Migros Bank Terms of Use for one

A General section

1. General Terms of Use for one

1.1 Terms of Use for one and other relevant documents
These provisions apply to the digital services (hereinafter **«card services»**) provided by Migros Bank AG (hereinafter the **«Bank»**) to the person making the application and the cardholder (hereinafter collectively the **«person entitled to a card»**) of a primary or additional card or the Bank's business or corporate card (hereinafter the **«card(s)»**) under the name **«one»**. one is operated by Viseca Payment Services SA (hereinafter the **«processor»**) on behalf of the Bank. The Bank uses the processor to perform certain tasks related to the card business. Within this scope, the processor processes (bank client) data on behalf of the Bank.

one is available through:
- the one website (hereinafter the **«website»**) and
- the one app (hereinafter the **«app»**)

With regard to the use of one,– and depending on the selected card product – the **General Information on data protection at Migros Bank AG** (available at migrosbank.ch/grundlagen) and the **Information on data protection for the Migros Bank AG Cumulus credit card** (available at cumulus.migrosbank.ch/documents) must also be observed.

These Terms of Use for one apply in addition to the provisions governing the use of the Bank's cards, depending on the selected card product (General Terms and Conditions of Migros Bank AG, Terms and Conditions for the use of debit or credit cards for private individuals or Migros Bank AG Business Cards, or the Terms and Conditions for the use of the Cumulus credit card, hereinafter collectively referred to as Migros Bank Terms).

The use of one requires registration of the person entitled to a card. These Terms of Use for one are deemed to have been accepted as soon as the person entitled to a card registers via the one app or the one website, and confirms these Terms of Use directly or indirectly (by initiating or continuing the registration or application process).

The Bank reserves the right to amend these Terms of Use for one at any time. Changes will be communicated to the person entitled to a card in an appropriate manner (e.g. via one or by e-mail). If the person entitled to a card does not agree to the amended Terms of Use for one, the app or the website or individual card services may not or no longer be used.

1.2 What is one and how is it developed?
one includes digital onboarding for the Bank's new customers and card services of the Bank, which are provided by the processor on behalf of the Bank.

New card services introduced are made available to the registered person entitled to a card through updates. The Bank will inform the person entitled to a card in an appropriate manner (e.g. via one or by e-mail) about further developments and the related changes to these Terms of Use for one, if necessary.

1.3 What functions does one offer?
Depending on the selected card product, one may include the following functions in particular – now or in the future:

- Digital onboarding for new customers (cf. section 5);
- User account for managing personal data;
- Control and confirmation of payments e.g. using 3D Secure (Mastercard SecureCode or Verified by Visa) in the app or by entering an SMS code (cf. section 6.2);
- Control and confirmation of certain actions (e.g. logins, contacts with the Bank) in the app or by entering an SMS code;
- Activation of cards for the use of payment options (cf. section 7);
- Exchange of all kinds of notices and notifications between the person entitled to a card and the Bank (including, for example, notification of an amendment to provisions), unless a special form of notice or notification is reserved (e.g. written complaint regarding a monthly invoice);
- Overview of transactions or cards, and electronic display of invoices;
- Overview of the bonus programme account and option to redeem points (currently surprize account);
- Information in relation with the use of the card (currently SMS services).

1.4 Advantages of one
one offers the person entitled to a card various advantages:

- one makes access to the card services more secure: a modern process for authenticating the person entitled to a card makes it possible to control and confirm that actions have actually been taken by the person entitled to a card – by using the mobile phone as a second authentication factor (in addition to login) and through a secure communication channel between the person entitled to a card and the Bank;
- one combines the Bank's card services on a single platform, thus making it more manageable;
- one makes it easier to access to the Bank's various card services: login name and password enable registration and login for various card services;
- Online payments with 3D Secure are quicker: instead of entering the 3D Secure password, the payment can be controlled and confirmed with the app or by entering the SMS code.

2. Using one

2.1 User authorisation
The person entitled to a card is only permitted to use one under the following conditions:

- He/she has accepted the Terms of Use for one and is capable of implementing these and the associated requirements (in particular section 3.2.1 and 3.2.3) and
- he/she wishes to apply for a card as part of the digital application process or is entitled to use a card.

2.2 Consent for registration of one
By accepting these Terms of Use for one or by using one, the person entitled to a card hereby expressly grants the Bank the following consents (for the consents in the digital application process, cf. also section 5):

- Consent for processing data that were or will be collected when using one. This includes, in particular, the consent to their association with data already held by the Bank and the creation of profiles, each for purposes of the risk management and marketing purposes of the Bank or the processor and third parties in accordance with the data protection provisions in Section C.
- Consent for the receipt of messages and information on products and services offered by the Bank and third parties for marketing purposes (advertising). These may be sent by the Bank by e-mail or directly in the app or on the website.
- Consent for the use of the e-mail address provided at registration and the website and app for mutual electronic communication with the Bank (e.g. notification of address changes, notification of changes to the Terms (Migros Bank Terms) or notification in relation to combating card fraud)
- Consent to process and forward customer data to third parties, provided it is necessary to fulfil contractual obligations, official orders, and domestic or foreign legal or regulatory reporting and disclosure requirements, and to safeguard legitimate interests. In this context, the card authorized person releases the Bank from bank client confidentiality.

