BANQUE MIGROS

Dispositions de la Banque Migros **relatives à l'utilisation de one**

Dispositions de la Banque Migros relatives à l'utilisation de one

A Partie générale
1. Dispositions générales relatives à l'utilisation de one
2. Utilisation de one
3. Risques, exclusion de garantie et obligations générales de diligence et de déclaration
4. Responsabilité

B Partie spéciale
5. 3-D Secure
6. Paiement mobile

C Dispositions relatives à la protection des données one
7. Traitement des données personnelles

A Partie générale

1. Dispositions générales relatives à l'utilisation de one

1.1 Dispositions relatives à l'utilisation de one et autres documents pertinents

Les présentes dispositions s'appliquent aux services numériques (ci-après dénommés **«services de cartes»**) mis à disposition par la Banque Migros SA (ci-après dénommée **«Banque»**) au titulaire (ci-après dénommé **«titulaire de la carte»**) d'une carte principale ou supplémentaire ou d'une Business Card ou d'une Corporate Card de la Banque (ci-après dénommée(s) **«carte(s)»**) sous la dénomination **«one»**. One est exploité par Viseca Payment Services SA (ci-après **«processeur»**) pour le compte de la banque. Le processeur assiste la banque dans l'accomplissement de ses tâches dans le domaine des cartes.

One est disponible via:
- le site internet one (ci-après dénommé **«site Web»**) et
- l'application one (ci-après dénommée **«App»**)

Concernant l'utilisation de one, il convient également de tenir compte des «Informations générales concernant la protection des données à la Banque Migros SA» (disponibles à l'adresse *www.migrosbank.ch/fr/informations-legales*) ainsi que des dispositions spécifiques relatives à la protection des données figurant ci-après sous C et des «Conditions d'utilisation pour one-digitalservice.ch» du processeur (disponibles sous *www.viseca.ch/fr/conditions-generales/one*).

Les présentes dispositions relatives à l'utilisation de one s'appliquent en plus des dispositions applicables en matière d'utilisation des cartes de la Banque (Conditions générales et Conditions d'utilisation des cartes de débit et de crédit de la Banque Migros, ci-après dénommées collectivement **«Dispositions de la Banque Migros»**). En cas de réglementation divergente, les présentes dispositions sur l'utilisation de one prévalent sur les dispositions de la Banque Migros.

L'utilisation de one suppose l'enregistrement du titulaire de la carte. Les présentes dispositions relatives à l'utilisation de one sont réputées acceptées dès que le titulaire de la carte s'enregistre via l'app one et confirme avoir lu et compris les présentes Conditions.

La Banque se réserve le droit de modifier à tout moment les présentes dispositions relatives à l'utilisation de one. Les modifications sont communiquées de manière appropriée au titulaire de la carte.

1.2 Qu'est-ce que one et comment la développe-t-on?

One comprend les services de cartes de la Banque fournis par le processeur pour le compte de la Banque.

Les nouveaux services de cartes seront mis à la disposition du titulaire de la carte enregistré au moyen de mises à jour. La Banque informera le titulaire de la carte de manière appropriée des développements et, le cas échéant, des modifications des présentes dispositions relatives à l'utilisation de one.

1.3 Quelles fonctions one offre-t-il?

One peut notamment comporter, à l'heure actuelle ou à l'avenir, les fonctions suivantes:

- un compte d'utilisateur pour la gestion des données personnelles;
- le contrôle et la confirmation de paiements, par exemple via 3-D Secure (MasterCard SecureCode ou Verified by Visa) dans l'app ou par saisie d'un code SMS (cf. ch. 5);
- le contrôle et la confirmation de certaines actions (p. ex. logins, contacts avec la Banque) dans l'app ou en saisissant un code SMS;
- l'activation de cartes pour l'utilisation de possibilités de paiement (cf. ch. 7 et ch. 8);
- l'échange de communications et de notifications de toute nature entre le titulaire de la carte et la Banque (y compris la communication d'une modification des dispositions), à moins qu'une forme particulière de communication ou de notification ne soit réservée (p. ex. réclamation écrite d'une facture mensuelle);
- l'aperçu des transactions ou des cartes et l'affichage électronique des factures;
- l'aperçu du compte du programme de bonus et la possibilité d'encaisser des points (actuellement compte surprize);
- les informations relatives à l'utilisation de la carte (actuellement services SMS).

