BEDINGUNGEN FÜR ELEKTRONISCHE BANKDIENSTLEISTUNGEN IM RAHMEN VON IPKO BIZNES

Bank Polski

Gültig ab 14.09.2019

§ 1 Allgemeine Bestimmungen

Die vorliegenden Bedingungen für elektronische Bankdienstleistungen iPKO biznes („**Bedingungen**“) regeln Grundsätze der Erbringung der elektronischen Bankdienstleistungen im Rahmen des iPKO biznes für Firmenkunden der PKO Bank Polski SA Niederlassung Deutschland.

§ 2 Definitionen

Die in den vorliegenden Bedingungen verwendeten Begriffe erhalten folgende Bedeutung:

1) Administrator: Nutzer, der die vom Kontoinhaber erteilten und für einzelne Nutzer geltenden Berechtigungen im dessen Namen verwaltet oder bei Übertragung der Konfigurierung der Berechtigungen der einzelnen Nutzer an die Bank, gilt als Nutzer der vom Kontoinhaber bestimmte Nutzer mit Berechtigung zur Ansicht der Kontoverwaltung-Maske des iPKO biznes-Kontexts,

2) Aktivierung-Freischaltung des Zugangs zum E-Banking iPKO biznes auf Antrag des Kontoinhabers,

3) Autorisierung-Erteilung der Bank der Zustimmung zur Durchführung eines Zahlungsauftrages, eines Auftrags oder sonstiger mittels elektronischer Zugangskanäle eingeleiteter Vorgänge durch den Kontoinhaber oder den Nutzer, für die eine vorherige Authentifizierung oder eine starke Authentifizierung erforderlich ist,

4) Elektronischer Zugangskanal- ein dem Nutzer durch die Bank zur Verfügung gestelltes technisches Verfahren zur Nutzung von Dienstleistungen mit Hilfe von drahtlosen und kabelgebundenen Kommunikationsgeräten, das insbesondere folgende Zugangskanäle umfasst:

a) E-Banking

b) Telefon-Banking

c) Mobile-Banking

(einzelne Zugangskanäle können hinsichtlich des Umfangs der angebotenen Optionen und Funktionen voneinander abweichen und eine aktuelle Beschreibung der in den Zugangskanälen zur Verfügung stehenden Funktionen ist auf der Internetseite der Bank zu finden),

5) Passwort: Zugangscode; ein individuelles und aus einer Reihenfolge von alphanummerischen Zeichen bestehendes Authentifizierungselement zur Verifizierung des Nutzers bei iPKO biznes,

6) Nutzer-ID- ein individuelles Authentifizierungselement zur Verifizierung des Nutzers bei iPKO biznes, das aus einer nur einem bestimmten Nutzer zugeteilten Nummer besteht,

7) individuelles Authentifizierungselement- individuelle und von der Bank zwecks Authentifizierung zur Verfügung gestellten Daten, die auch zur Erteilung der Zustimmung im Zusammenhang mit einem Auftrag und insbesondere zu dessen Autorisierung verwendet werden können,

8) Zahlungsinstrument-ein individualisiertes Gerät oder Verfahren, das dem Kontoinhaber die Erteilung eines Zahlungsauftrags ermöglicht,

9) Einmal verwendbare Transaktionsnummer (TAN) – ein individuelles Authentifizierungselement zur Autorisierung eines Auftrags, das aus eine Reihenfolge von alphanummerischen Zeichen besteht; TAN-Listen werden dem Nutzer als TAN-Block auf einer Chipkarte zur Verfügung gestellt oder mit Hilfe des Mobiltokens iPKO biznes oder des Vasco DigiPass 270-Tokens generiert,

10) Kontext- Kontenübersicht und Liste der zur Nutzung dieser Konten im Rahmen des iPKO biznes berechtigten Nutzer,

11) Benachrichtigung-Mitteilungen an den Kontoinhaber, die an ihn mittels E-Bankings, Service-Centers für Firmenkunden, Aushänge in Filialen der Bank oder auf Internetseiten der Bank oder auf Kontoauszügen übermittelt werden,

12) Starke Authentifizierung- eine Authentifizierung, die so ausgestaltet ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist und die unter Heranziehung von mindestens zwei der folgenden, in dem Sinne voneinander unabhängigen Elementen geschieht, dass die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt: Wissen, Besitz, Inhärenz.

