acrevis
Meine Bank fürs Leben

Besondere Bestimmungen digitale Banking Services

Dieser Text gilt sinngemäss für weibliche und eine Mehrzahl von Personen.

Die Besonderen Bestimmungen digitale Banking Services regeln die Nutzung der digitalen Services der Bank durch den Vertragspartner und andere Benutzer. Als "**Vertragspartner"** gilt diejenige Person, welche die Geschäftsbeziehung bei der Bank führt. Als "**Benutzer"** gelten diejenigen Personen, welche als Vertragspartner oder bevollmächtigte Person die digitalen Services nutzen.

Mit der Nutzung der digitalen Services anerkennt der Vertragspartner bzw. der Benutzer die vorliegenden Besonderen Bestimmungen digitale Banking Services sowie die Datenschutzerklärung. Die Allgemeinen Geschäftsbedingungen (AGB), das Depotreglement sowie weitere Vereinbarungen zwischen Vertragspartner und Bank, sind für den Benutzer verbindlich. Der Vertragspartner hat die Benutzer darüber sowie über weitere wesentliche Informationen, insbesondere Risikoaufklärungen, in Kenntnis zu setzen bzw. aufzuklären.

Die Bank behält sich jederzeit Änderungen der besonderen Bestimmungen digitale Banking Services vor.

1. Umfang der digitalen Services

Die digitalen Services ermöglichen es dem Vertragspartner, seine Bankgeschäfte online zu erledigen und Informationen abzurufen. Er kann insbesondere Konto- und Depotinformationen abrufen, Zahlungs- und Börsenaufträge abwickeln sowie Karteninformationen abfragen und Kartenmutationen vornehmen.

Der Umfang der jeweils verfügbaren digitalen Services wird durch die Bank festgelegt und kann jederzeit geändert, weiterentwickelt sowie erhöht oder reduziert werden.

2. Zugang zu den digitalen Services

2.1 Technische Voraussetzungen

Der Zugang zu den digitalen Services erfolgt über das Internet über einen Netzbetreiber (Provider). Hierzu benötigt der Benutzer die entsprechende Hard- und Software, welche im Verantwortungsbereich des Benutzers liegen.

Der Benutzer ist verpflichtet, die notwendigen Sicherheitsvorkehrungen zu treffen, insbesondere seine Zugriffsgeräte angemessen gegen den unbefugten Zugriff durch Dritte und gegen Cyberrisiken zu schützen und die Sicherheitseinstellungen seiner Zugriffsgeräte auf dem aktuellen Stand zu halten.

2.2 Legitimationsprüfung

Zugang zu den digitalen Services erhält, wer sich durch Eingabe der persönlichen Legitimationsmerkmale (wie z.B. Identifikation über acrevis Mobile Banking App, Passwort, Legitimationskennziffern, Hardware-Token nachstehend "Legitimationsmittel" genannt) gegenüber der Bank legitimiert hat. Dem Benutzer werden die persönlichen Legitimationsmittel zum bestimmungsmässigen Gebrauch zur Verfügung gestellt. Die Bank kann die Legitimationsmittel jederzeit aus sachlichen Gründen austauschen oder anpassen.

Erfolgt eine Legitimation mittels biometrischer Daten, liegt es am Benutzer, sicherzustellen, dass er die einzige Person ist, deren biometrische Daten auf dem Gerät hinterlegt sind. Die Bank hat weder die Möglichkeit, die auf dem jeweiligen Zugriffgerät hinterlegten, biometrischen Daten einzusehen noch diese zu kontrollieren oder zu beeinflussen. Das verwendete Gerät ist durch den Benutzer vor unbefugtem Zugriff zu schützen.

Im Rahmen der Legitimationsprüfung ist die Bank berechtigt, beauftragten Dritten die Legitimationsmittel des Benutzers bekannt zu geben.

2.3 Nutzungsverantwortung

Der Vertragspartner trägt das Risiko und die Schäden, welche Benutzer bei der Nutzung der digitalen Services verursachen.