1.4 Avantages de one

One doit offrir plusieurs avantages au titulaire de la carte:

- one rend l'accès aux services de cartes plus sûr: une procédure moderne d'authentification du titulaire de la carte permet de vérifier et de confirmer que les actions ont effectivement été effectuées par le titulaire de la carte – en utilisant le téléphone mobile comme deuxième facteur (en plus du login) et par un canal de communication sécurisé entre le titulaire de la carte et la Banque.
- one regroupe les services de cartes de la Banque sur une plate-forme uniforme, ce qui rend leur présentation plus claire.

– one facilite l'accès aux différents services de cartes de la Banque: le nom d'utilisateur et le mot de passe permettent l'enregistrement et la connexion à différents services de cartes.
– Les paiements en ligne avec 3-D Secure sont plus rapides: au lieu de saisir le mot de passe 3-D Secure, le paiement peut être contrôlé et confirmé avec l'app ou en saisissant le code SMS.

2. Utilisation de one

2.1 Droit d'utilisation

Le titulaire de la carte n'est autorisé à utiliser one que dans les conditions suivantes:

– Il a accepté les présentes dispositions relatives à l'utilisation de one et est en mesure de les mettre en œuvre ainsi que les exigences y afférentes (notamment les chiffres 3.2.1 et 3.2.3) et
– il est autorisé à utiliser une carte de la Banque en tant que titulaire d'une carte principale ou supplémentaire ou d'une Business ou Corporate Card de la Banque.

2.2 Autorisations pour l'enregistrement de one

En acceptant les présentes dispositions relatives à l'utilisation de one ou en utilisant one, le titulaire de la carte donne expressément les autorisations suivantes à la Banque:

– Consentement au traitement des données collectées ou à collecter lors de l'utilisation de one. Cela inclut notamment le consentement à leur combinaison avec les données existantes auprès de la Banque et la création de profils, à des fins de gestion des risques et de marketing de la Banque ou du processeur et de tiers, conformément aux dispositions relatives à la protection des données de la section C.
– Consentement à la réception de communications et d'informations sur les produits et services de la Banque et de tiers à des fins de marketing (publicité). Elles peuvent être envoyées par la Banque par e-mail, directement dans l'app ou sur le site internet.
– Consentement à l'utilisation de l'adresse e-mail fournie lors de l'enregistrement ainsi que du site internet et de l'app à des fins de communication électronique mutuelle avec la Banque (p. ex. communications de changements d'adresse, de modifications des dispositions (Dispositions de la Banque Migros) ou communications liées à la lutte contre l'utilisation abusive de cartes).
– Consentement au traitement et à la transmission de données client à des tiers dans la mesure nécessaire au respect d'obligations contractuelles, d'ordres des autorités et d'obligations légales ou réglementaires nationales ou étrangères de renseigner et de déclarer, ainsi qu'à la sauvegarde d'intérêts légitimes. Dans ce contexte, le titulaire de la carte délie la Banque du secret bancaire.

Le consentement du titulaire de la carte à la réception de communications relatives à des produits et services et/ou au traitement des données à des fins de marketing peut être révoqué à tout moment par celui-ci par communication écrite à la Banque avec effet à l'avenir (droit d'opt-out). Les coordonnées correspondantes figurent dans la déclaration relative à la protection des données de la Banque.

2.3 Rejet des autorisations dans le cadre de la poursuite du développement de one

Si le titulaire de la carte refuse de donner son consentement aux dispositions relatives à l'utilisation de one dans le cadre du développement de celui-ci (p. ex. en cas de mises à jour), l'app ou le site internet ou certains services de cartes de ces derniers peuvent ne pas ou ne plus être utilisés.

2.4 Effet des confirmations

Toute confirmation effectuée par l'intermédiaire de l'app ou par la saisie d'un code SMS est considérée comme une action du titulaire de la carte. Le titulaire de la carte s'engage à assumer les débits résultant de la confirmation de sa carte et autorise la Banque à exécuter les ordres et à prendre les mesures correspondantes.

2.5 Disponibilité/blocage/modifications

La Banque peut à tout moment, pour des raisons suffisantes, interrompre, restreindre ou supprimer la possibilité d'utiliser one, en tout ou en partie, ou le remplacer par une autre prestation, même sans communication préalable. La Banque a notamment le droit de bloquer l'accès du titulaire de la carte à one de manière temporaire ou définitive (p. ex. en cas de soupçon d'abus ou de non-respect des obligations de diligence par le titulaire de la carte).

2.6 Droits immatériels et licence

Tous les droits (notamment les droits d'auteur et les droits de marque) sur les logiciels, textes, images, vidéos, noms, logos et autres données et informations accessibles via one ou qui deviennent accessibles au fil du temps sont réservés à la Banque ou aux partenaires et tiers concernés (p. ex. processeur, Mastercard, Visa), sauf indication contraire dans les présentes dispositions sur l'utilisation de one. Les noms et logos visibles sur one sont des marques protégées.

