cornèrcard THREEWAY business solutions

APPLICATION VIRTUAL CORPORATE SOLUTION

Integrated with the Partner Collaboration Tool

New customers: please fill in the framework agreement

Important: all information is mandatory.

1. Details of the Partner (hereinafter the "Company")

Company legal name

Street/No.

Postal code/City | Country

2. Details of the Portal Administrator (hereinafter the "Administrator")

☐ Mr. ☐ Ms.

Surname | First name

Date of birth | Country of residence

Nationality | E-mail

Cell phone* | Function within the company

Correspondence language ☐ IT ☐ DE ☐ FR ☐ EN

3. Product selection and account information:

☐ VCS MCBGGI21SU01-00063

☐ VCS Plus (with insurance package) MCBGGI21SU01-00064

Expected annual turnover (CHF):

4. Main card request 1

Main card name (without spaces):

Desired monthly limit:

5. Main card request 2 (optional)

Main card name (without spaces):

Desired monthly limit:

6. Main card request 3 (optional)

Main card name (without spaces):

Desired monthly limit:

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

VISA mastercard Diners Club INTERNATIONAL

7. Form A – Declaration of identity of the beneficial owner (mandatory information) pursuant to the CDB 20

No information is required if:

– the assets used to conduct transactions with the prepaid card, and/or to settle the monthly credit card statements, and/or collected by the card issuer above this amount belong **solely** to the company **and**

– the said company is not a sole proprietorship or a simple partnership.

If this is not the case, the company declares that these assets (please tick only one answer as appropriate)

☐ belong to the cardholder.

☐ are held in trust by the company for the benefit of the person(s) listed below:

☐ belong to the person(s) listed below:

(last name(s) and first name(s), date of birth, place of birth, nationality, actual address of domicile, incl. country):

The company hereby undertakes to automatically inform the card issuer of any changes. It is a criminal offence to deliberately provide false information on this form (Article 251 of the Swiss Criminal Code, document forgery).

8. Portal activation information

Company ID

This field must contain an acronym or ID that identifies the company together with the user name (e.g.: john.companyname, no spaces, case sensitive). The field is mandatory and cannot be changed. If it is not filled in, an existing ID is used or a new ID is created based on the company name.

9. Two-factor authentication mode

☒ **SMS** (for all Users)

(*) NB: the field “Cell phone” in section 2 is mandatory

10. Declaration

Virtual Corporate Solution and Virtual Corporate Solution Plus (“VCS”): The Company and Cardholder hereby certify the information provided in this application to be accurate and acknowledge that they have received, understood, and accepted as binding the Terms and Conditions for Virtual Corporate Solution (“VCS-TC”) as well as the General Terms and Conditions for Cornèr Bank Ltd. (the «Bank») Visa, Mastercard® and Diners Club payment cards, issued by Cornèrcard (“GTC”).
The Cardholder/User (as defined in the VCS-TC) shall be severally liable together with the Company for all obligations resulting from the use of the Visa/Mastercard/Dinersclub cards and recognizes Lugano as the exclusive place of jurisdiction. The Bank is authorized to obtain any information it deems necessary about the company applicant and the prospect Cardholder/User.
Risks & Liability: On acceptance of this card application, the Company will receive the access credentials (e.g. User ID & PW) to the VCS. The Company assumes full responsibility for providing these credentials to appropriately trusted employees and for the correct use of these credentials in conformity with the Company’s internal guidelines. The Company further acknowledges and accepts that transactions with VCN Cards are not authenticated via 3D-Secure systems (e.g. a methodology that increases the security of online payments because a code must be entered to confirm the payment in addition to the card number, the expiration date, and the CVC (card verification code). The Bank expressly excludes any kind of liability for any loss or damage, including direct, indirect and/or consequential loss, or any consequences whatsoever, which may be suffered by the Company and/or the User of the VCN and/or third party as a result of accessing and/or using the VCS Portal, including, but not limited to, unauthorized access or improper use of the VCS Portal and/or the VCN, by directors, officers, employees, agents, professional advisers, suppliers, contractors or sub-contractors of the Company. The Company further acknowledges and accepts that Users may potentially consume the Company’s entire spending limit in only few transactions. The Bank accepts no responsibility for any abuse or non-authorized use of the spending limit set by the Company for its Users.
Acceptance of General terms and conditions: The GTC and the General Terms of Insurance (“GTI”) for insurance cover provided automatically and free of charge with Cornèrcard products, or made available upon request and for a fee, can be accessed at cornercard.ch/e/gtbusiness for Visa/Mastercard and at dinersclub.ch/firststep for Diners Club. By using the VCS, the Cardholder/User acknowledges that he or she has received, understands, and accepts in full the GTC, the VCS-TC as well as all applicable GTI. The company acknowledges and accepts that the Cardholder/User is entitled to apply independently for the electronic functionalities associated with Cornèrcard’s card products (iCornèr, E-Account, Mobile App, Mobile Payment, etc.) and, as part of the relevant activation process, to accept on a binding basis the related Conditions of Use in electronic form and without the company’s involvement. The Company further confirms with its signature that it has acknowledged the appropriate GTC and the VCS-TC and accepts these without restriction (the conditions can be viewed at cornercard.ch/e/gtbusiness for Visa, Mastercard, at dinersclub.ch/firststep for Diners Club or can be ordered by calling +41 91 800 41 41 for Visa, Mastercard or +41 58 880 88 00 for Diners Club).
Charges, interest rates, and fees: Information on charges, interest rates, and fees for the use and administration of the card is contained in a schedule of “Charges, Interest Rates, and Fees”. This may be accessed at any time by visiting cornercard.ch/e/prices-business or by calling +41 91 800 41 41. In addition, the company and the cardholder may be billed for any third-party charges and any costs incurred by them. The company and the cardholder hereby certify that they accept without reservation said charges, interest rates, and fees. A fee of CHF 2 is charged for each tokenisation of a card, and CHF 2 for each additional month of validity. The total amount will be charged directly to the company’s VCS account. Should the Company and the Cardholder/User apply for a further Cornèrcard product or wish to switch to a different product, the particular annual subscription fee or enrollment charge pertaining to such product will apply, and can also be accessed or requested via the above-mentioned contact details.
Exchange rates: Transactions conducted in foreign currency will be converted at the retail exchange rate of the Bank (for Visa/Mastercard cards) or at the exchange rate of Diners Club International (for Diners Club cards) on the booking date, plus foreign currency processing fees.