Jede sich mittels der Legitimationsmittel legitimierende Person, unabhängig von ihrem internen Rechtsverhältnis zum Vertragspartner und ungeachtet anderslautender Handelsregistereinträge, Veröffentlichungen oder Regelungen auf den Unterschriftendokumenten, darf seitens der Bank als korrekt legitimierter Benutzer betrachtet werden. Die Bank darf daher ohne weitere Überprüfung der Berechtigung von einer solchen Person Aufträge und rechtsverbindliche Mitteilungen entgegennehmen. Dies gilt auch, wenn es sich bei dieser Person um einen unberechtigten Benutzer handelt, der sich legitimieren konnte. Sämtliche Handlungen, die aufgrund der vorerwähnten Legitimationsprüfung erfolgen, sind vom Vertragspartner zu verantworten.

Der Vertragspartner anerkennt vorbehaltlos sämtliche Transaktionen, Geschäfte, Vereinbarungen und Erklärungen, welche im Rahmen der digitalen Services unter Verwendung der Legitimationsmittel des Benutzers getätigt werden. Sämtliche Instruktionen, Aufträge und Mitteilungen, welche die Bank auf diesem Weg erreichen, sind für den Vertragspartner verbindlich.

2.4 Auftragserteilung

Die Bank wird vom Vertragspartner beauftragt, die bei ihr über die digitalen Services eingehenden Aufträge auszuführen sowie den Instruktionen und Mitteilungen nachzukommen, falls die systemgemässe Legitimationsprüfung erfolgt ist. Werden der Bank im Rahmen der Nutzung der digitalen Services Aufträge erteilt, so ist sie berechtigt, einzelne Aufträge nach ihrem freien Ermessen abzulehnen.

Falls der Benutzer vom Vertragspartner gegenüber der Bank ausserhalb der digitalen Services nicht separat als Bevollmächtigter ernannt wurde und die Bank ihn als solchen akzeptiert hat, führt die Bank keine Aufträge aus und kommt keinen Instruktionen nach, falls diese vom Benutzer ausserhalb der digitalen Services übermittelt werden.

Die Bank hat das Recht, jederzeit und ohne Angabe von Gründen die Entgegennahme von Instruktionen, Aufträgen und Mitteilungen über die digitalen Services abzulehnen.

Erteilt der Benutzer der Bank einen Auftrag, welcher nicht oder nur teilweise auftragsgemäss ausgeführt wurde, muss dies umgehend bei der Bank beanstandet werden.

2.5 Sperrung des Zugangs

Der Benutzer kann seinen Zugang zu den digitalen Services selbst sperren oder sperren lassen. Der Vertragspartner kann die Sperrung des Zugangs eines Benutzers bei der Bank verlangen. Die Sperre kann während der üblichen Geschäftszeit bei der kontoführenden Geschäftsstelle der Bank oder ausserhalb der üblichen Geschäftszeiten beim Service Desk verlangt werden und muss der Bank unverzüglich schriftlich bestätigt werden.

In dringenden Fällen kann der Benutzer seinen Zugang in Eigenregie sperren, indem er die Legitimationsmittel bewusst mehrfach falsch eingibt, bis die sicherheitsbedingte Sperre aktiviert wird. Die Sperre kann auf Antrag des Vertragspartners bei der Bank wieder aufgehoben werden.

Besteht Anlass zum Verdacht, dass unbefugte Drittpersonen Kenntnis von Legitimationsmitteln des Benutzers gewonnen oder Zugang zu den digitalen Services erhalten haben oder bei Verdacht auf Missbrauch hat der Benutzer unverzüglich die Sperrung zu veranlassen und die Bank zu informieren.

Die Bank ist jederzeit berechtigt, den Zugang des Benutzers ganz oder teilweise zu sperren, ohne Angabe von Gründen und ohne vorgängige Kündigung.

3. Kosten und Entschädigungen

Dem Vertragspartner stehen die allgemeinen Dienstleistungen der Bank im Rahmen der digitalen Services kostenlos zur Verfügung. Die Bank hat das Recht Gebühren für die Nutzung der digitalen Services einzuführen und abzuändern. Die Einführung oder Änderung von Kosten wird dem Vertragspartner durch elektronische Anzeige, Mitteilung in den digitalen Services oder auf andere geeignete Weise mitgeteilt. Die Einführung oder Änderung gilt ohne schriftlichen Widerspruch innert Monatsfrist ab Bekanntgabe als genehmigt.