Pour l'utilisation de l'app, la Banque accorde au titulaire de la carte une licence non exclusive, non transférable, perpétuelle, révocable et gratuite pour télécharger l'app, l'installer sur un appareil détenu en permanence par le titulaire de la carte et l'utiliser dans le cadre des fonctions prévues.

Pour l'utilisation du site internet du processeur, les Dispositions relatives aux licences s'appliquent en outre, conformément aux Conditions d'utilisation du site Internet (sous le titre «Propriété du site internet, droits de marque et droits d'auteur»).

3. Risques, exclusion de garantie et obligations générales de diligence et de déclaration

3.1 Risques liés à l'utilisation de one

Le bénéficiaire de la carte prend acte et accepte que l'utilisation de one comporte des risques.

Il est notamment possible que des tiers non autorisés abusent de l'utilisation de cartes one, du nom d'utilisateur et du mot de passe, des appareils utilisés ou des données personnelles du titulaire de la carte. Le titulaire de la carte peut ainsi être lésé financièrement (par le débit de sa carte) et subir une atteinte à sa personnalité (par un abus de données personnelles). De plus, one ou l'un des services de cartes offerts sur one risquent de ne pas être utilisés (p. ex. pas de connexion sur one possible).

Les abus sont rendus possibles ou favorisés notamment par:

– la violation d'obligations de diligence ou de déclaration par le titulaire de la carte (p. ex. en raison d'une manipulation négligente du nom d'utilisateur / mot de passe ou de la non-déclaration de perte de la carte);
– les paramètres choisis par le titulaire de la carte ou l'entretien défectueux des appareils et systèmes employés pour l'utilisation de one (p. ex. ordinateur, téléphone portable, tablette

et autres infrastructures informatiques), p. ex. en raison d'un blocage d'écran, d'un pare-feu ou d'une protection antivirus manquants ou insuffisants, ou en raison d'un logiciel obsolète;
- les interventions de tiers ou les erreurs de transmission de données sur Internet (p. ex. piratage, hameçonnage ou perte de données);
- la confirmation erronée dans l'app ou la saisie d'un code SMS (p. ex. en cas de contrôle défectueux d'une demande de confirmation);
- Paramètres de sécurité plus faibles choisis par le titulaire de la carte pour one – en particulier pour l'app – (p. ex. enregistrement du login).

Si le titulaire de la carte respecte les obligations de diligence et de déclaration suivantes concernant les appareils mobiles et le mot de passe ainsi que les obligations de contrôle des demandes de confirmation, il peut réduire ces risques d'abus.

La Banque ne garantit pas que le site internet et l'app soient accessibles en permanence ou fonctionnent sans problème, ou que des abus puissent être détectés et évités avec certitude.

3.2 Obligations générales de diligence du titulaire de la carte

3.2.1 Obligations générales de diligence en rapport avec les appareils et systèmes utilisés, en particulier les appareils mobiles

One utilise des appareils mobiles (p. ex. téléphone mobile, tablette; soit «appareil mobile») du titulaire de la carte à des fins d'authentification. La détention à tout moment de ces appareils mobiles est donc un facteur de sécurité essentiel. Le titulaire de la carte doit traiter les appareils mobiles avec un soin approprié et assurer une protection adéquate de ceux-ci.

Par conséquent, le titulaire de la carte doit notamment respecter les obligations générales de diligence suivantes en rapport avec les appareils et systèmes utilisés, en particulier les appareils mobiles:

- pour les appareils mobiles, un blocage d'écran doit être activé et des mesures de sécurité supplémentaires doivent être prises afin d'éviter le déblocage par des personnes non autorisées;
- les appareils mobiles doivent être conservés en lieu sûr, à l'abri d'un accès de tiers, et ne doivent pas être transférés à des tiers pour une utilisation permanente ou non surveillée;
- les logiciels (p. ex. systèmes d'exploitation et navigateurs internet) doivent être mis à jour régulièrement;
- les interventions sur les systèmes d'exploitation (p. ex. «jailbreaking» ou «rooting») ne sont pas autorisées;
- des programmes de protection contre les virus et de sécurisation sur Internet doivent être installés et tenus à jour sur l'ordinateur portable/ordinateur;
- l'app ne peut être téléchargée qu'à partir des magasins officiels (p. ex. Apple Store et Google Play Store);
- les mises à jour de l'app doivent être installées immédiatement;
- en cas de perte d'un appareil mobile, tout ce qui est possible doit être fait pour empêcher l'accès non autorisé aux données transmises par la Banque à l'appareil mobile (p. ex. en bloquant la carte SIM, en bloquant l'appareil, en supprimant par ex. les données via «Rechercher mon iPhone» ou «Gestionnaire des appareils Android», en réinitialisant ou en renvoyant le compte utilisateur). La perte doit être annoncée à la Banque (voir ch. 3.3);
- l'app doit être supprimée avant la vente ou toute autre transmission permanente de l'appareil mobile à des tiers.