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

cornèrcard

General Terms and Conditions for Using the Partner Collaboration Tool (hereinafter referred to as the "PCT" or "Portal") of Cornèr Bank Ltd.

These General Terms and Conditions (hereinafter the "Terms and Conditions") set out the legal relationship between the company applying for administrator rights (hereinafter the "Company") and/or the individuals authorized to use the PCT (hereinafter the "Administrator" or "User") and Cornèr Bank Ltd. (hereinafter the "Bank") with regard to use of the PCT.

1. Authorization

1.1. The Company authorizes the Administrator to activate other Users for the purpose of using the Portal, provided that a valid employment contract has been concluded between them and the Company.

1.2. The Company shall have overall responsibility for ensuring that **all Users** fully comply with the **provisions and obligations set out in these GTC.** Accordingly, the Company shall provide to each individual User with detailed information concerning in particular the Portal, the relevant functions/functionalities, the obligation of due diligence incumbent upon the User and the related risks (see clauses 4 and 5).

1.3. Any authorizations granted shall not be invalidated automatically (for example due to death, incapacity to act, removal of signatory authority/powers, deletion from a register, or termination of the employment contract with the Company) but must be blocked or canceled individually (see clause 6).

2. Personal identifiers

2.1. At the request of the Company, the Bank shall provide Users with their personal contract number and the applicable means of authentication, such as user ID and password (hereinafter the "Identifiers"). On accessing for the first time, Users must replace the password assigned by the Bank with their own personal password.

2.2. Users shall gain access to the Portal and related services once they have been authenticated to the satisfaction of the Bank by means of the Identifiers.

2.3. The Bank reserves the right to replace or change the Identifiers at any time.

3. Authentication

3.1. **3.1. Any person who has been authenticated by entering Identifiers that are valid at the time of use,** in accordance with Portal guidelines (self-authentication), **shall be deemed by the Bank to be authorized to access the Portal and use the relevant services.** The foregoing shall apply irrespective of whether the person concerned is an actual User or has been authorized by the Company for such purpose. The Bank is deemed to have been appointed and authorized by the Company to execute orders received through the Portal once the underlying authentication process has been properly completed.

3.2. Accordingly, the Bank is expressly released from any further obligation to verify whether an individual is in fact entitled and/or authorized to use the Portal, **irrespective of the internal relationship between the Bank and the User, and the Bank shall be entitled to disregard any contrary provisions set forth in forms issued by the Bank, including, in particular, forms granting powers of attorney and/or forms stipulating signatory powers applicable to the contractual relationship with the Bank (including, for example, card contracts and consumer credit/private loan contracts [ècash]).**

3.3. The foregoing shall however be without prejudice to the right of the Bank to deny access to the Portal at any time, without stating any reasons, and to require Users to verify their identity by other means.

3.4. Any transaction, operation or act performed within the scope of the contractual relationship with the Bank (including card contracts and consumer credit/private loan contracts [ècash]) on the basis of prior authentication shall be imputed to the Company, which shall irrevocably accept it without any reservation whatsoever as legally valid and absolutely binding.

4. Obligation of due diligence

4.1. **The User is obliged to look after the Identifiers with particular care and attention and ensure that they are stored in a manner that is absolutely secure and confidential and are protected against any abuse. Identifiers may not be sent, disclosed, or otherwise made accessible in any way to third parties.** The personal password – and the user ID – must be kept secret, must not be recorded/noted down, and must not be stored electronically (or on any medium whatsoever). In addition, the personal passwords must not be readily identifiable (no telephone numbers, birthdays/dates of birth, car registration numbers or number sequences that can be easily guessed, etc.) and must meet the Bank's requirements in terms of integrity and complexity. The password chosen shall expire automatically in accordance with the rules set by the Bank and must therefore be renewed and replaced at regular intervals.

4.2. Furthermore, the Company and the User shall take all practicable security measures to protect their devices and workstations and, in particular, electronic data processing systems (IT systems and any data stored thereon) that are used to access the Portal, against tampering, abuse or hacking (for example by deploying the latest firewall and antivirus programs). It shall be specifically for the Company and the User to obtain detailed information concerning any security measures that need to be taken. **The Company undertakes to ensure that Users also adhere strictly to any such requirements and prohibitions and shall be fully liable for any and all consequences arising from any failure to comply with that duty to safeguard the Identifiers, as aforesaid, including by Users.**

4.3. It is not permitted to respond to e-mails that appear to be from the Bank and require Identifiers to be disclosed (for example by entering these into websites that can be opened or are accessible via a link). The Bank must be informed immediately of any such attempts. If there is reason to believe – or should any suspicion arise – that any third party has become aware of the Identifiers, and in particular the personal password, the User must **change it immediately.**

4.4. The Bank reserves the right to add and implement additional authentication methods (for instance, two or three level authentication systems), thus requiring Users to provide additional information such as, for example, a cell phone number for the purpose of sending an SMS or installing specific smartphone applications for the purpose of authentication using random one-time tokens.

4.5. Access to the Portal is provided through the public internet. Access to and the usage of a public network (internet) fall under the exclusive competence/responsibility of the Company and Users, who shall bear full responsibility and all risks, in particular for the consequences of any third-party interception of data (including tampering and hacking). The Bank shall not procure, arrange the provision of or warrant to the User any connection to the Portal over a public network or through any internet provider. The Bank shall provide a website of its own for accessing the Portal and related services over a public network, the address of which shall be communicated separately to the Company.

4.6. On setting up the connection for the first time, the User must change the password provided by the Bank. The Bank shall be entitled to change the Identifiers at any time without notice, if such action is deemed to be necessary, for example due to security reasons. In such circumstances, the Bank shall promptly issue new Identifiers to the User. If there are grounds to suspect that such Identifiers have become known to any unauthorized third parties, the Company and the Users shall notify the Bank immediately so that the codes can be replaced. This obligation shall apply in particular in the following circumstances:

- Access to the services available on the Portal is blocked;
- There is reason to suspect that the Identifiers have been misused by unauthorized third parties;
- Loss or theft of any or all of the Identifiers.

