder
— seine Authentifizierungselemente zur Nutzung des Online-Banking.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online- und Telefon-Banking-Zugang für einen Teilnehmer sperren oder ein Authentifizierungsinstrument nicht mehr zulassen, wenn

— sie berechtigt ist, den Online- und Telefon-Banking-Vertrag aus wichtigem Grund zu kündigen,
— sachliche Gründe im Zusammenhang mit der Sicherheit seiner Authentifizierungselemente dies rechtfertigen,
— der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht oder
— ein genutzter Zugangsweg bzw. ein im Zusammenhang mit einem Authentifizierungsverfahren zugelassenes Gerät von der Bank als unsicher eingestuft wird. Als Zugangsweg gelten auch Softwareanwendungen der Bank in allen zur Verfügung stehenden Versionen.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre postalisch, telefonisch oder online unter-

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

richten. 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. Der Teilnehmer kann eine von ihm veranlasste Sperrung nur postalisch oder mit telefonisch legitimiertem Auftrag aufheben lassen.

9.4 Automatische Sperre eines chipbasierten Besitzelements

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

(2) Wird die Geheimzahl zur WebSign-Chipkarte bzw. zur personalisierten Electronic-Banking-Karte dreimal hintereinander (Karten ab Bestelldatum 09/2012) bzw. achtmal hintereinander (Karten vor Bestelldatum 09/2012) falsch eingegeben, wird die Karte automatisch gesperrt.

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

(4) Die in den Absätzen 1, 2 und 3 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. Vereinbarung eines elektronischen Kommunikationswegs

(1) Der Kunde und die Bank vereinbaren, dass die Bank mit dem Nutzer elektronisch kommunizieren kann, d. h. per E-Mail über die durch den Nutzer angegebene E-Mail-Adresse.

(2) Der Kunde ist damit einverstanden, entsprechende Mitteilungen unverschlüsselt per E-Mail zu erhalten. Insbesondere ist die Bank berechtigt, dem Kunden Änderungen ihrer Allgemeinen Geschäftsbedingungen und der besonderen Bedingungen für einzelne Geschäftsbeziehungen auf diesem Weg zu übermitteln. Personenbezogene Daten werden auf diesem Weg nicht übertragen.

11. Haftung

11.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags[1] und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einer nicht autorisierten Online- und Telefon-Banking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten Online-/Telefon-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für Wertpapiergeschäfte).

11.2. Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

11.2.1. Haftung des Kunden für nicht autorisierte Zahlungsvorgänge[1] vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

— es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
— der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten 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 3
— 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 nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat. Eine starke

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

Bedingungen für den Zugang zur Deutsche Bank AG (nachstehend Bank) über elektronische Medien

Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Inhärenz (siehe Nr. 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 dieser Bedingungen nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kunde kein Verbraucher, gilt ergänzend Folgendes:

— Der Kunde haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 EUR 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, 1. Punkt findet keine Anwendung.

11.2.2. Haftung 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.

11.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-/Telefon-Banking-Verfügungen[1] entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2.4 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.

[1] Zum Beispiel Überweisung, Dauerauftrag und Lastschrift

Deutsche Bank
Aktiengesellschaft

Bedingungen für den Electronic Broking Service (EBS)

Für die Teilnahme am Electronic Broking Service (EBS) gelten ergänzend zu den „Bedingungen für den Zugang zur Bank über elektronische Medien“ die folgenden Bedingungen:

1. Leistungsumfang

Der Depotinhaber kann in Abhängigkeit von der konkreten Ausgestaltung der jeweiligen EBS Online-Anwendung (z. B. Internet-Broking) den Electronic Broking Service auf seinem Personal-Computer nutzen, um

— Informationen und Analysen über seine in den Electronic Broking Service einbezogenen Konten und Depots zu erhalten,
— Aufträge zum Kauf von Wertpapieren aus der EBS-Wertpapierpalette zu Lasten seiner in den Electronic Broking Service einbezogenen Konten nach Maßgabe der Ziffer 2 dieser Bedingungen zu erteilen,
— Aufträge zum Verkauf von Wertpapieren aus der EBS-Wertpapierpalette zu Lasten seiner im Electronic Broking Service geführten Depots zu tätigen,
— Informationen, Stammdaten, Kennzahlen und Einschätzungen, soweit vorhanden, zu den in der Wertpapierpalette des EBS geführten Wertpapiergattungen zu erhalten,
— Kursinformationen zu den in der Wertpapierpalette des EBS geführten Wertpapieren zu beziehen und Devisenkurse zu den wichtigsten Währungen abzufragen.

Die Bank erbringt im Rahmen des Electronic Broking Service keine Anlageberatung. Auch die vorgenannten Informationen, Stammdaten, Kennzahlen und Einschätzungen stellen keine Anlageberatung dar. Sie dienen ausschließlich dem Zweck, den Kunden in die Lage zu versetzen, eine selbstständige Anlageentscheidung zu treffen.

Alle Einzelheiten über den Umfang des Dienstleistungsangebotes der Bank im Rahmen der jeweiligen EBS Online-Anwendung sind in einer Benutzeranleitung enthalten, die mit der jeweiligen Software zur Verfügung gestellt wird.

2. Risikoklassenprüfung bei Kaufaufträgen

Die Bank ordnet jedem Verfügungsberechtigten auf der Grundlage seiner Angaben im KapitalAnlageCheck/Kundenangaben zum Wertpapiergeschäft eine persönliche Erfahrungs-Risikoklasse zu. Abhängig von der Depotform vergibt die Bank außerdem für bestimmte Unterdepots eine Depot-Risikoklasse auf der Grundlage der Angaben des Depotinhabers und teilt diese dem Depotinhaber mit. Über den Electronic Broking Service erteilte Kaufaufträge des Depotinhabers führt die Bank ungeachtet der vorgenannten Risikoklassen aus. Soweit eine andere verfügungsberechtigte Person als der Depotinhaber einen Kaufauftrag erteilt, wird dieser nur bis zur Grenze der Depot-Risikoklasse ausgeführt.

