IKB
Deutsche Industriebank

Bedingungen für das Online-Banking inklusive Online-Postfach

Stand 07/2021

1. Leistungsangebot

(1) Die Kontoführung erfolgt online über das Internet. Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online-Banking in dem von der Bank angebotenen Umfang abwickeln und Informationen der Bank mittels Online-Banking abrufen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte sind gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absatz 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können Inhaber von Zahlungskonten und dessen Bevollmächtigte von ihnen ausgewählte sonstige Drittdienste nutzen. Die Bank führt derzeit keine Zahlungskonten, sondern ausschließlich

- Konten, welche der Verwahrung von Guthaben und der Geldanlage dienen (**„Anlagekonten“**, z.B. IKB Tagesgeld, IKB Festgeld) sowie
- je Kunde ein Verrechnungskonto (IKB Cashkonto), welches der Verwahrung von Guthaben, der bargeldlosen Einzahlung von Beträgen in Euro, die angelegt werden sollen, der Umbuchung von Geldbeträgen zwischen Anlagekonten, der Gutschrift von Erträgen aus Geld- und Wertpapieranlagen sowie der bargeldlosen Rückzahlung von Beträgen auf ein in Deutschland geführtes Referenzkonto (Girokonto) dient.

Überweisungen von oder zu Anlagekonten können ausschließlich über das IKB Cashkonto, Überweisungen vom bzw. zum IKB Cashkonto können ausschließlich über das mit der Bank vereinbarte Referenzkonto erfolgen. Die Bank wird keine auf das Cashkonto gezogenen Lastschriften zulassen.

(2) Kunde und Bevollmächtigte werden einheitlich als **„Teilnehmer“**, Konto und Depot einheitlich als **„Konto“** bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

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

(4) Die Bank behält sich das Recht vor, das Angebot von Produkten und Dienstleistungen, welche über das Online-Banking abwickelt werden können, jederzeit zu erweitern oder einzuschränken.

(5) Die Bank hat das Recht, die Art und Weise der Nutzung des Online-Banking unter Berücksichtigung der Belange des Kunden jederzeit zu verändern oder von Auflagen abhängig zu machen. Die Bank wird den Kunden über derartige Änderungen rechtzeitig in geeigneter Form unterrichten.

2. Voraussetzungen zur Nutzung des Online-Banking

(1) Der Teilnehmer kann das Online-Banking nutzen, wenn die Bank ihn authentifiziert hat.

(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen sowie Aufträge erteilen.

(3) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z.B. persönliche Identifikationsnummer [**„Passwort“**]),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z.B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [**„TAN“**], die den Besitz des Teilnehmers nachweisen, wie das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

3. Zugang zum Online-Banking

(1) Der Teilnehmer erhält Zugang zum Online-Banking der Bank, wenn

- er seine individuelle Teilnehmerkennung (z.B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nrn. 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Online-Banking kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z.B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum Online-Banking nur ein Authentifizierungselement angefordert wurde. Der Name des Kontoinhabers und die Kontonummer sind für den vom Teilnehmer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Online-Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Online-Banking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Online-Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Online-Banking der Bank oder „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

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

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor.
- Das Konto weist ein ausreichendes Guthaben auf.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den Teilnehmer hierüber mittels Online-Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kunden über Online-Banking-Verfügungen
Die Bank unterrichtet den Kunden gemäß den für den Auftrag/das jeweilige Produkt geltenden Bestimmungen über die mittels Online-Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers
7.1 Schutz der Authentifizierungselemente
(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungsinstrumente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Online-Banking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vergleiche Nummer 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
(a) Wissenselemente (z.B. Passwort), sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Online-Banking in Textform (z.B. per E-Mail; Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z.B. Speicherung des Passworts im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. mobiles Endgerät) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für das Online-Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente (z.B. mobiles Endgerät) sind vor Missbrauch zu schützen, insbesondere
- 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 eine etwaige auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für das Online-Banking (z.B. Online-Banking-App, Authentifizierungs-App) nicht nutzen können,
- ist eine etwaige Anwendung für das Online-Banking (z.B. Online-Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb des Online Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) 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 ihr Gerät als Besitzelement für das Online-Banking des Teilnehmers aktivieren.

(c) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für das Online-Banking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Online Banking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Online Banking das von der Bank ausgegebene Wissenselement (z.B. Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das 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 sowie einem sonstigen Drittdienst verwenden (siehe Nummer 1 Absatz 1 Sätze 3 und 4 dieser Bedingungen). Sonstige Drittdienste hat der Teilnehmer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank
Der Teilnehmer muss die Sicherheitshinweise auf der Online-Banking-Seite der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten
Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z.B. Betrag, Bankverbindung des Zahlungsempfängers, Verzinsung) über das gesondert vereinbarte Gerät des Teilnehmers an (z.B. mittels mobilem Endgerät). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten
8.1 Sperranzeige
(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. mobiles Endgerät) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer hat folgende Möglichkeiten, eine Sperranzeige gegenüber der Bank abzugeben:
- über das Online-Banking,
- während der Service-Zeiten über die telefonische Kundenbetreuung,
- per Telefax.

(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 Teilnehmer 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 Nr. 8.1 dieser Bedingungen,
- den Online-Banking-Zugang für ihn oder für alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang zum Online-Banking für Teilnehmer sperren, wenn

- sie berechtigt ist, den Online-Banking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Der Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines Authentifizierungselements besteht insbesondere dann, wenn

- dreimal hintereinander ein falsches Passwort eingegeben wurde oder
- dreimal hintereinander eine falsche TAN eingegeben wurde.