Der Vertragspartner ermächtigt die Bank, allfällige Kosten und Gebühren einem Konto des Vertragspartners zu belasten.

4. Sorgfaltspflichten

Der Benutzer ist verpflichtet, sein Passwort bei einer allfälligen Zustellung durch die Bank unverzüglich nach Erhalt zu ändern. Das Passwort ist anschliessend durch den Benutzer regelmässig zu ändern.

Der Benutzer ist verpflichtet, alle Legitimationsmittel geheim zu halten und gegen missbräuchliche Verwendung durch Unbefugte zu schützen. Insbesondere darf ein allfälliges Passwort nach seiner Änderung nicht aufgezeichnet oder ungeschützt auf dem Computer des Benutzers gespeichert oder unbefugten Dritten offengelegt werden. Das Passwort darf überdies nicht aus naheliegenden, leicht ermittelbaren Daten (Namen, Geburtsdaten, Telefonnummern, Autokennzeichen usw.) bestehen.

Die Bank wird zu keinem Zeitpunkt weder mit dem Vertragspartner noch mit dem Benutzer elektronisch oder telefonisch in Kontakt treten, um Zugangsdaten zu erfragen oder dazu aufzufordern, Legitimationsmittel für die Nutzung der digitalen Services bekannt zu geben.

Der Vertragspartner trägt sämtliche Folgen, die sich aus der Preisgabe und der auch missbräuchlichen Verwendung der Legitimationsmittel der Benutzer ergeben.

Der Benutzer nimmt zur Kenntnis, dass er alle im Zusammenhang mit den digitalen Services abzuwickelnden Aufträge selbst erfassen muss. Fehlerhaft erfasste Aufträge können in der Regel nicht geändert werden. Der Bank obliegt keine Überwachungspflicht.

5. Elektronische Konto-/Depotdokumente

Der Vertragspartner anerkennt, dass die schriftliche Mitteilung und die Mitteilung in elektronischer Form in gleicher Weise verbindlich sind.

Sobald die elektronischen Konto-/Depotdokumente für den Benutzer auf der digitalen Services-Umgebung abrufbar sind, gelten diese dem Vertragspartner als zugestellt. Hat der Benutzer die Konto-/Depotdokumente abgerufen, so sind diese mindestens während drei Monaten verfügbar.

Die Verantwortung für die Aufbewahrung der Konto-/Depotdokumente liegt allein beim Benutzer. Für allfällige Beanstandungen bezüglich der getätigten Transaktionen gelten die Allgemeinen Geschäftsbedingungen der Bank. Der Vertragspartner hat jederzeit das Recht, Konto-/Depotdokumente in Papierform zu beziehen. Dabei erklärt sich der Vertragspartner mit der jeweiligen Gebührenordnung der Bank einverstanden.

6. Gesicherter Kommunikationskanal

Im Rahmen der digitalen Services stellt die Bank dem Benutzer einen gesicherten Kommunikationskanal mit der Bank zur Verfügung, über welchen der Benutzer und die Bank Mitteilungen sowie Dokumente austauschen können. Durch den Benutzer übermittelte Mitteilungen und Dokumente werden zu den üblichen Geschäftszeiten der Bank bearbeitet.

Über den gesicherten Kommunikationskanal dürfen keine zeitkritischen Aufträge (wie z.B. Zahlungs- oder Börsenaufträge) erteilt werden.

Mitteilungen und Dokumente gelten dem Vertragspartner als zugestellt, sobald diese für den Benutzer auf der digitalen Services-Umgebung abrufbar sind. Der Benutzer hat daher sicherzustellen, die entsprechenden Mitteilungen und Dokumente zeitgerecht zur Kenntnis zu nehmen und dem Vertragspartner zur Kenntnis zu bringen.

Der Benutzer ist bei Erhalt eines Dokuments über diesen Kommunikationskanal verpflichtet, die Dokumente ausserhalb der digitalen Services zu speichern.

Die Bank ist berechtigt, bei Überschreitung des Speicherplatzes oder nach Ablauf einer Frist die digital zur Verfügung gestellten Dokumente zu löschen.

