Raiffeisen Oberösterreich

Geschäftsbedingungen

von Raiffeisen Oberösterreich

Gegenüberstellung der Änderungen 2022

Besondere Bedingungen für Debitkarten
Gegenüberstellung der geänderten Bestimmungen

Fassung Dezember 2021	Fassung Oktober 2022
I. Allgemeine Bestimmungen	**I. Allgemeine Bestimmungen**
2. Ausgabe der Debitkarten **2.3 Ausgabe der digitalen Debitkarte** **2.3.2 Banken-Wallet** Das Kreditinstitut stellt dem Karteninhaber über App Stores Software für mobile Endgeräte mit dafür geeigneten Betriebssystemen zur Verfügung, die es dem Karteninhaber, der am Electronic Banking des Kreditinstitutes (kurz: **ELBA**) teilnimmt, ermöglicht, a. seine digitale Debitkarte, andere mobile Zahlkarten und andere Zahlungsdienste auf dem mobilen Endgerät zu aktivieren, anzuzeigen und zu nutzen; b. Mehrwertservices rund um das mobile Bezahlen zu nutzen und c. im in der Banken-Wallet integrierten Kundenkartenbereich […]	**2. Ausgabe der Debitkarten** **2.3 Ausgabe der digitalen Debitkarte** **2.3.2 Banken-Wallet** Das Kreditinstitut stellt dem Karteninhaber über App Stores Software für mobile Endgeräte mit dafür geeigneten Betriebssystemen zur Verfügung, die es dem Karteninhaber, der am Electronic Banking des Kreditinstitutes (kurz: **ELBA**) teilnimmt, ermöglicht, a. seine digitale Debitkarte, andere mobile Zahlkarten und andere Zahlungsdienste auf dem mobilen Endgerät zu aktivieren, anzuzeigen und zu nutzen; ~~a.~~b. die P2P-Funktion (Punkt II. 6) zu nutzen; ~~b.~~c. Mehrwertservices rund um das mobile Bezahlen zu nutzen und ~~c.~~d. im in der Banken-Wallet integrierten Kundenkartenbereich […]
Weiters kann der Karteninhaber zukünftig ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt in der Banken-Wallet a. wenn Vertragsunternehmen infolge Zahlungen des Karteninhabers im Rahmen des Fernabsatzes (Punkt II.5.3) ein digitales Abbild der Debitkarte (Token) in ihren Systemen hinterlegt haben, den Token -soweit er für die Bank erkennbar ist- verwalten (einschließlich Löschung bzw. Sperre des Tokens) b. die Daten seiner physischen Debitkarte (Kartennummer bzw. PAN, Ablaufdatum), Kartenprüfnummer (eine dreistellige Kartenprüfnummer, die sich auf der Rückseite der Debitkarte befindet; auch CVC bzw. Card Verification Code genannt) sowie den persönlichen Code der physischen Debitkarte abfragen. […]	Weiters kann der Karteninhaber ~~zukünftig ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt~~ in der Banken-Wallet a. wenn Vertragsunternehmen infolge Zahlungen des Karteninhabers im Rahmen des Fernabsatzes (Punkt II.5.3) ein digitales Abbild der Debitkarte (Token) in ihren Systemen hinterlegt haben, den Token -soweit er für die Bank erkennbar ist- verwalten (einschließlich Löschung bzw. Sperre des Tokens). Die Verwaltung von Tokens hat keinen Einfluss auf das Grundgeschäft zwischen Karteninhaber und Vertragsunternehmen (zB auf ein Streaming Abo). b. die Daten seiner physischen Debitkarte - (Kartennummer ~~bzw.~~ (auch als Primary Account Number – in weiterer Folge PAN bezeichnet), Ablaufdatum~~),~~ und Kartenprüfnummer (eine dreistellige Kartenprüfnummer, die sich auf der Rückseite der Debitkarte befindet; auch CVC bzw. Card Verification Code genannt) - sowie den persönlichen Code der physischen Debitkarte abfragen. Die Kundenauthentifizierung im Rahmen der Datenabfragen erfolgt gemäß Punkt I. 3.2. (Kundenauthentifizierung in der Banken-Wallet). […]