13) Vasco DigiPass-Token- kryptographisches Gerät zur Generierung von einmal verwendbaren Kennwörtern, die der Authentifizierung des Nutzers und Autorisierung der Aufträge bei Nutzung von iPKO biznes dienen,

14) Vertrag- Girokontovertrag,

15)Kontoauskunftsdienst- Online-Dienst, der darin besteht, Auskunft über auf mindestens einem Zahlungskonto des Kontoinhabers, das bei einem anderen oder mehreren anderen Zahlungsdienstleistern geführt wird, vorhandenen Geldmittel zu erteilen.

16) Kontoinformationsdienst - Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten des Zahlungsdienstnutzers bei einem oder mehreren anderen Zahlungsdienstleistern.

17) Zahlungsauslösungsdienst - Dienst, bei dem auf Veranlassung des Zahlungsdienstnutzers ein Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto ausgelöst wird.

18) Authentifizierung- ein Verfahren, mit dessen Hilfe die Bank die Identität eines Nutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann.

19) Nutzer- eine natürliche Person, die zu Rechtsgeschäften oder sonstigen Tätigkeiten im Rahmen seines Berechtigungsumfangs befugt ist und durch den Kontoinhaber zur Nutzung des iPKO biznes ermächtigt wurde und für den Kontoinhaber und in dessen Namen handelt.

§ 3 Zugang zum E-Banking und dessen Nutzung

1. Der Zugang zum E-Banking setzt das Vorhandensein der notwendigen Hardware- und Softwareausstattung voraus, die für die Zusammenarbeit mit der Bank erforderlich ist. Bei einer Nutzung einer Hard-bzw. Software von Drittanbietern durch den Nutzer übernimmt die Bank keine eigene Gewährleistung oder sonstige Verantwortung für eine andauernde Eignung oder Verfügbarkeit im Zusammenhang mit einem Authentifizierungsverfahren.

2. Die Bank teilt auf ihrer Internetseite Anforderungen an die Hardware- und Softwareausstattung mit.

3. Die Bank wird den Kontoinhaber über Grundsätze der ordnungsgemäßen und sicheren Nutzung des E-Bankings und über mögliche Betrugsfälle, verdächtige Ereignisse und atypische Angriffe unterrichten.

4. Informationen gem. Abs.1-3 werden dem Kontoinhaber auf der Internetseite der Bank oder als Benachrichtigungen oder mittels Telefon-Service zur Verfügung gestellt.

5. Eine Information, die dem Kontoinhaber über einen anderen Kommunikationskanal (z.B. per E-Mail) zugeht und sichere und ordnungsgemäße Nutzung von E-Banking betrifft, ist nicht glaubwürdig.

6. Mit Hilfe von E-Banking können Bankprodukte und Dienstleistungen aus dem Angebot der Bank zur Verfügung gestellt werden. Der Kontoinhaber kann Verträge mittels elektronischer Zugangskanäle abschließen, soweit die Bank eine solche Option zur Verfügung gestellt hat.

7. Informationen über Bankprodukte und Dienstleistungen der Bank und Grundsätze und Regeln der Nutzung des E-Bankings und insbesondere Angaben zu dessen Einstellungen und Funktionalität werden auf der Internetseite der Bank veröffentlicht.

8. Der Kontoinhaber ist verpflichtet, sich mit Informationen gem. Abs. 6-7 vor Beginn der Nutzung des E-Bankings vertraut zu machen.

9. Für Änderungen von Informationen und Grundsätzen und Regeln für die Nutzung des E-Bankings gem. Abs. 6-7 und insbesondere der Angaben zu dessen Einstellungen und Funktionalität oder für die Durchführung eines Software-Updates ist die Zustimmung des Kontoinhabers nicht erforderlich.

10. Der Nutzer darf die Anmeldung zum E-Banking und Verfügungen mittels elektronischer Zugangskanäle nur persönlich und mit Hilfe von individuellen Authentifizierungselementen vornehmen, ferner ist er auch verpflichtet:

1) Informationen über sichere Nutzung des E-Bankings vertraulich zu behandeln und keine individuellen Authentifizierungselemente und insbesondere das Passwort, TAN und die an die Bank zur Authentifizierung übermittelte Informationen an Dritte weiterzugeben. Dies gilt nicht für die Nutzung der Zahlungsauslöse- und Kontoinformationsdienste gem. § 4.

