

ANTRAG VIRTUAL CORPORATE SOLUTION

In das Partner Collaboration Tool integriert

Neukunden: bitte hier Rahmenvereinbarung ausfüllen

Wichtig: Alle Angaben sind obligatorisch.

1. Daten zum Partner (nachstehend «Unternehmen»)

Firmenname _____

Strasse/Nr. _____

PLZ/Ort _____ Land _____

2. Persönliche Daten des Administrators des Portals (nachstehend «Administrator»)

Herr Frau

Name _____ Vorname _____

Geburtsdatum _____ Wohnsitzland _____

Staatsangehörigkeit _____ E-Mail _____

Mobiltelefonnummer* _____ Funktion innerhalb des Unternehmens _____

Korrespondenzsprache IT DE FR EN

3. Produktauswahl und Kontoinformationen:

VCS MCBGGI21SU01-00063

VCS Plus (inkl. Versicherungspaket) MCBGGI21SU01-00064

Erwarteter jährlicher Nutzungsbetrag (CHF): _____

4. Hauptkarte 1

Name der Hauptkarte: _____

Gewünschtes Ausgabenlimit pro Monat: _____

5. Hauptkarte 2 (optional)

Name der Hauptkarte: _____

Gewünschtes Ausgabenlimit pro Monat: _____

6. Hauptkarte 3 (optional)

Name der Hauptkarte: _____

Gewünschtes Ausgabenlimit pro Monat: _____

7. Formular A – Feststellung des wirtschaftlich Berechtigten (Angaben obligatorisch) gemäss VSB 20

Es sind nachstehend keine Angaben nötig, wenn:

- die Vermögenswerte, die zur Benutzung der Prepaidkarte und/oder zur Begleichung der Kreditkarten-Monatsauszüge dienen und/oder über diesen Betrag hinaus beim Kartenherausgeber eingebracht werden **ausschliesslich** der Firma gehören **und**
- es sich bei der Firma nicht um ein Einzelunternehmen oder um eine einfache Gesellschaft handelt.

Trifft dies nicht zu, erklärt die Firma, dass diese Vermögenswerte (Zutreffendes ankreuzen, nur eine Antwort möglich)

- dem Karteninhaber gehören.
- von der Firma treuhänderisch zu Gunsten der/den nachfolgend aufgeführten Person/en gehalten werden:
- der/den nachfolgend aufgeführten Person/en gehören:
- (Vorname(n), Name(n), Geburtsdatum, Geburtsort, Nationalität, Effektive Wohnsitzadresse (inkl. Land):

Die Firma verpflichtet sich, dem Kartenherausgeber Änderungen jeweils unaufgefordert mitzuteilen. Die vorsätzliche Angabe falscher Informationen in diesem Formular ist eine strafbare Handlung (Urkundenfälschung gemäss Artikel 251 des Schweizerischen Strafgesetzbuches).

8. Informationen zur Aktivierung des Portals

Unternehmens-ID

Dieses Feld muss ein Akronym oder eine ID enthalten, die das Unternehmen zusammen mit dem Benutzernamen identifiziert (z. B.: john.companyname, keine Leerzeichen, Gross- und Kleinschreibung beachten). Das Feld ist obligatorisch und kann nicht geändert werden. Wird es nicht aufgefüllt, wird eine bestehende ID verwendet oder eine neue ID auf der Grundlage des Firmennamens erstellt.

9. Zwei-Faktor-Authentifizierung

SMS (für alle Benutzer)

(*) Hinweis: Das Feld «Mobiltelefonnummer» in Punkt 2 ist obligatorisch

10. Erklärung

Virtual Corporate Solution und Virtual Corporate Solution Plus (nachfolgend: «VCS»): Das Unternehmen bestätigt hiermit die Richtigkeit der in diesem Antrag gemachten Angaben und bestätigen, dass es die **Allgemeinen Geschäftsbedingungen für Virtual Corporate Solution (nachfolgend: «VCS-AGB»)** sowie die Allgemeinen Geschäftsbedingungen für die von der Cornèr Bank Ltd. (nachfolgend: die «Bank») Visa, Mastercard und Diners Club Zahlungskarten, herausgegeben von Cornèrcard (nachfolgend: «AGB»), zur Kenntnis genommen hat und vorbehaltlos als verbindlich akzeptiert.

Die Bank ist berechtigt, alle von ihr für notwendig erachteten Informationen über das antragstellende Unternehmen und den potenziellen Karteninhaber/Nutzer einzuholen.

Risiken und Haftung: Bei Annahme dieses Kartenantrags erhält das Unternehmen die **Zugangsdaten** (z.B. Benutzer-ID und PW) **zu VCS**. Das Unternehmen haftet in vollem Umfang dafür, dass diese Zugangsdaten an entsprechend vertrauenswürdige Mitarbeitende weitergegeben werden und dass diese Zugangsdaten in Übereinstimmung mit den internen Richtlinien des Unternehmens korrekt verwendet werden. Weiter ist das **Unternehmen verpflichtet, seine Mitarbeitenden bzw. die vom Administrator bezeichneten und ermächtigten Nutzer über den sorgfältigen Umgang mit den Zugangsdaten zu VCS entsprechend aufzuklären und die Nutzung von VCS adäquat und risikobasiert zu überwachen**. Das Unternehmen nimmt zur Kenntnis und anerkennt, dass der von ihm betraute **Administrator neue Benutzer definieren und virtuelle Karten ausstellen sowie Monatsauszüge und Transaktionen aller auf den Namen des Unternehmens ausgestellten Virtual Corporate Karten einsehen kann**. Das Unternehmen akzeptiert entsprechend der damit verbundenen Risiken, insbesondere, dass der Administrator nach eigenem Ermessen und ohne vorgängige Kontrolle durch das Unternehmen virtuelle Karten erstellen und benutzen kann. Ebenso akzeptiert das Unternehmen, dass der Administrator volle Einsicht auf alle Corporate-Karten des Unternehmens und die damit verbundenen Transaktionen nehmen kann. Das Unternehmen anerkennt und akzeptiert sodann, dass **Transaktionen mit VCN Karten nicht über 3D-Secure-Systeme authentifiziert werden** (z.B. eine Methode, die die Sicherheit von Online-Zahlungen erhöht, da zur Bestätigung der Zahlung neben der Kartennummer, dem Verfalldatum und der CVC (Kartenprüfnummer) ein Code eingegeben werden muss). Die **Bank schliesst ausdrücklich jegliche Art von Haftung für Verluste oder Schäden**, einschliesslich direkter, indirekter und/oder Folgeschäden, oder jegliche Folgen aus, die dem Unternehmen und/oder dem Nutzer von VCN und/oder Dritten durch den Zugang und/oder die Nutzung des VCS-Portals entstehen können, einschliesslich, aber nicht beschränkt auf den **unbefugten Zugang oder die unsachgemässe Nutzung des VCS-Portals und/oder von VCN** durch Direktoren, Führungskräfte, Mitarbeitende, Vermittler, professionelle Berater, Lieferanten, Auftragnehmer oder Unterauftragnehmer des Unternehmens. Ferner anerkennt und akzeptiert das Unternehmen, dass die Nutzer möglicherweise das gesamte Ausgabenlimit des Unternehmens in nur wenigen Transaktionen verbrauchen können. **Die Bank übernimmt keinerlei Haftung für den missbräuchlichen oder unberechtigten Gebrauch des vom Unternehmen für seine Nutzer festgelegten Ausgabenlimits.**

Annahme der Allgemeinen Geschäftsbedingungen: Die AGB und die Allgemeinen Versicherungsbedingungen (nachfolgend: «AVB») für den Versicherungsdeckung, der mit den Cornèrcard Produkten automatisch und kostenlos angeboten wird oder auf Anfrage und gegen eine Gebühr zur Verfügung gestellt wird, können unter cornercard.ch/e/gtbusiness für Visa/Mastercard und unter dinersclub.ch/firststep für Diners Club abgerufen werden. **Mit der Unterzeichnung des vorliegenden Antrages und/oder Nutzung von VCS durch den Karteninhaber bzw. Nutzer bestätigt das Unternehmen, dass es die AGB, die VCS-AGB sowie alle anwendbaren AVB erhalten sowie verstanden hat und diese in vollem Umfang akzeptiert** (die Bedingungen können unter cornercard.ch/e/gtbusiness für Visa, Mastercard, unter dinersclub.ch/firststep für Diners Club eingesehen oder unter der Telefonnummer +41 91 800 41 41 für Visa, Mastercard oder +41 58 880 88 00 für Diners Club bestellt werden). Das Unternehmen bestätigt zudem, dass die Nutzer über den sorgfältigen Umgang mit den Zugangsdaten zu VCS instruiert bzw. aufgeklärt zu haben und anerkennt, dass der Karteninhaber/Nutzer berechtigt ist, die mit den Kartenprodukten von Cornèrcard verbundenen elektronischen Funktionalitäten (iCornèr, Mobile App, Mobile Payment usw.) selbständig zu beantragen und im Rahmen des entsprechenden Aktivierungsprozesses die entsprechenden Nutzungsbedingungen in elektronischer Form und ohne Mitwirkung des Unternehmens verbindlich zu akzeptieren.

Preise, Zinsen und Gebühren: Die für die Nutzung und Verwaltung der Karte verrechneten Preise, Zinsen und Gebühren sind in einer «Preise, Zinsen und Gebühren»-Tabelle definiert, welche jederzeit im Internet für unter cornercard.ch/d/preise-business abgerufen oder unter +41 91 800 41 41 abgefragt werden kann. Für jede Tokenisierung einer Karte wird eine Gebühr von CHF 2 erhoben, für jeden weiteren Gültigkeitsmonat CHF 2. Der Gesamtbetrag wird direkt dem VCS-Konto des Unternehmens belastet. Des Weiteren können der Firma und dem Inhaber Drittkosten weiterverrechnet und von ihnen verursachte Aufwendungen in Rechnung gestellt werden. Die Firma und der Inhaber **erklären, diese Preise, Zinsen und Gebühren vorbehaltlos zu akzeptieren**.

Sollten das Unternehmen und der Karteninhaber/Nutzer ein weiteres Cornèrcard Produkt beantragen oder zu einem anderen Produkt wechseln wollen, gilt die jeweilige Jahresgebühr bzw. Anmeldegebühr für dieses Produkt, die ebenfalls über die oben genannten Kontaktdaten abgerufen oder angefordert werden kann.

Wechselkurs: In Fremdwährung getätigte Transaktionen werden zum Retail-Wechselkurs der Bank (für Visa/Mastercard Karten) oder zum Wechselkurs von Diners Club International (für Diners Club Karten) am Buchungstag umgerechnet, zuzüglich der Bearbeitungsgebühren für Fremdwährungen.