(3) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3 Aufhebung der Sperre

9.4 Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungslelemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich. Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto des Kunden verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs, es rechtfertigen. Die Bank wird den Kunden über eine solche Zugangsverweigerung auf dem vereinbarten Weg unterrichten. Die Unterrichtung erfolgt möglichst vor, spätestens jedoch unverzüglich nach der Verweigerung des Zugangs. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Sobald die Gründe für die Verweigerung des Zugangs nicht mehr bestehen, hebt die Bank die Zugangssperre auf. Hierüber unterrichtet sie den Kunden unverzüglich.

10. Haftung

10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrags richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst 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 Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

- Nummer 7.1 Absatz 2,
- Nummer 7.1 Absatz 4,
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

dieser Bedingungen verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3 dieser Bedingungen).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 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 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Kunden bei nicht autorisierten Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige

Beruhen nicht autorisierte Verfügungen außerhalb von Zahlungsdiensten (z.B. Wertpapiertransaktionen) vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Nutzung des Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach über das Online-Banking durch nicht autorisierte 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.

11. Nutzung des Online-Postfachs
11.1 Leistungsinhalt
Im Rahmen der Geschäftsbeziehung zwischen Bank und Kunde richtet die Bank diesem mit der Kontoeröffnung ein webbasiertes Online-Postfach ein, in welchem die Bank dem Kunden persönliche Mitteilungen der Bank zum Konto (z.B. Kontoauszüge, Rechnungsabschlüsse, etc.) in elektronischer Form online bereitstellt (**„Online-Postfach"**). Ausgenommen sind solche Dokumente, bei denen Schriftform gesetzlich vorgeschrieben ist. Die Dokumentenauswahl kann von der Bank jederzeit erweitert oder verringert werden. Die Bank wird den Kunden hierüber informieren.

11.2 Zugang
Die Mitteilungen der Bank gehen dem Kunden spätestens in dem Zeitpunkt zu, in dem dieser die Informationen im Postfach abgerufen hat.

11.3 Verzicht auf papierhafte Bereitstellung von Kundendokumenten
(1) Mit Einrichtung des Online-Postfachs erklärt sich der Kunde damit einverstanden, dass die Bank Mitteilungen zu allen bei der Bank geführten Konten des Kunden zur Erfüllung ihrer Informations- und Rechnungslegungspflichten – soweit gesetzlich zulässig – zum Abruf in dem Online-Postfach bereitstellt. Der Kunde verzichtet durch die Nutzung des Online-Postfachs auf den postalischen Versand der Informationen durch die Bank in papiergebundener Form, sofern nicht ausdrücklich der postalische Versand vereinbart wird.

(2) Die Nutzung des Online-Postfachs ist für den Kunden nicht mit Zusatzkosten verbunden.

(3) Die Bank ist berechtigt, dem Kunden die im Online-Postfach hinterlegten Mitteilungen auf dem Postweg oder auf andere Weise zuzusenden, wenn dies gesetzliche Vorgaben erforderlich machen oder die Bank dies unter Berücksichtigung des Kundeninteresses für zweckmäßig erachtet.

11.4 Zusendung von Kontoauszügen und sonstigen Mitteilungen der Bank auf Verlangen des Kunden
Wurde auf die papierhafte Bereitstellung von Kundendokumenten verzichtet, so wird die Bank in das Online-Postfach eingestellte Kundendokumente zusätzlich auf postalischem Weg in papiergebundener Form zusenden, sofern der Kunde dies ausdrücklich wünscht. Das hierfür anfallende Entgelt ergibt sich aus dem jeweils aktuellen Preis- und Leistungsverzeichnis der Bank, welches unter www.ikb.de eingesehen werden kann.

11.5 Mitwirkungspflicht des Kunden
(1) Der Kunde verpflichtet sich, das Online-Postfach regelmäßig auf neue Informationen zu prüfen, diese zeitnah abzurufen und die Richtigkeit und Vollständigkeit der in dem Online-Postfach hinterlegten Dokumente zu kontrollieren sowie etwaige Einwendungen unverzüglich zu erheben.

(2) Der Kunde ist verpflichtet, der Bank zu Korrespondenzzwecken eine gültige E-Mail-Adresse mitzuteilen.

11.6 Unveränderbarkeit der Daten
Die Bank stellt die Unveränderbarkeit der in das Postfach eingestellten Dokumente sicher, sofern diese innerhalb des Postfachs gespeichert oder aufbewahrt werden.

11.7 Speicherung der Dokumente
(1) In dem Online-Postfach werden Dokumente zur Verfügung gestellt und dort lesbar und abrufbar sein. Die Bank empfiehlt den Abruf und die lokale Speicherung bzw. Aufbewahrung eines eigenen Ausdrucks bei dem Teilnehmer.

(2) Die Bank selbst bewahrt die im Online-Postfach zur Verfügung gestellten Informationen im Rahmen der gesetzlichen Aufbewahrungsfristen auf. Nach Ablauf dieser Frist kann die Bank die Informationen löschen, ohne dass der Teilnehmer hierüber eine gesonderte Mitteilung erhält.

12. Kontostammdaten, Mitteilungspflicht
Vorbehaltlich der Bestimmungen gemäß Nr. 11 der Allgemeinen Geschäftsbedingungen der Bank ist es zur ordnungsgemäßen Abwicklung der Geschäftsbeziehung erforderlich, dass der Kunde der Bank Änderungen seiner persönlichen Daten (z.B. Name, Anschrift, E-Mail-Adresse) sowie der des Bevollmächtigten und Änderungen des Referenzkontos unverzüglich mitteilt. Die Änderung oder Ergänzung seiner persönlichen Daten muss der Teilnehmer grundsätzlich im Online-Banking vornehmen. Eine Änderung des Referenzkontos sowie der für das mobileTAN-Verfahren hinterlegten Mobilfunknummer ist aus Sicherheitsgründen nur schriftlich möglich.