2) seine Hardware- und Softwareausstattung, die zur Nutzung von E-Banking verwendet wird, immer im ordnungsgemäßen Zustand zu halten und dabei insbesondere:

a) ausschließlich rechtmäßig erworbene Software zu verwenden, sie laufend zu aktualisieren und Updates gemäß Anweisungen der Softwarehersteller zu installieren.

b) Virenschutzsoftware, Antispamsoftware und Firewall-Programme immer auf dem neusten Stand zu halten,

c) Internetbrowser in der aktuellsten Version zu verwenden,

d) Zugang zu seinem Rechner mit einem Passwort zu sichern, insbesondere wenn der Rechner durch mehrere Personen verwendet werden kann,

e) andere durch die Bank auf ihrer Internetseite empfohlene technische Verfahren zu verwenden,

3) der Bank den Verlust oder die Vernichtung von individuellen Authentifizierungselementen oder die Vornahme von unautorisierten, nicht oder nicht ordnungsgemäß ausgeführten Anweisungen oder Erhalt von Informationen gem. Abs.5 oder beim Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines individuellen Authentifizierungselements unverzüglich anzuzeigen:

– telefonisch unter der in den das E-Banking betreffenden Informationsunterlagen angegebenen Telefonnummer

– persönlich in Filialen der Bank

4) jeden Verlust oder vollständige Beschädigung einer Hard-bzw. Software oder eines individuellen Authentifizierungselements, die für die Nutzung des E-Banking verwendet werden, unverzüglich bei der Polizei zur Anzeige zu bringen.

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

a) Wissenselemente sind geheim zu halten. Sie dürfen insbesondere: nicht außerhalb des E-Banking (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden, nicht elektronisch gespeichert werden (z.B. im Klartext im Computer oder im mobilen Endgerät), nicht auf einem Gerät, das als Besitzelement oder zur Prüfung seines Seinselements verwendet wird, gespeichert oder aufbewahrt werden.

b) Besitzelemente:

-sind vor dem unbefugten Zugriff anderer Personen sicher zu verwahren

-der Nutzer hat sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Nutzes (z.B. Mobiltelefon) oder die auf ihm befindliche Anwendung für die Nutzung des E-Banking nicht zugreifen können

- die auf dem mobilen Endgerät des Nutzers befindliche Anwendung für die Nutzung des E-Banking ist zu löschen, bevor der Nutzer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf des Mobiltelefons)

-die Nachweise des Besitzelements wie z.B. TAN-Nummer dürfen nicht außerhalb des E-Banking mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden,

- der Nutzer hat den von der Bank einen zur Aktivierung des Besitzelements erhaltenen Code vor dem unbefugten Zugriff anderer Personen sicher zu verwahren.

c) Seinselemente dürfen auf einem mobilen Endgerät des Nutzers, das zur Nutzung des E-Banking verwendet wird, nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für iPKO Biznes genutzt wird, Seinselmente anderer Personen gespeichert, dann ist das Wissenselement (z.B. Passwort) zu verwenden.

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

7)Die Bank zeigt dem Nutzer vor der Ausführung eines von ihm erhaltenen Auftrags die von ihm empfangenen Daten wie Betrag, Kontonummer des Zahlungsempfängers auf dem zur Nutzung des E-Banking gesondert vereinbarten Gerät des Nutzers an (z.B. mittels einem mobilen Endgerät). Der Nutzer ist verpflichtet, vor der Authentifizierung die Übereinstimmung der angezeigten Daten mit den für den Auftrag

vorgesehenen Daten zu prüfen und hat den Vorgang abzubrechen und die Bank unverzüglich zu unterrichten, wenn die angezeigten Daten nicht übereinstimmen.

11. Zur Gewährleistung der Sicherheit der durch den Nutzer vorgenommenen Verfügungen werden von der Bank individuelle Authentifizierungselemente verwendet. Die Bank kann die Ausführung einer telefonisch oder per Internet erteilten Verfügung verweigern, wenn berechtigte Zweifel an der Identität des Nutzers oder dessen Authentifizierung bestehen. Für den Zugriff des Nutzers auf sensible Zahlungsdaten im Sinne des § 1 Abs.26 Satz1 ZAG (z.B. Änderung der Anschrift des Kontoinhabers) hat er sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum E-Banking nur ein Authentifizierungselement angefordert wurde, wobei der Name des Kontoinhabers und die Kontonummer keine sensiblen Daten darstellen.

12. Die Bank zeichnet die im Telefon-Service durchgeführten Telefongespräche auf und speichert die mit Hilfe von elektronischen Zugangskanälen vorgenommenen Verfügungen. Die gespeicherten Verfügungen des Nutzers stellen Beweis der Erteilung der jeweiligen Verfügung dar.