Allgemeine Geschäftsbedingungen für die Benutzung des Partner Collaboration Tool Portals (nachstehend auch «PCT» oder «Portal» genannt) der Cornèr Bank AG

Diese Allgemeinen Geschäftsbedingungen (nachstehend «AGB») regeln das Rechtsverhältnis zwischen dem Unternehmen, das die Administratorenrechte beantragt (nachstehend «Unternehmen») und/oder den Personen, die zur Benutzung des PCT berechtigt sind (nachstehend «Administrator» oder «Benutzer») und der Cornèr Bank AG (nachstehend «Bank») in Bezug auf die Benutzung des PCT.

1. Autorisation

- 1.1. Das Unternehmen gestattet dem Administrator, anderen Benutzern die Verwendung des Portals zu erlauben, sofern diese in einem gültigen Arbeitsverhältnis zum Unternehmen stehen.
- 1.2. Das Unternehmen trägt die gesamte Verantwortung dafür, dass **sämtliche Benutzer die in dieser AGB enthaltenen Bestimmungen und Pflichten vollumfänglich einhalten**. Das Unternehmen ist also verpflichtet, jeden Benutzer detailliert über das Portal, die dazugehörigen Funktionen/Funktionalitäten, die ihm obliegenden Sorgfaltspflichten und damit verbundenen Risiken zu informieren (vgl. Ziffern 4 und 5).
- 1.3. Erteilte Autorisationen werden nicht automatisch ungültig (z. B. durch Tod, Handlungsunfähigkeit, Streichung der Zeichnungsbefugnis, Löschen aus einem Register oder Beendigung des Arbeitsverhältnisses mit dem Unternehmen), sondern müssen einzeln gesperrt bzw. annulliert werden (vgl. Ziffer 6).

2. Persönliche Legitimationsmittel

- 2.1. Auf Antrag des Unternehmens stellt die Bank den Benutzern die eigene persönliche Vertragsnummer sowie die dazugehörigen Legitimationsmittel wie ID und Passwort zur Verfügung (nachstehend «Legitimationsmittel»). Das durch die Bank zugewiesene Passwort muss beim erstmaligen Zugang durch ein persönliches Passwort ersetzt werden.
- 2.2. Der Zugriff auf das Portal und die damit verbundenen Dienstleistungen erfolgt, nachdem sich der Benutzer durch die Legitimationsmittel gegenüber der Bank legitimiert hat.
- 2.3. Die Bank behält sich das Recht vor, die Legitimationsmittel jederzeit zu ersetzen oder zu ändern.

3. Legitimation

- 3.1. **Gegenüber der Bank ist zum Zugang zum Portal und zur Nutzung der damit verbundenen Dienstleistungen berechtigt, wer sich zum Zeitpunkt der Nutzung gemäss den Instruktionen des Portals mit den gültigen Legitimationsmitteln legitimiert hat** (Selbstlegitimation). Dies gilt unabhängig davon, ob es sich dabei tatsächlich um den Benutzer handelt bzw. ob dieser vom Unternehmen entsprechend autorisiert wurde. Die Bank gilt als vom Unternehmen beauftragt und ermächtigt, die über das Portal eingehenden Aufträge auszuführen, sobald das Legitimationsverfahren korrekt abgeschlossen wurde.
- 3.2. Die Bank ist also ausdrücklich von jeglichen weiteren Kontrollpflichten hinsichtlich der Legitimation und/oder Autorisation zur Nutzung des Portals befreit, **unabhängig von internen Vertragsverhältnissen zwischen der Bank und dem Benutzer und ohne Berücksichtigung etwaiger anderer Bestimmungen in den Formularen der Bank, insbesondere in Formularen zur Erteilung einer Vollmacht und/oder Zeichnungsbefugnis im Rahmen des Vertragsverhältnisses mit der Bank (einschliesslich bspw. Kartenverträge, Konsum-/Privatkredit [ëcash])**.
- 3.3. Die Bank behält sich jedoch das Recht vor, den Zugang zum Portal jederzeit und ohne Angabe von Gründen zu verweigern und zu verlangen, dass die Benutzer sich auf andere Weise legitimieren.
- 3.4. **Alle Transaktionen, Geschäfte oder Tätigkeiten, die im Rahmen der Vertragsbeziehung mit der Bank (einschliesslich Kartenverträge, Konsum-/Privatkredit [ëcash]) im Anschluss an die besagte Legitimation ausgeführt werden, werden dem Unternehmen zugeschrieben und von diesem vorbehaltlos als rechtsgültig und verbindlich akzeptiert**.

4. Sorgfaltspflichten

- 4.1. **Der Benutzer ist verpflichtet, die Legitimationsmittel besonders sorgfältig aufzubewahren, so dass diese absolut sicher, vertraulich und vor jeglichem Missbrauch geschützt sind. Diese dürfen weder versandt oder weitergegeben noch in einer anderen Weise Dritten zugänglich gemacht werden**. Das persönliche Passwort – ebenso die User-ID – muss geheim gehalten werden, es darf weder registriert/notiert noch elektronisch (oder auf Speichermedien jeglicher Art) gespeichert werden. Das Passwort darf nicht leicht zu erraten sein (keine Telefonnummern, Geburtstagsdaten, Autokennzeichen, einfach ermittelbare Zahlenfolgen usw.) und muss den von der Bank vorgegebenen Kriterien für Integrität und Komplexität entsprechen. Das gewählte Passwort verfällt automatisch gemäss den von der Bank definierten Regeln und muss deshalb regelmässig erneuert und ersetzt werden.
- 4.2. Das Unternehmen und der Benutzer verpflichten sich ausserdem, alle machbaren Sicherheitsmassnahmen zu ergreifen, um die für den Zugang zum Portal verwendeten Endgeräte und Arbeitsstationen, insbesondere das elektronische Datenverarbeitungssystem (EDV-System sowie die ggf. darauf gespeicherten

Daten), vor Manipulation, Missbrauch und Abfangen zu schützen (zum Beispiel durch ständige Aktualisierung der Firewall- und Antivirenprogramme). **Das Unternehmen und der Benutzer sind verpflichtet, sich genauestens über die notwendigen Sicherheitsmassnahmen zu informieren. Das Unternehmen verpflichtet sich, dafür zu sorgen, dass auch die Benutzer die oben genannten Pflichten und Verbote strikt einhalten, und haftet vollumfänglich für sämtliche Folgen, die aufgrund Nichteinhaltung dieser Pflicht zum Schutz der Legitimationsmittel durch die Benutzer entstehen.**

- 4.3. E-Mails, die dem Anschein nach von der Bank stammen und in denen zur Bereitstellung der Legitimationsmittel aufgefordert wird (z. B. durch Eingabe auf einer Website, die über einen Link aufgerufen werden soll), dürfen nicht beantwortet werden. In einem solchen Fall ist die Bank unverzüglich hierüber zu informieren. Besteht Grund zu der Annahme – oder auch nur der Verdacht –, dass Dritte Kenntnis von den Legitimationsmitteln erlangt haben und insbesondere, vom persönlichen Passwort, muss der Benutzer dieses **sofort ändern**.
- 4.4. Die Bank behält sich das Recht vor, weitere Authentifizierungssysteme (beispielsweise Zwei- oder Drei-Stufen-Authentifizierung) einzuführen und zu implementieren, und diesbezüglich vom Benutzer weitere Informationen anzufordern, beispielsweise die Mobiltelefonnummer zur Übermittlung von SMS oder die Installation spezifischer Applikationen auf dem Smartphone zur Authentifizierung mittels «Random-One-Time-Token» zu verlangen.
- 4.5. Der Zugang zum Portal erfolgt über das Internet. Der Zugang und die Benutzung des öffentlichen Netzes (Internet) liegen in der ausschliesslichen Zuständigkeit/Verantwortung des Unternehmens und der Benutzer, diese tragen die volle Verantwortung und alle Risiken, insbesondere für die Folgen des Abfangens durch Dritte (einschliesslich Manipulationen und «Hackingangriffe»). Die Bank stellt dem Benutzer keine Verbindung zum Portal über das öffentliche Netz oder über einen Internetanbieter bereit und gewährleistet dies auch nicht. Für den Zugang zum Portal und zu den damit verbundenen Dienstleistungen über das öffentliche Netz stellt die Bank eine eigene Website zur Verfügung, deren Adresse dem Unternehmen separat mitgeteilt wird.
- 4.6. Der Benutzer ist verpflichtet, beim erstmaligen Zugang das von der Bank bereitgestellte Passwort zu ändern. Die Bank ist befugt, die Legitimationsmittel jederzeit und ohne Vorankündigung zu ändern, soweit sie dies für notwendig erachtet, insbesondere aus Sicherheitsgründen. In diesem Fall übermittelt die Bank dem Unternehmen rechtzeitig die neuen Legitimationsmittel. Besteht der Verdacht, dass unberechtigte Dritte Kenntnis dieser Legitimationsmitteln erlangt haben, müssen das Unternehmen und die Benutzer die Bank unverzüglich darüber informieren, damit sie diese ersetzt. Diese Pflicht ist insbesondere in folgenden Fällen zwingend:
 - bei Sperrung des Zugangs zu den Dienstleistungen des Portals;
 - bei Verdacht einer missbräuchlichen Verwendung der Legitimationsmittel durch unbefugte Dritte;
 - bei Verlust oder Diebstahl der gesamten oder von Teilen der Legitimationsmittel.

