SONDERBEDINGUNGEN FÜR DAS ONLINE UND MOBILE BANKING

Stand: 20.07.2020

1 Leistungsangebot

(1) Der Kunde und dessen Bevollmächtigte können Bankgeschäfte mittels Online Banking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Online Banking abrufen. Des Weiteren sind sie gemäß § 675f Absatz 3 BGB berechtigt, Zahlungsauslösedienste und Kontoinformationsdienste gemäß § 1 Absätze 33 und 34 Zahlungsdiensteaufsichtsgesetz (ZAG) zu nutzen. Darüber hinaus können sie von ihnen ausgewählte sonstige Drittdienste nutzen.

(2) Kunde und Bevollmächtigte werden einheitlich als »Nutzer«, Konto und Depot einheitlich als »Konto« bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

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

2 Voraussetzungen zur Nutzung des Online Banking

(1) Der Nutzer 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 Nutzers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Nutzers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Nutzer sich gegenüber der Bank als berechtigter Nutzer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(3) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Nutzer weiß (z. B. persönliche Identifikationsnummer (PIN),
- Besitzelemente, also etwas, das nur der Nutzer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (TAN), die den Besitz des Nutzers nachweisen, wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
- Seinselemente, also etwas, das der Nutzer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Nutzers).

(4) Die Authentifizierung des Nutzers erfolgt, indem der Nutzer 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 Nutzer erhält Zugang zum Online Banking der Bank, wenn
- er seine individuelle Nutzerkennung (z. B. Kontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

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

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift des Kunden) fordert die Bank den Nutzer 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 Nutzer genutzten Zahlungsauslösedienst und Kontoinformationsdienst keine sensiblen Zahlungsdaten (§ 1 Absatz 26 Satz 2 ZAG).

4 Aufträge

4.1 Auftragserteilung

Der Nutzer muss einem Auftrag (zum Beispiel Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (zum Beispiel Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden.

Die Bank bestätigt mittels Online Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

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

4.3 Ausführungsplatz für Wertpapieraufträge

Für den Ausführungsplatz der per Online Banking erteilten Aufträge zum Kauf oder Verkauf von börsennotierten Wertpapieren gilt Nummer 2 der Sonderbedingungen für Wertpapiergeschäfte mit folgender Maßgabe:

Grundsätzlich kann der Nutzer auch bei der Auftragserteilung per Online Banking den Ausführungsplatz und die Ausführungsart bestimmen.

Aus technischen Gründen können für einzelne Wertpapiere nicht alle in Betracht kommende Börsenplätze systemseitig vorgegeben werden. In diesem Falle beschränkt sich das Bestimmungsrecht des Kunden gemäß Nr. 2 Absatz 1 der Sonderbedingungen für Wertpapiergeschäfte bei per Online Banking erteilten Wertpapieraufträgen auf die systemseitig vorgesehenen, systemtechnisch vorgegebenen Ausführungsorte. Die Möglichkeit der anderweitigen Auftragserteilung, z. B. unmittelbar über die Filiale oder über das HypoVereinsbank Wertpapier-Telefon, soweit hierfür angemeldet, bleibt davon unberührt.

5 Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im »Preis- und Leistungsverzeichnis« bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen 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-Seite der Bank oder »Preis- und Leistungsverzeichnis« der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Nutzer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- Die Berechtigung des Nutzers für die jeweilige Auftragsart (zum Beispiel Wertpapierorder) liegt vor.
- Das Online-Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online-Banking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zum Beispiel ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den Nutzer hierüber mittels Online Banking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6 Information des Kunden über Online-Banking-Verfügungen

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

7 Sorgfaltspflichten des Nutzers

7.1 Schutz der Authentifizierungselemente

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

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Nutzer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Online Banking in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Online Banking und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
- sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Nutzers (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 Nutzers zu deaktivieren, bevor der Nutzer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online Banking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weiter gegeben werden und
- muss der Nutzer, 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 Nutzers aktivieren.

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

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (zum Beispiel Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

(4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Nutzer diese Telefonnummer für das Online Banking nicht mehr nutzt.

(5) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 4 darf der Nutzer 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 Nutzer mit der im Verkehr erforderlichen Sorgfalt auszuwählen.

7.2 Sicherheitshinweise der Bank

Der Nutzer 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 Nutzer die von ihr empfangenen Auftragsdaten (zum Beispiel Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) über das gesondert vereinbarte Gerät des Nutzers an (zum Beispiel mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Nutzer 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 Nutzer
- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements

fest, muss der Nutzer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Nutzer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

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

(3) Hat der Nutzer 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 Nutzers

Die Bank sperrt auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Nummer 8.1 dieser Bedingungen,

- den Online-Banking-Zugang für ihn oder alle Nutzer oder
- seine Authentifizierungselemente zur Nutzung des Online-Banking.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Online-Banking-Zugang für einen Nutzer sperren, wenn

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

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

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

9.4 Automatische Sperre eines chip-basierten Besitzelements

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

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

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

9.5 Zugangssperre für Zahlungsauslösedienst und Kontoinformationsdienst

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

10 Haftung

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

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft.)