Bei der Installation der Banken-Wallet legt der Karteninhaber unter Verwendung des für ELBA vereinbarten Identifikationsverfahrens eine „Wallet-PIN“ fest, die in der Folge für den Zugriff auf Funktionen der Banken-Wallet verwendet wird. Eine Änderung der Wallet-PIN ist auf diesem Wege möglich. Nach 5-facher Falscheingabe der Wallet-PIN wird der Zugriff auf die Banken-Wallet automatisch gesperrt. […]	Bei der Installation der Banken-Wallet legt der Karteninhaber unter Verwendung des für ELBA vereinbarten Identifikationsverfahrens eine „Wallet-PIN“ fest, die in der Folge für den Zugriff auf Funktionen der Banken-Wallet verwendet wird. Eine Änderung der Wallet-PIN ist ~~auf diesem Wege möglich~~vom Karteninhaber durch Eingabe der zuletzt festgelegten Wallet-PIN zu bestätigen. **Nach 5-facher Falscheingabe der Wallet-PIN wird der Zugriff auf die Banken-Wallet automatisch gesperrt und die Banken-Wallet deaktiviert.** Eine neuerliche Aktivierung der installierten Banken-Wallet erfolgt unter Verwendung des für ELBA vereinbarten Identifikationsverfahrens. […]
4. Gültigkeit der Debitkarte, Dauer und Beendigung des Vertrags **4.3 Dauer der Vereinbarung zur P2P-Funktion (Punkt II. 6)** Auch die Vereinbarung über die P2P-Funktion wird auf unbestimmte Zeit abgeschlossen. Sie endet jedenfalls mit der Beendigung der Kontoverbindung, zu der die zugrunde liegende physische Debitkarte des Karteninhabers ausgegeben wurde und/oder mit Beendigung des Kartenvertrags über die zugrunde liegende physische Debitkarte. **Achtung:** Eine gesonderte Beendigung der Vereinbarung über die P2P-Funktion beendet nicht den zugrunde liegenden Kartenvertrag. Die Debitkarte kann im Umfang des Kartenvertrages weiterverwendet werden.	**4. Gültigkeit der Debitkarte, Dauer und Beendigung des Vertrags** ~~**4.3 Dauer der Vereinbarung zur P2P-Funktion (Punkt II. 6)**~~ ~~Auch die Vereinbarung über die P2P-Funktion wird auf unbestimmte Zeit abgeschlossen. Sie endet jedenfalls mit der Beendigung der Kontoverbindung, zu der die zugrunde liegende physische Debitkarte des Karteninhabers ausgegeben wurde und/oder mit Beendigung des Kartenvertrags über die zugrunde liegende physische Debitkarte.~~ ~~**Achtung:** Eine gesonderte Beendigung der Vereinbarung über die P2P-Funktion beendet nicht den zugrunde liegenden Kartenvertrag. Die Debitkarte kann im Umfang des Kartenvertrages weiterverwendet werden.~~

4.4 Kündigung **4.4.1 ordentliche Kündigung** **4.4.1.1 Kündigung durch Konto- oder Karteninhaber** Sowohl der Kontoinhaber als auch der Karteninhaber können den Kartenvertrag (für die physische und/oder digitale Debitkarte) insgesamt oder auch gesondert nur die Vereinbarung über die P2P-Funktion jederzeit zum Letzten eines jeden Monats kündigen. Kündigungen, die am letzten Geschäftstag eines Monats ausgesprochen werden, wirken erst zum ersten Geschäftstag des folgenden Monats.	**4.43 Kündigung** **4.43.1 ordentliche Kündigung** **4.43.1.1 Kündigung durch Konto- oder Karteninhaber** Sowohl der Kontoinhaber als auch der Karteninhaber können den Kartenvertrag (für die physische und/oder digitale Debitkarte) ~~insgesamt oder auch gesondert nur die Vereinbarung über die P2P-Funktion~~ jederzeit zum Letzten eines jeden Monats kündigen. Kündigungen, die am letzten Geschäftstag eines Monats ausgesprochen werden, wirken erst zum ersten Geschäftstag des folgenden Monats.