5. Risiken und Haftung

- 5.1. Die Nutzung des Portals ist **mit Risiken verbunden**, unter anderem könnten die im Portal angezeigten Informationen für andere über das Portal angebotene Dienstleistungen verwendet werden. Hauptsächlich bestehen folgende Risiken: (1) **Offenlegung der Bankbeziehung sowie von Bankkundeninformationen gegenüber Dritten, wodurch das Bankgeheimnis nicht mehr sichergestellt werden kann**; (2) Veränderungen bzw. Verfälschungen von Informationen (z. B. Vortäuschen/Bereitstellung falscher Informationen); (3) Unterbrechungen/Störungen des Systems und andere Probleme/Unterbrechungen bei der Übermittlung/Kommunikation, die zu Verzögerungen, Verfälschungen, Fehlleitungen, Abzweigungen oder Löschungen von Informationen führen können; (4) Missbrauch/bestimmungswidrige Nutzung und daraus resultierender Verlust oder Schäden infolge des Abfangens von Informationen durch Dritte.
- 5.2. **Im Einklang mit den bezüglich der Legitimation vereinbarten Bestimmungen (vgl. Ziffer 3.) tragen der Benutzer und/oder das Unternehmen alle Risiken aufgrund von (i) Manipulation/Störung des eigenen EDV-Systems – und/oder der eigenen Arbeitsstationen – durch unbefugte Personen, (ii) missbräuchlicher, unzulässiger oder vorschriftswidriger Anwendung/Benutzung der persönlichen Legitimationsmittel und/oder des Portals, (iii) Verstoß gegen die Sorgfaltspflicht oder (iv) Eingriffen unbefugter Dritter in die Datenübertragung (einschliesslich etwaiger Interferenzprobleme).**
- 5.3. Das Unternehmen und der Benutzer sind sich der Risiken bezüglich des Informations- und Datenaustauschs über öffentliche und private

Datenübermittlungsnetze, insbesondere des Risikos einer Offenlegung der Bankbeziehung und/oder des Vertragsverhältnisses mit der Bank sowie der Bankkundeninformationen gegenüber Dritten, bewusst. Auch wenn beim Zugriff auf das Portal die zu übermittelnden Daten, mit Ausnahme von Absender und Empfänger, automatisch kodiert/verschlüsselt werden, können gezielte Manipulationen/Störungen und/oder Verletzungen (einschliesslich «Hacking») des EDV-Systems des Benutzers durch Unbefugte nicht ausgeschlossen werden. **Die diesbezüglichen Risiken fallen in den Einflussbereich (und/oder unter die Kontrolle) des Unternehmens und/oder des Benutzers und werden somit vom Unternehmen getragen. Im Allgemeinen tragen das Unternehmen und der Benutzer alle mit der Datenübertragung über das öffentliche und private Netz verbundenen Risiken.** Das Unternehmen trägt das Risiko für die Verwendung der persönlichen Legitimationsmittel bis zum Wirksamwerden der Sperrung (vgl. Ziffer 6)

- 5.4. Unbeschadet der Beschränkungen aus zwingenden Gesetzesbestimmungen **ist jegliche Haftung der Bank für etwaige Schäden – ob direkte, indirekte oder Folgeschäden – oder Konsequenzen aller Art, die dem Unternehmen und/oder den Benutzern und/oder Dritten (einschliesslich Karteninhabern, Kunden von ecash und/oder anderer Produkte der Bank) durch den Zugang und/oder die Nutzung – auch in missbräuchlicher Weise – des Portals entstehen, ausdrücklich ausgeschlossen.**
- 5.5. Wenngleich die Bank durch Anwendung der erforderlichen Massnahmen und allgemein anerkannten Technik- und Sicherheitsstandards alle angemessenen Vorkehrungen zur Gewährleistung der Sicherheit des Portals getroffen hat, ist es unmöglich, absolute Sicherheit zu garantieren.
Das Unternehmen und der Benutzer nehmen insbesondere zur Kenntnis, dass:
- die Arbeitsstation und das EDV-System des Unternehmens und/oder des Benutzers nicht unter die Kontrolle der Bank fallen und Gegenstand von externen Angriffen sein können;
- ein potenzielles Risiko besteht, dass unbefugte Personen die Legitimationsmittel oder andere Daten des Unternehmens und/oder des Benutzers, einschliesslich Daten bezüglich der Vertragsbeziehung mit der Bank, entwenden oder abfangen und missbräuchlich einsetzen könnten;
- die Informationen über das öffentliche Netz übermittelt werden, hierbei zwar in verschlüsselte Pakete aufgesplittet sind, es jedoch nicht ausgeschlossen werden kann, dass die Übertragung ggf. über Leitungen und Knotenpunkte jenseits der Landesgrenze erfolgt, selbst wenn der Wohnort von Absender und Empfänger in der Schweiz liegen;
- die Betreiber des öffentlichen Netzes das Unternehmen und/oder den Benutzer sowie deren Kommunikationspartner im Internet identifizieren können;
- weder das Portal noch das öffentliche Netz die Einhaltung des Bankgeheimnisses garantieren können.
- 5.6. **Die Bank übernimmt insbesondere keinerlei Verantwortung und Haftung für Schäden zum Nachteil des Unternehmens, der Benutzer und/oder Karteninhaber, Kunden von ecash und/oder anderer Produkte der Bank oder Dritter infolge von Übermittlungsfehlern, technischen Mängeln, Überlastung, Störungen, Fehlern, Unterbrechungen oder Abfangaktionen, unzulässigen Eingriffen an Telekommunikationseinrichtungen, Sperrung von Telekommunikationsanlagen oder Netzwerken oder aufgrund anderer Fehler, die die Betreiber der Anlagen oder Netzwerke zu vertreten haben, und die bei der Benutzung des Portals und der Verarbeitung von Transaktionen auftreten. Die Bank haftet ebenfalls nicht für Schäden, die dem Unternehmen, den Benutzern, den Karteninhabern, den Kunden von ecash und/oder anderer Produkte der Bank oder Dritten aufgrund der Übermittlung von Daten bezüglich der Bankbeziehung über das öffentliche Netz entstehen.**
- 5.7. Unbeschadet der durch zwingende Rechtsvorschriften gesetzten Grenzen erklärt das Unternehmen, die Bank für jegliche Schäden oder Verluste in Bezug auf Vertragsverhältnisse mit der Bank zu entschädigen und schadlos zu halten, die Letzterer durch die Benutzung, auch durch Dritte und/oder infolge Missbrauchs, des Portals entstehen, dies gilt auch für den Fall, dass das Unternehmen und/oder die Benutzer kein Verschulden trifft (beispielsweise wenn es zu einem Hackingangriff kommt, obwohl das Unternehmen und die Benutzer alle Sicherheitsvorkehrungen getroffen hatten).

6. Sperrung

- 6.1. Der Administrator kann die Zugriffsberechtigung weiterer Benutzer jederzeit sperren.
- 6.2. Das Unternehmen kann die Sperrung der Zugriffsberechtigung des Administrators oder weiterer Benutzer jederzeit bei der Bank beantragen.
- 6.3. Die Bank kann jederzeit den Zugang der Benutzer zum Portal sperren.
- 6.4. Jeder Benutzer kann die Sperrung seiner Zugriffsberechtigung bei der Bank beantragen. Die Bank behält sich vor, einem solchen Antrag erst nach Rücksprache mit dem Administrator nachzukommen.

7. Informationen von Geldautomaten (ATM), Terminals, Bildschirmen oder anderen EDV-Systemen

- 7.1. Wenngleich die Bank alle angemessenen Vorkehrungen und geeigneten Massnahmen getroffen hat, um die Zuverlässigkeit, Korrektheit und Integrität der auf dem Portal bereitgestellten Informationen sicherzustellen, dienen diese Daten und Dokumente ausschliesslich zu Informationszwecken.
- 7.2. Aus diesen Informationen lässt sich keinerlei Verpflichtung oder Haftung der Bank ableiten und das Unternehmen, die Benutzer oder Dritte (einschliesslich Kunden) können darauf keine Ansprüche jeglicher Art gegenüber der Bank begründen.
- 7.3. Die angezeigten Informationen und Mitteilungen sind provisorisch und

unverbindlich, sofern die Informationen zu einer Leistung nicht ausdrücklich als verbindlich ausgewiesen sind. Ebenso stellen solche Informationen weder eine Empfehlung oder ein Angebot noch ein Anreiz/eine Aufforderung zur Tötigung von Transaktionen oder zum Abschluss irgendeines Rechtsgeschäfts dar, sofern dies nicht ausdrücklich vermerkt ist.

8. Elektronische Vereinbarungen, elektronisch angezeigte rechtliche Hinweise

- 8.1. Die Nutzung bestimmter, über das Portal zur Verfügung gestellter Leistungen kann an die Zustimmung zu separat vereinbarten Zusatzbestimmungen gebunden sein. Die Bank kann dem Benutzer diese Bestimmungen in elektronischer Form vorlegen, nachdem er sich über das Portal legitimiert hat. Dasselbe gilt für die Anpassung, Änderung oder Ergänzung der vorliegenden ABG.
- 8.2. Die Dienstleistungen werden aktiviert, sobald der Benutzer, sofern erforderlich, diese erfolgreich beantragt und den besonderen Zusatzbestimmungen elektronischen zugestimmt hat. Dadurch werden die Bestimmungen für das Unternehmen und den Benutzer verbindlich.
- 8.3. Elektronisch abgeschlossene Vereinbarungen sind handschriftlich unterzeichneten Vereinbarungen gleichgestellt. Die Bestimmungen können ausgedruckt werden und sind im Portal einsehbar. Die Bank kann ihr Dienstleistungsangebot jederzeit ändern. Aufgrund der Internationalisierung der Märkte und der ständigen Erweiterung der elektronischen Dienstleistungen muss die Bank zusätzliche rechtliche Hinweise zu elektronisch veröffentlichten Informationen und Dienstleistungen bereitstellen. Diese sind ab dem Zeitpunkt der Anzeige auf dem Bildschirm für den Benutzer verbindlich. Möchte der Benutzer diesen nicht zustimmen und deren Gültigkeit bestätigen, hat er keinen Zugriff auf die betreffenden Dienstleistungen und Informationen und kann diese nicht in Anspruch nehmen.