5. Risks and liability

5.1. There are **inherent risks** in using the Portal, such as, inter alia, the potential for information displayed on the Portal to be used for other purposes, also in relation to other services offered through the portal. The main risks involved are the following: (1) **disclosure of the banking relationship and client information to third parties, which means that bank-client confidentiality can no longer be ensured;** (2) changes to and falsification of information (for example impersonation or the provision of false information); (3) system failure/faults and other communication difficulties/disruptions that may cause delays, falsification, deficiencies, misrouting or the deletion of information; (4) misuse/improper use resulting in loss or damage due to the interception of information by third parties.

5.2. **Under the terms agreed with respect to authentication (compare clause 3), the User and/or the Company shall bear all risks associated with: (i) interference/tampering with their own IT systems – and/or their own workstations – by unauthorized persons; (ii) any use/misuse, unlawful use or irregular use of personal Identifiers and/or the Portal; (iii) the failure to exercise proper due diligence; or (iv) the interception by any unauthorized third party of data transmitted (including any related interference problems).**

5.3. The Company and the User are aware of the risks associated with sharing information and data across public and private networks, including in particular the risk that the banking relationship, or respectively the contractual relationship with the Bank and information relating to the client of the Bank may be disclosed to third parties. Notwithstanding that the data to be transmitted (with the

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

exception of sender and recipient information) are automatically encoded/encrypted on accessing the Portal, it is not possible to exclude the possibility of targeted interference/tampering with and/or breaches of (including the hacking of) the User's IT system by unauthorized persons. **The risks of such incidents occurring shall be deemed to fall within the influence (and/or under the control) of the Company and/or the User, and shall thus be borne by the Company. As a general rule, the Company and the User shall bear all risks associated with the transmission of data over public or private networks.** Until such time as any blocking of access takes effect (see clause 6), the Company shall bear the risks associated with the use of personal Identifiers.

5.4. Unless otherwise required under applicable law, **the Bank expressly declines all liability for any losses – whether direct, indirect and/or consequential – or consequences of any type whatsoever arising for the Company or respectively for Users and/or third parties (including cardholders, ècash clients and/or the recipients of other products of the Bank) as a result of access to and/or usage – including misuse – of the Portal.**

5.5. While the Bank has used all reasonable endeavors to ensure that the Portal is secure by taking such measures as are required and by deploying generally recognized technical and security standards, it is not possible to guarantee absolute security.
The Company and the User acknowledge in particular that:
- the workstations and IT systems of the Company and/or any designated User are not under the Bank's control and may be subject to external attacks;
- there is the potential risk that unauthorized persons may steal or intercept, and subsequently misuse, the Identifiers or other data of the Company and/or the User, including data pertaining to the contractual relationship with the Bank;
- information is sent over a public network and, although it is sent in the form of encrypted packets, it cannot be ruled out that information may pass through communication lines and nodes across national borders, even if the sender and recipient are resident in Switzerland;
- public network operators may be able to identify the Company and/or the User and any counterparties with whom the Company or User may be in contact through the internet;
- compliance with bank-client confidentiality requirements cannot be guaranteed under any circumstances, either with respect to the Portal or public networks.

5.6. **In particular, the Bank will not accept any responsibility and declines all liability for any loss suffered by the Company, by Users and/or by cardholders, ècash clients and/or the recipients of other products of the Bank or third parties due to transmission errors, technical defects, system overload, disruption, faults, breakdowns, tampering or interception, unlawful interference with telecommunications equipment, the blocking of telecommunications systems or networks, or as a result of other deficiencies attributable to system or network operators, while the Portal is being used or transactions are being processed, or in general any loss or damage that may arise for the Company, Users, cardholders, ècash clients and/or the recipients of other products of the Bank or for third parties as a result of the release onto a public network of data concerning the contractual relationship with the Bank.**

5.7. Without prejudice to the limits imposed under overriding legal provisions, the Company shall indemnify and hold harmless the Bank in respect of any damage or loss that may arise for it as a result of the use and/or abuse of the Portal, including by third parties, within the ambit of contractual relations with the Bank, including in the event that no fault can be imputed to the Company and/or to Users (for example in situations involving hacking notwithstanding the adherence by the Company and Users to all necessary security measures).

6. Bar on access

6.1. The Administrator may block access authorizations for Users at any time.

6.2. The Company may request the Bank to block access authorizations for the Administrator or other Users at any time.

6.3. The Bank may block access to the Portal for Users at any time.

6.4. Any User may request the Bank to block their access authorization. The Bank reserves the right not to comply with such request until it has consulted the Administrator.

7. Information on ATMs, terminals, computer screens or other IT systems

7.1. While the Bank has made all reasonable efforts and taken appropriate action to ensure the reliability, accuracy and integrity of information and notices provided on the Portal, any data and documents supplied are intended for information purposes only.

7.2. The provision of such data and documents shall not imply any obligation or liability for the Bank and may not be used by the Company, Users or third parties (including clients) to institute claims against the Bank.

7.3. Information and notices displayed shall be provisional and non-binding unless specific information is expressly stated to be binding in relation to a particular service. Similarly, such information shall not be construed as a recommendation, offer or incentive/solicitation to execute any transactions or conclude any legal transaction unless they are expressly stated as such.

8. Electronic agreements, legal disclaimers displayed electronically

8.1. The use of certain services provided through the Portal may be conditional upon the acceptance of supplementary terms agreed upon separately. The Bank may display such terms electronically to the User once the User has been authenticated through the Portal. The same procedure shall also apply to any adaptations, amendments, or supplements to these GTC.

8.2. The services shall be activated once the User has successfully requested them, where necessary, and has accepted electronically any supplementary special terms and conditions, whereupon the terms and conditions shall become binding on the Company and the User.

8.3. Agreements concluded electronically shall be deemed to be equivalent to agreements bearing a handwritten signature. The relevant terms and conditions may be printed out and viewed on the Portal. The Bank may change the range of services available at any time. Due to the globalization of markets and the continuing expansion of electronic services, the Bank is required to display additional legal notices in respect of information and services published and available electronically. Such notices shall become binding on the User as soon as they are displayed. Any User who is unwilling to acknowledge and accept their validity must also refrain from accessing and using the respective services and information.

9. Country-specific (legal) restrictions, foreign import and export restrictions

9.1. The Company confirms that it is aware of and has informed Users that in accessing and using the Portal (and related services) outside Switzerland they may, in certain circumstances, be in breach of foreign laws and regulations. Accordingly, the Company shall: (i) obtain information concerning the existence, content and scope of any legislation, regulations and in general any legal rules governing the use of banking services that may apply in any foreign countries from which it may access the Portal (and related services); (ii) only use the Portal (and related services) insofar as such use is consistent with the aforementioned local provisions and regulations and, in particular, scrupulously comply with any bans and/or restrictions on the use of banking services; (iii) also oblige Users to comply with the aforementioned requirements and ensure that they are complied with. The Company further undertakes to ensure that Users comply with the above requirements.