7. Elektronische Unterzeichnung von Dokumenten

Ausgewählte Dokumente können mittels digitalen Services entsprechend der Zeichnungsberechtigung elektronisch signiert werden. Dokumente, die zur elektronischen Unterzeichnung zur Verfügung gestellt werden, sind durch den Benutzer sorgfältig auf Vollständigkeit und Richtigkeit zu prüfen. Bei Unvollständigkeit oder Unrichtigkeit hat der Benutzer dies umgehend bei der Bank zu beanstanden. Diese Dokumente können digital signiert werden. Mittels elektronischer Signatur dieser Dokumente erklärt sich der Kunde mit dem Inhalt der Dokumente einverstanden und bestätigt, diese gelesen und verstanden zu haben. Elektronisch signierte Dokumente entfalten dieselbe Wirkung wie handschriftlich unterzeichnete. Ausgedruckte Kopien, die nachträglich handschriftlich unterzeichnet werden, entfalten nur Rechtswirkung, wenn sie von der Bank akzeptiert werden.

Zur Ausstellung entsprechender Zertifikate für die elektronische Signatur stellt der Benutzer der Bank die hierfür benötigten Daten (z.B. Vorname, Name, Geburtsdatum, Nationalität, Ausweisart und Ausweisnummer) zur Verfügung und ermächtigt die Bank diese zwecks Ausstellung des Zertifikats einem durch die Bank beauftragten Zertifizierungsdienstleister weiterzuleiten.

Auf der digitalen Services-Umgebung signierte Dokumente werden dem Benutzer für einen bestimmten Zeitraum durch die Bank zur Verfügung gestellt. Der Benutzer hat diese Dokumente ausserhalb der digitalen Services abzuspeichern.

Der Vertragspartner anerkennt ausdrücklich die Verbindlichkeit und Gültigkeit von Zertifikaten und elektronischen Signaturen, welche durch die von der Bank eingesetzten Zertifizierungsdienstleister ausgestellt werden als Beweismittel für alle Handlungen und Transaktionen zwischen dem Vertragspartner und der Bank.

8. Benachrichtigungsdienste

Im Rahmen der digitalen Services stellt die Bank dem Benutzer die Möglichkeit zur Verfügung, über bestimmte Ereignisse mittels elektronischer Kommunikation benachrichtigt zu werden (z.B. SMS, E-Mail oder Push-Benachrichtigungen). Mit der Aktivierung von Benachrichtigungsdiensten stimmt der Benutzer der Zustellung der gewählten Benachrichtigungen explizit zu. Der Vertragspartner und der Benutzer nehmen zur Kenntnis, dass im Rahmen dieser Benachrichtigungen personenbezogene Daten und dem Bankkundengeheimnis unterstehende Daten übermittelt werden. Diese Übermittlung kann über ungesicherte Kanäle erfolgen, welche durch die Bank nicht kontrolliert werden.

Aus technischen Gründen übernimmt die Bank keine Gewähr, dass diese Benachrichtigungen tatsächlich dem Benutzer zugehen. Technische Gründe können dabei z.B. Verzögerungen, Fehlleitungen oder Serviceunterbrüche sein.

9. API-Schnittstelle zu Drittdienstleistern

9.1 Umfang

Die Bank bietet dem Vertragspartner bzw. den Benutzern den Austausch von konto- und depotbezogenen Daten und Informationen mit Drittdienstleistern (z.B. Fintechs) an («Informationsaustausch»), welcher für die Erbringung von gewissen Dienstleitungen notwendig

ist. Dieser Informationsaustausch erfolgt über eine gesicherte API-Schnittstelle (Application Programming Interface), die von der Bank zur Verfügung gestellt wird. Mittels dieser Schnittstelle können Benutzer Software sowie andere technische Lösungen und Dienstleistungen von Drittdienstleistern in Verbindung mit den digitalen Services der Bank nutzen. Die sorgfältige Auswahl eines Drittdienstleisters sowie dessen Überwachung obliegt ausschliesslich dem Benutzer. Die Bank trifft weder eine Überwachungs- noch eine Kontrollpflicht des Drittdienstleisters.