3. Zugang zum Electronic Broking Service

EBS Online-Anwendungen können so ausgestaltet sein, dass der Kunde Zugang zu der Online-Nutzung durch Eingabe eines frei wählbaren persönlichen Kennworts erhält. Die Eingabe des persönlichen Kennworts ergänzt in diesen Fällen das Zugangsverfahren durch Eingabe von PIN und, falls im Einzelfall vorgesehen, TAN (Ziff. 4.1 der „Bedingungen für den Zugang zur Bank über elektronische Medien“). Einzelheiten werden dem Kunden jeweils in der Benutzerführung angezeigt.

4. Auftragserteilung zum Kauf und Verkauf von Wertpapieren

Aufträge zum Kauf bzw. Verkauf von Wertpapieren sind vom Kunden erst dann erteilt, wenn er die bei aufgebauter Online-Verbindung von der Bank zurückgesandte Rückmeldung im Bildschirmdialog bestätigt und die Order damit freigibt. Der in der Rückmeldung enthaltene voraussichtliche Kurswert beruht auf dem zuletzt verfügbaren Kurs aus den Systemen der Bank. Dieser Betrag dient lediglich als Richtgröße für den Kunden und entspricht weder dem genauen Preis des Ausführungsgeschäfts noch entspricht er dem endgültigen Abrechnungsbetrag der Wertpapiertransaktion. Der Preis des Ausführungsgeschäfts wird erst mit der Orderausführung an der Börse bestimmt; der endgültige Abrechnungsbetrag enthält zusätzlich das Entgelt der Bank und die von ihr in Rechnung gestellten Auslagen einschließlich fremder Kosten.

5. Orderänderung und Orderlöschung

Soweit einzelne EBS Online-Anwendungen die Möglichkeit vorsehen, erteilte Aufträge zum Kauf bzw. Verkauf von Wertpapieren nachträglich zu ändern oder zu löschen, bestehen diese Änderungs- und Widerrufsmöglichkeiten nur, sofern der ursprüngliche Wertpapierauftrag zwischenzeitlich noch nicht ausgeführt wurde. Maßgeblich ist dabei nicht der im „Orderbuch“ des Kunden ausgewiesene Orderstatus; dieser stellt keine Echtzeit-Information dar, sondern unterliegt aus technischen Gründen einer Zeitverzögerung. Entscheidend für die Möglichkeit der Orderänderung und Orderlöschung (Widerruf) ist vielmehr ausschließlich, ob diese Nachricht so rechtzeitig eingeht, dass die Bank die Ausführung des ursprünglichen Wertpapierauftrags tatsächlich noch verhindern kann.

6. Ausführungsplatz/Ausführungsart

Bei über EBS Online-Anwendungen erteilten Aufträgen zum Kauf oder Verkauf von Wertpapieren können Ausführungsplatz und Ausführungsart festgelegt werden. Wird kein Ausführungsplatz und keine Ausführungsart festgelegt, erfolgt die Ausführung gemäß den ‚Grundsätzen für die Ausführung von Aufträgen in Finanzinstrumenten‘ der Bank. Aus technischen Gründen können für einzelne Wertpapiere nicht alle in Betracht kommenden Börsenplätze systemseitig vorgegeben werden. In diesem Fall beschränkt sich das Weisungsrecht des Kunden im Rahmen des EBS auf die systemseitig vorgesehenen Ausführungsorte. Die Möglichkeit der andersweitigen Auftragserteilung, z. B. unmittelbar über den Kundenberater, besteht in jedem Fall.

7. Informationen, Meinungsaussagen, Einschätzungen

Die über den Electronic Broking Service abrufbaren Informationen, Stammdaten, Kennzahlen und Marktkurse bezieht die Bank aus öffentlich zugänglichen Quellen und von Dritten, die sie für zuverlässig hält. Eine Garantie für die Richtigkeit oder Vollständigkeit der Angaben kann die Bank nicht übernehmen und keine Aussage ist als solche Garantie zu verstehen. Alle Meinungsaussagen geben die aktuelle Einschätzung eines der Researchteams der Bank wieder. Die zum Ausdruck gebrachten Meinungen können sich ohne vorherige Ankündigung ändern. Weder die Bank noch deren übrige assoziierte Unternehmen haften für die Verwendung der über den Electronic Broking Service abgerufenen Informationen, Stammdaten, Kennzahlen, Marktdaten und Einschätzungen und deren Inhalt.

Deutsche Bank
Aktiengesellschaft

Bedingungen für den Electronic Broking Service (EBS)

8. Geheimhaltung der Berechtigungsmerkmale

EBS Online-Anwendungen stehen als persönliche Instrumente ausschließlich dem Depotinhaber zur Verfügung. Sieht die jeweilige EBS Online-Anwendung ein persönliches Kennwort des Kunden vor, gelten für dieses die Regelungen über die Geheimhaltung der PIN und der TAN in Ziff. 7 der „Bedingungen für den Zugang zur Bank über elektronische Medien" entsprechend.

Mit dem Bezug seiner Konto- und Depotdaten und deren Abspeicherung auf dem Personalcomputer ist der Kunde für die Geheimhaltung dieser Daten selbst verantwortlich.

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und die „Sonderbedingungen für Wertpapiergeschäfte", die in jeder Geschäftsstelle eingesehen werden können und die auf Wunsch dem Kunden zugesandt werden.

