SONDERBEDINGUNGEN FÜR DAS ONLINE UND MOBILE BANKING

Stand: 01.09.2018

1 Leistungsangebot

(1) Der Konto-/Depotinhaber 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. Sie sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.

(2) Konto-/Depotinhaber 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

Der Nutzer benötigt für die Nutzung des Online Banking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Bank als berechtigter Nutzer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Nutzers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Nutzer zum Zwecke der Authentifizierung bereitstellt. Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind beispielsweise

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

2.2 Authentifizierungsinstrumente

Authentifizierungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Nutzer zur Erteilung eines Online Banking-Auftrags verwendet werden. Insbesondere mittels folgender Authentifizierungsinstrumente kann das Personalisierte Sicherheitsmerkmal (z. B. TAN) dem Nutzer zur Verfügung gestellt werden:

- PIN-Brief,
- Liste mit einmal verwendbaren TAN,
- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- Online Banking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang oder Erzeugung von TAN,
- mobiles Endgerät (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- Chipkarte mit Signaturfunktion oder
- sonstiges Authentifzierungsinstrument, auf dem sich Signaturschlüssel befinden.

3 Zugang zum Online Banking

Der Nutzer erhält Zugang zum Online Banking, wenn

- dieser seine individuelle Online Banking Nummer und seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Nutzers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

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

Die Sätze 1 und 2 gelten auch, wenn der Nutzer Zahlungsaufträge über einen Zahlungsauslösedienst auslöst und Zahlungskontoinformationen über einen Kontoinformationsdienst anfordert (siehe Nummer 1 Absatz 1 Satz 3).

4 Online Banking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Nutzer muss Online Banking Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereit gestellten Personalisierten Sicherheitsmerkmal (z. B. TAN) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels Online Banking übermitteln. Die Bank bestätigt mittels Online Banking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Nutzer einen Zahlungsauftrag über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 3) auslöst und übermittelt.

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 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 kommenden Börsenplätzen 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 Online Banking Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. 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 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 Nutzer hat den Auftrag autorisiert.
- Die Berechtigung des Nutzers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Online Banking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online Banking-Verfügungslimit ist nicht überschritten.

– Die weiteren Ausführungsvoraussetzungen 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 Online Banking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. 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. 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 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.

7 Sorgfaltspflichten des Nutzers

7.1 Technische Verbindung zum Online Banking

Der Nutzer ist verpflichtet, die technische Verbindung zum Online Banking über die von der Bank gesondert mitgeteilten Online Banking-Zugangskanäle (z. B. Internetadresse) herzustellen. Zur Erteilung eines Zahlungsauftrags und zum Abruf von Informationen über ein Zahlungskonto kann der Nutzer die technische Verbindung zum Online Banking auch über einen Zahlungsauslösedienst beziehungsweise einen Kontoinformationsdienst (siehe Nr. 1 Absatz 1 Satz 3) herstellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Nutzer hat
– seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten 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 der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das Online Banking-Verfahren missbräuchlich nutzen.

Die Geheimhaltungspflicht bezüglich der Personalisierten Sicherheitsmerkmale nach Satz 1 wird nicht verletzt, wenn der Nutzer diese zur Erteilung eines Zahlungsauftrags oder zum Abruf von Informationen über ein Zahlungskonto an den von ihm ausgewählten Zahlungsauslösedienst beziehungsweise Kontoinformationsdienst übermittelt (siehe Nummer 1 Absatz 1 Satz 3).

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
– Das Personalisierte Sicherheitsmerkmal darf nicht ungesichert elektronisch gespeichert werden.
– Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
– Das Personalisierte Sicherheitsmerkmal darf nicht per E-Mail weitergegeben werden.
– Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
– Der Nutzer darf zur Autorisierung z. B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
– Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für das Online Banking genutzt werden.

7.3 Sicherheitshinweise der Bank

Der Nutzer 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 Nutzer Daten aus seinem Online Banking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Nutzers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Nutzer 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 Nutzer
– den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
– die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale fest, muss der Nutzer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Nutzer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgegeben.

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

(3) Hat der Nutzer 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 Nutzers

Die Bank sperrt auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Nummer 8.1
– den Online Banking-Zugang für ihn oder alle Nutzer oder
– sein Authentifizierungsinstrument.

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 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 auf dem vereinbarten Weg 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 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 Authentifizierungsinstrumente 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.

10 Haftung

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

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

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Authentifizierungsinstruments sowie Haftung für sonstige 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 Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber den hierdurch entstandenen Schaden. Grobe Fahrlässigkeit des Nutzers 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 ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2 1.Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),
- das Personalisierte Sicherheitsmerkmal per E-Mail weitergegeben hat (siehe Nummer 7.2 Absatz 2 3.Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2 4.Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 5.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 6.Spiegelstrich).

(2) Abweichend von Absatz 1 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Nutzer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangte, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Nutzer weiß, z. B. PIN), Besitz (etwas, das der Nutzer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Nutzer ist, z. B. Fingerabdruck).

(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 Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn der Nutzer die Sperranzeige nach Nummer 8.1 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.

(6) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:

- § 675v des Bürgerlichen Gesetzbuchs findet keine Anwendung.
- Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen, wenn der Nutzer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Nr. 10.2 (2) dieser Bedingungen findet keine Anwendung.

10.3 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.

10.4 Haftung der Bank 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.

10.5 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 Einstellung von Dokumenten bei Bevollmächtigten und gesetzlichen Vertretern

(1) Soweit der Nutzer bei Anmeldung zum Online Banking ausschließlich oder zusätzlich Bevollmächtigter bzw. gesetzlicher Vertreter eines Kontos oder Depots ist, wird die Bank den Kontoinhaber einmalig über die Einstellung von Dokumenten in das Postfach des Nutzers informieren.