10.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

10.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Nutzer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Nutzers 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.

(2) Abweichend von Absatz 1 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Nutzer 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).

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

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

(5) Die Absätze 2 bis 4 finden keine Anwendung, wenn der Nutzer in betrügerischer Absicht gehandelt hat.

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

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

10.2.3 Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Nutzers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online-Banking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Nutzer 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 Postfach

11.1 Leistungsangebot

Die Bank stellt dem Nutzer ein Postfach im Online Banking als seinen elektronischen Briefkasten zur Verfügung. Sie ist berechtigt, dem Nutzer sämtliche für ihn – auch als Kontomitinhaber, Bevollmächtigten oder gesetzlichen Vertreter – bestimmte persönliche Mitteilungen und Informationen (im Folgenden einheitlich Dokumente), die die Geschäftsverbindung mit der Bank betreffen, im PDF-Format in sein Postfach einzustellen. Die Bank ist berechtigt, diese Dokumente dem Nutzer ausschließlich auf elektronischem Wege zur Verfügung zu stellen.

Eine Liste der für das Postfach verfügbaren Dokumente lässt sich unter www.hvb.de/online-dokumente abrufen.

11.2 Unveränderbarkeit der Daten

Die Bank gewährleistet die Unveränderbarkeit der in das Postfach eingestellten und dort gespeicherten Dokumente.

11.3 Verzicht auf papierhafte Zurverfügungstellung

(1) Der Nutzer verzichtet ausdrücklich nach Maßgabe dieser Bedingungen auf die papierhafte Zurverfügungstellung (z. B. durch Postversand) der in das Postfach einzustellenden bzw. eingestellten Dokumente. Die Bank kommt ihrer Verpflichtung zur Mitteilung, Übermittlung, Unterrichtung oder Zurverfügungstellung durch Einstellung der betreffenden Dokumente in das Postfach nach.

(2) Der Nutzer stimmt der elektronischen Übermittlung von Rechnungen zu (§ 14 UStG).

(3) Hinweis für buchführungs- bzw. aufbewahrungspflichtige Personen:
Elektronische Dokumente werden von der Finanzverwaltung grundsätzlich als Buchungsbelege anerkannt, wenn die gesetzlichen Anforderungen insbesondere in Bezug auf Vollständigkeit, Richtigkeit und Unveränderbarkeit beachtet werden. Gleiches gilt für die Erfüllung der Aufbewahrungspflichten. Bitte lassen Sie sich im Zweifel hierzu steuerlich beraten.

11.4 Benachrichtigung und Zugang

(1) Die Bank wird den Nutzer auf dem (z. B. bei Kontoeröffnung) vereinbarten Kommunikationsweg (z. B. E-Mail oder SMS) über die Einstellung neuer Dokumente benachrichtigen.

(2) Die Dokumente gehen dem Nutzer in dem Zeitpunkt zu, in dem sie jeweils in abruf- und speicherbarer Form in seinem Postfach zur Verfügung gestellt worden sind, der Nutzer über die Einstellung benachrichtigt worden ist und er die Dokumente unter gewöhnlichen Umständen zur Kenntnis nehmen konnte.

Unbeschadet von Absatz 2 gehen die Dokumente dem Nutzer jedoch spätestens zu dem Zeitpunkt zu, in dem der Nutzer diese abgerufen hat.

11.5 Mitwirkungs- und Sorgfaltspflichten des Nutzers

(1) Über Änderungen seiner Kontaktdaten für die Benachrichtigung nach Nr. 11.4 wird der Nutzer die Bank unverzüglich informieren.

(2) Soweit der Online Banking-Zugang auf Veranlassung (siehe Nr. 9.1) oder aufgrund einer Handlung des Nutzers gesperrt worden ist, ist dieser verpflichtet, alle erforderlichen Maßnahmen zu unternehmen, die es der Bank ermöglichen die Funktionsfähigkeit des Online Banking-Zugangs des Nutzers wiederherzustellen.

(3) Der Nutzer ist verpflichtet, die in sein Postfach eingestellten Dokumente regelmäßig und zeitnah abzurufen.