4.4.1.2 Kündigung durch das Kreditinstitut Das Kreditinstitut kann den Kartenvertrag (für die physische und/oder digitale Debitkarte) insgesamt oder auch gesondert nur die Vereinbarung über die P2P-Funktion unter Einhaltung einer Kündigungsfrist von 2 Monaten kündigen.	**4.43.1.2 Kündigung durch das Kreditinstitut** Das Kreditinstitut kann den Kartenvertrag (für die physische und/oder digitale Debitkarte) ~~insgesamt oder auch gesondert nur die Vereinbarung über die P2P-Funktion~~ unter Einhaltung einer Kündigungsfrist von 2 Monaten kündigen.
4.4.2 außerordentliche Kündigung Bei Vorliegen eines wichtigen Grundes können der Kartenvertrag und die Vereinbarung über die P2P-Funktion vom Kontoinhaber, vom Karteninhaber und von dem Kreditinstitut mit sofortiger Wirkung aufgelöst werden.	**4.43.2 außerordentliche Kündigung** Bei Vorliegen eines wichtigen Grundes ~~können~~kann der Kartenvertrag ~~und die Vereinbarung über die P2P-Funktion~~ vom Kontoinhaber, vom Karteninhaber und von dem Kreditinstitut mit sofortiger Wirkung aufgelöst werden.
4.5 Rechtsfolgen der Kündigung […]	**4.~~5~~4 Rechtsfolgen der Kündigung** […]
5. Sorgfaltspflichten des Karteninhabers Der Karteninhaber ist auch im eigenen Interesse verpflichtet, – eine physische Debitkarte sorgfältig zu verwahren. Eine Weitergabe der Debitkarte an dritte Personen ist nicht zulässig, – das mobile Endgerät, auf dem eine digitale Debitkarte oder die P2P-Funktion aktiviert ist, sorgfältig zu verwahren und vor dem Zugriff Dritter zu schützen. Eine Weitergabe des mobilen Endgerätes an dritte Personen ohne vorherige Deaktivierung der darauf gespeicherten digitalen Debitkarte(n) oder P2P-Funktionen ist nicht zulässig. Warnhinweis: Wenn die am mobilen Endgerät in der Banken-Wallet gespeicherte digitale Debitkarte nicht deaktiviert wird, sind Kleinbetragszahlungen ohne Eingabe des persönlichen Codes (siehe Punkt II. 3) weiterhin möglich. Der persönliche Code, die Wallet-PIN und bei Verwendung der P2P-Funktion die P2P-PIN sind geheim zu halten und dürfen niemandem, insbesondere auch nicht Mitarbeitern des Kreditinstitutes, anderen Kontoinhabern oder anderen Karteninhabern bekannt gegeben werden. Der persönliche Code, die Wallet-PIN und die P2P-PIN dürfen nicht am mobilen Endgerät abgespeichert werden. Bei der Verwendung des persönlichen Codes, der Wallet-PIN und der P2P-PIN ist darauf zu achten, dass diese nicht von Dritten ausgespäht werden.	**5. Sorgfaltspflichten des Karteninhabers** ~~Der Karteninhaber ist auch im eigenen Interesse verpflichtet,~~ – ~~eine physische Debitkarte sorgfältig zu verwahren.