9.2. The Company shall release the Bank from all liability in respect of the foregoing and accepts – irrevocably and without exception – full responsibility in respect of any consequence, penalty or breach that may arise as a consequence of usage of the Portal (and related services) outside Swiss territory.

9.3. The Company and the User also agree to indemnify the Bank in full in respect of any direct, indirect and/or consequential damage, loss, expense, or consequence that may arise due to any failure to comply with the above and in general these Terms and Conditions for Using the Portal and Related Services (GTC).

9.4. **The Bank shall be entitled to adjust or restrict the range of services offered/available at any time without notice.** The Bank shall not be responsible for and shall not incur any liability in respect of any loss – whether direct, indirect and/or consequential – that may be suffered by the Company and/or any User due to any block on, suspension of, adjustment to or interruption of access to any Portal service or services, or to the Portal as a whole. It shall be for the User to obtain information on, knowing and complying with any relevant restrictions and legislation/rules. The Bank accepts no liability in respect of such compliance.

10. Transmission errors, technical interference/faults, outages, and unlawful interference

The Bank accepts no liability for any loss or damage caused by transmission errors, defective lines, defects/faults and technical disruptions or outages and/or any unlawful interference in the IT systems of Users or third parties (including systems and networks that can be accessed by anyone), unless the Bank failed to exercise the customary standard of care. Insofar as the Bank has exercised the customary standard of care, it provides no warranty that access to its services will be continuous, unlimited, error-free and/or uninterrupted. The Bank likewise accepts no liability for any loss or damage due to faults, malfunctions, outages (including systems maintenance) or overloading of the Bank's ATMs or IT systems.

11. Prices

11.1. The prices charged for use of the Portal, the provision of related services, and the issue of Identifiers (including replacements and any additional Identifiers ordered) as well as the related hardware are set out in a separate price list.

11.2 Any adjustments to prices shall be notified by suitable means. The prices stipulated shall be charged to the Company immediately, monthly, quarterly, or annually, at the option of the Bank.

12. Bank-client confidentiality/data protection, marketing

12.1. Swiss law (for example governing bank-client confidentiality and data protection) applies solely within Swiss territory. As a result, any data transferred outside Switzerland will no longer be protected under Swiss law.

12.2. The Bank or any third parties appointed by it shall be authorized to store, process, and use any information and data obtained from the Company and/or the User in connection with usage of the Portal. More specifically, the Bank or any third parties appointed by it may assess and analyze the aforementioned

data, use them for marketing purposes to create client profiles, and process them for market research purposes. This will enable the Bank to offer individual and personalized advisory services to its clients and to provide customized offers and information concerning the Bank's products and services. The following data will typically be processed: data relating to the Company and Users as well as data relating to card transactions, consumer credit/private loan contracts (ècash) and additional services/products.

12.3. The Company and/or the User may at any time opt out of receiving offers and information concerning the Bank's products and services by submitting a written opt-out request to the Bank. Any agents of the Bank and their employees are required to comply with Swiss data protection legislation.

13. Technical prerequisites for access to the Portal

The Portal is only available if the devices and related software (operating systems, browsers, applications) used by the Company/the User are compatible with the technical prerequisites specified from time to time or made available by the Bank through its own communication channels. It shall be exclusively for the Company/the User, acting at its own cost, to obtain devices and to install software, including any updates to it, in order to ensure adherence to the applicable technical requirements at all times. The Bank reserves the right to alter the technical prerequisites and compatibility requirements at any time, subject to appropriate advance notice, and the Company and the User shall be responsible for implementing any updates and upgrades necessary in order to comply with any such new prerequisites.

14. Intellectual property rights

The Bank hereby grants the User (and the Company) a non-transferable, non-assignable, non-exclusive, personal license free of charge to use the Portal and in particular the applications and functionalities owned by the Bank or that the Bank has been authorized to grant by the holder of the respective intellectual property rights. This license is granted solely for the usage of the respective services available to the User (and to the Company) in accordance with the limits set forth in these GTC. Without prejudice to the rights granted under license to the User (and to the Company) under the terms of these GTC and the rights of any third-party licensors, the Bank reserves all rights in relation to the Portal, and in particular to the Bank's applications, functionalities and websites used in order to provide the respective services. The User and the Company acknowledge that any software necessary in order to access the Portal other than that made available by the Bank under the terms of the license provided for in the previous paragraph, including in particular operating systems or browsers, is the property of the respective third-party providers and that the usage thereof is governed by the contractual provisions adopted by those third-party providers. The User and the Company acknowledge that the Bank is not a party to the license for any such software of third-party providers and undertake to comply with the terms of use and the terms of license applied by such third-party providers and to pay any license fees directly to the third-party provider. The User and the Company acknowledge and accept that, depending upon the means of communication used, any data transmitted from and received on their devices will be subject to the data and text charges applied by their provider of mobile, landline or wi-fi services. The User/Company shall be exclusively responsible for the payment of any such charges and any other charge that may arise during usage of the device and its connection to the internet.

15. Availability of the Portal and related services/functionalities

The Portal and related services shall as a general rule remain available throughout the entire day, including on public holidays. However, the Bank is unable to guarantee unlimited access to the Portal or that the related services can be used without interruption. The Bank moreover reserves the right at any time to limit, block, suspend, alter and/or cancel either entirely or in part the provision of the services/functionalities and applications provided through the Portal with immediate effect, including without prior notice, in particular due to legal or security reasons, for the purpose of regular or occasional technical updates or maintenance and otherwise whenever necessary at its absolute discretion, under all circumstances without any fear of adverse consequences from the Company, Users or third parties (including cardholders, ècash clients and/or recipients of other products of the Bank).

16. Amendments

The Bank reserves the right at any time to amend these GTC, any supplementary agreements or any special terms and conditions applicable to individual services. Notice of such amendments shall be given in writing, electronically on the computer screen (compare clause 8) and/or by circular letter and/or by any other appropriate means and shall be deemed under all circumstances to have been approved unless objected to in writing within 30 (thirty) days of notification, although in all instances at the time when the Identifiers are first entered/used after notification.