Die Bank übermittelt die Daten gemäss Auftrag des Benutzers an den Drittdienstleister. Der entsprechende Drittdienstleister ist vom Benutzer zu wählen und zu aktivieren.

Die Übermittlung der Daten erfolgt indirekt über die Plattform «bLink» von der SIX BBS AG (SIX) ("Plattform"), Die Pflicht der Bank ist dabei auf die Übermittlung der Daten bzw. der Entgegennahme von Daten ("Use Cases") über diese Schnittstelle beschränkt.

Nach erfolgter Freigabe der Schnittstelle durch die Bank, wird die Bank entsprechende Datenabfragen beantworten und Aufträge von den Drittdienstleitstern entgegennehmen ("Service Calls"). Sofern der Service Call einen Auftrag an die Bank enthält (z.B. Zahlungsauftrag), kann eine zusätzliche Freigabe in den digitalen Services der Bank erforderlich sein.

Die im Rahmen des Informationsaustauschs übermittelten Daten können gegenüber anderen von der Bank übermittelten Daten und Belegen abweichen. So wird zum Beispiel der Wert der Transaktionen per Transaktionsdatum statt per Valutadatum berücksichtigt.

Die Bank behält sich das Recht vor, den Umfang des Leistungsangebots anzupassen. Insbesondere können neue Use Cases eingeführt, bestehende geändert oder eingestellt werden.

9.2 Identifizierungsschlüssel
Nach der Aktivierung des Informationsaustauschs in den digitalen Services der Bank unter Verwendung der gültigen Legitimationsmittel, wird die Bank einen elektronischen Identifizierungsschlüssel («Token») ausstellen. Der Token wird von der Bank über die Plattform an den Drittdienstleister übermittelt. Die Bank hat keinen Einfluss auf die rechtmässige Verwendung des Tokens beim Drittdienstleister. Sofern ein Service Call vom Drittdienstleister oder der Plattform mit dem entsprechenden Token versehen ist, beantwortet die Bank diesen. Der Drittdienstleister ist für die sichere Verwaltung und die durch ihn erbrachte Datenbearbeitung selbst verantwortlich. Die Bank übernimmt hierfür keine Überwachungs- oder sonstige Pflichten.

9.3 Spezielle Sorgfaltspflichten
Falls der Benutzer den Informationsaustausch zwischen der Bank und einem von ihm gewählten und aktivierten Drittdienstleister beenden oder auf einzelne Geräte einschränken möchte, muss der Benutzer den Informationsaustausch zum entsprechenden Drittdienstleister löschen oder einschränken. Die Beendigung oder Einschränkung hat in den digitalen Services der Bank zu erfolgen. Bis zu dieser Löschung oder Einschränkung durch den Benutzer werden Service Calls des Drittdienstleisters beantwortet.

Der Drittdienstleister überprüft die Zugriffsberechtigung des Benutzers anhand von ihm ausgestellten Legitimationsmitteln. Der Benutzer hält diese Legitimationsmittel gemäss den Bestimmungen des Drittdienstleisters geheim und schützt sie gegen missbräuchliche Verwendung durch Unbefugte.

Der Vertragspartner nimmt zur Kenntnis, dass sämtliche Benutzer entsprechende API-Schnittstellen zu Drittdienstleistern einrichten können.

9.4 Zugelassene Drittdienstleister
Benutzer können selbst wählen, welche Drittdienstleister aktiviert werden sollen. Sie können jedoch nur solche Drittdienstleister wählen, die von der Bank und der Plattform zugelassen wurden. Die Bank behält sich das Recht vor, bestimmte Drittdienstleister, ohne Angabe von Gründen, auszuschliessen.

Der Vertragspartner und die Benutzer nehmen zur Kenntnis, dass die Zugriffsberechtigung beim Drittdienstleister von derjenigen der Bank abweichen kann. Der Drittdienstleister erbringt seine Dienstleistungen ohne Mitwirkung oder Kontrolle durch die Bank. Es liegt daher im Verantwortungsbereich des Vertragspartners bzw. des Benutzers die Zugriffsberechtigung beim Drittdienstleister zu überwachen und bei Bedarf anzupassen.

