

Wüstenrot & Württembergische.
Der Vorsorge-Spezialist.

Wüstenrot Bank AG
Pfandbriefbank
Privatkundenservice
71630 Ludwigsburg

Per Fax an 07141 16-5367

Antragsteller
 Herr **oder** Frau

<input type="text"/>	<input type="text"/>
----------------------	----------------------

Zutreffendes bitte ankreuzen

Nur Verbraucher können für Ihre Privatkundenkonten am Online-Service teilnehmen. Bei Gemeinschaftskonten (zum Beispiel Eheleuten) muss jeder Kontomitinhaber, der den Online-Service nutzen will, einen eigenen Antrag stellen.

Jeder Konto(mit)inhaber erhält einen einzigen persönlichen Online-Zugang, unter dem alle online geführten Produkte angezeigt werden.

Der Versand der Zugangsmedien erfolgt ausschließlich an die Privatanschrift. Etwaige abweichende Versandanschriften können nicht berücksichtigt werden.

 **Ich möchte am Online-Banking teilnehmen.
Wüstenrot Bank AG Pfandbriefbank:**

 **Ich beantrage die Online-Vertragsauskunft.
Wüstenrot Bausparkasse AG:**

 **Ich bin bereits Online-Kunde.
Meine Online-Kundennummer (OKN):**

Es werden alle online-fähigen Produkte, bei denen ich Vertragsinhaber oder Vertragsmitinhaber bin, für den Online-Service freigeschaltet. Sollte schon ein Online-Zugang vorhanden sein, da z. B. bereits die Online-Vertragsauskunft für Bausparverträge genutzt wird, wird das Konto unter der bestehenden Online-Kundennummer freigeschaltet. Ich kann dann unter dem Punkt „Vertragsübersicht“ meine Verträge einsehen und erhalte keine weitere Bestätigung.

Kontoauszüge (außer für Termingeld Flex und Top Depot direct) werden dem Kontoinhaber in Textform im Rahmen des Online-Bankings zur Verfügung gestellt. Für Bausparverträge gilt weiterhin die postalische Zustellung.

Es gelten die Allg. Geschäftsbedingungen (AGB), die anhängenden Bedingungen für das Online-Banking und die Nutzungsordnung / Nutzungsbedingungen für Online-Service (Online-Vertragsauskunft). Weitere Informationen und sämtliche Bedingungen erhalte ich auf www.wuestenrotdirect.de.

Erstausstattung: kostenlos/Ersatz PIN: 12,00 EUR

Keine Gebühren werden erhoben für Leistungen, die aufgrund eines überwiegenden Verschuldens der Bank oder ihrer Erfüllungsgehilfen erforderlich werden sollten.

Bitte Formular vollständig ausfüllen und unterschreiben!



Wüstenrot Bank AG
Pfandbriefbank
71630 Ludwigsburg
– nachfolgend Bank genannt –

1. Leistungsangebot

(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang für Privatkundenkonten abwickeln. Zudem kann er Informationen der Bank mittels Online-Banking abrufen.

(2) Konto-/Depotinhaber werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(3) Zur Nutzung des Online-Banking gelten die mit der Bank gesondert vereinbarten Verfügungsmitte.

2. Voraussetzungen zur Nutzung des Online-Banking

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels Online-Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),
- der Nutzungscode für die elektronische Signatur.

2.2 Authentifizierungsinstrumente

Die TAN beziehungsweise die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- auf einer Liste mit einmal verwendbaren TAN,
- mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- mittels eines mobilen Endgerätes (zum Beispiel Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- auf einer Chipkarte mit Signaturfunktion oder
- auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden. Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zum Online-Banking

Der Teilnehmer erhält Zugang zum Online-Banking, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online-Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss Online-Banking-Aufträge (zum Beispiel Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Bank mittels Online-Banking übermitteln. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Online-Banking-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 Widerrufmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Online-Banking-Aufträgen durch die Bank

(1) Die Bearbeitung der Online-Banking-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 angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so

gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

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

- der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert;
- die Berechtigung des Teilnehmers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor;
- das Online-Banking-Datenformat ist eingehalten;
- das gesondert vereinbarte Online-Banking-Verfügungsmitte ist nicht überschritten;
- die Ausführungsvoraussetzungen 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 Online-Banking 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 Online-Banking-Auftrag nicht ausführen und dem 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-Banking eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online-Banking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg (außer wenn die Verfügung auf ein persönliches Auszahlungskonto erfolgt).