~~ Eine Weitergabe der Debitkarte an dritte Personen ist nicht zulässig~~.~~. – ~~das mobile Endgerät, auf dem eine digitale Debitkarte oder die P2P-Funktion aktiviert ist, sorgfältig zu verwahren und vor dem Zugriff Dritter zu schützen.~~ Eine Weitergabe des mobilen Endgerätes an dritte Personen ohne vorherige Deaktivierung der darauf gespeicherten digitalen Debitkarte(n) ~~oder P2P-Funktionen~~ ist nicht zulässig. Warnhinweis: Wenn die am mobilen Endgerät in der Banken-Wallet gespeicherte digitale Debitkarte nicht deaktiviert wird, sind Kleinbetragszahlungen ohne Eingabe des persönlichen Codes (siehe Punkt II. 3) weiterhin möglich. Der persönliche Code~~,~~ und die Wallet-PIN ~~und bei Verwendung der P2P-Funktion die P2P-PIN~~ sind geheim zu halten und dürfen niemandem, insbesondere auch nicht Mitarbeitern des Kreditinstitutes, anderen Kontoinhabern oder anderen Karteninhabern bekannt gegeben werden. Der persönliche Code~~,~~ und die Wallet-PIN ~~und die P2P-PIN~~ dürfen nicht am mobilen Endgerät abgespeichert werden. Bei der Verwendung des persönlichen Codes~~,~~ und der Wallet-PIN ~~und der P2P-PIN ist darauf zu achten, dass diese nicht von Dritten ausgespäht werden~~hat der Kunde alle zumutbaren Vorkehrungen zu treffen, um diese vor unbefugten Zugriffen zu schützen.
Bei Zahlungen mit der Debitkarte im Fernabsatz (Punkt II. 5) ist der Karteninhaber verpflichtet, – bei Eingabe der Kartendaten und Verwendung der Signatur-App darauf zu achten, dass die Eingabe nicht von Dritten ausgespäht wird, und die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten zu schließen und nicht nur deren Anzeige zu beenden, sodass es einem unberechtigten Dritten nicht möglich ist, auf diese zuzugreifen, – unverzüglich die Sperre der Debitkarte für Zahlungen im Fernabsatz zu veranlassen, wenn er in Kenntnis davon ist, dass ein unbefugter Dritter Zugang zu seinen Kartendaten hat.	Bei Zahlungen mit der Debitkarte im Fernabsatz (Punkt II. 5) ist der Karteninhaber verpflichtet, bei ~~Eingabe der Kartendaten und~~ Verwendung der Signatur-App ~~darauf zu achten, dass die Eingabe nicht von Dritten ausgespäht wird, und die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten zu schließen und nicht nur deren Anzeige zu beenden, sodass es einem unberechtigten Dritten nicht möglich ist, auf diese zuzugreifen,~~ ~~unverzüglich die Sperre der Debitkarte für Zahlungen im Fernabsatz zu veranlassen, wenn er in Kenntnis davon ist, dass ein unbefugter Dritter Zugang zu seinen Kartendaten hat~~alle zumutbaren Vorkehrungen zu treffen, um den Signatur-Code vor unbefugten Zugriffen zu schützen.