9. (Gesetzliche) Restriktionen sowie Ein- und Ausfuhrbeschränkungen bestimmter Länder

- 9.1. Das Unternehmen bestätigt, sich darüber im Klaren zu sein und die Benutzer darüber informiert zu haben, dass der Zugang und die Nutzung des Portals (und der damit verbundenen Dienstleistungen) ausserhalb der Schweiz unter Umständen gegen die Gesetze und Vorschriften des betreffenden Landes verstossen könnte. Das Unternehmen verpflichtet sich daher unwiderruflich, (i) sich über das Vorliegen, den Inhalt und den Geltungsbereich von allfälligen Gesetzen, Vorschriften sowie Rechtsnormen allgemein über die Nutzung von Bankdienstleistungen desjenigen Landes zu informieren, von dem aus der Zugriff auf das Portal (und die damit verbundene Dienstleistungen) ggf. erfolgt; (ii) das Portal (und die damit verbundene Dienstleistungen) nur in dem Masse zu nutzen, wie dies mit den genannten lokalen Bestimmungen und Vorschriften vereinbar ist und insbesondere strikt alle dort geltenden Verbote und/oder Beschränkungen bezüglich der Nutzung von Bankdienstleistungen einzuhalten; (iii) das Vorstehende auch den Benutzern als Pflicht aufzuerlegen und die Einhaltung sicherzustellen. Das Unternehmen verpflichtet sich des Weiteren dafür zu sorgen, dass die Benutzer die vorstehenden Bestimmungen einhalten.
- 9.2. Das Unternehmen befreit die Bank diesbezüglich von jeglicher Haftung und erkennt unwiderruflich und ausnahmslos an, im vollen Umfang für alle etwaigen Folgen, Strafen oder Verstösse haftbar zu sein, die infolge der Nutzung des Portals (und der damit verbundenen Dienstleistungen) ausserhalb des schweizerischen Staatsgebiets entstehen.
- 9.3. Ausserdem erklärt das Unternehmen, die Bank von jeglichen direkten, indirekten und/oder daraus resultierenden Schäden, Lasten, Unkosten und Folgen vollständig schadlos zu halten, die aufgrund des Verstosses gegen vorgenannte Bestimmungen sowie diese Bedingungen (AGB) für die Nutzung des Portals und/oder der damit verbundenen Dienstleistungen entstehen.
- 9.4. **Die Bank ist berechtigt, den Umfang der angebotenen/verfügbaren Dienstleistungen jederzeit und ohne Vorankündigung anzupassen oder zu beschränken.** Die Bank ist nicht verantwortlich und haftet nicht für direkte, indirekte oder resultierende Schäden, die dem Unternehmen und/oder Benutzer durch eine Sperrung, Unterbrechung, Änderung oder Aufhebung des Zugangs zu einer oder mehreren mit dem Portal verbundenen Dienstleistungen oder zum gesamten Portal entstehen. Der Benutzer ist verpflichtet, alle Beschränkungen und einschlägigen Gesetze/Bestimmungen zu kennen und einzuhalten. Diesbezüglich lehnt die Bank jede Haftung ab.

10. Übermittlungsfehler, Interferenzen/technische Störungen, Unterbrechungen und unzulässige Eingriffe

Die Bank übernimmt keinerlei Haftung für Schäden, die durch Übermittlungsfehler, defekte Leitungen, technische Mängel/Fehler und Störungen, Unterbrechungen oder unzulässige Eingriffe und/oder Interferenzen an EDV-Systemen des Benutzers oder eines Dritten (einschliesslich an öffentlich zugänglichen Systemen und Übertragungsnetzen) verursacht werden, sofern die Bank nicht gegen die geschäftsübliche Sorgfaltspflicht verstossen hat. Solange die Bank ihre geschäftsübliche Sorgfaltspflicht erfüllt, übernimmt sie keine Gewähr für einen ungestörten, unbegrenzten, fehlerfreien und/oder unterbrechungsfreien Zugang zu ihren Dienstleistungen. Darüber hinaus ist jegliche Haftung ausgeschlossen für Schäden aufgrund von Fehlern, Funktionsstörungen, Unterbrechungen (einschliesslich systembedingter Wartungsarbeiten) oder Überlastungen der Geldautomaten oder EDV-Systeme der Bank.

11. Preise

- 11.1. Die Preise für die Benutzung des Portals und der damit verbundenen Dienstleistungen sowie für die Bereitstellung der Legitimationsmittel

(einschliesslich Ersatz und zusätzliche Anfragen) und der entsprechenden Hardware sind in einer separaten Preisliste aufgeführt.

- 11.2. Änderungen werden in geeigneter Weise bekannt gegeben. Die vereinbarten Preise werden dem Unternehmen je nach Wahl der Bank sofort, monatlich, vierteljährlich oder jährlich in Rechnung gestellt.

12. Bankgeheimnis/Datenschutz, Marketing

- 12.1. Das schweizerische Recht (z. B. bezüglich Bankgeheimnis, Datenschutz) beschränkt sich auf das schweizerische Staatsgebiet und somit verlieren alle ins Ausland übermittelte Daten den Schutz durch das schweizerische Recht.
- 12.2. Die Bank oder durch diese beauftragte Dritte sind befugt, die im Rahmen der Nutzung des Portals erlangten Daten des Unternehmens und/oder des Benutzers zu speichern, zu verarbeiten oder zu nutzen. Insbesondere dürfen die Bank selbst oder durch diese beauftragte Dritte die genannten Daten auswerten und analysieren, zu Marketingzwecken und zur Erstellung von Kundenprofilen nutzen sowie zu Marktforschungszwecken bearbeiten. Dies ermöglicht es, den Bankkunden eine individuelle und persönliche Beratung sowie massgeschneiderte Angebote und Informationen über die Produkte und Dienstleistungen der Bank anzubieten. Im Allgemeinen werden folgende Daten verarbeitet und behandelt: Unternehmens- und Benutzerdaten sowie Daten zu Kartentransaktionen, Verbraucher-/Privatkreditverträgen (ècash) und zusätzlichen Dienstleistungen/Produkten.
- 12.3. Das Unternehmen und/oder der Benutzer können jederzeit auf Angebote und Informationen über Produkte und Dienstleistungen der Bank verzichten. Von der Bank beauftragte Dritte und deren Mitarbeitende sind zur Einhaltung des schweizerischen Datenschutzgesetzes verpflichtet.

13. Technische Voraussetzungen für den Zugang zum Portal

Das Portal ist nur zugänglich, wenn die Endgeräte und dazugehörige Software (Betriebssysteme, Browser, Anwendungen) des Unternehmens/Benutzers den von Zeit zu Zeit mitgeteilten oder über die Kommunikationskanäle der Bank bekanntgegebenen technischen Anforderungen entsprechen. Das Unternehmen/der Benutzer ist ausschliesslich dafür verantwortlich, auf eigene Kosten Endgeräte zu beschaffen und Software zu installieren und ggf. zu aktualisieren, um so deren ständige technische Kompatibilität sicherzustellen. Die Bank behält sich vor, die Anforderungen an Technik und Kompatibilität jederzeit nach angemessener Vorankündigung zu ändern und das Unternehmen und der Benutzer sind dafür verantwortlich, die zur Erfüllung der neuen Anforderungen erforderlichen Aktualisierungen und Upgrades durchzuführen.

14. Rechte an geistigem Eigentum

Die Bank erteilt dem Benutzer (und dem Unternehmen) eine nicht übertragbare, nicht veräusserliche, nicht ausschliessliche, persönliche und unentgeltliche Lizenz zur Benutzung des Portals und insbesondere der Anwendungen und Funktionalitäten, die Eigentum der Bank sind oder zu deren Erteilung die Bank vom Inhaber der geistigen Eigentumsrechte ermächtigt wurde. Diese Lizenz wird ausschliesslich zur Nutzung der dem Benutzer (und dem Unternehmen) zur Verfügung gestellten Dienstleistungen und innerhalb der durch diese AGB festgelegten Grenzen erteilt. Unbeschadet der Rechte, die dem Benutzer (und dem Unternehmen) aufgrund dieser AGB eingeräumt werden, sowie der Rechte von Drittlizenzgebern, behält sich die Bank alle Rechte bezüglich des Portals vor und insbesondere der Anwendungen, Funktionalitäten und Websites der Bank, die zur Erbringung dieser Dienstleistungen genutzt werden. Der Benutzer und das Unternehmen erkennen an, dass die ggf. für den Zugang zum Portal erforderliche Software, die nicht von der Bank im Rahmen der im vorstehenden Absatz genannten Lizenz zur Verfügung gestellt wird, insbesondere Betriebssysteme und Browser, Eigentum von Drittanbietern sind und dass deren Benutzung durch Vertragsbestimmungen der jeweiligen Drittanbieter geregelt ist. Der Benutzer und das Unternehmen erkennen an, dass die Bank nicht Partei des Lizenzvertrags für diese Software von Drittanbietern ist, und verpflichten sich, die vom Drittanbieter festgelegten Benutzungs- und Lizenzbedingungen einzuhalten und etwaige Lizenzgebühren direkt an den Drittanbieter zu

entrichten. Der Benutzer und das Unternehmen erkennen an und akzeptieren, dass für das Senden und Empfangen von Daten über seine/ihre Endgeräte je nach Übertragungsart Gebühren für die Daten- und Textübertragung ihres Providers für Mobilfunk, Festnetz oder WLAN anfallen. Diese Gebühren sowie sonstige Kosten für die Benutzung des Endgeräts und dessen Netzanschluss durch den Benutzer/das Unternehmen, gehen ausschliesslich zu dessen Lasten.

15. Verfügbarkeit des Portals und der dazugehörigen Dienstleistungen/Funktionalitäten

Das Portal und die damit verbundenen Dienstleistungen sind in der Regel den ganzen Tag verfügbar, auch an Feiertagen. Die Bank kann jedoch weder den unbegrenzten Zugang zum Portal, noch die unterbrechungsfreie Benutzung der damit verbundenen Dienstleistungen garantieren. Der Bank ist das Recht vorbehalten, jederzeit mit sofortiger Wirkung, auch ohne Vorankündigung, die Bereitstellung auch nur eines Teils der über das Portal bereitgestellten Dienstleistungen/Funktionalitäten und Anwendungen zu beschränken, zu sperren, zu unterbrechen, zu ändern und/oder einzustellen, insbesondere aus rechtlichen Gründen, aus Sicherheitsgründen, für regelmässige oder gelegentliche technische Aktualisierungen und Wartungsmassnahmen, sowie immer, wenn sie dies nach ihrem Ermessen für erforderlich erachtet, in jedem Fall ohne dadurch einen Schaden des Unternehmens, der Benutzer oder Dritter (einschliesslich Karteninhaber, Kunden von ècash und/oder anderer Produkte der Bank) befürchten zu müssen.

16. Änderung der Bestimmungen

Die Bank behält sich vor, die vorliegenden AGB, allfällige Zusatzvereinbarungen oder besonderen Bestimmungen zu den einzelnen Dienstleistungen jederzeit zu ändern. Diese Änderungen werden schriftlich, elektronisch am Bildschirm (vgl. Ziff. 8) und/oder auf dem Zirkularweg und/oder über sonstige geeignete Kanäle bekannt gegeben und, sofern innert 30 (dreissig) Tagen nach Bekanntgabe nicht schriftlich widersprochen wird, gelten diese in jedem Fall mit der ersten Eingabe/Verwendung der Legitimationsmittel nach der Bekanntgabe als genehmigt.

17. Kündigung

- 17.1. Das Unternehmen und die Bank können jederzeit die Nutzung des Portals mit Wirkung für sämtliche oder nur einzelne Benutzer kündigen.
- 17.2. Zudem kann jeder Benutzer die Nutzung des Portals mit Wirkung für sich selbst jederzeit kündigen.
- 17.3. **Die Bank bleibt trotz Kündigung berechtigt, sämtliche vor der Kündigung erteilte Aufträge für das Unternehmen rechtsverbindlich auszuführen und abzuschliessen.**
- 17.4. Die Bank ist berechtigt, einzelne über das Portal angebotene Dienstleistungen fristlos zu kündigen, ohne das Unternehmen oder den Benutzer vorab hierüber zu informieren.