(2) Nach Beendigung der Vertretungsberechtigung werden keine weiteren Dokumente mehr in das Postfach des Bevollmächtigten oder gesetzlichen Vertreters eingestellt.

11.3 Unveränderbarkeit der Daten

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

11.4 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) 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.

11.5 Benachrichtigung und Zugang

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

11.6 Mitwirkungs- und Sorgfaltspflichten des Nutzers

(1) Über Änderungen seiner Kontaktdaten für die Benachrichtigung nach Nr. 11.5 wird der Nutzer die Bank unverzüglich informieren.

(2) Der Nutzer ist verpflichtet, die in sein Postfach eingestellten Dokumente regelmäßig und zeitnah abzurufen. Ebenso ist der Nutzer zur unverzüglichen Benachrichtigung der Bank bei Ausbleiben von Dokumenten verpflichtet, die er erwartet.

11.7 Bereitstellung und Aufbewahrung

(1) Die Bank verpflichtet sich, dem Nutzer die Dokumente in seinem Postfach für die Dauer von mindestens drei Jahren nach deren Einstellung zur Verfügung zu stellen. Dies gilt, solange der Nutzer mit mindestens einem Konto oder Wertpapierdepot, bei dem er Kontoinhaber, Bevollmächtigter oder gesetzlicher Vertreter ist, zum Online Banking angemeldet ist und er die Dokumente nicht gelöscht hat. Der Nutzer hat jederzeit innerhalb dieser Frist die Möglichkeit, im Postfach vorhandene Dokumente online anzusehen, auszudrucken, zu löschen 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 beispielsweise aufgrund von gesetzlichen oder aufsichtsrechtlichen Verpflichtungen berechtigt, einzelne oder alle Dokumente auf dem Postweg oder in sonstiger Weise an den Nutzer zu übermitteln.

12 Online Kontoauszug

12.1 Leistungsangebot

(1) Soweit für das Konto die Nutzung des Kontoauszugsdruckers vereinbart worden ist, kann sich der Nutzer die jeweiligen Kontoauszüge, mithin alle Informationen und Mitteilungen, die der Nutzer bisher auf dem papierhaften Kontoauszug erhielt, alternativ auch im Online Banking per Einzelabruf oder automatisiert im PDF-Format zum Abruf bereitstellen lassen. Ein abgerufener Online Kontoauszug ersetzt dabei jeweils den per Kontoauszugsdrucker abrufbaren Kontoauszug.

(2) Es werden je Konto bis zu 60 Kontoauszüge gespeichert. Bei Überschreitung dieser Begrenzung wird der älteste vorhandene Kontoauszug unwiderruflich gelöscht.

12.2 Einzelabruf

Ruft der Nutzer seine Kontoauszüge per Einzelabruf ab, kann er den abgerufenen Kontoauszug online im Archiv speichern, herunterladen und/oder ausdrucken.

12.3 Automatisierter Abruf

Im Fall des automatisierten Abrufs der Kontoauszüge stellt die Bank dem Nutzer je nach Vereinbarung die Kontoauszüge wöchentlich oder monatlich im Archiv zur Verfügung.

12.4 Beendigung des automatisierten Abrufs

(1) Beendigung durch den Nutzer:
Der Nutzer kann die Teilnahme am automatisierten Kontoauszugabrufverfahren jederzeit im Online Banking oder über seinen Betreuer beenden. Die Bank stellt dem Nutzer die Kontoauszüge in diesem Fall zum Abruf am Kontoauszugsdrucker bereit.

(2) Beendigung durch die Bank:
Ruft der Nutzer die für ihn eingestellten Kontoauszüge über einen Zeitraum von sechs Monaten nicht ab, endet der automatisierte Abruf der Kontoauszüge. Die Bank wird den Nutzer hierüber rechtzeitig informieren. Die Bank stellt dem Nutzer alle weiteren Kontoauszüge zum Abruf am Kontoauszugsdrucker bereit.

12.5 Ersatzkontoauszug

Sofern der Nutzer ausnahmsweise eine Nacherstellung einzelner Kontoauszüge wünscht, wird die Bank ihm diese gegen Berechnung eines gesonderten Entgelts zur Verfügung stellen. Die Höhe des Entgelts ergibt sich aus dem zu diesem Zeitpunkt geltenden Preis- und Leistungsverzeichnis.

12.6 Mitwirkungs- und Sorgfaltspflichten des Nutzers

Der Nutzer ist verpflichtet, die in sein Archiv eingestellten Kontoauszüge regelmäßig und zeitnah abzurufen und auf ihre Richtigkeit und Vollständigkeit hin unverzüglich zu überprüfen sowie etwaige Einwendung unverzüglich zu erheben. Ebenso ist der Nutzer zur unverzüglichen Benachrichtigung der Bank bei Ausbleiben von Kontoauszügen verpflichtet.

12.7 Hinweis für buchführungs- bzw. aufbewahrungspflichtige Personen:

Online Kontoauszüge 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.

13 Mobile Banking App

13.1 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).

13.2 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.

13.3 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.

13.4 Rechnungsscanner

13.4.1 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.

13.4.2 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.

13.5 Push-Benachrichtigungen

13.5.1 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.

13.5.2 Datenschutzhinweise

(1) Für Push-Benachrichtigungen werden personen- und gerätebezogene Informationen genutzt (siehe Nr. 13.3 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.

14 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.