Filialnummer + Kundennummer/kontoführende Filiale (Ort, Straße)

Konto-/Depotbezeichnung

Ich (wir) möchte/-n den Electronic Broking Service der Deutsche Bank AG zu den oben stehenden Bedingungen, einschließlich Erteilung von Wertpapieraufträgen, nutzen.

Datum/Ort

Unterschrift

X

Deutsche Bank
Aktiengesellschaft

Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking

Stand: 02/2025

Präambel

Kunden der Deutsche Bank AG (im Folgenden „Bank") haben die Möglichkeit, im Online-Banking ein digitales Postfach (im Folgenden „Postfach") zu nutzen. Das Postfach nutzt die Bank, um dem Kunden Bankdokumente zukommen zu lassen, die der Kunde dann in digitaler Fassung abrufen, herunterladen und speichern kann. Das Postfach dient der Kommunikation zwischen Bank und Kunden.

1. Allgemeines

1.1 Das Postfach ist ein elektronischer Briefkasten, in dem für den Kunden bestimmte persönliche Mitteilungen der Bank (im Folgenden „Bankmitteilungen") in elektronischer Form verschlüsselt und dauerhaft abrufbar eingestellt werden.

1.2 Die Bank behält sich das Recht vor, das Postfach und zugehörige Funktionalitäten teilweise oder insgesamt weiterzuentwickeln, zu ändern oder zu ergänzen.

2. Aktivierung des Postfachs

2.1 Die Aktivierung des Postfachs setzt einen hierauf gerichteten Antrag zum Online-Banking bzw. Service-Portal angemeldeten Kunden voraus. Der Antrag kann auch im Zusammenhang mit der Beantragung des Online-Banking Zugangs, der Eröffnung einer Kundenverbindung oder einer Produkteröffnung gestellt werden.

2.2 Die Annahme des Antrags seitens der Bank erfolgt durch die Freischaltung des Postfachs.

3. Voraussetzung und Zugangswege

Der Kunde benötigt zur Nutzung des Postfachs einen Internetzugang, eine gültige und üblicherweise für die Kommunikation mit Dritten verwendete E-Mail-Adresse, einen aktuellen, marktüblichen Internetbrowser und/oder einen Zugang zum jeweiligen Online-Banking oder sonstigen von der Bank zugelassen Zugang über elektronische Medien (z.B. Mobile Banking App) sowie eine Zugangsberechtigung (z.B. mittels aktivem TAN-Verfahren) bei der Bank.

4. Zugang zum Postfach und Nutzungsrecht

4.1 Der Zugang zum Postfach erfolgt über eine Anmeldung im Online-Banking, Service-Portal oder sonstigen von der Bank zugelassenen Zugang über elektronische Medien.

4.2 Bei der erstmaligen Anmeldung mit einem noch nicht für das Postfach autorisierten Gerät muss die Anmeldung im Postfach mit einer TAN bestätigt werden.

4.3 Der Kunde hat mit der TAN-Bestätigung die Möglichkeit, das Gerät als vertrauenswürdig einzustufen, sodass keine wiederholte Eingabe einer TAN notwendig ist. Der Kunde kann sich mit der Anmeldung in seinem Online-Banking, Service-Portal oder sonstigen von der Bank zugelassenen Zugang über elektronische Medien dann automatisch im Postfach anmelden.

5. Leistungsangebot und -umfang

5.1 Im Postfach werden dem Kunden Bankmitteilungen in elektronischer Form eingestellt, soweit dies nach den gesetzlichen Vorgaben zulässig ist. Dabei handelt es sich insbesondere um folgende vertragsrelevante Bankerklärungen und vertraglich, gesetzlich und aufsichtsrechtlich geschuldete Informationen:

- Vertragsangebote,
- Bankmitteilungen unter anderem zu Allgemeinen Geschäftsbedingungen sowie ggfs. deren Änderungen, Preisverzeichnis etc.,
- Kontoauszüge, Kontoabrechnungen, Zinsänderungen, Mitteilungen zu eingeräumten Kontoüberziehungen (z. B. DispoKredit, Kreditlinien etc.) und zu geduldeten Kontoüberziehungen (z. B. Sollzinsen, Inanspruchnahmen, Beratungsangebote, Änderungen zur Höhe eines Dispokredites etc.),
- Informationen, Mitteilungen und Erklärungen zum Inhalt, der Durchführung und der Beendigung von Darlehensverträgen (z. B. Zins- und Tilgungsplan, Saldenmitteilung, Angebot eines neuen gebundenen Sollzinssatzes nach Auslauf der Sollzinsbindung etc.),
- Wertpapierabrechnungen, regelmäßige Berichte über Finanzinstrumente oder Wertpapierdienstleistungen (z. B. Berichte nach Art. 59 f. Delegierte Verordnung (EU) 2017/565 etc.), Informationen zu Kapitalmaßnahmen (z. B. Dividendenzahlungen, Kapitalerhöhungen etc.), Informationen zu Finanzinstrumenten sowie Verkaufsunterlagen etc.
- Mahnungen, Kündigungsandrohungen und Kündigungserklärungen.

5.2 Der Kunde kann die Bankmitteilungen dauerhaft online abrufen, herunterladen, speichern oder löschen. Das Löschen einer Mitteilung erfolgt durch den Kunden und ist endgültig.

5.3 Die Nutzung des Postfachs ist ausschließlich dem Kunden selbst und den von ihm hierzu berechtigten Personen vorbehalten.

5.4 Über den Eingang von Bankmitteilungen wird der Kunde mindestens einmal täglich an die von ihm mitgeteilte E-Mail-Adresse benachrichtigt.