9.5 Datenverwendung durch den Drittdienstleister
Der Vertragspartner und die Benutzer nehmen zur Kenntnis, dass mit der Übermittlung der Daten über die Plattform an den Drittdienstleister diese Kenntnis über die entsprechenden Daten erhalten und entbindet hiermit die Bank von den Geheimhaltungspflichten und willigt in die entsprechende Datenbekanntgabe ein. Der Datenfluss erfolgt über den Service Call, der vom Drittdienstleister indirekt über die Plattform an die Bank gesendet wird.

Die Übermittlung der Daten über die Plattform zum Drittdienstleister bzw. vom Drittdienstleister in die Systeme der Benutzer sowie die Datenverwendung beim Drittdienstleister selbst richten sich ausschliesslich nach den Verträgen des Drittdienstleisters, insbesondere nach dessen Datenschutzerklärung. Der Drittdienstleister ist für die Gewährleistung der Sicherheit sowie die Einhaltung des Datenschutzes in seinem Leistungsbereich verantwortlich. Die Bank hat keinerlei Einfluss auf oder Kontrolle über die Datenverwendung und die Sicherheitsmassnahmen des Drittdienstleisters. Daten können durch diesen auch im Ausland gespeichert werden. In diesem Fall unterliegen die Daten nicht den Schutzvorschriften des schweizerischen Rechts, insbesondere nicht dem Bankkundengeheimnis. Der Drittdienstleister handelt ausschliesslich als vom Benutzer beigezogene Hilfsperson. Deshalb lehnt die Bank jegliche Überwachungs- oder Kontrollpflicht und jegliche sonstige Verantwortung für Leistungen oder Unterlassungen des Drittdienstleisters ab.

9.6 Datenverwendung durch die Plattform
Die Daten des Vertragspartners bzw. des Benutzers können von der Betreiberin der Plattform bearbeitet und gespeichert werden. Die Daten können durch die Betreiberin der Plattform für folgende Zwecke verwendet werden:

- Betrieb der Plattform
- Unterstützung und Überwachung von Datenabfragen und Aufträgen
- Weiterentwicklung des Informationsaustauschs

Die Bank hat keine Kontrolle über die Verwendung der Daten durch die Betreiberin der Plattform.

9.7 Datenverwendung durch die Bank
Der Vertragspartner und der Benutzer stimmen zu, dass die Bank die Daten, welche sie im Rahmen des Informationsaustauschs von Dritten erhält, zur gesamtheitlichen Beratung nutzen, überprüfen sowie im Rahmen der gesetzlichen Vorgaben weiterverwenden darf.

9.8 Haftung bei Nutzung des Informationsaustauschs
Die Bank hat keinen Einfluss auf den Informationsaustausch, die Leistungserbringung durch den Drittdienstleister sowie die Betreiberin der Plattform. Der Bank obliegt keine Überwachungs- oder Kontrollfunktion über den Drittdienstleister sowie die Betreiberin der Plattform und sie lehnt jegliche Gewährleistung oder Haftung für deren Tätigkeiten oder Unterlassungen ab.

10. Multibanking

10.1 Umfang

Mittels Multibanking kann der Benutzer die Bank beauftragen, Daten von Drittbanken zu empfangen sowie Aufträge an diese zu übermitteln. Hierfür stellt die Bank entsprechende Schnittstellen zur Verfügung oder zieht Plattformen eines Drittdienstleisters bei (z.B. bLink von der SIX BBS AG).

Die Bank behält sich das Recht vor, Einbindungen von Drittbanken abzulehnen, sofern diese nicht ihren bankinternen Anforderungen entsprechen. Weiter behält sich die Bank das Recht vor, unvollständige Datenübermittlungen abzulehnen (z.B. unvollständige Zahlungsaufträge).

10.2 Identifizierungsschlüssel

Der Aktivierungsprozess und der nachfolgende Datenaustausch zwischen der Bank und dem an Multibanking angeschlossenen Konto einer Drittbank erfolgt mittels deren Token. Dieser Token wird mit dem für die digitalen Services gültigen Legitimationsmittel verknüpft.