The person entitled to a card may revoke his/her consent to receive messages about products and services and/or to data processing for marketing purposes at any time, by giving written notice to the Bank with effect for the future (opt-out right). The corresponding contact details can be found in **General Information on data protection at Migros Bank AG.** (available at migrosbank.ch/grundlagen).

2.3 Refusal of consent within the scope of further developing one
If the person entitled to a card refuses to consent to the Terms of Use for one in the context of the further development of one (e.g. for updates), the app, the website or individual card services may not or no longer be used.

2.4 Impact of making confirmations
Every confirmation made via the app or by entering an SMS code is considered as action taken by the person entitled to a card. The person entitled to a card thereby makes a binding commitment (and can thus be held accountable) for purchases, transactions or for other business transacted, and for any resulting debits to his/her card. He/she authorises the Bank to execute corresponding orders and to take corresponding actions.

2.5 Availability / blocking / changes
The Bank may totally or partially interrupt, restrict or discontinue the possibility for using one, or replace it with another service, at any time and without giving prior notice. In particular, the Bank has the right to temporarily or permanently block the access of the person entitled to a card to one (e.g. in the event of suspected abuse or failure by the person entitled to a card to comply with due diligence obligations).

2.6 Intellectual property rights and license
All rights (in particular copyright and trademark rights) to software, texts, images, videos, names, logos and other data and information that are accessible via one or will become accessible over time, are the exclusive property of the Bank or the relevant partners and third parties (e.g. processor, Mastercard, Visa), unless otherwise provided for in these Terms of Use for one. The names and logos visible on one are protected trademarks.

To enable the person entitled to a card to use the app, the Bank grants the person entitled to a card a non-exclusive, non-transferable, indefinite, revocable and royalty-free licence to download the app, install it on a device in permanent possession of the person entitled to a card and use it within the scope of the intended functions.

The use of the processor's website is additionally subject to the **license provisions** (available at https://viseca.ch/de/app-pages/licensing-en) in accordance with the **terms of use** (available at https://viseca.ch/en/terms-of-use/viseca) of its website (under the heading «Ownership of the website, trademark rights and copyrights»).

3. Risks, disclaimer of warranty and general due diligence and reporting requirements

3.1 Risks arising in relation to the use of one
The person entitled to a card acknowledges and accepts that the use of one entails risks.

In particular, it is possible that by using one, cards, login name and password, devices used or personal data of the person entitled to a card, may be misused by unauthorised third parties. This can result in monetary losses for the person entitled to a card (by having his/her card charged) and infringement of his/her privacy (through misuse of personal data). There is also a risk that one or some of the card services offered on one cannot be used (e.g. login on one not possible).

Abuses are made possible or encouraged, in particular by:

- A breach of due diligence or reporting obligations by the person entitled to a card (e.g. through careless handling of login name/password or failure to report loss of card);
- The settings chosen by the person entitled to a card or poor maintenance of the devices and systems used for the use of one (e.g. PC, mobile phone, tablet and other EDP infrastructure), for example, due to a lack of screen lockout, a lack of or inadequate firewall and virus protection, or outdated software;
- Third-party intervention or errors in online data transmission (e.g. hacking, phishing or data loss);
- Faulty confirmations in the app or by entering an SMS code (e.g. inadequate or insufficient control of a confirmation request);
- Weaker security settings chosen by the person entitled to a card for one – especially for the app (e.g. storing the login).

The person entitled to a card can reduce the risk of abuse if he/she complies with the following due diligence and reporting requirements when handling the mobile devices and the password, as well as the duties to control the confirmation requests.
The Bank does not warrant or guarantee that the website and the app will be permanently accessible or will function without disruption, or that abuse can be detected and prevented with certainty.

3.2 General due diligence obligations of the person entitled to a card
3.2.1 General due diligence requirements in connection with the devices and systems used, in particular the mobile devices
one uses, among other things, the mobile devices of the person entitled to a card (e.g. mobile phones, tablet; hereinafter «mobile device») for authentication purposes. The safekeeping of these mobile devices at all times is therefore an essential security factor. The person entitled to a card must handle mobile devices with reasonable care and ensure that they are adequately protected.