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online-Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online-Banking nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online-Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren. Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online-Banking-Verfahren missbräuchlich nutzen.

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

- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (zum Beispiel im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (zum Beispiel nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online-Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung zum Beispiel eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online-Banking genutzt werden.

7.3 Sicherheit des Kundensystems

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.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem Online-Banking-Auftrag (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapier-Kennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (zum Beispiel Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Persönlichen Sicherheitsmerkmals fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

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

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

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

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Konto-/Depotinhaber 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

- den Online-Banking-Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

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 des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

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

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments

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

(2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in Absätzen 1 und 2 genannten Authentifizierungsinstrumente können dann nicht mehr für das Online-Banking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten Online-Banking-Verfügung und einer nicht oder fehlerhaft ausgeführten Online-Banking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers 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 Authentifizierungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,- Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigen Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150,- Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150,- Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 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 und der Schaden dadurch eingetreten ist.

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

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich); siehe auch die nachfolgenden Punkte,
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online-Banking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 6. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das Online-Banking nutzt (siehe Nummer 7.2 Absatz 2 7. Spiegelstrich).

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

10.2.2 Haftung des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

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

10.2.3 Haftung der Bank ab der Sperranzeige

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

10.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

Stand: 21.11.2011

Nähere Angaben zur Bank sind im „Preis- und Leistungsverzeichnis“ enthalten.

Nutzungsbedingungen für Online-Service (Online-Vertragsauskunft)

Der W&W Online-Service ermöglicht den Kunden der Wüstenrot Bausparkasse AG, der Wüstenrot Bank AG Pfandbriefbank und den Kunden anderer Tochtergesellschaften der Wüstenrot & Württembergische AG, wichtige Daten ihrer Verträge über das Internet abzurufen. Um die Vertraulichkeit der Datenübermittlung zu gewährleisten, wird dazu die Wüstenrot Bank AG Pfandbriefbank mit der Durchführung des Datenaustausches betraut, wobei die vom Online-Banking bekannten hohen Sicherheitsmaßnahmen wie SSL-Verschlüsselung sowie PIN/TAN-Identifizierung zur Anwendung kommen.

1. Freischaltung

Mit dem Antrag auf Freischaltung der Online-Vertragsauskunft ermächtigt der Kunde die Wüstenrot Bank AG Pfandbriefbank, die für die Auskunft benötigten Vertragsdaten bei den Tochtergesellschaften der Wüstenrot & Württembergische AG anzufordern und in einer Datenbank für den Online-Abruf des Kunden bereitzuhalten.

Dies gilt auch für die Daten von Verträgen, die der Kunde bei anderen Tochtergesellschaften der Wüstenrot & Württembergische AG abschließt, sobald der Kunde der ihm angebotenen Freischaltung zustimmt.

2. Umfang der Online-Vertragsauskunft

Die Online-Vertragsauskunft ermöglicht einen Überblick über die wichtigsten Vertragsdaten der Kunden. Die Wüstenrot Bank AG Pfandbriefbank bemüht sich um die Verfügbarkeit rund um die Uhr, behält sich jedoch vor, den Dienst wegen Wartungsarbeiten oder bei Störungen vorübergehend auszusetzen.

3. Form von Willenserklärungen

Im Rahmen der Online-Vertragsauskunft kann der Kunde gegenüber der Wüstenrot Bank AG Pfandbriefbank und den

Gesellschaften, welche Vertragsdaten für die Online-Vertragsauskunft zur Verfügung stellen, rechtsverbindliche Mitteilungen und Willenserklärungen abgeben. Der Kunde und die daran beteiligten Gesellschaften verzichten für den Fall der Nutzung des Online-Auskunftsdienstes auf die Einhaltung einer eventuell vertraglich vereinbarten Schriftform.