18. Weitere Bestimmungen

Diese Geschäftsbedingungen (AGB) für die Benutzung des Portals und der damit verbundenen Dienstleistungen ergänzen und vervollständigen sonstige anwendbare Bestimmungen, die das Verhältnis zwischen dem Unternehmen (und/oder dem Benutzer) und der Bank regeln.

19. Anwendbares Recht und Gerichtsstand

- 19.1. Die vorliegenden Geschäftsbedingungen für die Benutzung des Portals und der damit verbundenen Dienstleistungen unterliegen schweizerischem Recht.
- 19.2. **Ausschliesslicher Gerichtsstand für die Beilegung von Rechtsstreitigkeiten zwischen den Parteien im Zusammenhang mit dem Abschluss, der Durchführung und der Auslegung dieser Bestimmungen ist Lugano. Die Bank behält sich jedoch das Recht vor, das Gericht am Wohnsitz des Benutzers bzw. am Sitz des Unternehmens oder jedes andere zuständige Gericht anzurufen. Vorbehalten bleiben ausserdem die im schweizerischen Gesetz vorgesehenen zwingenden Gerichtsstände.**

Vertragsbestimmungen Virtual Corporate Solution

Allgemeine Geschäftsbedingungen betreffend den Gebrauch von Virtual Card Numbers (nachfolgend: «VCN»), welche über Virtual Corporate Solution und Virtual Corporate Solution Plus, (nachfolgend: «VCS») generiert werden.

Diese allgemeinen Geschäftsbedingungen (nachfolgend: «Geschäftsbedingungen») regeln die Rechtsbeziehung zwischen der Cornèr Bank Ltd. (nachfolgend: «Bank») und dem Unternehmen, das sich um die Verwalterrechte bewirbt (nachfolgend: «Unternehmen»), und/oder den zur Nutzung des VCS via das Portal (VCS-Portal), die mobile App, die API oder eine Integration mit Dritten autorisierten Personen (nachfolgend: «Administrator» oder «Nutzer») im Hinblick auf die Verwendung von VCN und VCS.

Bedingung für die Zugriffserlaubnis des Unternehmens auf das VCS ist die Ausführung einer verbindlichen Rahmenvereinbarung für die Ausstellung von Cornèrcard Business Karten sowie ein gültiger Antrag für ein Visa Finanzierungsprodukt.

1. **Allgemeine Bestimmungen betreffend den Zugriff auf das Portal, den Gebrauch von VCN**
 - 1.1 Die Bank gewährt dem Unternehmen auf Antrag Zugang zum VCS für die Generierung von VCN, sofern das Unternehmen Gewähr dafür bietet, seinen daraus fließenden finanziellen Verpflichtungen ordnungsgemäss und jederzeit wie hierin sowie auf dem Einzelmonatsauszug vereinbart nachzukommen.
 - 1.2 Das Unternehmen/der Nutzer erhält Zugang zum VCS-Portal, Mobile App-Zugang zur API oder gewährt Dritten Zugang, für die Generierung von auf den Unternehmensnamen ausgestellten VCN samt Zugangsdaten und zugehörigen Informationen. Das Portal darf nur von Personen, die vom Unternehmen explizit dazu ermächtigt wurden, genutzt werden.
 - 1.3 Das Unternehmen erhält von der Bank monatlich eine Rechnung über die aufgelaufenen Belastungen. Die Rechnung ist mit Erhalt zur Zahlung fällig. Wird die Rechnung nicht innerhalb von 25 Tagen ab Rechnungsdatum beglichen, erhebt die Bank auf alle Transaktionen ab Verbuchungsdatum bis zur vollständigen Bezahlung einen Jahreszinssatz gemäss «Preise, Zinsen und Gebühren»-Tabelle. Falls die Zahlungen gegenüber der Bank im Lastschriftverfahren (LSV) erfolgen, kann die Bank der Korrespondenzbank des Unternehmens die erforderlichen Daten betreffend das Unternehmen, das VCS sowie die kumulierten Ausgabenbeträge bekannt geben. Vorbehalten bleibt zudem die Verrechnung weiterer Kosten und Auslagen, welche der Bank von Dritten im Zusammenhang mit den VCN belastet werden.
 - 1.4 **Das Unternehmen ist zur sorgfältigen Aufbewahrung der Portal-Zugangsdaten und der über das Portal erstellten VCN-Nummern nach Massgabe der ausführlicheren Bestimmungen in Ziffer 2 ff. hiernach verpflichtet. Gehen VCN-Nummern bzw. Nutzer-Zugangsdaten verloren oder werden sie gestohlen oder unternehmensintern unrechtmässig verwendet, muss das Unternehmen dies der Bank unverzüglich schriftlich melden, damit VCN und Nutzer-Zugangsdaten gesperrt werden können.** Die Bank behält sich das Recht vor, vom Unternehmen eine Anzeige bei der zuständigen Polizei zu verlangen. Bis zum Eingang einer entsprechenden Meldung an die Bank haftet das Unternehmen für alle offenen Rechnungen, Transaktionen und Belastungen, die sich aus der Nutzung des Portals und der generierten VCN ergeben.
 - 1.5 Das Unternehmen darf das VCS-Portal nur so lange und so weit nutzen, als es sich in einwandfreien finanziellen Verhältnissen befindet, die es ihm gestatten, die künftigen Monatsrechnungen sofort zu begleichen. **Die Bank behält sich das Recht vor, das Portal nach eigenem Ermessen und auch ohne Angabe von Gründen jederzeit zu sperren.** Für das Unternehmen aus einer solchen Sperre allenfalls erwachsene Nachteile oder Schäden übernimmt die Bank keinerlei Verantwortung. Jede missbräuchliche Verwendung einer abgelaufenen oder gesperrten VCN ist unzulässig und kann strafrechtliche Folgen haben.
 - 1.6 Die über das Portal angebotenen Dienstleistungen können vom Unternehmen sowie seitens der Bank jederzeit in schriftlicher Form gekündigt werden. Die nach der Kündigung noch anfallenden VCN-Belastungen sind vom Unternehmen mit der nächstfolgenden Rechnung im Sinne von Ziffer 1.4 hiervor unverzüglich zu begleichen.
 - 1.7 Das Unternehmen ist damit einverstanden, dass im Rahmen von allfälligen Incentiveprogrammen Informationen betreffend die über die VCN abgewickelten Transaktionen an den entsprechenden Partner (zum Beispiel eine Fluggesellschaft) weitergeleitet werden. **Das Unternehmen ermächtigt die Bank, sämtliche im Zusammenhang mit einem Antrag für das VCS-Portal oder mit der Verwendung von VCN von der Bank für notwendig erachteten Auskünfte bei öffentlichen Ämtern und bei der angegebenen Bank bzw. dem Finanzinstitut einzuholen.**
 - 1.8 Die Nutzung von VCN für unrechtmässige Zwecke oder für Zwecke, die eine Verletzung der vorliegenden Allgemeinen Geschäftsbedingungen darstellen, ist nicht gestattet. In Ländern, in denen es relevante nationale und/oder internationale Sanktionen und Embargos in Bezug auf eine Kartennutzung gibt, sind keine Transaktionen gestattet. Die aktuelle Liste der relevanten Sanktionsmassnahmen (zum Beispiel in Bezug auf Länder, Personen, Unternehmen, Transaktionsarten, die betroffen sind) kann – zum Beispiel im Hinblick auf die Schweiz – auf der Website des Staatssekretariats für Wirtschaft SECO eingesehen werden (www.seco.admin.ch).
2. **Ermächtigung des Administrators und weiterer Nutzer zur Nutzung des VCS-Portals**
 - 2.1. Das Unternehmen ermächtigt den Administrator, weitere Nutzer für die Nutzung des Portals freizuschalten.
 - 2.2. Das Unternehmen trägt die gesamte Verantwortung dafür, dass sämtliche Nutzer die vorliegenden AGB vollumfänglich beachten. Das Unternehmen ist sodann verpflichtet, jeden einzelnen Nutzer detailliert über das Portal, dessen Funktionalitäten und die damit verbundenen Sorgfaltspflichten (s. Ziffer 4 und 5 hiernach) zu informieren.
 - 2.3. Erteilte Bevollmächtigungen werden nicht automatisch (z.B. durch Tod, Handlungsunfähigkeit, Streichung der Zeichnungsbefugnis oder Löschen aus einem Register, Auflösung des Arbeitsverhältnisses mit dem Unternehmen) ungültig, sondern müssen einzeln gesperrt bzw. annulliert werden (s. Ziffer 6 hiernach).
3. **Persönliche Legitimationsmittel**
 - 3.1. Die Bank stellt den Nutzern auf Antrag des Unternehmens die persönliche Vertragsnummer mit den zugehörigen Legitimationsmitteln (Nutzername, Passwort, nachstehend „Legitimationsmittel“ genannt) zur Verfügung. Das durch die Bank zugewiesene Passwort muss beim erstmaligen Login durch ein persönliches Passwort des Nutzers ersetzt werden.
 - 3.2. Der Zugriff auf das Portal und die damit verbundenen Dienstleistungen erfolgt, nachdem sich ein Nutzer unter Gebrauch der Legitimationsmittel gegenüber der Bank legitimiert hat.
 - 3.3. Die Bank kann die Legitimationsmittel jederzeit nach Ermessen anpassen oder ersetzen.
4. **Legitimation**
 - 4.1. **Gegenüber der Bank ist jedermann befugt, sich Zugang zum Portal und den damit verbundenen Dienstleistungen zu beschaffen und diese zu nutzen, der sich – zum Zeitpunkt der Benutzung – durch die Eingabe gültiger Legitimationsmittel, den Anleitungen des Portals (Selbstlegitimation) entsprechend, legitimiert hat.** Dies gilt unabhängig davon, ob es sich bei der Person tatsächlich um einen Nutzer handelt bzw. dieser vom Unternehmen entsprechend autorisiert wurde. Die Bank gilt als vom Unternehmen beauftragt und ermächtigt, die bei ihr über das Portal eingehenden Aufträge auszuführen, sobald ihnen eine korrekte Legitimationsprüfung zugrunde liegt.
 - 4.2. Die Bank ist daher ausdrücklich von jeder weiteren Kontrollpflicht bezüglich der tatsächlichen Berechtigung zur Nutzung des Portals befreit, **unabhängig von den internen Beziehungen zwischen der Bank und dem Nutzer, wobei die Bank allfällige anderslautende Bestimmungen nicht berücksichtigen muss, die auf Formularen der Bank enthalten sind, insbesondere auf Formularen betreffend die Regelung der Zeichnungsberechtigung im Zusammenhang mit der Vertragsbeziehung zur Bank** (insbesondere Vollmachtformulare und/oder Formulare, die Zeichnungsberechtigungen begründen, die auf die Vertragsbeziehungen mit der Bank anwendbar sind (einschliesslich zum Beispiel Kartenverträge, Konsum-/Privatkreditvereinbarungen).
 - 4.3. Die Bank behält sich jedoch das Recht vor, den Zugang zum Portal jederzeit und ohne Angabe von Gründen zu verweigern und zu verlangen, dass die Nutzer sich auf andere Weise legitimieren.
 - 4.4. **Jede Transaktion, jeder Vorgang oder jede Tätigkeit, die im Rahmen der Vertragsbeziehung mit der Bank (einschliesslich Kartenverträge) mittels einer solchen vorgängigen Legitimation ausgeführt wird, wird dem Unternehmen zugerechnet, die sie ohne jeglichen Vorbehalt als rechtsgültig und verbindlich akzeptiert.**
5. **Sorgfaltspflichten**
 - 5.1. **Der Nutzer ist verpflichtet, die Legitimationsmittel besonders sorgfältig aufzubewahren. Diese dürfen weder versandt, weitergegeben noch in einer anderen Weise anderen Personen zugänglich gemacht werden.** Das persönliche Passwort ist geheim zu halten, darf weder notiert, elektronisch gespeichert noch leicht ermittelbar sein (keine Telefonnummern, Geburtsdaten, Autokennzeichen, einfach ermittelbare Zahlenfolgen, etc.) und muss entsprechend die Anforderungen der Bank in Bezug auf Integrität und Komplexität erfüllen. Das gewählte Passwort verfällt automatisch gemäss den