10.3 Spezielle Sorgfaltspflichten bei der Nutzung von Multibanking

Der Benutzer ist verpflichtet, Daten, die an eine Drittbank übermittelt werden (z.B. Zahlungsaufträge) zu prüfen und die Drittbank bei allfälligen Unstimmigkeiten umgehend zu informieren.

10.4 Datenschutz bei der Nutzung von Multibanking

Der Vertragspartner und der Benutzer stimmen zu, dass die Bank die Daten, welche sie im Rahmen von Multibanking von Dritten erhält, zur gesamtheitlichen Beratung nutzen, überprüfen sowie im Rahmen der gesetzlichen Vorgaben weiterverwenden darf.

10.5 Haftung beim Einsatz von Multibanking

Die Bank übernimmt keine Haftung für die Plattformen von Drittdienstleistern, Drittbanken und von diesen beigezogenen Hilfspersonen. Die Erbringung der Dienstleistung erfolgt mit der banküblichen Sorgfalt. Die Bank hat jedoch keinen Einfluss auf oder Überwachungsfunktion bei den beigezogenen Plattformen von Drittdienstleistern, den Drittbanken und den von diesen beigezogenen Dritten.

11. Elektronische Rechnungen (eBill)

Die Bank stellt dem Benutzer die Möglichkeit zur Verfügung, am e-Bill-Rechnungssystem teilzunehmen und elektronische Rechnungen zu erhalten und zu begleichen. Die Rechnungen können entweder einzeln oder mittels Sammel- oder Dauerfreigabe freigegeben werden. Der Benutzer definiert die entsprechenden Regeln.

Damit der Vertragspartner am eBill-Rechnungssystem teilnehmen kann, muss sich der Vertragspartner im Rahmen der digitalen Services legitimieren und sich einmalig bei SIX auf dem eBill-Portal registrieren.

Der Benutzer kann, die mittels eBill-Rechnungssystem eingegangenen elektronischen Rechnungen direkt im Rahmen der digitalen Services zur Zahlung freigeben oder auf elektronische Weise ablehnen. Der Benutzer ist verantwortlich die Zahlungsaufträge auf Richtigkeit und Vollständigkeit zu prüfen.

Die Bank übernimmt keine Gewähr für die Richtigkeit und Vollständigkeit der elektronischen Rechnungen. Beanstandungen bezüglich dieser Rechnungen (z.B. Art der Zustellung, Inhalt und Betrag) hat der Vertragspartner an den Rechnungssteller zu richten.

Die Dienstleistung eBill wird von der SIX Paynet AG erbracht.

12. Besonderheiten beim Bankverkehr über das Internet und das öffentliche Fernmeldenetz

Im Rahmen der Nutzung der digitalen Services bei der Bank eingehende und von der Bank versandte Daten werden, mit Ausnahme von Angaben über Absender und Empfänger, von der Bank verschlüsselt, soweit dies die jeweils verwendeten technischen Verfahren zulassen.

Der Vertragspartner anerkennt, dass das Internet und das öffentliche Funknetz weltweite und offene, grundsätzlich jedermann zugängliche Netze darstellen und, dass der digitalen Services Verkehr zwischen dem Benutzer und der Bank über öffentliche, nicht speziell geschützte Einrichtungen erfolgt; dies gilt sowohl für die bei der Bank eingehenden elektronischen Anweisungen des Benutzers als auch für die von der Bank zum Transport übergebenen elektronischen Meldungen an den Benutzer. Die über das Internet zu übermittelnden Daten können das Gebiet der Schweiz in nicht voraussehbarer Weise verlassen und zwar auch dann, wenn Absender und Empfänger sich in der Schweiz befinden. Da Absender und Empfänger im Rahmen der digitalen Services nicht verschlüsselt werden, können die entsprechenden Angaben von unbefugten Dritten gelesen werden. Unbefugte Dritte können deshalb sowohl in der Schweiz wie auch im Ausland Rückschlüsse auf eine Kundenbeziehung zwischen der Bank und dem Vertragspartner ziehen.

Die Nutzung der digitalen Services aus dem Ausland oder über ein privates Gateway (z.B. VPN) erfolgt auf eigenes Risiko des Benutzers. Die Bank lehnt jede Haftung für Risiken oder Folgen aus einer solchen Nutzung ausdrücklich ab.