The person entitled to a card is therefore required to comply in particular with the following general due diligence obligations in connection with the devices and systems used, in particular the mobile devices:

- A screen lock must be activated for mobile devices and further security measures must be taken to prevent unlocking by unauthorised persons;
- Mobile devices must be kept in a safe place where they are protected from third-party access and they must not be given to third parties for permanent or unsupervised use;
- Software (e.g. operating systems and internet browsers) must be updated regularly;
- Interventions in the operating systems (e.g. jailbreaking or rooting) are to be refrained from;
- Anti-virus and internet security programmes must be installed on the laptop/PC and kept up to date;
- The app may only be downloaded from the official stores (e.g. Apple Store and Google Play Store);
- Updates to the app must be installed immediately;
- If a mobile device is lost, everything possible must be done to prevent unauthorised persons from accessing the data transmitted by the Bank to the mobile device (e.g. by blocking the SIM card, locking the device, deleting the data, for example, via «Find

my iPhone» or «Android Device Manager», resetting the account or allowing the user account to be reset). The loss must be reported to the Bank (cf. section 3.3);
- The app must be deleted before the mobile device is sold or permanently transferred to a third party.

3.2.2 General due diligence requirements in connection with the one password
In addition to owning the mobile device, the login name and password serve as additional factors for the authentication of the person entitled to a card.

The person entitled to a card must comply, in particular, with the following general duties of care in connection with the password:

- The person entitled to a card must set a password that he/she has not already used for other services and that does not consist of easily ascertainable combinations (inadmissible would be e.g. phone number, date of birth, car registration number, names of the person entitled to a card or his/her close relatives, repeated or direct consecutive number or letter sequences, such as «123456» or «aabbcc»);
- The password must be kept confidential. It may not be disclosed or made accessible to third parties. The person entitled to a card acknowledges that the Bank will never ask the person entitled to a card to disclose the password;
- The password must not be written down or stored unsecured;
- The person entitled to a card must change the password or reset the user account or have it reset by the Bank if there is a suspicion that third parties have obtained access to the password or other data;
- The password may only be entered in such a way that it cannot be seen by third parties.

3.2.3 General due diligence requirements in connection with the confirmation requests, in particular control
Confirmations in the app or entering an SMS code obligate the person entitled to a card.

The person entitled to a card must therefore comply with the following general due diligence requirements in connection with confirmations in the app or by entering an SMS code:

- The person entitled to a card may only then confirm if the confirmation request is directly related to a specific action or transaction (e.g. payment, login, contact with the Bank) of the person entitled to a card;
- Before confirming, the person entitled to a card must check that the subject of the confirmation request is consistent with the transaction in question. In particular, the payment details displayed must be checked for confirmation requests in connection with 3D Secure.

3.3 General reporting requirements of the person entitled to a card
The following events must be reported immediately to the Bank:

- Loss of a mobile device (but not when mislaid only temporarily);
- Confirmation requests that are not related to an online payment, a login by the person entitled to a card, a contact with the Bank or similar processes (suspicion of abuse);
- Further suspicion that confirmation requests in the app or the SMS code do not originate from the Bank;
- Suspicion of abuse of login name, password, mobile devices, the website, the app etc. or suspicion that unauthorised third parties have come into possession of the same;
- Changes to the phone number and other relevant personal data;
- Change of mobile device used for one (in this case, the app must be reregistered).

Possible abuse or loss of a mobile device must be reported immediately by phone to the Bank's card blocking hotline (24h): +41 800 811 820.

4. Liability

Subject to the following, the Bank will compensate damages in connection with the use of one (without deductible) that is not covered by insurance taken out by the person entitled to a card,

- if the damages in question are incurred:
  - As a result of a demonstrably unlawful interference in the facilities of network and/or telecommunication operators or with the devices and/or systems used by the person entitled to a card (e.g. PCs, mobile devices and other EDP infrastructure) and
  - The person entitled to a card has complied with the general and special due diligence and reporting requirements stated in section 3.2, 3.3 and 7.5, in particular the obligations to control confirmation requests and review the monthly invoice as stated in Migros Bank Terms, as well as the timely complaint of abusive transactions, and
  - The person entitled to a card is also not otherwise at fault for the occurrence of the damage and
- if the damages in question have arisen exclusively as a result of a breach of the Bank's customary duty of care.

The Bank excludes any liability for any indirect damage, loss of profit, loss of data or consequential damage of any kind suffered by the person entitled to a card, provided the Bank has acted neither with gross negligence nor with intent. Neither the Bank nor the processor shall be liable for any damages resulting from the use of the one app by the person entitled to a card in breach of the law or the contract.

The Bank shall not be liable either if the spouse, directly related family members (especially children and parents) or other persons close to the person entitled to a card, authorised representatives, and/or persons living in the same household have performed an action (e.g. confirmation in the app or by SMS code).

B Special section

5. Digital order process and digital identification service

5.1 Digital ordering of a Cumulus credit card and using the identification service
The Bank offers natural persons who are resident in Switzerland as persons entitled to a card the option of ordering a Cumulus credit card digitally, using the digital identification service provided by Intrum AG (hereinafter **«Intrum»**) commissioned by the processor.