3.2.2 Obligations générales de diligence en rapport avec le mot de passe

Outre la possession de l'appareil mobile, le nom d'utilisateur et le mot de passe servent d'autres facteurs d'authentification du titulaire de la carte.

Le titulaire de la carte doit notamment respecter les obligations générales de diligence suivantes en rapport avec le mot de passe:

- le titulaire de la carte doit définir un mot de passe qu'il n'a pas déjà utilisé pour d'autres services et qui n'est pas constitué de combinaisons facilement identifiables (p. ex. numéro de téléphone, date de naissance, plaque d'immatriculation, nom du titulaire de la carte ou de ses proches, séquences de chiffres ou de lettres répétées ou se suivant immédiatement comme «123456» ou «aabbcc»);
- le mot de passe doit être tenu secret. Il ne peut être divulgué ou mis à la disposition de tiers. Le titulaire de la carte prend acte du fait que la Banque n'invitera jamais le titulaire de la carte à communiquer le mot de passe;
- le mot de passe ne doit pas être écrit ni enregistré de manière non sécurisée;
- le titulaire de la carte doit modifier le mot de passe ou réinitialiser le compte utilisateur ou le faire réinitialiser par la Banque s'il est soupçonné que des tiers sont entrés en possession du mot de passe ou d'autres données;
- le mot de passe ne peut être saisi que de manière à ce qu'il ne soit pas visible par des tiers.

3.2.3 Obligations générales de diligence en rapport avec les demandes de confirmation, notamment le contrôle

Les confirmations engagent le titulaire de la carte de manière contraignante.

Le titulaire de la carte doit donc respecter les obligations générales de diligence suivantes en rapport avec les confirmations dans l'app ou en saisissant un code SMS:

- le titulaire de la carte ne peut confirmer que si la demande de confirmation est directement liée à une action ou à un processus spécifique (p. ex. paiement, login, contact avec la Banque) du titulaire de la carte;
- le titulaire de la carte doit vérifier, avant la confirmation, si l'objet de la demande de confirmation coïncide avec le processus en question. En cas de demandes de confirmation liées à 3-D Secure, les détails de paiement affichés doivent notamment être contrôlés.

3.3 Obligations générales de déclaration du titulaire de la carte

Les événements suivants doivent être immédiatement signalés à la Banque:

- la perte d'un appareil mobile, mais pas une absence de courte durée;
- les demandes de confirmation qui ne sont pas liées à un paiement en ligne, à une connexion par le titulaire de la carte, à un contact avec la Banque ou à des opérations similaires (soupçon d'abus);
- tout autre soupçon que les demandes de confirmation dans l'app ou le code SMS ne proviennent pas de la Banque;
- le soupçon d'abus de nom d'utilisateur, de mot de passe, d'appareils mobiles, de site internet, d'app, etc., ou le soupçon de possession de ces éléments par des tiers non autorisés;

– les modifications du numéro de téléphone et d'autres données personnelles pertinentes;
– le changement de l'appareil mobile utilisé pour one (dans ce cas, l'app doit être réenregistrée).

Les abus éventuels ou la perte d'un appareil mobile doivent être immédiatement signalés par téléphone à la hotline de la Banque chargée du blocage des cartes (24h/24): +41 800 811 820.

4. Responsabilité

Sous réserve de ce qui suit, la Banque rembourse les dommages (sans franchise) qui ne sont pas pris en charge par une assurance du titulaire de la carte,

– si les dommages en question sont survenus:
  – à la suite d'une intervention illégale avérée dans des installations d'opérateurs de réseau et/ou de télécommunications ou dans des équipements et/ou systèmes utilisés par le titulaire de la carte (p. ex. ordinateurs, appareils mobiles et autres infrastructures informatiques); et
  – le titulaire de la carte a respecté les obligations générales et particulières de diligence et de déclaration énoncées aux ch. 3.2 et 3.3 ci-dessus, en particulier les obligations de contrôle des demandes de confirmation et l'obligation de vérification de la facture mensuelle prévue par les dispositions de la Banque Migros ainsi que la contestation en temps utile de transactions abusives; et
  – le titulaire de la carte n'est en aucun cas responsable de la survenance des dommages; et
– si les dommages en cause ont résulté exclusivement d'un manquement à la diligence usuelle de la Banque.