17. Termination

17.1. Either the Company or the Bank may, at any time, terminate use of the Portal in respect of any or all of the Users.

17.2. In addition, any User may request at any time that their personal status as a User of the Portal be terminated.

17.3. Notwithstanding termination, the Bank shall be entitled to execute and conclude in a legally binding manner for the Company all orders initiated before notice of termination was given.

17.4. The Bank shall be entitled, at any time, to terminate individual services provided through the Portal with immediate effect without notifying the Company or the User.

18. Further provisions

These Terms and Conditions for Using the Portal and Related Services (GTC) shall supplement and complete the other applicable terms governing the relationship between the Company (and/or the User) and the Bank.

19. Applicable law and place of jurisdiction

19.1. These Terms and Conditions for Using the Portal and Related Services shall be governed by Swiss law.

19.2. **Exclusive jurisdiction over any judicial proceedings relating to any dispute that may arise between the parties with respect to the conclusion, implementation and interpretation of the provisions hereof shall lie in Lugano. However, the Bank reserves the right to launch legal action before the courts at the domicile of the User or respectively the registered office of the Company or before any other competent court. The foregoing is without prejudice to any mandatory places of jurisdiction prescribed under Swiss law.**

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

cornèrcard

Terms & Conditions Virtual Corporate Solution.

General Terms and Conditions governing the use of Virtual Card Numbers ("VCN") generated via the Virtual Corporate Solution and Virtual Corporate Solution Plus (such system hereinafter referred to as "VCS").
These General Terms and Conditions (hereinafter the "Terms and Conditions") set out the legal relationship between Cornèr Bank Ltd. (the "Bank") and the company applying for administrator rights (the "Company") and/or the individuals authorized to use the VCS via portal (VCS-Portal), mobile app, API or integration with third parties, (hereinafter the "Administrator" or "User(s)") with regard to the use of VCN and VCS.
Condition precedent allowing the Company's access to the VCS is the execution of a binding framework agreement for the issuance of Cornèrcard Business Cards and the valid request for a funding product.

1. General provisions concerning the Portal's access; use of VCN;

1.1. Upon request, the Bank shall grant the Company access to the VCS for the generation of VCN provided the Company guarantees that it will meet its financial obligations resulting therefrom in a timely manner as agreed herein and on the individual monthly statement.

1.2. The Company/User will receive access to the VCS-Portal, Mobile App access to API or grant access to third parties, for the generation of VCN issued in the name of the Company, together with credentials and related information. The portal shall be used exclusively by persons explicitly authorized by the Company.

1.3. The Company receives from the Bank a monthly invoice listing all charges. The invoice is due and payable upon receipt. If the invoice is not paid within 25 days from the date of invoice, the Bank will, as of the accounting date, charge an annual rate of interest on all transactions in accordance with the "Charges, Interest Rates, and Fees" table until all outstanding amounts have been settled. If payments are made to the Bank by direct debit (LSV), the Bank may disclose any information regarding the Company, the VCS, and total amounts of expenditure, which may be required by the applicable correspondent bank. In addition, the Bank reserves the right to charge for costs and expenses charged by third parties in connection with the VCN.

1.4. The **Company shall exercise utmost care in safeguarding the Portal's access data and the VCN numbers** created via the Portal as provided for in further detail in sections 2 ss. here below. **If a VCN number or User's Credentials are lost, stolen, or used without authorization within the Company, the Bank is to be notified immediately in writing by the Company so that it can block VCN and User credentials.** The Bank reserves the right to require the Company to file a police report. Until such notice has been received by the Bank, the Company is liable for all unpaid invoices, transactions, and charges resulting from the use of the portal and the generated VCNs.

1.5. The Company may make use of the VCS Portal only to the extent that its financial situation is sufficiently sound to promptly pay all future monthly invoices. **The Bank reserves the right to block the Portal at its discretion and at any time** without the need to justify its decision. The Bank will not be held liable for any losses or damage suffered by the company as a result of such action. Each unauthorized use of an expired or blocked VCN is unlawful and may result in criminal prosecution.

1.6. The services provided via the Portal can be terminated at any time in writing by the Company or the Bank. Any charges posted to the VCN subsequent to such termination are to be paid immediately by the Company upon receipt of the next invoice in accordance with section 1.4 above.

1.7. The Company accepts that incentive program information with regard to transactions processed via VCN will be forwarded to the respective partner (such as the airline company). The **Company authorizes the Bank to collect** from government agencies and designated bank or financial **institutions any information deemed necessary by the Bank in connection with a VCS Portal application** request or the use of VCN.

1.8. VCN use for purposes that are unlawful or in breach of the present terms and conditions is prohibited. No transactions are permitted in countries in which there are relevant national and/or international sanctions and embargoes against card use. The current list of relevant sanction measures (e.g. regarding countries, persons, companies, transaction types affected) can be viewed, e.g. in relation to Switzerland, on the website of the State Secretariat for Economic Affairs (SECO) (www.seco.admin.ch).

2. Authorization of Administrator and User to use VCS Portal

2.1. The Company authorizes the Administrator to activate other Users for the purpose of using the Portal.

2.2. The Company has overall responsibility for ensuring that all Users fully comply with these Terms and Conditions. Accordingly, the Company shall supply to each individual User detailed information on the Portal, the relevant functions, and the obligation of due diligence incumbent upon the User (see clauses 4 and 5 below).

2.3. Any authorizations conferred will not be invalidated automatically (for example due to death, incapacity to act, removal of signatory powers, deletion from a register, or termination of employment with the Company), but must be specifically blocked or canceled (see clause 6 below).

3. Personal identifiers

3.1. At the request of the Company, the Bank shall supply to Users their personal contract number and the applicable means of authentication, such as username and password (hereinafter referred to as the "Identifiers"). On logging in for the first time, Users must replace the password assigned by the Bank with their own personal password.

3.2. Users will gain access to the Portal and related services once they have been authenticated to the satisfaction of the Bank by means of the Identifiers.

3.3. The Bank may, at its discretion, change or replace the Identifiers at any time.

4. Authentication

4.1. Any person who has been authenticated by entering Identifiers that are valid at the time of use, in accordance with Portal guidelines (self-authentication), **are deemed by the Bank to be authorized to access the Portal and use the relevant services.** The foregoing applies irrespective of whether the person concerned is an actual User or has been authorized by the Company for such purpose. The Bank is deemed to have been appointed and authorized by the Company to execute orders received through the Portal, once the underlying authentication process has been properly completed.