von der Bank definierten Regeln und muss deshalb regelmässig erneuert bzw. ersetzt werden.

- 5.2. Der Nutzer verpflichtet sich ausserdem, sämtliche möglichen Sicherheitsmassnahmen zum Schutze der Arbeitsstationen, insbesondere des elektronischen Datenverarbeitungssystems (EDV-System und allfällige, auf besagtem System abgespeicherte Daten), die für den Zugang zum Portal verwendet werden, vor unbefugten Eingriffen, unbefugter Nutzung und Manipulation oder Abfangaktionen zu ergreifen (zum Beispiel mittels Anwendung von aktualisierten Versionen der Firewall- und Antivirenprogramme). Das Unternehmen und der Nutzer haben ausführliche Informationen über die zu treffenden, notwendigen Sicherheitsmassnahmen einzuholen. **Es obliegt dem Unternehmen, diese Pflichten und Verbote von sämtlichen Nutzern strikte einhalten zu lassen, wobei es vollumfänglich für jede und alle Folgen haftet, die sich aus der Nichtbeachtung besagter Schutzpflicht der Legitimationsmittel auch seitens der Nutzer ergeben.**
- 5.3. Auf E-Mails, die angeblich von der Bank stammen und zur Bekanntgabe von Legitimationsmitteln auffordern (z.B. durch Eingabe auf Webseiten, die via Link aufgerufen werden können) darf nicht reagiert werden. Die Bank ist umgehend zu informieren. Besteht Grund zur Annahme, dass eine andere Person vom persönlichen Passwort Kenntnis erhalten hat, muss der Nutzer diesen unverzüglich ändern.
- 5.4. Die Bank behält sich vor, zusätzliche Legitimationsanforderungen zu definieren (zwei- oder dreistufige Authentifizierungssysteme). Entsprechend kann der Nutzer aufgefordert werden, zusätzliche Informationen an die Bank zu übermitteln, z.B. die Mobile-Telefonnummer zwecks Übermittlung von SMS, oder die Installation besonderer Software-Applikationen für Smartphone zwecks Authentifizierung über Randomome on-time Token.
- 5.5. Der Zugang zum Portal erfolgt über das öffentliche Internet. **Der Zugang und die Benutzung des öffentlichen Internets obliegen ausschliesslich dem Unternehmen und den Nutzern, welche jegliche Haftung und Risiken diesbezüglich übernehmen, insbesondere für Folgen, die aus allfälligen Manipulationen und Abfangaktionen seitens Dritter entstehen.** Die Bank besorgt weder eine Verbindung, noch liefert sie dieselbe, noch garantiert sie dem Nutzer die Verbindung zum Portal über das öffentliche Internet oder irgendeinen Internet-Provider. Für den Zugang zum Portal und den damit verbundenen Dienstleistungen ab öffentlichem Internet stellt die Bank eine eigene Internet-Seite zur Verfügung, deren Adresse dem Kunden separat mitgeteilt wird.
- 5.6. Anlässlich des ersten Verbindungsaufbaus ist der Nutzer dazu verpflichtet, das ihm von der Bank gelieferte Passwort zu ändern. Die Bank ist befugt, die Legitimationsmittel jederzeit und ohne Vorankündigung zu ändern, soweit sie dies für notwendig erachtet, namentlich aus Sicherheitsgründen. In einem solchen Fall übermittelt die Bank dem Nutzer unverzüglich die neuen Legitimationsmittel. Sollte der Verdacht entstehen, dass unbefugte Dritte Kenntnis von diesen Legitimationsmittel erhalten haben, müssen das Unternehmen sowie die Nutzer unverzüglich die Bank darüber informieren, um die Codes zu ersetzen. Diese Pflicht ist insbesondere in folgenden Fällen zwingend:
 - Sperrung des Zugangs zu den Dienstleistungen des Portals;
 - Verdacht auf Missbrauch bei der Verwendung der Legitimationsmittel seitens unbefugter Dritter;
 - Verlust oder Diebstahl auch nur eines Teils der Legitimationsmittel.

6. Risiken und Haftung

- 6.1. Die Nutzung des Portals ist mit Risiken verbunden, u.a. aufgrund der Möglichkeit der weiteren Verwendung der im Portal angezeigten Informationen. Im Wesentlichen sind dies folgende Risiken: (1) **Offenlegung der Bankbeziehung sowie von Bankkundeninformationen gegenüber Dritten, wodurch das Bankgeheimnis nicht mehr sichergestellt werden kann;** (2) Veränderungen bzw. Verfälschungen von Informationen (z.B. Vortäuschen falscher Informationen); (3) Systemunterbrüche und andere Übermittlungsstörungen, die Verzögerungen, Verfälschungen, Fehlleitungen oder Löschungen von Informationen verursachen können; (4) Missbrauch mit Schädigungsfolge durch das Abfangen von Informationen durch Dritte.
- 6.2. **Die Legitimationsabrede (vgl. Ziff. 3) bedeutet, dass jene Risiken beim Nutzer bzw. beim Unternehmen liegen, die sich (i) aus Manipulationen an dessen EDV-System durch Unbefugte, (ii) aus missbräuchlicher Verwendung der persönlichen Legitimationsmittel, (iii) aus Verletzung von Sorgfaltspflichten oder (iv) aus Eingriffen unberechtigter Dritter in die Datenübermittlung ergeben.**
- 6.3. Das Unternehmen bzw. der Nutzer ist sich zudem der Risiken bezüglich des Informations- und Datenaustauschs über öffentliche und private Datenübermittlungsnetze, namentlich auch das Risiko der Offenlegung der Bankbeziehung und der Bankkundeninformationen gegenüber Dritten, bewusst. Auch wenn beim Zugriff auf das Portal der zu übermittelnde Dateninhalt, mit Ausnahme von Absender und Empfänger, automatisch verschlüsselt wird, können gezielte Manipulationen am EDV-System des Nutzers durch Unbefugte nicht ausgeschlossen werden. **Die entsprechenden Risiken aus solchen Manipulationen fallen in den Einflussbereich des Unternehmens bzw. des Nutzers und sind vom Unternehmen zu tragen.** Das Unternehmen trägt das Risiko von Einsätzen der persönlichen Legitimationsmittel bis zum

Wirksamwerden der Sperre (s. Ziffer 6 hiernach).

- 6.4. **Jegliche Haftung der Bank für etwaige Schäden – unmittelbare, mittelbare und/oder Folgeschäden – oder Folgen jeglicher Art ist ausdrücklich ausgeschlossen, die sich zum Nachteil des Unternehmens bzw. der Nutzer, der Karteninhaber und/oder Dritter aus dem Zugang zum Portal und/oder der Nutzung des Portals, auch unbefugterweise, umfassend, aber nicht beschränkt auf den unbefugten Zugang oder die unsachgemässe Nutzung des Portals und/oder von VCN durch Direktoren, Führungskräfte, Mitarbeitende, Vermittler, professionelle Berater, Lieferanten, Auftragnehmer oder Unterauftragnehmer des Unternehmens, ergeben.**
 - 6.5. Obwohl die Bank jede zumutbare Anstrengung unternommen hat, um die Sicherheit des Portals - mittels Anwendung der notwendigen und allgemein anerkannten Massnahmen und technischen sowie sicherheitsmässigen Standards - zu gewährleisten, kann eine absolute Sicherheit nicht garantiert werden.