6. Einstellung von Bankmitteilungen

6.1 Die Bank kommt ihrer Verpflichtung zur Übermittlung, Unterrichtung oder Zurverfügungstellung von Bankmitteilungen auf einem dauerhaften Datenträger durch deren Einstellung in das Postfach nach. Hiervon bleiben etwaige Aufbewahrungspflichten der Bank (vgl. Nr. 7.3) unberührt.

6.2 Mit der Einrichtung des Postfachs ist der Kunde nach Maßgabe dieser Bedingungen ausdrücklich damit einverstanden, dass kein postalischer Versand der in das Postfach einzustellenden Bankmitteilungen stattfindet. Hiervon umfasst sind Bankmitteilungen sowohl für aktuelle als auch für zukünftig vom Kunden gewählte Bankleistungen, insbesondere auch diejenigen, die der Textform unterliegen. Die Bestimmung unter Nr. 1.2 bleibt unberührt.

6.3 Die Bankmitteilungen gehen dem Kunden spätestens einen Tag nach dem Zeitpunkt zu, in dem die Bank die Mitteilungen in das Postfach eingestellt und den Kunden über den Eingang von Bankmitteilungen per E-Mail informiert hat.

6.4 Kann die E-Mail-Benachrichtigung nicht zugestellt werden (z. B. wenn die E-Mail Adresse nicht mehr gültig ist), kann die Bank den Kunden kontaktieren. Die Bankmitteilungen können papierhaft zur Verfügung gestellt werden. Die Bank stellt dem Kunden hierfür kein Entgelt, sondern nur ihren Aufwendungsersatz (insbesondere Porto) in Rechnung.

Bedingungen zur Nutzung des digitalen Postfachs im Online-Banking

7. Speicherung der Bankmitteilungen

7.1 Die Bank speichert die eingestellten Bankmitteilungen während der Gesamtdauer der Nutzung des Online-Bankings durch den Kunden im Rahmen einer bestehenden Konto- oder Depotverbindung.

7.2 Die Bank stellt die Unveränderbarkeit der in das Postfach eingestellten und dort gespeicherten Bankmitteilungen im Rahmen einer bestehenden Konto- oder Depotverbindung sicher.

7.3 Die Bank ist innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit in der Lage, dem Kunden auf dessen Anforderung eine papierhafte Ausfertigung dieser Bankmitteilungen zur Verfügung zu stellen. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

8. Gewährleistung und Haftung

8.1 Das Postfach ist üblicherweise entsprechend der Online-Banking Funktionalität und vorbehaltlich üblicher Wartungsfenster ständig verfügbar. Für Störungen, insbesondere für vorübergehende, technisch bedingte Zugangsbeschränkungen zum Postfach, haftet die Bank nur bei Vorsatz und grober Fahrlässigkeit und stellt die Postfach Funktionalität lediglich in der jeweils aktuellen Form bereit. Soweit aus technischen Gründen ausnahmsweise Wartungsarbeiten mit Auswirkungen auf die Postfach Funktionalität erforderlich werden, wird die Bank den Kunden nach Möglichkeit rechtzeitig im Online-Banking oder auf einem anderen Weg (z.B. postalisch) darüber informieren.

8.2 Für die Anbindung an das Internet und zugehöriger Netzverbindung auf Kundenseite trägt der Kunde selbst Sorge. Im Falle länger anhaltender Störungen kann die Bank für Bankmitteilungen andere Kommunikationswege (z. B. postalischer Versand) nutzen.

9. Kündigung

9.1 Der Kunde kann das Postfach jederzeit ohne Angabe von Gründen kündigen. Eine Kündigung kann auch im Online-Banking erfolgen.

9.2 Die Bank kann das Postfach nach Nr. 19 ihrer Allgemeinen Geschäftsbedingungen kündigen.

10. Folgen der Kündigung

10.1 Die Bank wird dem Kunden die für das Postfach vorgesehenen Bankmitteilungen nach Kündigung des Postfachs auf einem vereinbarten oder neu zu vereinbarenden Weg zukommen lassen. Ein hierfür ggf. anfallendes Entgelt ergibt sich aus dem Preis- und Leistungsverzeichnis der Bank.

10.2 Die bis zu diesem Zeitpunkt in das Postfach eingestellten Bankmitteilungen bleiben für den Kunden weiterhin abrufbar. Hierfür benötigt der Kunde weiterhin eine gültige E-Mail-Adresse, einen aktuellen, marktüblichen Internetbrowser, einen Zugang zum jeweiligen Online-Banking sowie eine Zugangsberechtigung (z.B. mittels aktivem TAN-Verfahren) bei der Bank.

11. Folgen der Beendigung der Geschäftsbeziehung

11.1 Bei Beendigung der Geschäftsbeziehung, Schließung des Online-Banking Zugangs, Service-Portals oder sonstigen von der Bank zugelassenen Zugangs über elektronische Medien werden die zu diesem Zeitpunkt im Postfach eingestellten Bankmitteilungen – sofern noch nicht vom Kunden gelöscht – für einen Zeitraum von vier Jahren weiterhin über einen Download-Link zur Verfügung gestellt. Die Frist beginnt einen Tag nach Beendigung der Geschäftsbeziehung, des Online-Bankings, Service-Portals oder sonstigen von der Bank zugelassenen Zugangs über elektronische Medien.

11.2 Der Link wird dem Kunden per E-Mail zugesendet. Ein entsprechendes Passwort, welches den Zugriff des Kunden auf den Link legitimiert, wird dem Kunden auf postalischem Weg zur Verfügung gestellt.