La Banque exclut dans tous les cas, dans la mesure permise par la loi, toute responsabilité pour dommages indirects, pertes de gain, perte de données ou dommages consécutifs éventuels de quelque nature que ce soit par le titulaire de la carte. Ni la Banque ni le processeur ne sont responsables des dommages résultant de l'utilisation illégale ou contraire au contrat de l'app one.

La responsabilité de la Banque est également exclue, dans la mesure permise par la loi, lorsque le titulaire de la carte, son conjoint, les membres de la famille directement liés (notamment les enfants et les parents) ou d'autres personnes proches du titulaire de la carte, des mandataires et/ou des personnes vivant dans le même ménage ont accompli une action (p. ex. confirmation dans l'app ou par code SMS).

B Partie spéciale

5. 3-D Secure

5.1 Qu'est-ce que 3-D Secure?

3-D Secure est une norme de sécurité internationalement reconnue pour les paiements par carte sur Internet. On l'appelle «SecureCode» chez MasterCard et «Verified by VISA» chez VISA. Le titulaire de la carte s'engage, en vertu des présentes dispositions, à utiliser cette norme de sécurité pour les paiements, dans la mesure où elle est proposée par le point d'acceptation (le commerçant).

L'utilisation de 3-D Secure n'est possible qu'après inscription chez one.

5.2 Comment fonctionne 3-D Secure?

Les paiements réalisés avec 3-D Secure peuvent être confirmés (autorisés) de deux manières:

– dans l'app one ou
– en saisissant un code que la Banque envoie au titulaire de la carte par message court (code SMS), dans la fenêtre correspondante du navigateur pendant le processus de paiement.

Conformément aux présentes dispositions relatives à l'utilisation de one, toute utilisation autorisée de la carte avec 3-D Secure est réputée effectuée par le titulaire de la carte.

5.3 Activation de cartes pour 3-D Secure

3-D Secure est activé par l'inscription sur one pour toutes les cartes libellées au nom du titulaire de la carte et liées à la relation d'affaires enregistrée du titulaire de la carte avec la Banque.

5.4 Désactivation de cartes pour 3-D Secure

Pour des raisons de sécurité, il n'est plus possible de désactiver 3-D Secure après l'activation.

6. Paiement mobile

6.1 Qu'est-ce que le paiement mobile?

Le paiement mobile désigne des solutions pour l'utilisation de cartes sur un appareil mobile. Le paiement mobile permet au titulaire de la carte disposant d'un appareil mobile compatible d'utiliser les cartes autorisées via une appli mobile (app) de la Banque (voir ch. 6.7) ou d'un prestataire tiers pour le paiement sans contact, ainsi que pour le paiement dans les boutiques en ligne et les applis.

Pour des raisons de sécurité, un numéro (token) différent est généré en lieu et place du numéro de la carte et enregistré comme «carte virtuelle». Les cartes virtuelles peuvent être utilisées comme une carte physique via le paiement mobile. Lors du paiement avec une carte virtuelle, le numéro de carte n'est pas transmis au commerçant, mais uniquement le numéro généré (token).

6.2 Quels appareils mobiles sont compatibles et quelles cartes sont approuvées?

Les appareils mobiles tels que les ordinateurs, les téléphones portables, les smartwatches et les trackers de fitness sont compatibles, pour autant qu'ils prennent en charge l'utilisation de cartes virtuelles et qu'ils soient approuvés par la Banque. La Banque décide en outre librement quelles cartes sont approuvées pour quels prestataires.

6.3 Activation et désactivation

Pour des raisons de sécurité, l'activation d'une carte exige que le titulaire de la carte accepte les conditions d'utilisation de la carte de débit ou de crédit du fournisseur concerné et qu'il prenne connaissance de ses dispositions en matière de protection des données. Le titulaire de la carte est tenu de rembourser la Banque en cas de dommages résultant d'une violation des présentes conditions.

Les cartes virtuelles peuvent être utilisées jusqu'à blocage ou désactivation de la carte via l'app par le titulaire de la carte. Les restrictions d'utilisation de la carte conformément aux dispositions applicables de la Banque Migros restent réservées. Le titulaire de la carte peut à tout moment mettre fin à l'utilisation du paiement mobile en supprimant sa (ses) carte(s) virtuelle(s) auprès du prestataire concerné.