13. Der Nutzer kann auf die durch das Bankgeheimnis umfassten Informationen im Umfang zurückgreifen, der sich aus dem Umfang der ihm erteilten Berechtigungen ergibt.

14. Alle Verfügungen, die durch eine als berechtigten Nutzer korrekt verifizierte Person vorgenommen wurden, werden als Verfügungen des im Namen des Kontoinhabers handelnden Nutzers behandelt. Die Bank haftet nicht für Verfügungen, die unter Verstoß gegen Abs. 10 vorgenommen wurden.

15. Die Bank darf Verfügungsrahmen für Zahlungsvorgänge für bestimmte elektronische Zugangskanäle festlegen.

16. Im Fall des Abs. 15 wird die entsprechende Information auf der Internetseite der Bank veröffentlicht.

17. Die Bank darf ganz oder teilweise den Zugang zum E-Banking oder einzelne individuelle Authentifizierungselemente aus sachlichen Gründen im Zusammenhang mit der Einhaltung der Sicherheit des E-Bankings oder beim Verdacht einer unberechtigten Verschaffung des Zugangs zum E-Banking oder vorsätzlicher Vornahme einer unautorisierten Zahlungsverfügung unter bei Verwendung des E-Bankings sperren oder wenn die Bank berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen.

18. Die Bank unterrichtet den Kontoinhaber mittels elektronischer Zugangskanäle über die Sperrung des Zugangs zum E-Banking und insbesondere über die Sperrung der einzelnen individuellen Authentifizierungselementen vor der Sperre oder wenn dies unmöglich ist, unverzüglich nach der Sperre, es sei denn, die Unterrichtung wäre aus Sicherheitsgründen nicht zweckmäßig oder aus rechtlichen Gründen verboten.

19. Die Aufhebung der Sperre und der Austausch der einzelnen individuellen Authentifizierungselementen setzten voraus, dass die zur Sperre führenden Gründe nicht mehr vorliegen. Der Nutzer wird über die Aufhebung der Sperre unverzüglich unterrichtet.

20. Die Nutzung des E-Bankings durch den Kontoinhaber setzt das Vorliegen folgender Voraussetzungen voraus:

a) Inkenntnisnahme der Informationsunterlagen über das E-Banking

b) Abschluss des Vertrages, eines Nachtrages oder Anhangs zum Vertrag

c) Festlegen von Nutzerberechtigungen und insbesondere die Bestimmung zumindest eines Nutzers als Administrator

d) Erhalt der individuellen Authentifizierungselementen

e) Aktivierung des Zugangs

21. Die Nutzung des E-Bankings setzt das Vorhandensein folgender individueller Authentifizierungselemente e voraus:

a) Passwort

b) Nutzer-ID

c) TAN-Block auf einer Chipkarte mit einem Lesegerät oder mobile iPKO biznes-Tokenanwendung - oder Vasco DigiPass 270-Token

22. Die Bestimmung des Umfangs der Berechtigungen der einzelnen Nutzer übernimmt der vom Kontoinhaber bestimmte Administrator mittels der dazu vorgesehenen Optionen im E-Banking oder die Bank gemäß der Verfügung des Kontoinhabers nach Stellung eines separaten Antrages auf Konfigurierung des Zugangs zum iPKO biznes.

23. Die Bank haftet nicht für die Folgen der durch den Administrator, der die Berechtigungen der einzelnen Nutzer verwaltet, vorgenommenen Handlungen. Bei der Übertragung der Konfigurierung der durch den Kontoinhaber bestimmten Nutzerberechtigungen an die Bank ist die Haftung der Bank für die gemäß Anweisungen des Kontoinhabers vorgenommenen Handlungen und deren Folgen ausgeschlossen.

24. Die Bank braucht die Begründetheit der Übertragung der Berechtigungen an einzelne Nutzer und insbesondere der Zuweisung der Rechte zur Erteilung von Zahlungsaufträgen durch den im Namen des Kontoinhabers handelnden Administrator nicht zu prüfen.

25. Die Bearbeitung von E-Banking-Aufträgen richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (zum Beispiel Bedingungen für den Überweisungsverkehr).