By applying for a Cumulus credit card and participating in the digital application process, person entitled to a card acknowledges and agrees that personal data (of person entitled to a card (hence including primary and additional cardholders), e.g. first and last name, gender, date of birth, place of birth, nationality, ID number, issuing authority, address, e-mail address, phone number) may be processed by the Bank as part of the application process, stored and passed on to third parties (such as the processor, Intrum, the Federation of Migros Co-operatives (MGB) and the online analysis services listed below). This data is also passed on to third parties (such as the processor, the Central Office for Credit Information [ZEK], authorities [e.g. debt enforcement and tax offices, residents' registration offices, adult protection authorities], credit agencies (such as CRIF Ltd.), the employer, other companies of the Federation of Migros Co-operatives or to other bodies provided for by law [e.g. the Consumer Credit Information Office [Informationsstelle für Konsumkredit, IKO]] or suitable information and disclosure centres) for the purpose of checking the information provided above and, in particular, as part of the necessary creditworthiness check before the card is issued.

The MGB processes this data together with additional MGB data on its own responsibility in accordance with the **Migros Privacy Statement** (available at privacy.migros.ch/en). The MGB processes this data, in particular, to be able to assign cards to existing Migros accounts and to optimise the application process (analysis of aborted applications). Further details on this data disclosure can be found in **Information on data protection for the Migros Bank Cumulus credit card** (available at cumulus.migrosbank.ch/documents).

When using the one App and the cumulus.migrosbank.ch website, the following third-party providers are consulted (by the processor, the Bank and/or the MGB) in the course of online analysis activities to optimise the application process:

Google Analytics and Google Firebase
On its own websites, Migros Bank AG uses Google Analytics, an analytics service provided by Google LLC (1600 Amphitheatre Parkway, Mountain View, CA, USA) and Google Ireland Ltd. (Google Building Gordon House, Barrow St, Dublin 4, Ireland; collectively «Google», with Google Ireland Ltd. being responsible for the processing of personal data). Google uses cookies and similar technologies to collect certain information about the behaviour of individual users on or in the relevant website and the terminal used for this purpose (tablet, PC, smartphone, etc.). This includes, for example, how often the website was opened, how many purchases were made, what interests are present, as well as data about the terminal used, such as the operating system). You will find further details about this at this link.

The data are also used for the purpose of collecting statistics, improving the application process and for business communication with you after the application process has ended or been cancelled (cf. section 8).

The identification service is used to identify natural persons and verify official identity documents within the scope of ordering the digital credit card.

The Bank is obliged by law (in particular the Anti-Money Laundering Act and the Federal Act on Electronic Signatures) to establish the identity of a person entitled to a card in the digital ordering process. Licensed identification software from a third-party company is used for identification. The identification service is available via the website and also through the one app.

5.2 Identification process
The identification service is system and process-controlled, whereby the verification of identity documents can also be carried out manually. The individual steps of the identification process are as follows:

- By using the identification service, an identification number is assigned to the natural person;
- The Bank (or the processor on its behalf) collects personal data (such as first and last name, gender, date of birth, place of birth, nationality, ID number, issuing authority, address, e-mail address, phone number) directly from the person entitled to a card within the framework of a predefined input mask, which is suitable and necessary to verify the identity of the person entitled to a card. The data collected accordingly will be forwarded to Intrum. The collected data may be forwarded to other processors for further processing on behalf of the Bank;
- The person entitled to a card uses a technical terminal (e.g. PC, tablet or smartphone) to record the identity document with the help of the integrated camera. Intrum matches the data collected by the Bank (or by the processor on its behalf) with the uploaded identity document (e.g. identity card, passport, driving licence). Depending on the configuration, photos of the face of the person entitled to a card are taken with the licensed software and compared with the identity document in a second step. These comparisons can be automated or manual.

The Bank can only identify the person entitled to a card if the person entitled to a card provides all the documents required for verification, which are requested by Intrum as part of the ordering process.

The data collected during the identification process are deleted from Intrum's servers within 90 days.

5.3 Obligations of the person entitled to a card
The person entitled to a card is obliged to provide the Bank with all the documents required for the provision of the identification service according to section 5 of these provisions and to enter all information truthfully in the data fields provided.

A suitable terminal (e.g. PC, smartphone or tablet) and an internet connection are required to use the identification service. The person entitled to a card can only use the identification service via a mobile terminal using the one app. It is the responsibility of the person entitled to a card to ensure the performance and compatibility of the relevant terminal.

The person entitled to a card must keep the data provided to him/her (e.g. transaction number) confidential and protect it against use by unauthorised third parties. The person entitled to a card shall inform the Bank immediately in case of suspicion of unauthorised use of his/her data.