4.2. Accordingly, the Bank is expressly released from any further obligation to verify whether an individual is in fact authorized to use the **Portal, irrespective of the relationship between the Bank and the User inter se, and the Bank is entitled to disregard any contrary provisions set forth in forms issued by the Bank, including, in particular, forms stipulating the signatory owers applying to the contractual relationship with the Bank** (in particular power of attorney forms and/or forms that establish the signature powers applicable to the contractual relationship with the Bank (including, for example, card contracts, consumer/private credit agreements).

4.3. Notwithstanding the foregoing, the Bank is entitled to deny access to the Portal at any time, without giving any reasons, and to require Users to verify their identity by other means.

4.4. Any transaction, operation or activity performed under the contractual relationship with the Bank (including card contracts) on the basis of prior authentication will be imputed to the Company, which duly and unconditionally agrees to any such transaction or act with binding legal effect.

5. Obligation of due diligence

5.1. The User shall take special care to ensure that the Identifiers are kept safely. Identifiers may not be sent, disclosed, or otherwise made accessible to other persons. Personal passwords must be kept confidential and may not be noted down, stored electronically, or readily identifiable (no telephone numbers, dates of birth, car registration numbers, or number sequences that can be easily guessed, etc.) and must meet the Bank's requirements in terms of integrity and complexity. The password selected will expire automatically in accordance with the rules defined by the Bank and must therefore be renewed and replaced at regular intervals.

5.2. Furthermore, Users shall take all practicable security measures to protect their workstation and, in particular, electronic data processing system (computer system and any data stored thereon), which are used to access the Portal, against unauthorized access, unauthorized use, and tampering or hacking (for example by deploying the latest firewall and antivirus programs). **The Company and the User shall obtain detailed information on any security measures required to be taken. The Company is responsible for ensuring that all Users strictly adhere to such requirements and prohibitions and is fully liable for any and all consequences arising from failure to comply with the**

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

requirement to safeguard the Identifiers, as aforesaid, including any noncompliance on the part of Users.

5.3. It is not permitted to respond to e-mails that appear to be from the Bank and require Identifiers to be disclosed (for example by entering these on websites accessible via a link). The Bank must be informed immediately. Users must change their personal password immediately if there are grounds for suspecting that this has become known to another person.

5.4. The Bank reserves the right to define additional authentication methods (two or three level authentication systems). Accordingly, Users may be required to provide additional information to the Bank, for example a cell phone number for the purpose of sending text messages (SMS) or installing specific smartphone applications to authenticate Users using random one-time tokens.

5.5. Access to the Portal is provided through the public Internet. **Access to and use of the public Internet are the sole responsibility of the Company and the Users, and the Company and the Users shall assume all liability and risk in respect thereof, including in respect of any consequences arising from tampering and hacking by third parties where applicable.** The Bank cannot guarantee a connection, and is not responsible for providing a connection; neither can the Bank guarantee that Users will be able to connect to the Portal through the public Internet or any Internet service provider. The Bank shall provide its own website for the purpose of accessing the Portal and related services from the public Internet and the address of the website will be notified to the client separately.

5.6. On setting up the connection for the first time, Users will be required to change the password supplied by the Bank. The Bank is entitled to change the Identifiers at any time without notice, if such action is deemed to be necessary, for example for security reasons. In such circumstances, the Bank shall issue new Identifiers to the User without delay. Where there are grounds for suspecting that such Identifiers have become known to unauthorized third parties, the Company and the Users shall notify the Bank immediately to allow the codes to be replaced. The foregoing obligation specifically applies in the following circumstances:

- Access to the services available on the Portal is barred.
- There is reason to suspect that the Identifiers have been misused by unauthorized third parties.
- Loss or theft of any or all of the Identifiers.

6. Risks and liability

6.1. There are inherent risks in using the Portal, such as the potential for information displayed on the Portal to be used for other purposes. The main risks involved are the following: (1) **Disclosure of the banking relationship and client information to third parties, which means that bank-client confidentiality can no longer be ensured;** (2) Changes to and falsification of information (for example impersonation and the provision of false information); (3) System failure and other communication disruptions which may cause delays, falsification, misrouting, or deletion of information; (4) Misuse resulting in loss or damage due to information being intercepted by third parties.

6.2. Under the terms agreed with respect to authentication (compare clause 3), the User and/or the Company shall assume the risks associated with (i) tampering with computer systems by unauthorized parties, (ii) misuse of personal Identifiers, (iii) failure to exercise proper due diligence, or (iv) interference incidents during data transmission caused by unauthorized third parties.

6.3. The Company and the User are also aware of the risks associated with sharing information and data across public and private networks, including the risk that the banking relationship and client information may be disclosed to third parties. Deliberate tampering or hacking into the User's computer system by unauthorized parties cannot be ruled out, even if the data transmitted (with the exception of sender and recipient information) are automatically encrypted on accessing the Portal. **The risks of such incidents occurring are deemed to be under the control of the Company and/or the User, and are to be borne by the Company.** Until such time as any bar on access takes effect (see clause 6 below), the Company shall bear the risks associated with the use of personal Identifiers.

6.4. The Bank expressly excludes all liability for any loss or damage, including direct, indirect and/or consequential loss, or any consequences whatsoever, which may be suffered by the Company and/or the User, any cardholder, and/or third party as a result of accessing and/or using the Portal, including, but not limited to, unauthorized access or improper use of the Portal and/or the VCN by directors, officers, employees, agents, professional advisers, suppliers, contractors or sub-contractors of the Company.

6.5. While the Bank has used all reasonable endeavors to ensure that the Portal is secure by taking such measures as are required and generally recognized and by deploying appropriate technical and security standards, total security cannot be guaranteed. The Company and the User are aware, in particular, that:

- the workstations and computer systems of the Company and/or any designated User are not under the Bank's control and may be subject to external attacks;
- there is the potential risk that unauthorized parties steal or intercept, and subsequently misuse, the Identifiers or other data of the Company and/or the User;
- information is sent over a public network and, although it is sent in the form of encrypted packets, it cannot be ruled out that information may pass through communication lines and nodes across national borders, notwithstanding that the sender and recipient are resident in Switzerland;
- public network operators may be able to identify the Company, the User, and any counterparties with whom the Company or User may be in contact through the Internet;
- **compliance with bank-client confidentiality requirements cannot be guaranteed under any circumstances, either with respect to the Portal or public networks.**

6.6. In particular, the Bank assumes no responsibility and accepts no liability for any loss or damage whatsoever that may be suffered by the Company, any designated User, and/or cardholder, (i) due to transmission errors, technical faults, system overload, disruption, damage, breakdowns, tampering or interception, (ii) due to unlawful interference with or hacking into telecommunications equipment or the blocking of telecommunications systems or networks, (iii) or due to other faults caused by system or network operators, while the Portal is being used. Neither is the Bank liable in general for any loss or damage that may be caused to the Company, Users, the cardholder, or third parties as a result of supplying data pertaining to the banking relationship over public networks.