Der Kunde nimmt insbesondere zur Kenntnis, dass:

 - die Arbeitsstation und das EDV-System des Unternehmens und/oder des designierten Nutzers nicht unter die Kontrolle der Bank fallen und Gegenstand von externen Angriffen sein können;
 - ein potenzielles Risiko besteht, dass unbefugte Personen die Legitimationsmittel oder andere Daten des Unternehmens und/oder des Nutzers;
 - die Informationen über das öffentliche Netz übermittelt werden und - obwohl sie in verschlüsselte Pakete unterteilt sind - nicht ausgeschlossen werden kann, dass sie über Leitungen und Knotenpunkte jenseits der Landesgrenze verlaufen können, und zwar unabhängig davon, dass Wohnort von Absender und Empfänger in der Schweiz liegen;
 - die Betreiber des öffentlichen Netzes das Unternehmen, den Nutzer und die Gegenparteien, mit denen dieser über das Internet in Verbindung tritt, identifizieren können;
 - in keinem Falle, weder das Portal noch das öffentliche Netz die Einhaltung des Bankkundengeheimnisses gewährleisten können.
 - 6.6. **Die Bank übernimmt im Besonderen keinerlei Verantwortung für und haftet für keinerlei Schäden, die zum Nachteil des Unternehmens, der designierten Nutzer und/oder der Karteninhaber auftreten, und zwar, (i) die als Folge von Übermittlungsfehlern, technischen Mängeln, Überlastung, Störungen, Schäden, Unterbrechungen, Manipulationen oder Abfangaktionen, (ii) infolge von widerrechtlichen Eingriffen an Telekommunikationseinrichtungen oder der Sperrung von Telekommunikationsanlagen oder Netzwerken, (iii) oder als Folge von anderen Fehlern, die von den Betreibern der Anlagen oder der Netzwerke verursacht werden, während der Benutzung des Portals. Die Bank haftet allgemein ebenfalls nicht für Schäden, die dem Unternehmen, den Nutzern, dem Karteninhaber oder Dritten als Folge des Umstandes entstehen könnten, dass Daten im Zusammenhang mit der Bankbeziehung über das öffentliche Netz zur Verfügung gestellt werden.**
- ## 7. Sperre
- 7.1. Der Administrator kann die Zugriffsberechtigung weiterer Nutzer jederzeit sperren.
 - 7.2. Das Unternehmen kann die Sperrung der Zugriffsberechtigung des Administrators oder weiterer Nutzer jederzeit bei der Bank beantragen.
 - 7.3. Die Bank kann den Zugang der Nutzer jederzeit sperren (zum Beispiel wenn das Risiko besteht, dass VCN-Transaktionen schweizerische oder internationale Embargobestimmungen oder Sanktionsmassnahmen verletzen oder die Bank sonstigen rechtlichen, regulatorischen oder wirtschaftlichen Risiken aussetzen oder ihre Reputation gefährden).
 - 7.4. Jeder Nutzer kann die Sperrung seiner Zugriffsberechtigung bei der Bank beantragen. Die Bank behält sich vor, einem solchen Antrag erst nach Rücksprache mit dem Administrator nachzukommen.
 - 7.5. Die Bank lehnt jegliche Haftung für Konsequenzen ab, die für das Unternehmen infolge einer Sperrung des VCS oder einer Sperrung oder einer Kündigung der VCN entstehen könnten. Die Nutzung einer gesperrten VCN ist unrechtmässig und kann zu gerichtlicher Verfolgung führen, ebenso wie die daraus resultierenden Verbindlichkeiten des Unternehmens. Die Bank behält sich das Recht vor, den zugehörigen Händlern oder autorisierten Banken jegliche Informationen bereitzustellen, die diese zum direkten Erhalt des geschuldeten Betrags vom Karteninhaber oder vom Unternehmen benötigen könnten. Die Bank ist nicht zur Durchführung von VCN-Transaktionen verpflichtet, wenn durch diese anwendbares Recht, rechtliche oder regulatorische (darunter ausländische) Bestimmungen, Einschränkungen, Aufträge, Verbote oder Massnahmen der zuständigen Behörden (zum Beispiel Embargobestimmungen, nationale oder internationale Sanktionsbestimmungen oder Geldwäscheregulierungen) verletzt werden.
- ## 8. Informationen von Automaten, Terminals, Bildschirmen oder anderen EDV-Systemen
- 8.1. Obwohl die Bank jede zumutbare Anstrengung unternommen und angemessene Massnahmen eingeführt hat, um die Zuverlässigkeit, Genauigkeit und Unversehrtheit der auf dem Portal zur Verfügung gestellten Informationen und Mitteilungen zu gewährleisten, haben die zur Verfügung gestellten Daten und Dokumente einen rein informativen Charakter.
 - 8.2. Sie haben keinerlei Verpflichtung oder Haftung für die Bank zur Folge und

können nicht benutzt werden, um Forderungen irgendwelcher Art gegenüber der Bank seitens des Kunden, der Designierten Nutzer, des Karteninhabers oder Dritter geltend zu machen

- 8.3. Die angezeigten Informationen und Mitteilungen gelten als vorläufig und unverbindlich, es sei denn, gewisse Angaben würden im Rahmen einer Dienstleistung ausdrücklich als verbindlich bezeichnet. Ebenso stellen solche Informationen weder eine Empfehlung noch ein Angebot oder eine Aufforderung zur Tätigung von Transaktionen oder zum Abschluss irgendeines Rechtsgeschäfts dar, es sei denn, sie werden ausdrücklich als solche bezeichnet

9. Elektronische Vereinbarungen, elektronisch angezeigte rechtliche Hinweise

- 9.1. Die Nutzung gewisser, über das Portal zur Verfügung gestellter Dienstleistungen, kann von der Vereinbarung zusätzlicher Bestimmungen abhängig gemacht werden. Diese Bestimmungen kann die Bank dem Nutzer in elektronischer Form vorlegen, nachdem er sich über das Portal legitimiert hat. Dies gilt auch für die Anpassung oder Ergänzung der vorliegenden Vereinbarung.
- 9.2. Die Dienstleistungen werden freigegeben, sobald der Nutzer, sofern erforderlich, diese erfolgreich beantragt und den zusätzlichen besonderen Bestimmungen elektronisch zugestimmt hat. Damit werden die Bestimmungen für den Nutzer bzw. das Unternehmen verbindlich.
- 9.3. Elektronisch abgeschlossene Vereinbarungen werden den handschriftlich unterzeichneten Vereinbarungen gleichgestellt. Die Bestimmungen können ausgedruckt werden und sind im Portal einsehbar. Die Bank kann ihr Dienstleistungsangebot jederzeit ändern. Aufgrund der Internationalisierung der Märkte und der laufenden Erweiterung der elektronischen Dienstleistungen muss die Bank elektronisch veröffentlichte Informationen und Dienstleistungen mit zusätzlichen rechtlichen Hinweisen versehen. Diese sind mit Anzeige für den Nutzer verbindlich. Will er sie nicht anerkennen, hat er auf die betreffenden Informationen/Dienstleistungen zu verzichten

10. Länderspezifische Schranken, ausländische Import- und Exportbeschränkungen

- 10.1. Das Unternehmen bestätigt, sich darüber bewusst zu sein und auch die Nutzer darüber informiert zu haben, dass der Zugang zum Portal und/oder zu den damit verbundenen Dienstleistungen wie auch deren Nutzung ausserhalb der Schweiz unter bestimmten Umständen gegen ausländische Gesetze und Vorschriften verstossen könnte. Das Unternehmen verpflichtet sich aus diesem Grund, (i) sich über die Existenz, den Inhalt und die Tragweite von allfälligen Gesetzen und Vorschriften sowie ganz allgemein von Regelwerken betreffend Nutzung von Bankdienstleistungen zu informieren, die in ausländischen Staaten gelten, von denen aus er auf das Portal bzw. damit verbundene Dienstleistungen zugreifen könnte; (ii) das Portal und die damit verbundenen Dienstleistungen nur insoweit zu nutzen, als dies mit den genannten lokalen Bestimmungen und Vorschriften vereinbar ist und insbesondere gewissenhaft allfällige Verbote und/oder Einschränkungen bezüglich der Nutzung von Bankdienstleistungen einzuhalten; (iii) auch die Nutzer zu Oberstehendem zu verpflichten.
- 10.2. Das Unternehmen befreit die Bank in diesem Zusammenhang von jeglicher Haftung und anerkennt - unwiderruflich und ausnahmslos - umfassend für alle etwaigen Folgen, Strafen oder Verstösse zu haften, die als Folge der Nutzung des Portals und der damit verbundenen Dienstleistungen ausserhalb des schweizerischen Staatsgebiets zurückzuführen sind.
- 10.3. Ausserdem erklärt der Kunde, die Bank von jeglichen direkten, indirekten Schäden und/oder Folgeschäden, Lasten, Kosten und Auswirkungen schadlos zu halten, die ihr durch den Verstoß gegen vorgenannte Bedingungen oder andere Bestimmungen der vorliegenden Bedingungen für die Nutzung des Portals oder damit verbundener Dienstleistungen entstehen.
- 10.4. Die Bank ist berechtigt, den Umfang der zur Verfügung stehenden Dienstleistungen jederzeit und ohne vorgängige Anzeige anzupassen bzw. zu beschränken. Die Bank ist nicht verantwortlich und haftet für keinerlei Schäden - weder direkte noch indirekte oder Folgeschäden - die dem Unternehmen oder einem Nutzer infolge Sperrung, Aufhebung, Änderung oder Unterbrechung des Zugangs einer oder mehrerer Dienstleistungen oder des gesamten Portals entstehen könnten. Die Kenntnis und die Beachtung aller relevanten Restriktionen und Gesetze obliegen dem Nutzer. Die Bank lehnt diesbezüglich jede Haftung ab.

11. Übermittlungsfehler, technische Störungen, Betriebsausfälle und rechtswidrige Eingriffe

Für die durch Übermittlungsfehler, Fehlleitungen, technische Mängel und Störungen, Betriebsausfälle oder rechtswidrige Eingriffe in EDV-Systeme des Nutzers oder eines Dritten (inkl. jedermann zugänglicher Systeme und Übermittlungsnetze) verursachten Schäden übernimmt die Bank keine Haftung, es sei denn, die Bank habe die geschäftsübliche Sorgfalt verletzt. Solange die Bank die geschäftsübliche Sorgfalt wahrnimmt, übernimmt die Bank keine Gewähr für störungsfreien, jederzeit ununterbrochenen Zugang zu ihren Dienstleistungen. Damit entfällt auch jede Haftung für Schäden infolge Störung, Unterbrüchen (inkl. systembedingter Wartungsarbeiten) oder Überlastungen von Automaten bzw. EDV-Systemen der Bank.

12. Preise und Gebühren

- 12.1. Die Preise für die Benützung des Portals und der damit zur Verfügung gestellten Dienstleistungen sowie für das Überlassen der Legitimationsmittel (inkl. deren Ersatz und Zusatzbestellungen) sind in einer separaten Preisliste aufgeführt, die im Antragsformular enthalten ist.
- 12.2. Änderungen werden in geeigneter Weise bekannt gegeben. Die vereinbarten Preise werden dem Unternehmen je nach Wahl der Bank umgehend, monatlich, vierteljährlich oder jährlich belastet.