5.4 Consent to data collection, disclosure, storage and deletion in connection with the digital ordering process and the digital identification service
The Bank works with other processors in Switzerland and other European countries when collecting, processing and using personal data (such as first and last name, gender, date of birth, place of birth, nationality, ID number, issuing authority, address, e-mail address, phone number) for the purpose of identification, credit assessment and compliance with the Anti-Money Laundering Act.

During the verification process, the person entitled to a card uses a technical terminal (e.g. PC, tablet or smartphone) to record his/her identity document with the help of the integrated camera. The verification and identification process is explained below with the corresponding steps and the associated data processing. The Bank generally requires the following data from the person entitled to a card to carry out these processes: first and last name, address, date of birth, place of birth, phone number, e-mail address. The person entitled to a card enters these data on the website **cumulus.migrosbank.ch** or in the one app. During the identification process, photographs of the identify document are taken to match the data previously obtained with the data on the identity document. Data collected by the bank may differ depending on the identity document of the person entitled to a card and the application. With passports and identity cards, in particular the first and last name, gender and date of birth are collected. For identification under the Anti-Money Laundering Act, the issuing authority, ID number, nationality and the address of the person entitled to a card are also collected. Besides the data of the person entitled to a card, the Bank also stores the photographs of the identity documents. In a second step, the licensed software takes photos of the face of the person entitled to a card and compares them with the identity document, depending on the configuration.

When the verification and identification is completed, the data will be deleted from Intrum's server at the latest after 90 days. Due to legal retention periods (e.g. within the scope of the Anti-Money Laundering Act), the Bank may retain the data for a period of at least ten years after termination of the business relationship between the person entitled to a card and the Bank.

6. 3D Secure

6.1 What is 3D Secure?
3D Secure is an internationally recognised security standard for online card payments. It is called «SecureCode» for Mastercard and «Verified by Visa» for Visa. With these Terms of Use for one, the person entitled to a card undertakes to use this security standard for payments, provided it is offered by the merchant (acceptance point).

3D Secure can only be used after registration with one.

6.2 How does 3D Secure work?
Payments made with 3D Secure can be confirmed (authorised) in two ways:

- in the one app or
- by entering a code sent by the Bank to the person entitled to a card by SMS in the browser's corresponding window during payment processing.

According to the current Terms of Use for one, any authorised use of the card with 3D Secure is deemed to have been made by the person entitled to a card.

6.3 Activating cards for 3D Secure
By registering on one, 3D Secure is activated for all cards registered in the name of the person entitled to a card and related to the registered business relationship of the person entitled to a card with the Bank.

6.4 No deactivation of cards for 3D Secure
For security reasons, 3D Secure can no longer be deactivated once it has been activated.

7. Mobile payment

7.1 What is mobile payment?
Mobile payment allows a person entitled to a card who has a compatible device to use authorised cards via a mobile application (app) offered by the Bank (cf. section 7.7) or a third-party provider for contactless payments as well as for payments in online shops and apps.
For security reasons, a different number (token) is generated instead of the card number and stored as a «virtual card». Virtual cards can be used through mobile payment in the same way as a physical card. When paying with a virtual card, only the generated number (token) is passed on to the merchant but not the card number.

7.2 What devices are compatible and what cards are admitted?
Compatible devices include for example PC, mobile phones, smartwatches and fitness trackers, provided they support the use of virtual cards and are approved by the Bank. The Bank is also free to decide what cards are approved for which providers.

7.3 Activation and deactivation
For security reasons, the activation of a card requires that the person entitled to a card accepts the applicable **Migros Bank Terms** and takes note of the data protection provisions (cf. section 1.1).

Virtual cards can be used until they are blocked or deactivated by the person entitled to a card or the Bank. Restrictions on the use of the card in accordance with the applicable Migros Bank Terms remain reserved. The person entitled to a card may terminate the use of mobile payment at any time by removing his/her virtual card(s) from the compatible devices.

The person entitled to a card shall bear the costs incurred in connection with the activation and use of virtual cards (e.g. costs for mobile internet use abroad).

7.4 Use of the virtual card (authorisation)
The use of a virtual card corresponds to a standard card transaction. Any use of a virtual card is deemed as authorised by the person entitled to a card.
The use of virtual cards must be authorised in the manner provided for by the provider (e.g. the respective mobile payment) or merchant, e.g. by entering a device PIN or by fingerprint or facial recognition. The person entitled to a card acknowledges that this increases the risk that virtual cards can be used by unauthorised persons if the additional means of authorisation required by the provider or merchant (device PIN or card PIN) comprise combinations that are easy to ascertain (such as «1234»). The person entitled to a card acknowledges that, depending on the provider or merchant, no authorisation is required up to an amount to be determined by the provider or merchant. Liability shall otherwise be governed by section 4 of the Terms of Use for one.