11.6 Bereitstellung und Aufbewahrung

(1) Die Bank verpflichtet sich, dem Nutzer die Dokumente in seinem Postfach für die Dauer von mindestens zehn Jahren nach deren Einstellung zur Verfügung zu stellen. Dies gilt, solange der Nutzer mit mindestens einem Konto oder Wertpapierdepot, bei dem er Kontoinhaber, Kontomitinhaber, Bevollmächtigter oder gesetzlicher Vertreter ist, zum Online Banking angemeldet ist. Unbeschadet von Satz 2 endet die zur Verfügungstellung der Dokumente für Bevollmächtigte und gesetzliche Vertreter mit erlöschen der Vollmacht bzw. Vertretungsberechtigung. Der Nutzer hat innerhalb dieser Frist jederzeit die Möglichkeit, im Postfach vorhandene Dokumente online anzusehen, auszudrucken, zu archivieren oder auf einem eigenen Datenträger zu speichern.

(2) Nach Ablauf der Frist nach Absatz (1) ist die Bank berechtigt, die Dokumente aus dem Postfach zu entfernen.

(3) Die Bank ist jederzeit berechtigt, bei technischen Problemen einzelne oder auch alle Dokumente auf dem Postweg oder in sonstiger Weise an den Nutzer zu übermitteln, wenn dies von der Bank unter Berücksichtigung des Nutzerinteresses als zweckmäßig erachtet wird. Die Bank ist darüber hinaus jederzeit aufgrund von gesetzlichen oder aufsichtsrechtlichen Verpflichtungen berechtigt, einzelne oder alle Dokumente auf dem Postweg oder in sonstiger Weise an den Nutzer zu übermitteln.

12 Mobile Banking App

12.1 Leistungsangebot

Der Nutzer kann mittels der Mobile Banking App in dem von der Bank angebotenen Umfang Bankgeschäfte abwickeln und Informationen abrufen. Zusätzlich kann der Nutzer als Authentifizierungsinstrument das appTAN-Verfahren verwenden. Die Nutzung der Mobile Banking App und des appTAN-Verfahrens setzen einen Online Banking Zugang voraus (siehe Nr. 3).

12.2 Sorgfaltspflichten des Nutzers

(1) Der Nutzer hat seine Sicherheitsmerkmale (siehe Nr. 2.1) geheim zu halten sowie seine Authentifizierungsinstrumente (siehe Nr. 2.2) vor dem Zugriff anderer Personen sicher zu verwahren. Insbesondere sind diese nicht außerhalb der Mobile Banking App auf dem Endgerät zu speichern oder zusammen mit diesem aufzubewahren. Auf Nr. 7.2 Abs. 2 wird Bezug genommen.

(2) Bei der Nutzung von biometrischen Merkmalen ist bei den System-Einstellungen darauf zu achten, dass ausschließlich die eigenen Merkmale (z. B. Fingerabdrücke, Gesichtsscan) hinterlegt sind und auch der sicherheitsrelevante Code zur Änderung der Systemeinstellungen nur dem Nutzer selbst bekannt ist. Jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen personalisierten Sicherheitsmerkmals das Online und Mobile Banking-Verfahren missbräuchlich nutzen.

12.3 Datenschutzerklärung

Die Bank erhebt und nutzt personenbezogene Daten, welche einen direkten Rückschluss auf die Identität des Nutzers zulassen. Dies kann z. B. der Name, die Anschrift oder eine eindeutige Gerätekennung sein.

Im Mobile Banking werden folgende personen- und gerätebezogenen Informationen genutzt:

(1) Die gerätespezifische ID wird als Grundlage für die Nutzung und Aktivierung von Push-Benachrichtigungen erfasst.

(2) Informationen zum mobilen Gerät, Browser und Betriebssystem sowie zur Aktualisierung bzw. Veränderung von Standardsoftware werden genutzt, um eine angepasste, grafische Darstellung der App-Inhalte und eine störungsfreie Bereitstellung des appTAN-Services auf dem Endgerät zu gewährleisten. Im Fehlerfall werden diese Daten für die Analyse gespeichert und verwendet.

(3) Die Push-Notification-ID wird zur korrekten Zustellung der Push-Benachrichtigungen auf das Endgerät benötigt. Da es sich bei Push-Benachrichtigungen um Standarddienste des jeweiligen Anbieters (z. B. Google Cloud Messaging bzw. Apple Push Notification Service) handelt, ist nicht auszuschließen, dass Dritte von der Geschäftsbeziehung und den Inhalten der Nachrichten Kenntnis erlangen können.

(4) Es werden keine personenbezogenen Daten auf dem Endgerät des Nutzers gespeichert, daher ist für die Nutzung der App grundsätzlich eine Netzverbindung erforderlich. Dazu fragt die App Informationen zum Netzwerkstatus des Endgerätes ab. Um zu verhindern, dass kontobezogene Informationen auf einem manipulierten Endgerät abgerufen werden, überprüft die Mobile Banking App, dass das Endgerät im vom Hersteller ausgelieferten Zustand ist (z. B. keine Modifikation des Betriebssystems, wie Jailbreak oder Rooting aufweist).