7. Sperre, Limitsenkung **7.1 Sperre durch den Kontoinhaber oder den Karteninhaber** **7.1.1 Sperre der Debitkarte** Die Sperre einer Debitkarte kann vom Kontoinhaber für jede zum Konto ausgegebene Debitkarte oder vom betreffenden Karteninhaber wie folgt beauftragt werden: […] – ab dem 1. April 2021 jederzeit durch Eingabe des Sperrauftrags im vom Kontoinhaber bzw. Karteninhaber	**7. Sperre, Limitsenkung** **7.1 Sperre durch den Kontoinhaber oder den Karteninhaber** **7.1.1 Sperre der Debitkarte** Die Sperre einer Debitkarte kann vom Kontoinhaber für jede zum Konto ausgegebene Debitkarte oder vom betreffenden Karteninhaber wie folgt beauftragt werden: […] – ~~ab dem 1. April 2021~~ ausschließlich in Bezug auf eine physische Debitkarte jederzeit durch Eingabe des Sperr-

genutzten ELBA des Kreditinstitutes unter Verwendung des dafür vereinbarten Identifikationsverfahrens. […]	auftrags im vom Kontoinhaber bzw. Karteninhaber genutzten ELBA des Kreditinstitutes unter Verwendung des dafür vereinbarten Identifikationsverfahrens. […]
7.1.2 Sperre der Zahlungen im Fernabsatz und der P2P-Funktion Die Möglichkeit, mit einer Debitkarte Zahlungen im Fernabsatz (Punkt II. 5) zu tätigen, kann für sich allein vom Karteninhaber – nicht jedoch vom Kontoinhaber - ebenso gesondert gesperrt werden wie die zur Debitkarte vereinbarte P2P-Funktion (siehe Punkt II. 6). Diese Sperren kann auch nur der Karteninhaber wieder aufheben. Eine Sperre der P2P-Funktion ohne Angabe der Kartenfolgenummer bewirkt bis auf weiteres die Sperre der P2P-Funktion aller zum Konto ausgegebenen Debitkarten. Nach vorgenommener Sperre wird die P2P-Funktion nur aufgrund eines Auftrags des Karteninhabers wieder aktiviert.	**7.1.2 Sperre der Zahlungen im Fernabsatz ~~und der P2P-Funktion~~** Die Möglichkeit, mit einer Debitkarte Zahlungen im Fernabsatz (Punkt II. 5) zu tätigen, kann für sich allein vom Karteninhaber – nicht jedoch vom Kontoinhaber - ~~ebenso~~ gesondert gesperrt werden~~ wie die zur Debitkarte vereinbarte P2P-Funktion (siehe Punkt II. 6)~~. Diese Sperre~~n~~ kann auch nur der Karteninhaber wieder aufheben. ~~Eine Sperre der P2P-Funktion ohne Angabe der Kartenfolgenummer bewirkt bis auf weiteres die Sperre der P2P-Funktion aller zum Konto ausgegebenen Debitkarten. Nach vorgenommener Sperre wird die P2P-Funktion nur aufgrund eines Auftrags des Karteninhabers wieder aktiviert.~~
II. Benützung der Geldausgabeautomaten und bargeldlose Zahlungen	**II. Benützung der Geldausgabeautomaten und bargeldlose Zahlungen**
5. Zahlungen mit der physischen Debitkarte im Fernabsatz **5.3. Zahlungen im Fernabsatz** […]	**5. Zahlungen mit der physischen Debitkarte im Fernabsatz** **5.3. Zahlungen im Fernabsatz** […] **5.3.4 Vertrauenswürdige Empfänger** Der Kontoinhaber hat die Möglichkeit im Rahmen des 3D-Secure-Verfahrens des auf der Debitkarte ersichtlich gemachten Debitkarten-Service Vertragsunternehmen im In- und Ausland als vertrauenswürdige Empfänger zu definieren. Zahlungen mit der physischen Debitkarte im Fernabsatz an Vertragsunternehmen, die der Kontoinhaber zuvor als vertrauenswürdige Empfänger definiert hat, sind ohne Anwendung des 3D-Secure-Verfahrens (Punkt I. 5.3.1.1.) - auch durch den Karteninhaber - bloß mittels Bekanntgabe der Kartendaten möglich. Der Karteninhaber weist in diesem Fall durch Bekanntgabe der Kartendaten das Kreditinstitut unwiderruflich an, den Rechnungsbetrag im Rahmen des dafür mit dem Kontoinhaber vereinbarten Limits an den jeweiligen vertrauenswürdigen Empfänger zu zahlen. Das Kreditinstitut nimmt diese Anweisung bereits jetzt an. Bei wiederkehrenden Zahlungsvorgängen gilt die Anweisung zum ersten Zahlungsvorgang auch für alle nachfolgenden Zahlungsvorgänge. Aus Gründen der Sicherheit ist das Kreditinstitut berechtigt, auch bei Zahlungen an vertrauenswürdige Empfänger im Einzelfall eine Authentifizierung im Rahmen des 3D-Secure-Verfahrens zu verlangen oder einzelne Vertragsunternehmen nicht als vertrauenswürdige Empfänger zu akzeptieren. Der Kontoinhaber kann vertrauenswürdige Empfänger mittels Auftrag an das Kreditinstitut entfernen lassen. Ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt kann der Kontoinhaber im ELBA des Kreditinstituts unter Verwendung des dafür vereinbarten Identifikationsverfahrens die von ihm definierten vertrauenswürdigen Empfänger abfragen sowie entfernen. **5.4 Abfrage der Kartenprüfnummer (CVC) im ELBA** Nutzt der Karteninhaber das ELBA des Kreditinstituts kann er zukünftig die Kartenprüfnummer (CVC) ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt unter Verwendung des für ELBA vereinbarten Identifikationsverfahrens dort abfragen.