Les coûts liés à l'activation et à l'utilisation de cartes virtuelles (p. ex. les coûts liés à l'utilisation mobile d'Internet à l'étranger) sont à la charge du titulaire de la carte.

6.4 Utilisation de la carte virtuelle (autorisation)

L'utilisation d'une carte virtuelle correspond à une transaction habituelle par carte. Toute utilisation d'une carte virtuelle est considérée comme autorisée par le titulaire de la carte.

L'utilisation de cartes virtuelles doit être autorisée selon les modalités prévues par le fournisseur ou le commerçant, p. ex. en saisissant le code PIN de l'appareil ou en identifiant les empreintes digitales ou le visage. Le titulaire de la carte prend acte du fait que cela accroît le risque que des cartes virtuelles puissent être utilisées par des personnes non autorisées lorsque le moyen d'autorisation supplémentaire requis par le fournisseur ou le distributeur (PIN de l'appareil ou PIN de la carte) se compose de combinaisons faciles à déterminer («1234»). Le titulaire de la carte prend acte du fait que, selon le prestataire ou le commerçant, aucune autorisation n'est exigée jusqu'à concurrence d'un montant à déterminer par celui-ci. Par ailleurs, la responsabilité est régie par le chiffre 4 de ces dispositions concernant l'utilisation de one.

6.5 Obligations de diligence particulières

Le titulaire de la carte prend acte et accepte que l'utilisation du paiement mobile présente des risques malgré toutes les mesures de sécurité. Il est notamment possible que la ou les cartes virtuelles et des données personnelles soient abusivement utilisées ou consultées par des personnes non autorisées. Cela peut nuire financièrement au titulaire de la carte (en raison de l'utilisation abusive d'une carte) et à sa personnalité (par l'abus de données personnelles).

Le titulaire de la carte doit donc traiter avec soin les appareils et les cartes virtuelles utilisés et veiller à leur protection. Outre les obligations de diligence conformément aux dispositions applicables de la Banque Migros et aux obligations générales de diligence et de déclaration énoncées aux ch. 3.2 et 3.3, le titulaire de la carte doit notamment respecter les obligations particulières de diligence suivantes:

- Les appareils employés doivent être utilisés et conservés à l'abri de tout accès de tiers, conformément à leur destination;
- comme les cartes physiques, les cartes virtuelles sont personnelles et non transférables. Elles ne doivent pas être transmises à des tiers pour utilisation (p. ex. en déposant des empreintes digitales ou en scannant le visage de tiers pour déverrouiller l'appareil utilisé);
- en cas de changement ou de transmission d'un appareil mobile (p. ex. en cas de vente), toute carte virtuelle doit être supprimée de l'app du fournisseur et de l'appareil mobile;
- tout soupçon d'utilisation abusive d'une carte virtuelle ou d'un appareil utilisé à cet effet doit être immédiatement signalé à la Banque afin que la carte virtuelle concernée puisse être bloquée.

6.6 Exclusion de la garantie

Il n'existe aucun droit à l'utilisation du paiement mobile. La Banque peut interrompre ou mettre fin à l'utilisation – c'est-à-dire la possibilité d'utiliser des cartes virtuelles – à tout moment, notamment pour des raisons de sécurité ou en cas de modification de l'offre du paiement mobile ou de limitation des cartes autorisées ou appareils compatibles. En outre, la Banque n'est pas responsable des actions et offres du prestataire ou d'autres tiers, tels que les fournisseurs d'accès à Internet et de téléphonie.

6.7 Utilisation de la carte via l'app one

Le titulaire de la carte disposant d'un appareil compatible peut activer sa (ses) carte(s) dans l'app one et l'utiliser comme carte virtuelle. Afin de garantir la sécurité du paiement mobile, le titulaire de la carte doit définir un code secret lors de l'activation. La Banque peut adapter ce service à tout moment. Par ailleurs, les présentes dispositions s'appliquent à l'utilisation de one pour le paiement mobile, en particulier les obligations particulières de diligence selon le ch. 6.5.