7.5 Special due diligence obligations
The person entitled to a card acknowledges and accepts that the use of mobile payment entails risks, despite all the security measures taken. In particular, it is possible that virtual card(s) and personal data may be misused or accessed by unauthorised persons. As a result, the person entitled to a card may be financially damaged (through misuse of a card) and have his/her privacy violated (through misuse of personal data).

The person entitled to a card must therefore handle the devices used and the virtual cards with care and ensure their protection. In addition to the due diligence obligations pursuant to the relevant Migros Bank Terms and the general due diligence and reporting requirements under section 3.2 and section 3.3 – the person entitled to a card shall in particular comply with the following special due diligence obligations:

- The equipment used must be used for its intended purpose, and securely stored in a manner that protects it from access by third parties;
- Virtual cards, like physical cards, are personal and non-transferable. They may not be passed on to third parties for use (e.g. by depositing fingerprints or scanning the face of third parties to unlock the device used);
- In case of a change or transfer of a compatible device (e.g. in case of a sale), any virtual card must be deleted in the provider's app and on the compatible device;
- Suspicion of abuse of a virtual card or a device used for this purpose must be reported to the Bank immediately, so that the virtual card concerned can be blocked.

7.6 Disclaimer of warranty
There is no entitlement to the use of mobile payment. The Bank may interrupt or terminate the use – i.e. the possibility of using virtual cards – at any time, in particular for security reasons or in case of changes to the mobile payment offering or restriction of authorised cards or compatible devices. Furthermore, the Bank is not responsible for the actions and offers of the provider or other third parties, such as online and telephone service providers.

7.7 Card use via the one app
The person entitled to a card who has a compatible device can activate his/her card(s) in the one app and use it as a virtual card. To ensure security with mobile payment, the person entitled to a card must set a confidential PIN when activating it. The Bank can adjust this service at any time. Besides, these present terms of use for one apply for mobile payment, in particular the special due diligence obligations under section 7.5.

7.8 Mobile payment data protection
The third-party provider (in particular the respective mobile payment provider) and the Bank are independently responsible for their respective processing of personal data. The person entitled to a card acknowledges that personal data in connection with the offer and use of mobile payment (in particular, information about the person entitled to a card and activated cards, as well as transaction data from the use of virtual cards) will be collected by the third-party provider and stored and processed in Switzerland or abroad. The processing of personal data by the third-party provider in connection with mobile payment and the use of the third-party provider's offers and services, including its devices and software, is governed by its terms of use and data protection provisions. With each activation of a card, the person entitled to a card therefore confirms that he/she has read and understood the relevant data protection provisions of the respective third-party provider and that he/she expressly agrees to the corresponding data processing by the third-party provider. If he/she does not consent to the corresponding processing, it is the responsibility of the person entitled to a card not to activate a card or to object to the processing vis-à-vis the third-party provider. The data protection provisions set out under C below and the **Information on data protection for the Migros Bank Cumulus credit card** (available at cumulus.migrosbank.ch/documents) govern the processing of personal data by the Bank and the processor.

C Data protection provisions for the use of one

The following data protection provisions provide information on how the Bank processes personal data (hereinafter «data») as the responsible party in the context of the use of one. Processing includes any handling of personal data, in particular the acquisition, storage, use, disclosure or deletion of data. You will find contact details for information on the subject of data protection and data processing in the **General information on data protection at Migros Bank AG** (available at migrosbank.ch/grundlagen).

When registering for one, the person entitled to a card expressly agrees to the data processing in this privacy statement. Information on further data processing in the context of the card relationship can be found in the Migros Bank Terms and the Terms of Use for one. Please refer also to the global privacy statements and your enforcement rights as a third-party beneficiary of **Mastercard** and **Visa**.

8. Processing of personal data

8.1 What are the Terms of Use for one about?
Via the website or app, the Bank provides digital onboarding under the name «one» for new customers as well as various card services in connection with the use of the issued cards (collectively «one digital services»). The provision of digital onboarding and card services requires the Bank to process data of the person entitled to a card. These Terms of Use for one provide the person entitled to a card with detailed and transparent information on data processing when using one digital services. For the digital application process for Cumulus credit cards, please refer also to section 5 for additional information. Please also take note of the **General Information on data protection at Migros Bank AG** (available at migrosbank.ch/grundlagen) and the **Information on data protection for the Migros Bank Cumulus credit card** (available at cumulus.migrosbank.ch/documents, cf. section 1.1).

8.2 How is data procured?
8.2.1 Which data of the person entitled to a card is recorded?
When registering for one digital services, logging in and managing the user account, the person entitled to a card may be asked to provide his/her e-mail address, date of birth, mobile phone number, card number and activation code.