6. P2P-Zahlungen **6.1 Beschreibung der P2P-Funktion** Die P2P-Funktion ermöglicht dem Karteninhaber, der auch Inhaber des Kontos ist, zu dem die physische Debitkarte ausgegeben wurde, mit Hilfe der in der Banken-Wallet gespeicherten digitalen Debitkarte über ein mobiles Endgerät – das unbare Senden von Geldbeträgen an einen von ihm gewählten Empfänger, der Inhaber einer von dem Kreditinstitut oder einem anderen österreichischen Kreditinstitut ausgestellten Debitkarte oder Kreditkarte ist, und – das Empfangen von Geldbeträgen (= der Geldbetrag wird von einer dritten Person an den Karteninhaber bezahlt). Ab dem 7.6.2022 steht diese Funktion auch Karteninhabern, die nicht auch Inhaber des Kontos sind, zu dem die physische Debitkarte ausgegeben wurde, zur Verfügung.	**6. P2P-Zahlungen** **6.1 Beschreibung der P2P-Funktion** Die P2P-Funktion ermöglicht dem Karteninhaber~~, der auch Inhaber des Kontos ist, zu dem die physische Debitkarte ausgegeben wurde,~~ mit Hilfe der in der Banken-Wallet gespeicherten digitalen Debitkarte über ein mobiles Endgerät – das unbare Senden von Geldbeträgen an einen von ihm gewählten Empfänger, der Inhaber einer von dem Kreditinstitut oder einem anderen österreichischen Kreditinstitut ausgestellten Debitkarte oder Kreditkarte ist, und – das Empfangen von Geldbeträgen (= der Geldbetrag wird von einer dritten Person an den Karteninhaber bezahlt). ~~Ab dem 7.6.2022 steht diese Funktion auch Karteninhabern, die nicht auch Inhaber des Kontos sind, zu dem die physische Debitkarte ausgegeben wurde, zur Verfügung.~~

6.2 Authentifizierung der P2P-Zahlung, P2P-PIN Die Authentifizierung im Rahmen des Sendens eines Geldbetrages, erfolgt über die mit dem Kreditinstitut vereinbarte Signatur-App, durch Eingabe der vom Karteninhaber im Zuge der Registrierung für die P2P-Funktion zu wählenden P2P-PIN oder über die am mobilen Endgerät eingerichteten biometrischen Mittel (zB Fingerabdruck, Gesichtserkennung, Iris-Scan). Ab dem 7.6.2022 erfolgt die Authentifizierung durch Kundenauthentifizierung gemäß Punkt I.3.2.	**6.2 Authentifizierung der P2P-Zahlung~~, P2P-PIN~~** Die Authentifizierung im Rahmen des Sendens eines Geldbetrages~~,~~ erfolgt ~~über die mit dem Kreditinstitut vereinbarte Signatur-App, durch Eingabe der vom Karteninhaber im Zuge der Registrierung für die P2P-Funktion zu wählenden P2P-PIN oder über die am mobilen Endgerät eingerichteten biometrischen Mittel (zB Fingerabdruck, Gesichtserkennung, Iris-Scan). Ab dem 7.6.2022 erfolgt die Authentifizierung durch Kundenauthentifizierung~~ gemäß Punkt I.3.2 (Kundenauthentifizierung in der Banken-Wallet).