12. Datenschutz

Die Bank verarbeitet die personenbezogenen Daten des Kunden im Rahmen der geltenden Datenschutzgesetze ausschließlich zu den oben unter Nr. 1 genannten Zwecken. Der Kunde bzw. dessen Vertretungsberechtigter trägt dafür Sorge, dass im Rahmen einer Bevollmächtigung persönliche Mitteilungen und darin enthaltene personenbezogene Daten betreffend seine Person durch den Bevollmächtigten legitim zur Kenntnis genommen werden dürfen. Hinsichtlich weiterführender datenschutzrechtlicher Informationen wird verwiesen auf die geltenden Datenschutzhinweise des Online-Banking der Bank.

13. Ergänzende Geltung der Allgemeinen Geschäftsbedingungen

Ergänzend gelten die Allgemeinen Geschäftsbedingungen und Sonderbedingungen der Bank, insbesondere die Bedingungen für den Zugang zur Bank über elektronische Medien und die Bedingungen für den Verzicht auf papierhafte Kontoauszüge, die in den Geschäftsräumen der Bank oder unter www.deutsche-bank.de/agb eingesehen werden können und dem Kunden auf Wunsch zur Verfügung gestellt werden.

Datenschutzhinweise gemäß EU-Datenschutz-Grundverordnung für „Natürliche Personen“

Stand: 02/2026

Mit den nachfolgenden Informationen geben wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch uns und Ihre Rechte aus dem Datenschutzrecht. Welche Daten im Einzelnen verarbeitet und in welcher Weise genutzt werden, richtet sich maßgeblich nach den jeweils beantragten bzw. vereinbarten Dienstleistungen.

Bitte geben Sie die Informationen auch den aktuellen und künftigen vertretungsberechtigten Personen und wirtschaftlichen Berechtigten sowie etwaigen Mitverpflichteten eines Kredites weiter. Dazu zählen z. B. Begünstigte im Todesfall, Prokuristen oder Bürgen.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden

Verantwortliche Stelle ist:

Deutsche Bank AG
Taunusanlage 12
60325 Frankfurt am Main
Telefon: (069) 910-10000
Fax: (069) 910-10001
E-Mail-Adresse: deutsche.bank@db.com

Sie erreichen unseren betrieblichen Datenschutzbeauftragten unter

Deutsche Bank AG
Datenschutzbeauftragter
Taunusanlage 12
60325 Frankfurt am Main
Telefon: (069) 910-10000
E-Mail-Adresse: datenschutz.db@db.com

2. Welche Quellen und Daten nutzen wir

Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von unseren Kunden erhalten. Zudem verarbeiten wir – soweit für die Erbringung unserer Dienstleistung erforderlich – personenbezogene Daten, die wir von anderen Unternehmen der Deutsche Bank-Gruppe oder von sonstigen Dritten (z. B. SCHUFA) zulässigerweise (z. B. zur Ausführung von Aufträgen, zur Erfüllung von Verträgen oder aufgrund einer von Ihnen erteilten Einwilligung) erhalten haben. Zum anderen verarbeiten wir personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Grundbücher, Handels- und Vereinsregister, Presse, Medien, Internet) zulässigerweise gewonnen haben und verarbeiten dürfen.

Relevante personenbezogene Daten im Interessentenprozess, bei der Stammdateneröffnung, im Zuge einer Bevollmächtigung (Kontovollmacht und/oder Kreditkarteninhaber) oder als Mitverpflichteter eines Kredits (z. B. Bürge) können sein:

Name, Adresse/andere Kontaktdaten (Telefon, E-Mail-Adresse), Geburtsdatum/-ort, Geschlecht, Staatsangehörigkeit, Familienstand, Geschäftsfähigkeit, Berufsgruppenschlüssel/Partnerart (unselbständig/selbständig), Wohnstatus (Miete/Eigentum), Legitimationsdaten (z. B. Ausweisdaten), Authentifikationsdaten (z. B. Unterschriftsprobe), Steuer-ID, FATCA-Status, SCHUFA-Score, Kennzeichnung EU-Basiskonto.

Bei Abschluss und Nutzung von Produkten/Dienstleistungen aus den im Folgenden aufgelisteten Produktkategorien können zusätzlich zu den vorgenannten Daten weitere personenbezogene Daten erhoben, verarbeitet und gespeichert werden. Diese umfassen im Wesentlichen:

Konto und Zahlungsverkehr (inkl. Online-Banking)

Auftragsdaten (z. B. Zahlungsaufträge), Daten aus der Erfüllung unserer vertraglichen Verpflichtungen (z. B. Zahlungsverkehrsdaten).

Spar- und Einlagen

Daten aus der Erfüllung unserer vertraglichen Verpflichtungen (z. B. Umsätze), steuerliche Informationen (z. B. Angabe zur Kirchensteuerpflicht), Angaben zu etwaigen Drittbegünstigten, Lastschriftdaten, Dokumentationsdaten (z. B. Beratungsprotokolle).

Wertpapiergeschäft

Angaben zu Kenntnissen und/oder Erfahrungen mit Wertpapieren (MiFID-Status), Anlageverhalten/-strategie (Umfang, Häufigkeit, Risikobereitschaft), Beruf, finanzielle Situation (Vermögen, Verbindlichkeiten, Einkünfte aus un-/selbständiger Arbeit/Gewerbebetrieb, Ausgaben), absehbare Änderungen in den Vermögensverhältnissen (z. B. Eintritt Rentenalter), konkrete Ziele/wesentliche Anliegen in der Zukunft (z. B. geplante Anschaffungen, Ablösung Verbindlichkeiten), steuerliche Informationen (z. B. Angabe zur Kirchensteuerpflicht), Dokumentationsdaten (z. B. Geeignetheitserklärungen).