7. Bar on access

7.1. The Administrator may block access authorizations for other Users at any time.

7.2. The Company may submit a request to the Bank to block access authorizations for the Administrator or other Users at any time.

7.3. The Bank may bar Users from accessing the Portal at any time (e.g. if there is a risk that VCN-transactions violate Swiss or international embargo provisions or sanction measures or expose the Bank to other legal, regulatory or economic risks or jeopardise its reputation).

7.4. All Users may submit a request to the Bank for their access authorizations to be blocked. The Bank reserves the right not to comply with such request until it has consulted the Administrator.

7.5. The Bank declines all liability for consequences that might arise for the Company as a result of blocking of the VCS or blocking and recalling the VCN. The use of a blocked VCN is unlawful and may result in prosecution, as may the obligations incurred by the Company as a result. The Bank reserves the right to provide the affiliated merchants or authorized banks with any information they may require to obtain payment of the amount due directly from the Cardholder or the Company. The Bank is not obliged to execute VCN transactions if they violate applicable law, legal or regulatory (including foreign) provisions, restrictions, orders, prohibitions or measures of competent authorities (e.g. embargo provisions, national or international sanction provisions or money laundering provisions).

8. Information on ATMs, terminals, computer screens or other IT systems

8.1. While the Bank has used all reasonable endeavors and taken all reasonable steps to ensure the reliability, accuracy, and integrity of information and notices provided on the Portal, any data and documents supplied are intended for information purposes only.

8.2. The provision of such data and documents are not to be construed as implying any obligation or liability on the part of the Bank and may not be used by the client, designated Users, the cardholder, or third parties to institute claims, of whatever nature, against the Bank.

8.3. Information and notices displayed are deemed to be nonbinding and of a temporary nature only, unless specific information is expressly stated to be binding in relation to a particular service. Neither is such information to be construed as constituting a recommendation, offer, or solicitation to carry out transactions or enter into any legal transaction unless expressly stated as such.

9. Electronic agreements, electronic legal disclaimers

9.1. The use of certain services provided through the Portal may be conditional upon agreeing to separate terms. The Bank may display such terms to the User in electronic form once the User has been authenticated through the Portal. The foregoing also applies to any variations or amendments to these Terms and Conditions.

9.2. The services will be activated once the User has successfully applied for the same, where necessary, and has agreed, electronically, to any additional special terms and conditions, whereupon the terms and conditions will become binding upon the User and the Company.

9.3. Agreements concluded electronically are deemed equivalent to agreements bearing a handwritten signature. The relevant terms and conditions may be printed out and viewed on the Portal. The Bank may change the range of services available at any time. Due to the globalization of markets and the continuing expansion of online services, the Bank is required to display additional legal notices in respect of information published and services available online. Such notices will become binding upon the User as soon as they are displayed. Users who are unwilling to acknowledge and accept such notices must also refrain from accessing the information/using the services.

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

10. Country-specific restrictions, foreign import and export restrictions

10.1. The Company confirms that it is aware of and has informed Users that in accessing and using the Portal and/or related services outside Switzerland they may, in certain circumstances, be in breach of foreign laws and regulations. Accordingly, the Company shall (i) obtain information on the existence, contents, and scope of any legislation, regulations, and rules, in general, governing the use of banking services, which may apply in foreign countries from which it may access the Portal and related services; (ii) only use the Portal and related services insofar as such use is consistent with the aforementioned local provisions and regulations and, in particular, scrupulously comply with any bans and/or restrictions on the use of banking services; (iii) ensure that Users also comply with the aforementioned obligations.

10.2. The Company exempts the Bank from all liability in respect of the foregoing and accepts, irrevocably and without exception, full responsibility and liability in respect of any consequences, penalties, or breaches, that may arise as a consequence of using the Portal and related service outside Swiss territory.

10.3. The Company and the User also agree to indemnify the Bank from and against any direct or indirect loss or damage and/or consequential loss, charges, costs, and consequences, which may arise due to any breach of the aforementioned provisions or any other provisions of these Terms and Conditions governing use of the Portal or related services.

10.4. The Bank is entitled to adjust or restrict the range of services available at any time without notice. The Bank is not responsible for and is not liable in respect of any direct or indirect loss or damage or any consequential loss, which may be suffered by the Company or any User due to any bar on, suspension of, adjustment to, or interruption of access to any service or services, or to the Portal as a whole. The User is responsible for obtaining information on and complying with any relevant restrictions and legislation. The Bank accepts no liability in respect of such compliance

11. Transmission errors, technical faults, outages, and unlawful interference

The Bank accepts no liability for any loss or damage caused by transmission errors, misrouting, technical faults and disruptions, outages, or unlawful interference in the computer systems of Users or third parties (including systems and networks that can be accessed by anyone), unless the Bank failed to exercise the standard of care customary in the industry. Insofar as the Bank has exercised the standard of care customary in the industry, the Bank makes no warranty that access to the services will be continuous, uninterrupted, or error-free. Neither is the Bank liable for any loss or damage due to malfunctions, outages (including systems maintenance), or overloading of the Bank's IT systems or ATMs.

12. Prices and charges

12.1. The prices charged for use of the Portal, the supply of related services, and the provision of Identifiers (including replacements and any additional Identifiers ordered) are set out in a separate price list included in the application form.

12.2. Any adjustments to prices will be notified by suitable means. The prices stipulated will be charged to the Company immediately, monthly, quarterly, or on an annual basis at the option of the Bank.