6.3 Nutzung der P2P-Funktion **6.3.1 Geld senden** Der Karteninhaber ist berechtigt, mit seiner Debitkarte mittels der P2P-Funktion bis zu dem mit ihm für diese Funktion vereinbarten Limit bargeldlos Zahlungen in Euro durchzuführen, wofür im Zuge der Zahlungsanweisung entweder die Mobiltelefonnummer des Empfängers oder die Kartennummer (PAN) der Debit- oder Kreditkarte des Empfängers abgefragt wird. Der Karteninhaber weist durch Authentifizierung (siehe Punkt 6.2.) das Kreditinstitut an, den Zahlungsbetrag an den jeweiligen Empfänger zu zahlen. Nach erfolgter Zahlungsanweisung können die mittels P2P-Funktion erteilten Zahlungsaufträge nicht mehr widerrufen werden. Das Kreditinstitut nimmt die mit einem solchen Zahlungsauftrag erteilte Anweisung bereits jetzt an.	**6.3 Nutzung der P2P-Funktion** **6.3.1 Geld senden** Der Karteninhaber ist berechtigt, mit seiner Debitkarte mittels der P2P-Funktion bis zu dem mit ihm für diese Funktion vereinbarten Limit bargeldlos Zahlungen in Euro durchzuführen, wofür im Zuge der Zahlungsanweisung ~~entweder die Mobiltelefonnummer des Empfängers oder~~ die Kartennummer (PAN) der Debit- oder Kreditkarte des Empfängers abgefragt wird. Der Karteninhaber weist durch Authentifizierung (siehe Punkt 6.2.) das Kreditinstitut an, den Zahlungsbetrag an den jeweiligen Empfänger zu zahlen. Nach erfolgter Zahlungsanweisung können die mittels P2P-Funktion erteilten Zahlungsaufträge nicht mehr widerrufen werden. Das Kreditinstitut nimmt die mit einem solchen Zahlungsauftrag erteilte Anweisung bereits jetzt an.

Bedingungen für Electronic Banking-Leistungen (Internetbanking und ELBA business) Gegenüberstellung der geänderten Bestimmungen

In den gesamten Bedingungen wurde die Begriffsterminologie folgendermaßen angepasst:

Fassung Dezember 2021	Fassung Oktober 2022
Telefonservice	Kundenkontakt Center

Fassung Dezember 2021	Fassung Oktober 2022
6. Sorgfaltspflichten der Kunden und Haftung Jeden Kunden treffen nachstehende Sorgfaltspflichten: i. Die im Rahmen des vereinbarten Identifikationsverfahrens (einschließlich einer sonstigen elektronischen Signatur (Punkt 4 a) (iii)) zu verwendenden Identifikationsmerkmale müssen geheim gehalten werden. Es ist sicherzustellen, dass unbefugte Dritte keinen Zugriff auf die Identifikationsmerkmale haben. Zulässig ist die Weitergabe der mit dem Kreditinstitut vereinbarten Identifikationsmerkmale an Zahlungsauslöse-dienstleister oder Kontoinformationsdienstleister, **wobei Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte dazu auch ohne Zustimmung des Kontoinhabers berechtigt sind**. Ist für die Verwendung eines vereinbarten Identifikationsverfahrens ein Mobiltelefonanschluss erforderlich, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf die Telefone dieses Mobiltelefonanschlusses haben. Wird für das Identifikationsverfahren ein sonstiges Endgerät verwendet, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf dieses Endgerät haben. […]	**6. Sorgfaltspflichten der Kunden und Haftung** Jeden Kunden treffen nachstehende Sorgfaltspflichten: i. Die im Rahmen des vereinbarten Identifikationsverfahrens (einschließlich einer sonstigen elektronischen Signatur (Punkt 4 a) (iii)) zu verwendenden Identifikationsmerkmale müssen geheim gehalten werden. ~~Es ist sicherzustellen, dass unbefugte Dritte keinen Zugriff auf die Identifikationsmerkmale haben.