6.8 Protection des données paiement mobile

Le prestataire tiers et la Banque sont responsables de leur traitement des données personnelles en toute indépendance. Le titulaire de la carte prend acte du fait que les données personnelles liées à l'offre et à l'utilisation du paiement mobile (notamment les informations sur le titulaire et les cartes activées et les données de transaction issues de l'utilisation de cartes virtuelles) sont collectées par le prestataire tiers et stockées et traitées en Suisse ou à l'étranger. Le traitement des données personnelles par le prestataire tiers en relation avec le paiement mobile et l'utilisation d'offres et de prestations du tiers, y compris de ses appareils et logiciels, est régi par ses règles d'utilisation et de protection des données. Par conséquent, le titulaire de la carte confirme par chaque activation d'une carte qu'il a lu et compris les dispositions relatives à la protection des données du prestataire tiers concerné et qu'il accepte expressément le traitement des données du prestataire tiers. S'il ne souhaite pas le traitement correspondant, il incombe au titulaire de la carte de renoncer à l'activation d'une carte ou de s'opposer au traitement vis-à-vis du prestataire tiers. Les dispositions relatives à la protection des données ci-après sous C, les informations générales sur la protection des données de la Banque Migros SA ainsi que les dispositions et la déclaration relative à la protection des données pour l'utilisation de one du processeur de one s'appliquent au traitement des données personnelles par la Banque et le processeur.

C Déclaration relative à la protection des données one

Les dispositions suivantes en matière de protection des données vous informent de la manière dont la Banque traite vos données personnelles (ci-après dénommées «données») en tant que responsable. Le traitement comprend toute gestion de données personnelles, notamment l'acquisition, l'enregistrement, l'utilisation, la divulgation ou la suppression de données. Vous trouverez les détails relatifs à la protection et au traitement des données dans les informations générales sur la protection des données de la Banque Migros SA.

En s'inscrivant à one, les titulaires de cartes acceptent expressément les traitements de données contenus dans la présente déclaration relative à la protection des données. Dans les dispositions de la Banque Migros et dans les dispositions relatives à l'utilisation de one, vous trouverez des informations sur d'autres traitements de données dans le cadre de la relation de carte. Veuillez également tenir compte des déclarations mondiales de protection des données ainsi que de vos droits d'intervention en tant que tiers bénéficiaire de Mastercard® et Visa.

7. Traitement des données personnelles

7.1. De quoi s'agit-il dans la Déclaration relative à la protection des données?

Par l'intermédiaire du site internet ou de l'app, la Banque met à disposition, sous la dénomination «one», divers services de cartes liés à l'utilisation des cartes émises (collectivement «one digital services»). La fourniture des services de cartes nécessite un traitement par la

Banque des données des titulaires de cartes. La présente déclaration relative à la protection des données informe les titulaires de cartes de manière détaillée et transparente du traitement des données lors de l'utilisation des services numériques one.

7.2. Comment les données sont-elles collectées?

7.2.1 Quelles données du titulaire de la carte sont divulguées?

Lors de l'enregistrement pour les services numériques one, de l'inscription et de la gestion du compte utilisateur, le titulaire de la carte peut être invité à indiquer l'adresse e-mail, la date de naissance, le numéro de téléphone mobile, le numéro de carte et le code d'activation.

7.2.2 Quelles données sont collectées automatiquement?

- les données relatives à l'utilisation des appareils mobiles du titulaire de la carte, telles que le fabricant, le type d'appareil, le système d'exploitation avec numéro de version, l'ID de périphérique, l'adresse IP;
- les données relatives à l'utilisation d'ordinateurs et de navigateurs ainsi qu'à l'accès à Internet, telles que le type d'appareil, le système d'exploitation, l'adresse IP;
- les données relatives à l'utilisation du compte utilisateur, telles que le nombre de connexions avec la date et l'heure, les modifications du compte utilisateur, l'acceptation des dispositions relatives à l'utilisation des services numériques one et de la déclaration relative à la protection des données;
- les données relatives aux paramètres souhaités par le titulaire de la carte, telles que l'enregistrement du nom d'utilisateur ou du login;
- les données relatives aux visites et au comportement d'utilisation sur le site web et les données générées lors de l'utilisation de l'app, telles que les mises à jour ou informations sur l'appareil concernant le comportement d'utilisation, p. ex. dans l'app ou par code SMS

7.2.3 Quelles sont les informations collectées lors de l'enregistrement et de l'activation des services de cartes sur one?