13. Compliance with Statutory Requirements/Exchange of Information

The Company acknowledges and agrees that for the purposes of its business relationship with the Bank, it will be solely responsible for complying with all statutory and regulatory requirements, including but not limited to any requirements pertaining to tax, which may apply to the Company pursuant to the law of the jurisdiction in which it is domiciled, or in general, pursuant to the laws of all jurisdictions in which it is required to pay tax in respect of any credit balance available on the VCN. The Bank will have no liability whatsoever in respect of such compliance. The Company shall consult an expert adviser if it is in any doubt as to its compliance with these requirements. The Company is aware that the Bank may be required under agreements between Switzerland and other countries and as a result of individual or group requests pursuant to such agreements, or on the basis of internationally recognized standards, for example standards applying to the automatic exchange of information, to disclose information regarding VCN to the relevant Swiss or foreign tax authorities. The Company also acknowledges that, in addition to the aforementioned automatic exchange of information, the Bank is required to comply with its legal, regulatory or supervisory information and communication obligations and/or to respond to requests for information from Swiss or foreign authorities. In this context, requests for information from foreign authorities generally take the form of international mutual legal assistance. In exceptional cases, however, foreign authorities may request information and documents directly from the Bank (e.g. current US legislation provides that under certain conditions the competent criminal authorities may request directly a foreign bank that holds an account with a correspondent bank in the USA to issue information and documents relating to any of the foreign bank's accounts and/or clients, even if such documents are held outside the USA and the account or client in question has no direct connection with the foreign bank's activity in the USA). In particular, when operating in foreign markets, the Bank may be called upon to respond directly to requests from foreign supervisory authorities involving the disclosure of customer data. The Company acknowledges and accepts that the Bank may be required to provide personal data, information and documents to Swiss and foreign authorities and to this extent release the Bank, its organs and employees from their/their obligation of secrecy and waives banking secrecy.

14. Bank-client confidentiality/data protection, marketing

14.1. Swiss law (for example governing bank-client confidentiality and data protection) solely applies within Swiss territory. As a result, any data transferred outside Switzerland will no longer be protected under Swiss law.

14.2. The Bank is entitled to commission partner companies in Switzerland or abroad, in particular affiliated companies of Cornèr Bank Group with seat in the European Union to perform all or part of the services pertaining to the VCS (e.g. Portal application reviews, VCN issuance, contract management, online services, payment collections, client communications, credit risk calculations, fraud prevention, charge-back procedures, payment processing, IT) and for the improvement of the risk models used in granting credit limits and fraud prevention. The Company authorises the Bank to provide these third parties with the data necessary for the diligent performance of the tasks assigned to them and, if required, to transmit this data abroad for this purpose. In doing so, the Bank may also pass on personal data of the Company to such partner companies for the processing purposes specified in the Privacy Notice (clause 3 – cornercard.ch/dataprotection). The processing of such personal data is carried out in full compliance with the applicable data protection regulations, namely the Swiss Data Protection Act (DPA) and the European General Data Protection Regulation (GDPR). Accordingly, the Bank or third parties appointed by the Bank may store, process, and use Company, User and/or Administrator data including transaction data, in particular for the purposes of marketing, market research, and creating client profiles. The storage, processing, and use of Company data will allow personalized advice, customized offers, and information on the Bank's products and services to be supplied to the Cardholder. The following data may be processed in particular: information on the Company, VCB-transactions, and any additional or ancillary services. The Company has read and understood these General Terms and Conditions and accepts them in full by using the Portal.

15. Amendments

The Bank reserves the right at any time to amend these Terms and Conditions, any additional agreements, or special terms and conditions applying to individual services. Notice of such amendments will be given in writing, electronically on the computer screen (compare clause 8), by circular letter, or by other means

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

and are deemed to have been approved unless an objection is raised in writing within 30 days of notification, but in any event upon the next occasion that the Identifiers are used.

16. Termination

16.1. Either the Company or the Bank may, at any time, terminate use of the Portal to take effect for any or all of the Users.

16.2. Notwithstanding termination, the Bank is entitled to process any orders initiated prior to the date on which termination takes effect, which is legally binding upon the Company.

16.3. The Bank is entitled, at any time, to terminate individual services provided through the Portal with immediate effect without notifying the Company or the User.

17. Further provisions

These Terms and Conditions governing use of the Portal and related services complement and supplement all other terms and conditions governing the relationship between the Company and/or User and the Bank.

18. Applicable law and place of jurisdiction

18.1. These Terms and Conditions governing use of the Portal and related services are governed by and construed in accordance with Swiss law.

18.2. Lugano is the exclusive place of jurisdiction for any disputes that may arise between the parties with respect to the agreement set forth in these Terms and Conditions or the implementation and interpretation of the provisions hereof. The Bank is, however, also entitled to take legal action against the client in the court having jurisdiction in the client's place of residence or in any other court of competent jurisdiction. The foregoing is without prejudice to any mandatory places of jurisdiction prescribed under Swiss law.

11.Signature

In signing this Contract, the Company and the Administrator declare that they have read, understood, and accepted in full the General Terms and Conditions for Using the Partner Collaboration Tool (PCT) Portal of Cornèr Bank Ltd., which are annexed to this Contract. The credentials shall be sent in writing to the Administrator by registered post and/or e-mail.

The Company further confirms that it has duly informed, or respectively that – before the Portal is used for the respective client – it will duly inform the cardholder and/or the applicant for consumer credit/a private loan (ècash) and/or any other products of Cornèr Bank Ltd. concerning the functions/functionalities available on the Portal through which the Administrator and other Users authorized by the Company can, for example, manage the life cycle of the payment card (request PIN, blocking/unblocking of card, etc.), or respectively enter, update and manage data relating to the consumer credit/private loan application, and view information relating to the cardholder and card usage (personal data, transactions, balance, spending limit, monthly statements, etc.), or respectively the applicant for consumer credit/a private loan (specifically, personal data, amount disbursed, documentation produced), etc.

Signature of the Administrator

Place/date _____ Surname _____

First name _____ Signature ✗ _____

Company signature

Place/date _____ Company stamp

Last name _____ Last name _____

First name _____ First name _____

Signature*1 ✗ _____ Signature*1 ✗ _____

*1 Authorized signatures as recorded in the Commercial Register (individual or joint signature).

Please complete, sign, and return the card application to:
Business Client Management, Cornèr Banca SA, Cornèrcard, Via Canova 16, 6901 Lugano.

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 91 800 41 41, cornercard.ch

GAS/ECR/ICR

nicht frankieren
ne pas affranchir
non affrancare
50416832
000002

B

pro clima

LA POSTA

Business Client Management
Cornèrcard
Via Canova 16
6901 Lugano_Switzerland