4. Vertragsdauer

Die Vereinbarung wird auf unbegrenzte Zeit geschlossen. Der Kunde kann die Vereinbarung ohne Einhaltung einer Kündigungsfrist mit sofortiger Wirkung gegenüber der Wüstenrot Bank AG Pfandbriefbank kündigen. Bei der Kündigung durch die Wüstenrot Bank AG Pfandbriefbank gegenüber dem Kunden ist eine einmonatige Kündigungsfrist einzuhalten.

5. Sicherheit

Zur Sicherheit der Kunden sperrt die Wüstenrot Bank AG Pfandbriefbank den Online-Zugang bei missbräuchlicher Nutzung. Einzelheiten zu den Regelungen in Bezug auf Geheimhaltung, Kennwort und Zugangssperre ergeben sich aus der Online-Nutzungsordnung (s. Ziff. 6).

6. Nutzungsordnung

Verhaltensregeln und Sicherheitsbestimmungen sind in der Nutzungsordnung geregelt, welche von der Wüstenrot Bank AG Pfandbriefbank den aktuellen Bedürfnissen angepasst werden kann. Auf Änderungen werden die Kunden bei Anmeldung zur Vertragsauskunft ausdrücklich hingewiesen.

7. Anwendbares Recht

Auf diese Vereinbarung findet deutsches Recht Anwendung.

Nutzungsordnung für Online-Service

Nutzungsberechtigte und Zugangsmedien

Nutzer des Online-Service (d. h. Online-Vertragsauskunft und des Online-Bankings) werden im Folgenden als der Nutzer bezeichnet.

Zur Abgabe von Willenserklärungen in der Online-Vertragsauskunft für Verträge und zur Abwicklung von Bankgeschäften mittels Online-Banking hat der Nutzer Zahlencodes in Form von PIN und TAN einzugeben. Hierzu erhält der Nutzer von der Wüstenrot Bank AG Pfandbriefbank jeweils eine Online-Kundennummer (OKN), eine persönliche Identifikationsnummer (PIN) sowie Transaktionsnummern (TAN).

Geheimhaltung der PIN und der TAN

(1) Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und der TAN erlangt. Jede Person, welche die Online-Kundennummer, die PIN und – falls erforderlich – eine TAN kennt, hat die Möglichkeit, das Online-Service-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zu Lasten des Girokontos erteilen. Insbesondere Folgendes ist bei dem Umgang mit PIN und TAN zu beachten:

- Online-Kundennummer, PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;
- die dem Nutzer zur Verfügung gestellte TAN-Liste ist sicher zu wahren;
- bei Eingabe der Online-Kundennummer, PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

(2) Stellt der Nutzer fest, dass eine andere Person von seiner PIN oder von einer TAN oder von beiden Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er die Wüstenrot Bank AG Pfandbriefbank unverzüglich zu unterrichten. In diesem Fall wird die Bank den Online-Service-Zugang sperren, um Schäden für den Nutzer zu vermeiden.

Änderung der PIN

Der Nutzer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

Sperre des Online-Service-Angebotes

- (1) Wird dreimal hintereinander eine falsche PIN eingegeben, so wird der Online-Service-Zugang gesperrt. In diesem Falle sollte sich der Nutzer mit der Wüstenrot Bank AG Pfandbriefbank in Verbindung setzen. Diese Sperre kann mittels Online-Service nicht aufgehoben werden.
- (2) Werden dreimal hintereinander falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN für das betreffende Konto gesperrt. In diesem Falle sollte sich der Nutzer mit der Bank in Verbindung setzen.
- (3) Der Online-Service-Zugang wird gesperrt, wenn der Verdacht einer missbräuchlichen Nutzung des Online-Service-Zuganges besteht. Der Nutzer wird hierüber außerhalb des Online-Service informiert. Diese Sperre kann mittels Online-Service nicht aufgehoben werden.
- (4) Der Online-Service-Zugang kann auch auf Wunsch des Nutzers gesperrt werden. Auch diese Sperre kann nicht mittels Online-Service aufgehoben werden.