13. Einhaltung der gesetzlichen Anforderungen/Informationsaustausch

Das Unternehmen nimmt zur Kenntnis und willigt ein, dass es für die Zwecke seiner Geschäftsbeziehung mit der Bank allein für die Einhaltung aller gesetzlichen und regulatorischen Anforderungen verantwortlich ist, einschliesslich, jedoch nicht beschränkt auf jegliche Anforderungen in Bezug auf Steuern, die für das Unternehmen gemäss dem Recht des Gerichtsstands seines Sitzes anwendbar sein können, oder allgemein gemäss dem Recht aller Gerichtsstände, in denen es zum Zahlen von Steuern in Bezug auf jegliche Guthabensaldos, die auf den VCN verfügbar sind, verpflichtet ist. Die Bank übernimmt keinerlei Haftung für eine solche Einhaltung. Bei Zweifeln bezüglich der Einhaltung dieser Anforderungen lässt sich das Unternehmen von einem Experten beraten. Dem Unternehmen ist bewusst, dass die Bank aufgrund von Vereinbarungen zwischen der Schweiz und anderen Ländern sowie infolge von Einzel- oder Gruppenanfragen aufgrund von solchen Vereinbarungen oder auf der Grundlage international anerkannter Standards, zum Beispiel von Standards in Bezug auf den automatischen Informationsaustausch, möglicherweise Informationen in Bezug auf VCN an die relevanten Steuerbehörden in der Schweiz oder im Ausland offenlegen muss. Das Unternehmen nimmt ebenfalls zur Kenntnis, dass zusätzlich zum oben genannten automatischen Informationsaustausch die Bank ihre rechtlichen, regulatorischen oder aufsichtsbezogenen Informations- und Kommunikationsverpflichtungen einhalten muss und/oder Anfragen in Bezug auf Informationen von Schweizer oder ausländischen Behörden beantworten muss. In diesem Kontext nehmen Anfragen in Bezug auf Informationen von ausländischen Behörden generell die Form von internationaler Rechtshilfe an. In Ausnahmefällen können ausländische Behörden Informationen und Dokumente allerdings direkt bei der Bank anfragen (zum Beispiel können nach aktuellem US-Recht unter bestimmten Bedingungen die zuständigen Strafverfolgungsbehörden direkt bei einer ausländischen Bank, die ein Konto bei einer entsprechenden Bank in den USA hält, die Ausgabe von Informationen und Dokumenten in Bezug auf irgendein Konto und/oder irgendeinen Kunden der ausländischen Bank anfragen, selbst wenn solche Dokumente ausserhalb der USA aufbewahrt werden und das betreffende Konto oder der betreffende Kunde keine direkte Verbindung mit den Aktivitäten der ausländischen Bank in den USA hat. Insbesondere kann, beim Tätigsein in ausländischen Märkten, die Bank aufgefordert werden, direkt auf Anfragen von ausländischen Aufsichtsbehörden, einschliesslich in Bezug auf die Offenlegung von Kundendaten, zu reagieren. Das Unternehmen nimmt zur Kenntnis und akzeptiert, dass die Bank möglicherweise personenbezogene Daten, Informationen und Dokumente an Schweizer und ausländische Behörden bereitstellen muss und die Bank, ihre Organe und ihre Mitarbeitenden in diesem Umfang von ihren Geheimhaltungspflichten und vom Bankgeheimnis befreit sind bzw. darauf verzichten.

14. Bankgeheimnis/Datenschutz, Marketing

- 14.1. Das schweizerische Recht (z.B. bezüglich Bankgeheimnis, Datenschutz) beschränkt sich allein auf schweizerisches Territorium. Somit verlieren alle ins Ausland gelangenden Daten den Schutz nach schweizerischem Recht.
- 14.2. Die Bank ist berechtigt, Partnerunternehmen in der Schweiz oder im Ausland, insbesondere Tochtergesellschaften der Cornèr Bank Gruppe mit Sitz in der Europäischen Union, für die Durchführung aller oder eines Teils der Dienstleistungen in Bezug auf das VCS (zum Beispiel Portalantragsprüfungen, VCN-Ausstellung, Vertragsverwaltung, Online-Services, Einzug von Zahlungen, Kundenkommunikation, Berechnung des Kreditrisikos, Betrugsprävention, Rückbuchungsvorgänge, Zahlungsverarbeitung, IT) und für die Verbesserung der Risikomodelle, die zur Erteilung von Kreditlimiten und Betrugsprävention verwendet werden, zu beauftragen. Das Unternehmen berechtigt die Bank, diesen Dritten die für die sorgfältige Durchführung der ihnen zugewiesenen Aufgaben erforderlichen Daten bereitzustellen und, falls erforderlich, diese Daten zu diesem Zweck ins Ausland zu übermitteln. Dabei kann das Unternehmen auch personenbezogene Daten des Unternehmens an solche Partnerunternehmen für die in der Datenschutzerklärung (Ziffer 3 – cornercard.ch/dataprotection) angegebenen Verarbeitungszwecke übermitteln. Die Verarbeitung solcher Daten erfolgt unter vollumfänglicher Einhaltung der anwendbaren Datenschutzbestimmungen, das heisst des Schweizer Datenschutzgesetzes (DSG) und der europäischen Datenschutz-Grundverordnung (DSGVO). Entsprechend können die Bank oder von der Bank ernannte Dritte Unternehmens-, Nutzer- und/oder Verwalterdaten, einschliesslich Transaktionsdaten, insbesondere für Marketing- und Marktforschungszwecke sowie zum Erstellen von Kundenprofilen speichern, verarbeiten und verwenden. Das Speichern, Verarbeiten und Nutzen der Unternehmensdaten ermöglicht

individuelle Beratung und Offerten sowie das Bereitstellen von Informationen zu Produkten und Dienstleistungen der Bank an den Karteninhaber. Es können insbesondere die folgenden Daten verarbeitet werden: Informationen zum Unternehmen, zu VCB-Transaktionen sowie zu jeglichen zusätzlichen oder ergänzenden Dienstleistungen. Das Unternehmen hat diese Allgemeinen Geschäftsbedingungen gelesen und verstanden und stimmt ihnen durch die Nutzung des Portals vollumfänglich zu.

15. Änderungen der Bestimmungen

Die Bank behält sich die jederzeitige Änderung der vorliegenden AGB, von allfälligen Zusatzvereinbarungen oder besonderen Bestimmungen zu den einzelnen Dienstleistungen vor. Diese werden schriftlich, elektronisch am Bildschirm (vgl. Ziff. 8), auf dem Zirkularweg oder auf andere Weise bekannt gegeben und gelten ohne schriftliche Widerspruch innert 30 Tagen seit Bekanntgabe als genehmigt, auf jeden Fall aber mit dem nächsten Einsatz der Legitimationsmittel.

16. Kündigung

- 16.1. Eine Kündigung der Nutzung des Portals mit Wirkung für sämtliche oder nur einzelne Nutzer kann jederzeit sowohl durch das Unternehmen als auch durch die Bank erfolgen.
- 16.2. Die Bank **bleibt trotz Kündigung berechtigt, sämtliche noch vor rechtswirksamer Kündigung ausgelösten Aufträge rechtsverbindlich für das Unternehmen zu verarbeiten.**
- 16.3. Die Bank ist jederzeit berechtigt, einzelne über das Portal angebotene Dienstleistungen fristlos und ohne Anzeige an das Unternehmen oder den Nutzer zu kündigen.

17. Weitere Bestimmungen

Diese Bedingungen für die Benutzung des Portals und der damit verbundenen Dienstleistungen vervollständigen und ergänzen alle anderen Bestimmungen, die das Verhältnis des Unternehmens bzw. des Nutzers mit der Bank regeln.

18. Anwendbares Recht und Gerichtsstand

18.1. Die vorliegenden Bedingungen für die Benutzung des Portals und der damit verbundene Dienstleistungen unterstehen schweizerischem Recht.

18.2. Ausschliesslicher Gerichtsstand für sämtliche Rechtstreitigkeiten, welche zwischen den Parteien im Rahmen der Vereinbarung der vorliegenden Bedingungen, ihrer Umsetzung und Auslegung entstehen ist Lugano. Die Bank behält sich indessen das Recht vor, den Kunden beim zuständigen Gericht seines Wohnsitzes oder jedem anderen zuständigen Gericht zu belangen. Die vom Schweizer Gesetz vorgesehenen zwingenden Gerichtsstände bleiben ausserdem vorbehalten.

11. Unterschriften

Mit der Unterzeichnung dieses Vertrags bestätigen das Unternehmen und der Administrator, dass sie die beiliegenden Allgemeinen Geschäftsbedingungen für die Benutzung des Partner Collaboration Tool (PCT) Portals der Cornèr Bank AG vollständig gelesen, verstanden und akzeptiert haben. Die Anmeldedaten werden dem Administrator schriftlich mit eingeschriebenem Brief und/oder per E-Mail mitgeteilt.

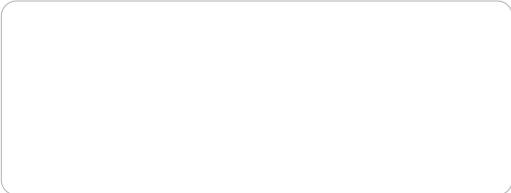
Das Unternehmen bestätigt ausserdem, den Karteninhaber und/oder Antragsteller des Konsum-/Privatkredits (ècash) und/oder sonstiger Produkte der Cornèr Banca SA ordnungsgemäss informiert zu haben, bzw. – vor der Benutzung des Portals für den jeweiligen Kunden – ordnungsgemäss zu informieren bezüglich der über das Portal verfügbaren Funktionen/Funktionalitäten, mit denen der Administrator und die anderen vom Unternehmen autorisierten Benutzer beispielsweise den Lebenszyklus der Zahlungskarte verwalten (PIN-Anforderung, Sperrung/Entsperrung der Karte, Aufladung der Karte usw.) bzw. Daten zur Beantragung des Konsum-/Privatkredits eingeben, aktualisieren, verwalten und Informationen zum Inhaber und zur Kartenbenutzung (Stammdaten, Transaktionen, Saldo, Ausgabenlimite, Monatsauszug usw.) beziehungsweise zum Antragsteller des Konsum-/Privatkredit (insbesondere Stammdaten, ausbezahlter Betrag, vorgelegte Dokumentation) einsehen können usw.

Unterschrift des Administrators

Ort, Datum _____ Name _____

Vorname _____ Unterschrift **X** _____

Unterschrift der Firma

Ort, Datum _____ Firmenstempel 

Name _____ Name _____

Vorname _____ Vorname _____

Unterschrift*1 **X** _____ Unterschrift*1 **X** _____

*1 Rechtsgültige Unterschrift/-en gemäss Handelsregister (Einzel- oder Kollektivunterschrift)



**Bitte den vollständig ausgefüllten und unterzeichneten Kartenantrag einsenden an:
Business Client Management, Cornèr Banca SA, Cornèrcard, Via Canova 16, 6901 Lugano.**



GAS/ECR/ICR

nicht frankieren
ne pas affranchir
non affrancare
50416832
000002

B



Business Client Management
Cornèrcard
Via Canova 16
6901 Lugano_Switzerland