8.2.2 Which data is collected automatically?
- Data concerning the mobile devices of the person entitled to a card, such as manufacturer, device type, operating system with version number, device ID, IP address;
- Data on PC and browser used, as well as on access to the internet, such as device type, operating system, IP address;
- Data about the use of the user account, such as number of logins with date and time, changes in the user account, acceptance of Terms of Use for one digital services and the privacy statement;
- Data about the settings requested by the person entitled to a card, such as storage of the login name or login;
- Data about visits to and usage user behaviour on the website, as well as data that accrues when using the app, such as updates or device information about user behaviour, such as in the app or via SMS code.

8.2.3 What information is collected when registering for and activating the card services on one?
- Information about the person entitled to a card and his/her cards registered for one, which is stored in the user account;
- Information that 3D Secure is used for the registered cards, through a confirmation in the app or by entering an SMS code;
- Delivery address and mobile phone number.

8.2.4 What information is collected when using mobile payment?
- Information on the use of mobile payment, such as activating or deactivating cards and using the cards for mobile payment;
- Information on the transaction amount;
- Information on the use of the card, time of transaction, type of verification.

When using a mobile payment solution from a third-party provider, the third-party provider may also collect and process personal data of the person entitled to a card. Depending on the offer, this includes for example name, card number and transaction data, if necessary. To this end, the third-party provider's terms of use and data protection provisions should be noted.

8.2.5 What information is collected when using 3D Secure?
- Information about the merchant, the transaction and its processing, as well as on confirmation of the transaction with 3D Secure;
- Information relating to the devices used for the transaction and the confirmation;
- Information relating to the access to the internet or mobile phone network, such as IP address, name of the access provider.

8.2.6 What data is collected when displaying the map section of the merchant's location?
- Location data of the merchants that are established in Switzerland;
- Location data, such as merchant's name, location, country and sector;
- Automated periodic Google search to clarify the merchant's location.

8.3 For what purpose does the Bank process my data?
8.3.1 Provision of the card services and processing of the card relationship
- Facilitating the registration, login and use of the one digital services by the person entitled to a card;
- Developing a secure connection between one digital services and the mobile device of the person entitled to a card;
- Transmission of confirmation requests, such as to confirm online payments via one digital services, by push message or by SMS code to the person entitled to a card;
- Transmission of the information about confirmations made to the Bank;
- Authentication of the person entitled to a card when carrying out transactions and actions in general. The app or the mobile device used are clearly allocated to the person entitled to a card when registering for one. The Bank can thus ensure that the confirmation is made in the registered app or mobile device;
- Communication with the person entitled to a card and transmission of information in connection with the card relationship or card use, such as information about new invoices, fraud alerts or enquiries about unusual transactions via one digital services and the mobile device;
- Receipt of notifications from the person entitled to a card;
- Display of transactions and invoices;
- Processing of the card relationship with the person entitled to a card and with the transactions made with the card. Reference is made here to the Bank's privacy statement and the Terms of Use for one.

8.3.2 Mobile payment
- For the decision regarding the approval of the card for mobile payment;

- For activating, deactivating and updating the cards for mobile payment;
- For preventing abuse of the added cards;
- To communicate with any third-party provider of a mobile payment solution within the framework of these Terms of Use for one and the terms and conditions of use or data protection provisions of the provider concerned, which apply in the relationship between the person entitled to a card and the third party.

8.3.3 Marketing
- To assign this data to data already held by the Bank (including data from third-party sources);
- To create individual customer, consumption and preference profiles that enable the Bank to develop and offer products and services to the person entitled to a card;
- To communicate information about the Bank's and third parties' existing or new products and services (advertising material) to the person entitled to a card;
- For processing by the third-party provider within the framework of its own terms and conditions of use or data protection provisions.

8.3.4 Further processing purposes
- Calculating credit and market risks that are relevant to the business;
- Improving security in using card services, for example, by reducing the risk of fraudulent transactions or abuse of devices or means of identification or of legitimisation, such as through phishing or hacking;
- Evidence of actions and defence against accusations or claims against the Bank;
- Improving the general services of the Bank and one digital services;
- Meeting legal and regulatory requirements;
- Processing by the third-party provider for its own purposes as part of its own terms and conditions of use or data protection provisions.

8.4 Will my data be disclosed to other recipients?
8.4.1 Disclosure and transfer to third parties, data collection by third parties
Third parties are persons or companies who process data for their own purposes. Contracted service providers of the Bank are not considered as third parties. In connection with cards to which the Migros Bank Terms apply, subject to the following and depending on the selected card product (in particular, other provisions for the Cumulus credit card), the Bank generally does not transfer any data – in particular no transaction data – to third parties for their own purposes, unless the person entitled to a card himself/herself has consented to such a transfer or has requested or arranged for such a transfer. In particular, the Bank shall not transfer, without the separate, express consent of the person entitled to a card, to third parties any individual customer, consumption and preference profiles it has created. If and to the extent that a transfer of data is permissible in the light of these Terms of Use for one, in particular this section 8.4, the person entitled to a card releases the Bank from bank client confidentiality in this context. For the digital application form for Cumulus credit cards, please also refer to the explanatory notes in section 5.