§ 4 Nutzung von Zahlungsauslöse-und Kontoinformationsdiensten

1. Zur Auslösung eines Zahlungsauftrages und zum Abruf von Information über ein Zahlungskonto kann der Nutzer gemäß § 675f Abs. 3 BGB auf einen Zahlungsauslösedienst gem. § 1 Abs.33 ZAG beziehungsweise einen Kontoinformationsdienst gem. § 1 Abs.34 ZAG zurückgreifen, der zu diesem Zweck eine technische Verbindung mit der Bank herstellen wird.
2. Die Bank kann Kontoinformationsdienstleistern oder Zahlungsauslösediensten den Zugang zu einem Zahlungskonto verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstes zum Zahlungskonto es rechtfertigen. Die Bank wird den Kontoinhaber über eine solche Zahlungsverweigerung 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 und unterrichtet darüber den Kontoinhaber unverzüglich.

§ 5 Haftung

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

2. Ansprüche und Einwendungen des Kontoinhabers gegen die Bank aufgrund nicht oder fehlerhaft ausgeführter oder aufgrund nicht autorisierter E-Banking-Aufträge sind ausgeschlossen, wenn der Kontoinhaber die Bank nicht spätestens 13 Monate nach dem Tag der Belastung mit einem nicht autorisierten oder fehlerhaft ausgeführten E-Banking-Auftrag hiervon schriftlich unterrichtet hat. Der Lauf der Frist beginnt nur, wenn die Bank

den Kontoinhaber über die Belastungsbuchung des E-Banking-Auftrags entsprechend dem für Kontoinformationen vereinbarten Weg spätestens innerhalb eines Monats nach der Belastungsbuchung unterrichtet hat; anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich.

3. Beruhen nicht autorisierte E-Banking-Aufträge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen individuellen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines individuellen Authentifizierungselements , haftet der Kontoinhaber für den hierdurch entstehenden Schaden bis zu einem Betrag von 50,00 Euro, ohne dass es darauf ankommt, ob den Nutzer ein Verschulden trifft.

4. Der Kontoinhaber 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 eines individuellen Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust eines individuellen Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

5. Handelt es sich bei dem Kontoinhaber nicht um einen Verbraucher, trägt er den aufgrund nicht autorisierter E-Banking-Aufträge entstehenden Schaden auch über einen Betrag von maximal 50,00 Euro hinaus, wenn der Nutzer die ihm nach diesen Bedingungen obliegenden Pflichten fahrlässig verletzt hat. Hat die Bank durch eine Verletzung ihrer Pflichten zur Entstehung des Schadens beigetragen, haftet die Bank für den entstandenen Schaden im Umfang des von ihr zu vertretenden Mitverschuldens.

6. Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absätzen 3,5,7 verpflichtet, wenn der Nutzer die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte. Dies gilt auch dann, wenn die Bank vom Nutzer keine starke Authentifizierung nach § 1 Abs. 24 ZAG verlangt hat

7. Kommt es vor der Sperranzeige zu nicht autorisierten E-Bank-Aufträgen und hat der Nutzer in betrügerischer Absicht gehandelt oder seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Nutzers liegt insbesondere beim Verstoß gegen Bestimmungen des § 3 Absatz 10 vor.

8. Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den geltenden Verfügungsrahmen.

9. Die vorstehenden Absätze 4,6,8 finden keine Anwendung, wenn der Nutzer in betrügerischer Absicht gehandelt hat.

10. Sobald die Bank eine Sperranzeige eines Nutzers erhalten hat, übernimmt sie alle danach durch nicht autorisierte E-Banking-Aufträge entstehenden Schäden. Dies gilt nicht, wenn der Nutzer in betrügerischer Absicht gehandelt hat.

§ 6 Schlussbestimmungen

1. Soweit in diesen Bedingungen nicht anderweitig bestimmt, wird die durch diese Bedingungen begründete Geschäftsbeziehung durch die Allgemeinen Geschäftsbedingungen und die Grundregeln für die Beziehung zwischen dem Kunden und der Bank geregelt („AGB“). Die besonderen Geschäftsbeziehungen sind außerdem durch die Besonderen Bedingungen geregelt, die eine Abweichung oder Ergänzung der AGB darstellen. Diese Besonderen Bedingungen finden insbesondere Anwendung auf die Nutzung von Überweisungen und Lastschriftzahlungen. Der Wortlaut der genannten Bedingungen kann in den Geschäftsräumen der Bank eingesehen werden. Auf Wunsch können die Teilnehmer auch beantragen, dass ihnen ein Exemplar der AGB sowie der Besonderen Bedingungen zu einem späteren Zeitpunkt zur Verfügung gestellt wird.

2. Die Änderung dieser Bedingungen richtet sich nach Ziff.1 Abs.2 AGB.