Bausparen

Bausparvertragsnummer, Basis-/Steuerdaten, Tarife, Zuteilungs-/Auszahlungsdaten, staatliche Förderung, Umsatzdaten/-verlauf, Lastschriftdaten, Drittrechte, Qualitätsdaten.

Lebens- und Rentenversicherungen, Erwerbs-/Berufsunfähigkeits- und Pflegeversicherung, private Krankenversicherung

Versicherungsnummer, Produktdaten (z. B. Tarif, Leistung, Beitrag), Dokumentationsdaten (z. B. Beratungsprotokolle). Sofern eine Anlage der Beiträge in Wertpapieren erfolgt, werden die personenbezogenen Daten unter Punkt 2.3 Wertpapiergeschäft herangezogen.

Kreditkarten

Beruf, Einkommen, Mietkosten bzw. Rate Baufinanzierung, unterhaltsberechtigte Kinder, bei Nicht-EU-Staatsangehörigen Aufenthalts-/Arbeitserlaubnis.

Konsumentenfinanzierung (Verbraucher)

Bonitätsunterlagen (Einkommen, Ausgaben, Fremdkontoauszüge), Arbeitgeber, Art und Dauer Beschäftigungsverhältnis, Anzahl unterhaltspflichtiger Kinder, bei Nicht-EU-Staatsangehörigen Aufenthalts-/Arbeitserlaubnis, Scoring-/Ratingdaten, Verwendungszweck, Dokumentationsdaten (z. B. Beratungsprotokolle).

Baufinanzierung (Verbraucher und Selbständige)

Bonitätsunterlagen (Gehaltsabrechnungen, Einnahmen-/Überschussrechnungen und Bilanzen, Steuerunterlagen, Angaben/Nachweise zu Vermögen und Verbindlichkeiten, übernommene Bürgschaften, Fremdkontoauszüge, Ausgaben), Arbeitgeber, Art und Dauer Beschäftigungsverhältnis, Art und Dauer der Selbständigkeit, Anzahl unterhaltspflichtiger Kinder, Güterstand, bei Nicht-EU-Staatsangehörigen Aufenthalts-/Arbeitserlaubnis, Scoring-/Ratingdaten, Angaben/Nachweise zum Verwendungszweck, Eigen- und Fremdsicherheiten: Objektunterlagen (z. B. Grundbuchauszüge, Objektbewertungen), Dokumentationsdaten (z. B. Beratungsprotokolle).

Datenschutzhinweise gemäß EU-Datenschutz-Grundverordnung für „Natürliche Personen“

Gewerbliche Finanzierung (Selbständige)

Bonitätsunterlagen geschäftlich: Einnahmen-/Überschussrechnungen, Bilanzen, betriebswirtschaftliche Auswertung, Art und Dauer der Selbständigkeit.

Bonitätsunterlagen privat: Selbstauskunft mit Angaben zu Ein- und Ausgaben sowie Vermögen und Verbindlichkeiten, Gehaltsabrechnungen, Steuerunterlagen, Nachweise zu Vermögen, übernommene Bürgschaften, Anzahl unterhaltspflichtiger Kinder, Güterstand, bei Nicht-EU-Staatsangehörigen Aufenthalts-/Arbeitserlaubnis, Scoring-/Ratingdaten privat, Angaben/Nachweise zum Verwendungszweck, Informationen zu gestellten Sicherheiten, Objektunterlagen (z. B. Grundbuchauszüge, Objektbewertungen).

Bei persönlichen Bürgschaften durch Dritte (Fremdsicherheiten) können von der Bank an den jeweiligen Bürgen vergleichbare Anforderungen zur Offenlegung der wirtschaftlichen und finanziellen Verhältnisse gestellt werden.

Zins- und Währungsmanagement

Angaben zu Kenntnissen und/oder Erfahrungen mit Zins-/Währungsprodukten/Geldanlage (MiFID-Status), Anlageverhalten/-strategie (Umfang, Häufigkeit, Risikobereitschaft), Beruf, finanzielle Situation (Vermögen, Verbindlichkeiten, Einkünfte aus un-/selbständiger Arbeit/Gewerbebetrieb, Ausgaben), absehbare Änderungen in den Vermögensverhältnissen (z. B. Eintritt Rentenalter), konkrete Ziele/wesentliche Anliegen in der Zukunft (z. B. geplante Anschaffungen, Ablösung Verbindlichkeiten), steuerliche Informationen (z. B. Angabe Kirchensteuerpflicht), Dokumentationsdaten (z. B. Beratungsprotokolle).

Kundenkontaktinformationen

Im Rahmen der Geschäftsanbahnungsphase und während der Geschäftsbeziehung, insbesondere durch persönliche, telefonische oder schriftliche Kontakte, durch Sie oder von der Bank initiiert, entstehen weitere personenbezogene Daten, z. B. Informationen über Kontaktkanal, Datum, Anlass und Ergebnis; (elektronische) Kopien des Schriftverkehrs sowie Informationen über die Teilnahme an Direktmarketingmaßnahmen.

Digitale Services

Hinsichtlich der beim Einsatz von digitalen Serviceprodukten verarbeiteten Daten wird verwiesen auf weiterführende Informationen zum Datenschutz im Zusammenhang mit dem jeweiligen digitalen Service (Bsp.: Verarbeitung von Umsatzdaten eingebundener Fremdbankkonten im Rahmen der Multibanken-Aggregation bei Benutzung der Applikation FinanzPlaner).

3. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage

Wir verarbeiten die vorab genannten personenbezogenen Daten im Einklang mit den Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG):

a. Zur Erfüllung von vertraglichen Pflichten (Artikel 6 Abs.1 b DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt zur Erbringung von Bankgeschäften und Finanzdienstleistungen im Rahmen der Durchführung unserer Verträge mit unseren Kunden oder zur Durchführung vorvertraglicher Maßnahmen, die auf Ihre Anfrage hin erfolgen.

Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem konkreten Produkt (siehe unter Punkt 2) und können unter anderem Bedarfsanalysen, Beratung, Vermögensverwaltung und -betreuung sowie die Durchführung von Transaktionen umfassen. Die weiteren Einzelheiten zum Zweck der Datenverarbeitung können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.

b. Im Rahmen der Interessenabwägung (Artikel 6 Abs. 1 f DSGVO)

Soweit erforderlich, verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten. Beispiele:

- Konsultation von und Datenaustausch mit Auskunfteien (z. B. SCHUFA) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken und des Bedarfs beim Pfändungsschutzkonto oder Basiskonto
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und zu direkter Kundenansprache; inkl. Kundensegmentierungen und Berechnung von Abschlusswahrscheinlichkeiten
- Werbung oder Markt- und Meinungsforschung, soweit Sie der Nutzung Ihrer Daten nicht widersprochen haben
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten
- Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank
- Verhinderung von Straftaten
- Videoüberwachungen zur Wahrung des Hausrechts, zur Sammlung von Beweismitteln bei Überfällen und Betrugsdelikten oder zum Nachweis von Verfügungen und Einzahlungen, z. B. an Geldautomaten
- Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen)
- Maßnahmen zur Sicherstellung des Hausrechts
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten
- Risikosteuerung im Konzern

c. Aufgrund Ihrer Einwilligung (Artikel 6 Abs. 1 a DSGVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Weitergabe von Daten im Verbund/Konzern) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der EU-Datenschutz-Grundverordnung, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen. Eine Statusübersicht der von Ihnen erteilten Einwilligungen können Sie jederzeit bei uns anfordern bzw. teilweise im Online-Banking einsehen.

Datenschutzhinweise gemäß EU-Datenschutz-Grundverordnung für „Natürliche Personen“

d. Aufgrund gesetzlicher Vorgaben (Artikel 6 Abs.1 c DSGVO) oder im öffentlichen Interesse (Artikel 6 Abs.1 e DSGVO)

Zudem unterliegen wir als Bank diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z. B. Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze) sowie bankaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht). Zu den Zwecken der Verarbeitung gehören unter anderem die Kreditwürdigkeitsprüfung, die Identitäts- und Altersprüfung, Betrugs- und Geldwäscheprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken in der Bank und im Konzern.

4. Wer bekommt meine Daten

Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Dienstleister und Erfüllungsgehilfen können zu diesen Zwecken Daten erhalten, wenn diese das Bankgeheimnis und unsere schriftlichen datenschutzrechtlichen Weisungen wahren. Dies sind im wesentlichen Unternehmen aus den im Folgenden aufgeführten Kategorien.

Im Hinblick auf die Datenweitergabe an Empfänger außerhalb der Bank ist zunächst zu beachten, dass wir als Bank zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis gemäß Nr. 2 unserer Allgemeinen Geschäftsbedingungen). Informationen über Sie dürfen wir nur weitergeben, wenn gesetzliche Bestimmungen dies gebieten, Sie eingewilligt haben, wir zur Erteilung einer Bankauskunft befugt sind und/oder von uns beauftragte Auftragsverarbeiter gleichgerichtet die Einhaltung des Bankgeheimnisses sowie die Vorgaben der EU-Datenschutz-Grundverordnung/des Bundesdatenschutzgesetzes garantieren.

Unter diesen Voraussetzungen können Empfänger personenbezogener Daten z. B. sein:

— Öffentliche Stellen und Institutionen (z. B. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht, Europäische Bankenaufsichtsbehörde, Europäische Zentralbank, Finanzbehörden, Bundeszentralamt für Steuern) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.

— Andere Kredit- und Finanzdienstleistungsinstitute, vergleichbare Einrichtungen und Auftragsverarbeiter, an die wir zur Durchführung der Geschäftsbeziehung mit Ihnen personenbezogene Daten übermitteln. Im Einzelnen: Abwicklung von Bankauskünften, Unterstützung/Wartung von EDV-/IT-Anwendungen, Archivierung, Belegbearbeitung, Callcenter-Services, Compliance-Services, Controlling, Datenscreening für Anti-Geldwäsche-Zwecke, Datenvernichtung, Einkauf/Beschaffung, Flächenmanagement, Immobiliengutachten, Kreditabwicklungsservice, Sicherheitenverwaltung, Beitreibung, Zahlkartenabwicklung (Debitkarten/Kreditkarten), Kundenverwaltung, Lettershops, Marketing, Medientechnik, Meldewesen, Research, Risikocontrolling, Spesenabrechnung, Telefonie, Videolegitimation, Webseitenmanagement, Wertpapierdienstleistung, Aktienregister, Fondsverwaltung, Wirtschaftsprüfungsdienstleistung, Zahlungsverkehr.

Weitere Datenempfänger können diejenigen Stellen sein, für die Sie Ihre Einwilligung zur Datenübermittlung erteilt haben bzw. für die Sie uns vom Bankgeheimnis gemäß Vereinbarung oder Einwilligung befreit haben.

5. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt

Eine Datenübermittlung in Länder außerhalb der EU bzw. des EWR (sogenannte Drittstaaten) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (z. B. Zahlungs- und Wertpapieraufträge) erforderlich, gesetzlich vorgeschrieben ist (z. B. steuerrechtliche Meldepflichten), Sie uns eine Einwilligung erteilt haben oder im Rahmen einer Auftragsdatenverarbeitung. Werden Dienstleister im Drittstaat eingesetzt, sind diese zusätzlich zu schriftlichen Weisungen durch die Vereinbarung der EU-Standardvertragsklauseln zur Einhaltung des Datenschutzniveaus in Europa verpflichtet.