Die oben genannten personen- oder gerätebezogenen Daten werden von der Bank im Rahmen der Zweckbindung ausschließlich für die Bereitstellung und Nutzung des Mobile Bankings verwendet und nicht an Dritte weitergegeben.

Im Rahmen der Nutzungsbedingungen des Endgeräts (iPhone oder Android Smartphone) können durch Apple Inc. bzw. Google Inc. Daten erhoben, verarbeitet und genutzt werden. Insoweit wird auf die entsprechenden Datenschutzerklärungen/Einstellungen des vom Nutzer gewählten Anbieters verwiesen.

12.4 Rechnungsscanner

12.4.1 Leistungsangebot

Die Bank bietet dem Nutzer innerhalb der Mobile Banking App eine Rechnungsscannerfunktion (Dokumentenauswertungssystem) an. Der Rechnungsscanner unterstützt den Nutzer bei der Übertragung von Daten aus Rechnungen, Überweisungsbelegen und QR-Codes (im Folgenden einheitlich Dokumente) in Überweisungsvorlagen im Mobile Banking. Die übertragenen Dokumente werden dabei von der Bank nicht dauerhaft gespeichert. Voraussetzung für die Nutzung des Rechnungsscanners ist, dass der Nutzer sich für das appTAN-Verfahren registriert hat.

12.4.2 Sorgfalts- und Mitwirkungspflichten

(1) Der Nutzer ist verpflichtet, die eingescannten Dokumente und die vorausgefüllten Überweisungsvorlagen im Mobile Banking eigenverantwortlich auf Richtigkeit und Vollständigkeit hin zu kontrollieren und ggf. zu berichtigen.

(2) Dem Nutzer ist es untersagt, Dokumente zu übertragen, deren Speicherung, Bereitstellung und/oder Nutzung gegen geltende Gesetze verstößt. Bei Verstößen ist die Bank berechtigt, die Nutzung der Funktion »Rechnungsscanner« zu sperren.

12.5 Push-Benachrichtigungen

12.5.1 Leistungsangebot

Die Bank bietet dem Nutzer die Möglichkeit, Informationen über den Kontostand und Kontostandsbewegungen mittels Push-Benachrichtigungen zu erhalten. Dies setzt voraus, dass der Nutzer die Mobile Banking App nutzt und für das appTAN-Verfahren registriert ist. Push-Benachrichtigungen können nur bei aktiver Internetverbindung übermittelt werden.

12.5.2 Datenschutzhinweise

(1) Für Push-Benachrichtigungen werden personen- und geräte bezogene Informationen genutzt (siehe Nr. **12.3 Abs. 3**).

(2) Sollten sich mehrere Nutzer mit einem Gerät für das appTAN-Verfahren registriert haben, gehen Push-Benachrichtigungen für alle registrierten Nutzer auf diesem Gerät ein. In diesem Falle sind alle Push-Benachrichtigungen für den jeweiligen Besitzer des Endgeräts einsehbar.

13 paydirekt

Die Bank bietet dem Nutzer mit paydirekt ein internetbasiertes Verfahren für bargeldlose Zahlungen im elektronischem Geschäftsverkehr an. Für die Nutzung von paydirekt gelten die mit dem Nutzer gesondert vereinbarten Bedingungen für Zahlungen mittels paydirekt.

14 Änderung Sonderbedingungen Online und Mobile Banking – Ergänzung PFM

Der Persönliche Finanzmanager der UniCredit Bank AG (nachfolgend »Bank«) wird für alle im Online Banking eingebundenen Konten und Kreditkarten aktiviert und erstellt mittels grafischer Darstellungen, die auf kategorisierten Umsätzen, Budgetierung und ggf. Sparzielen des Nutzers basieren, für den Nutzer einen Überblick über seine Finanzen. Die mit dem Persönlichen Finanzmanager erfolgte Kategorisierung der Umsätze dient ausschließlich der Unterstützung der persönlichen Finanzplanung des Nutzers und kann nur von dem jeweiligen Nutzer eingesehen und angepasst werden. Es werden keine personenbezogenen Informationen aus dem Finanzmanager an Dritte weitergegeben. Die Daten werden von der HVB nur bei Vorliegen einer separaten Einwilligung z. B. zur gezielten Kundenberatung oder für individuelle Angebote herangezogen. Soweit die grafischen Darstellungen im Persönlichen Finanzmanager gegenüber den Umsatzdaten und Salden in den eingebundenen Konten und Kreditkarten abweichen, sind allein die in den jeweiligen Produktbereichen des Online Banking ausgewiesenen Umsätze und Salden verbindlich.