~~Der Kunde hat alle zumutbaren Vorkehrungen zu treffen, um die Identifikationsmerkmale vor unbefugtem Zugriff zu schützen. Zulässig ist die Weitergabe der mit dem Kreditinstitut vereinbarten Identifikationsmerkmale an Zahlungsauslösedienstleister oder Kontoinformations-dienstleister, **wobei Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte dazu auch ohne Zustimmung des Kontoinhabers berechtigt sind.** Ist für die Verwendung eines vereinbarten Identifikationsverfahrens ein Mobiltelefonanschluss erforderlich, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf die Telefone dieses Mobiltelefonanschlusses haben. Wird für das Identifikationsverfahren ein sonstiges Endgerät verwendet, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf dieses Endgerät haben. […]
15. Telefonservice (TSC) Telefonservice ermöglicht - nach elektronischer Autorisierung - die telefonische Erteilung von Zahlungsaufträgen und Wertpapieraufträgen an das Kreditinstitut über deren Telefonservice-Center und die telefonische Abfrage von Kontoinformationen nach Maßgabe der vorliegenden Teilnahmebedingungen. Bei Inanspruchnahme des Telefonservice hat der Kunde seinen Namen und allfällige sonstige Identifikationsmerkmale bekannt zu geben und sich durch Eingabe der verlangten Stellen der PIN über die Telefontastatur oder durch Verwendung eines anderen vereinbarten Identifikationsverfahrens zu identifizieren. Alle vom Kunden mit dem Telefonservice-Center geführten Telefonate werden aus Sicherheitsgründen aufgezeichnet und dürfen als Beweismittel verwendet werden.	**15. ~~Telefonservice~~Kundenkontakt Center (~~TS~~KKC)** ~~Telefonservice~~Die telefonische Kundenservicierung durch das Kundenkontakt Center ermöglicht - nach ~~elektronischer~~ Autorisierung - unter anderem die telefonische Durchführung von Terminvereinbarungen mit Mitarbeitern des Kreditinstituts, die Erteilung von Zahlungsaufträgen und Wertpapieraufträgen an das Kreditinstitut ~~über deren Telefonservice-Center und~~, die ~~telefonische Abfrage~~ Beauskunftung von Konto- und Produktinformationen nach Maßgabe der vorliegenden Teilnahmebedingungen, die Bestellung, Aktivierung und Änderung von Bankprodukten nach Vorgabe des Kunden sowie technische und fachliche Hilfestellungen. Die telefonische Kundenservicierung wird entweder von Mitarbeitern des Kreditinstitutes selbst erbracht oder kann von Mitarbeitern eines beauftragten Dienstleisters übernommen werden. Bei Inanspruchnahme des ~~Telefonservice~~Kundenkontakt Centers hat der Kunde seinen Namen und allfällige sonstige Identifikationsmerkmale bekannt zu geben und sich durch Eingabe der verlangten Stellen der PIN über die Telefontastatur, über die Signatur-App oder durch Verwendung eines anderen vereinbarten Identifikationsverfahrens zu identifizieren. ~~Alle vom Kunden mit dem Telefonservice-Center geführten Telefonate werden aus Sicherheitsgründen aufgezeichnet und dürfen als Beweismittel verwendet werden.~~ Telefonate mit dem Kundenkontakt Center können bspw. aufgrund rechtlicher Erfordernisse, aus Sicherheitsgründen oder im Rahmen der Einwilligung aufgezeichnet und als Beweismittel verwendet werden. Einen entsprechenden Hinweis erhält der Kunde jeweils vor den davon betroffenen Gesprächen. Nähere Informationen zur Telefonaufzeichnung finden sich bspw. auf der Homepage des Kreditinstitutes unter der Rubrik Datenschutz.