6. Wie lange werden meine Daten gespeichert

Wir verarbeiten und speichern Ihre personenbezogenen Daten, solange es für die Erfüllung unserer vertraglichen und gesetzlichen Pflichten erforderlich ist. Dabei ist zu beachten, dass unsere Geschäftsbeziehung ein Dauerschuldverhältnis ist, welches auf mehrere Jahre angelegt ist.

Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese regelmäßig gelöscht, es sei denn, ihre – befristete – Weiterverarbeitung ist zu folgenden Zwecken erforderlich:

— Erfüllung handels- und steuerrechtlicher Aufbewahrungsfristen: Zu nennen sind das Handelsgesetzbuch, die Abgabenordnung, das Kreditwesengesetz, das Geldwäschegesetz und das Wertpapierhandelsgesetz. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre.

— Erhaltung von Beweismitteln im Rahmen der Verjährungsvorschriften. Nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) können diese Verjährungsfristen bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist drei Jahre beträgt.

7. Welche Datenschutzrechte habe ich

Jede betroffene Person hat das Recht auf Auskunft nach Artikel 15 DSGVO, das Recht auf Berichtigung nach Artikel 16 DSGVO, das Recht auf Löschung nach Artikel 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO, das Recht auf Widerspruch aus Artikel 21 DSGVO sowie das Recht auf Datenübertragbarkeit aus Artikel 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V. m § 19 BDSG).

Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der EU-Datenschutz-Grundverordnung, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Datenschutzhinweise gemäß EU-Datenschutz-Grundverordnung für „Natürliche Personen“

Vertragspartner der von Ihnen abgeschlossenen Bausparverträge ist die BHW Bausparkasse AG; Vertragspartner der von Ihnen direkt abgeschlossenen Versicherungsverträge sind insbesondere unsere Kooperationspartner Zurich Deutscher Herold Lebensversicherungs AG (Kapital-/Risikoversicherungen) und Deutsche Pensionsfonds AG sowie die Deutsche Krankenversicherung AG. Bitte wenden Sie sich bzgl. Ihrer Datenschutzrechte unmittelbar an die Datenschutzbeauftragten der vorgenannten Unternehmen.

8. Gibt es für mich eine Pflicht zur Bereitstellung von Daten

Im Rahmen unserer Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und die Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel den Abschluss des Vertrages oder die Ausführung des Auftrages ablehnen müssen oder einen bestehenden Vertrag nicht mehr durchführen können und ggf. beenden müssen.

Insbesondere sind wir nach den geldwäscherechtlichen Vorschriften verpflichtet, Sie vor der Begründung der Geschäftsbeziehung beispielsweise anhand Ihres Personalausweises zu identifizieren und dabei Ihren Namen, Geburtsort, Geburtsdatum, Staatsangehörigkeit sowie Ihre Wohnanschrift zu erheben und festzuhalten. Damit wir dieser gesetzlichen Verpflichtung nachkommen können, haben Sie uns gemäß den Vorgaben des Geldwäschegesetzes die notwendigen Informationen und Unterlagen zur Verfügung zu stellen und sich im Laufe der Geschäftsbeziehung ergebende Änderungen unverzüglich anzuzeigen. Sollten Sie uns die notwendigen Informationen und Unterlagen nicht zur Verfügung stellen, dürfen wir die von Ihnen gewünschte Geschäftsbeziehung nicht aufnehmen oder fortsetzen.

9. Inwieweit gibt es eine automatisierte Entscheidungsfindung (einschließlich Profiling)

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung gemäß Artikel 22 DSGVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

10. Findet „Profiling“ statt

Wir verarbeiten Ihre Daten teilweise automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Wir setzen Profiling beispielsweise in folgenden Fällen ein:

— Aufgrund gesetzlicher Vorgaben sind wir zur Geldwäsche- und Betrugsbekämpfung verpflichtet. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch Ihrem Schutz.

— Um Sie zielgerichtet über Produkte informieren und beraten zu können, setzen wir Auswertungsinstrumente ein. Diese ermöglichen eine bedarfsgerechte Kommunikation und Werbung einschließlich Markt- und Meinungsforschung.

— Im Rahmen der Beurteilung Ihrer Kreditwürdigkeit nutzen wir das Scoring. Dabei wird die Wahrscheinlichkeit berechnet, mit der ein Kunde seinen Zahlungsverpflichtungen vertragsgemäß nachkommen wird. In die Berechnung können beispielsweise Einkommensverhältnisse, Ausgaben, bestehende Verbindlichkeiten, Beruf, Beschäftigungsdauer, Erfahrungen aus der bisherigen Geschäftsbeziehung, vertragsgemäße Rückzahlung früherer Kredite sowie Informationen von Kreditauskunfteien einfließen. Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren. Die errechneten Scorewerte unterstützen uns bei der Entscheidungsfindung und gehen in das laufende Risikomanagement mit ein.

Information über Ihr Widerspruchsrecht nach Artikel 21 EU-Datenschutz-Grundverordnung (DSGVO)

1. Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Abs. 1 e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Abs. 1 f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Artikel 4 Abs. 4 DSGVO.

Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

2. Widerspruchsrecht gegen Verarbeitung von Daten zu Werbezwecken

In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um Direktwerbung zu betreiben. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und sollte möglichst telefonisch gerichtet werden an: 069 910-10000 oder alternativ in der Filiale.