13. Haftung der Bank

Die Bank beachtet bei der Erbringung der digitalen Services und beim Betrieb ihres Rechenzentrums die üblichen Sorgfaltspflichten. Voraussehbare Betriebsunterbrüche werden, wenn immer möglich, im Voraus angekündigt; Betriebsunterbrüche zu Wartungszwecken und zur Erweiterung oder Anpassung des Systems der Bank sowie Betriebsunterbrüche bei vermuteten oder festgestellten Gefährdungen der Betriebssicherheit bleiben ausdrücklich vorbehalten und lösen keinerlei Rechtsansprüche des Vertragspartners aus. Verarbeitungsunterbrüche werden nach Möglichkeit so rasch wie möglich behoben. Durch Verarbeitungsunterbrüche entstehen keine Schadenersatzansprüche des Vertragspartners. Die Bank vermittelt nicht den technischen Zugang zu ihren Dienstleistungen. Dies ist alleinige Sache des Benutzers. Er nimmt insbesondere zur Kenntnis, dass die Bank die für die digitalen Services erforderliche spezielle Sicherheits-Software grundsätzlich nicht vertreibt. Die Bank übernimmt deshalb keine Gewähr weder für Provider noch für die Sicherheits-Software.

Die Bank übernimmt keinerlei Gewähr für Richtigkeit und Vollständigkeit der im Rahmen der digitalen Services angezeigten oder übermittelten Daten und Informationen. Insbesondere Informationen über Konti und Depots (Saldo, Auszüge, Transaktionen usw.) sind vorläufig und unverbindlich. Ebenso stellen sämtliche Mitteilungen im Rahmen der digitalen Services keine verbindlichen Offerten dar, es sei denn, das Angebot werde ausdrücklich als verbindliche Offerte gekennzeichnet. Ferner sind Angaben über Devisen oder Notenkurse stets unverbindliche Informationen.

Der Vertragspartner anerkennt, dass der Transport von elektronischen Daten vom Benutzer bis zum Rechenzentrum der Bank und vom Rechenzentrum der Bank bis zum Benutzer nicht in den Verantwortungsbereich der Bank fällt; dieser ist vielmehr vom Benutzer selbst oder von den von ihm beigezogenen Dritten zu besorgen. Für die Bank verbindlich sind stets die auf dem System der Bank getätigten Transaktionen, wie sie in elektronischen Aufzeichnungen und allfälligen Computerausdrucken der Bank wiedergegeben sind. Jede Haftung der Bank für Schäden, die dem Vertragspartner infolge von Übermittlungsfehlern, technischen Mängeln, Störungen oder Eingriffen Dritter in die Datenübertragungsinfrastruktur entstehen, ist ausgeschlossen.

Die Haftung der Bank für Schäden, die dem Vertragspartner aus der Nichterfüllung seiner vertraglichen Verpflichtung oder den vertraglichen Verpflichtungen des Benutzers entstehen, sowie für indirekte Schäden und Folgeschäden, wie entgangener Gewinn oder Ansprüche Dritter, ist ausgeschlossen.

Die Bank übernimmt keine Haftung für nicht fristgerecht oder nicht vollständig ausgeführte Aufträge und damit zusammenhängende Schäden, insbesondere durch Kursverluste, soweit die übliche Sorgfalt angewendet wurde.

14. Vollmachtsbestimmungen

Die Ermächtigung der Benutzer zur Inanspruchnahme der digitalen Services behält ihre Wirkung bis zu einem an die Bank gerichteten Widerruf, ungeachtet anderslautender Veröffentlichungen und/oder Handelsregistereinträge. Der Widerruf muss schriftlich erfolgen, wobei die Bank das Recht − nicht aber die Pflicht − hat, auch einen mündlichen Widerruf zu akzeptieren. Die Ermächtigung erlischt weder mit dem Tod, der Verschollenerklärung oder der Handlungsunfähigkeit des Vertragspartners noch mit der Handlungsunfähigkeit eines Benutzers.

15. Kündigung

Die Kündigung des digitale Banking Services-Vertrages kann jederzeit ohne Einhaltung einer Kündigungsfrist durch die Bank oder schriftlich durch den Vertragspartner erfolgen.