8.4.2 Additional categories of third parties to which data is disclosed
- The additional cardholder's data (including transaction data) can be disclosed to the primary cardholder;
- The data of the person entitled to a Business Card can be disclosed to the company;
- Persons authorised by the person entitled to a card;
- When using the Cumulus Credit Card, personal data may be disclosed to the Federation of Migros Co-operatives (MGB) in accordance with the **Information on data protection for the Migros Bank Cumulus credit card** (available at cumulus.migrosbank.ch/documents), notably (master data) for linking with existing Migros accounts, points credits for the Cumulus programme, and behavioural and transaction data (including details of cash withdrawals) also for personalised direct marketing;
- By official order or based on legal obligations, the Bank discloses data to governmental agencies such as law enforcement or supervisory authorities.

8.4.3 Transmission of data of a person entitled to a card to third parties through the use of mobile payment
- The card and transaction data required to process the transaction are routed via the card organisations' servers during payment processing. Additional information on data processing, the transfer of data and the involvement of third parties can be found in the Migros Bank Terms;
- When using mobile payment via a third-party provider, the third-party provider collects and processes data in accordance with its own terms of use and data protection provisions.

8.4.4 Electronic data transmission
When using electronic data transmission, data of the person entitled to a card may also be disclosed to third parties (in Switzerland and abroad) without any action from the Bank.

When using the app and/or mobile devices in particular, manufacturers of devices or of software (such as Apple or Google) may receive personal data. These manufacturers can process and pass on the data in accordance with their own terms and conditions of use or data protection provisions. As a result, these third parties may infer that there is a relationship between the person entitled to a card and the Bank. SMS are subject to the applicable legal provisions concerning the interception of telecommunications and are stored on the mobile phone. Third parties may thereby obtain possession of the relevant information.

8.5 How do we protect your data?
The transmission of information between the Bank, the processor and the app and/or mobile devices of the person entitled to a card (but not the sending of SMS and only in a limited manner the sending of e-mail) is encrypted. However, communication with the person entitled to a card takes place via the public communication networks. This data is generally visible to third parties, can be lost during transmission or intercepted by unauthorised third parties. It therefore cannot be ruled out that third parties may gain access to communication with the person entitled to a card when using one despite all the security measures taken. Furthermore, when using the internet, data may also be transmitted via third countries that may not offer the same level of data protection as Switzerland, even though the person entitled to a card is located in Switzerland.

The data security also depends on the cooperation of the person entitled to a card. The person entitled to a card is therefore required to avail of the options available to him/her to protect his/her devices and data. The minimum due diligence and reporting requirements for this are set out in Section A. Appropriate security measures enhance safety and further reduce the risks associated with the use of one.

8.6 What are your rights in relation to your data?
- The right to request information regarding your personal data saved by us;
- The right to have inaccurate or incomplete information rectified;
- The right to request deletion of your data or transformation of your data into an anonymous form;
- The right to receive specific personal data in a structured, common and machine-readable format;
- The right to revoke consent with effect for the future, provided that processing is based on consent;
- The right to object to our processing of your personal data;
- The right to file a complaint with the competent supervisory authority against our processing of your personal data.

The Bank can only grant your rights subject to the legal requirements. Even if you withdraw your consent, for example, your personal data can still be processed to the extent required by law.

8.7 How long does the Bank store the data?
The Bank stores your data for as long as necessary for the purpose for which it was collected. The Bank also stores personal data if there is a legitimate interest in storing it, e.g. if the data is needed to enforce or defend claims, to ensure IT security or if periods of limitation expire or deletion is not yet definitely possible for technical reasons. Finally, your data is stored in order to comply with legal and regulatory obligations.

D Release from bank client confidentiality

9. Release from bank client confidentiality

The Bank shall take appropriate measures to ensure compliance with bank client confidentiality. However, it shall disclose customer data (e.g. first and last name, gender, date of birth, place of birth, nationality, ID number, issuing authority, address, e-mail address, phone number), in particular as stated above under section 2.2, 5.1, 5.2 and 8 for various purposes, namely to process digital card applications (in particular by the processor), fulfil contractual obligations, official orders, and domestic or foreign legal or regulatory reporting and disclosure obligations, and to safeguard legitimate interests.

Further information on the scope of disclosures and release from bank client confidentiality can be found in the Migros Bank Terms, in **General information on data protection at Migros Bank** (available at migrosbank.ch/grundlagen) or **Information on data protection for the Migros Bank Cumulus credit card** (available at cumulus.migrosbank.ch/documents).

The person entitled to a card consciously and voluntarily waives the protection of bank client confidentiality to the extent of the aforementioned disclosures. To this extent, he/she releases the Bank (and any other third parties involved) from bank client confidentiality and from any further confidentiality provisions, namely trade and official secrecy.

Version 07/2022