- les informations sur le titulaire de la carte et sur ses cartes enregistrées pour one, qui sont stockées dans le compte utilisateur
- l'information selon laquelle 3-D Secure est utilisé pour les cartes enregistrées par une confirmation dans l'app ou par la saisie d'un code SMS
- l'adresse de livraison et le numéro de téléphone mobile

7.2.4 Quelles informations sont collectées lors de l'utilisation du paiement mobile?

- les informations relatives à l'utilisation du paiement mobile, telles que l'activation ou la désactivation de cartes et l'utilisation des cartes pour le paiement mobile
- les informations sur le montant de la transaction
- les informations relatives à l'utilisation de la carte, à la date de la transaction, au type de vérification

En cas d'utilisation d'une solution paiement mobile d'un prestataire tiers, celui-ci peut également collecter et traiter des données personnelles du titulaire de la carte. Selon l'offre, il s'agit notamment du nom, du numéro de carte et, le cas échéant, des données de transaction. À cet effet, il convient de respecter les dispositions d'utilisation et de protection des données du prestataire tiers.

7.2.5 Quelles informations sont collectées lors de l'utilisation de 3-D Secure?

- les informations relatives au distributeur, à la transaction et à son traitement ainsi qu'à la confirmation de la transaction avec 3-D Secure
- les informations relatives aux appareils utilisés pour la transaction et la confirmation
- les informations relatives à l'accès à Internet ou au réseau mobile, telles que l'adresse IP, le nom du fournisseur d'accès

7.2.6 Quelles données sont collectées lors de l'affichage de la section de carte de l'emplacement du commerçant?

- les données de localisation des distributeurs établis en Suisse
- les données de localisation, telles que le nom du distributeur, le lieu, le pays et le secteur d'activité
- la consultation périodique automatisée de Google pour préciser l'emplacement du commerçant

7.3. Dans quel but la Banque traite-t-elle mes données?

7.3.1 Fourniture des services de cartes et traitement du rapport de carte

- Permettre l'enregistrement, l'inscription et l'utilisation des services numériques one par le titulaire de la carte
- Mise en place d'une connexion sécurisée entre les services numériques one et l'appareil mobile du titulaire de la carte
- Transmission de demandes de confirmation, p. ex. pour confirmation de paiements en ligne via des services numériques one, par message push ou par code SMS au titulaire de la carte
- Transmission à la Banque de l'information sur les confirmations effectuées
- Authentification du titulaire de la carte lors de l'exécution d'actions. L'app ou l'appareil mobile utilisé sont clairement attribués au titulaire de la carte lors de l'enregistrement sur one. La Banque peut s'assurer que la confirmation a été effectuée dans l'app enregistrée ou avec l'appareil mobile enregistré
- Communication avec le titulaire de la carte et transmission d'informations relatives à la relation ou à l'utilisation de la carte, telles que des informations sur les nouvelles factures, alertes de fraude ou demandes en cas de transactions inhabituelles via les services numériques one et l'appareil mobile
- Réception des communications du titulaire de la carte
- Affichage des transactions et des factures
- Traitement de la relation contractuelle de carte avec le titulaire de la carte et les transactions effectuées avec la carte. À cet égard, il est fait référence à la déclaration relative à la protection des données de la Banque ainsi qu'aux dispositions relatives à l'utilisation de one.

7.3.2 Paiement mobile

- Pour la décision d'admission de la carte au paiement mobile
- Pour l'activation, la désactivation et l'actualisation des cartes pour le paiement mobile
- Pour prévenir toute utilisation abusive des cartes ajoutées
- Aux fins de la communication avec un éventuel prestataire tiers d'une solution paiement mobile dans le cadre des présentes dispositions relatives à l'utilisation de one et des dispositions relatives à l'utilisation ou à la protection des données du prestataire concerné, qui s'appliquent au rapport entre le titulaire de la carte et le prestataire tiers.

7.3.3 Marketing

- Pour relier ces données à des données déjà détenues par la Banque (y compris des données provenant de sources tierces)
- Pour créer des profils individuels de clients, de consommation et de préférences de profil permettant à la Banque de développer et de proposer des produits et des services au titulaire de la carte
- Pour transmettre des informations sur les produits et services existants ou nouveaux de la Banque et de tiers (matériel publicitaire) au titulaire de la carte

– Pour le traitement par le prestataire tiers dans le cadre de ses propres dispositions d'utilisation ou de protection des données

7.3.4 Autres objectifs de traitement
- Calcul des risques de crédit et de marché pertinents pour l'opération
- Améliorer la sécurité de l'utilisation des services de cartes, par exemple en réduisant le risque de transactions abusives ou d'abus de matériel ou de moyens de légitimation tels que l'hameçonnage ou le piratage
- Prouver les actions et défendre les réclamations contre la Banque
- Améliorer les prestations générales de la Banque et les services numériques one
- Respect des exigences légales et réglementaires
- Traitement par le prestataire tiers à ses propres fins dans le cadre de ses propres dispositions d'utilisation ou de protection des données

7.4. Mes données seront-elles divulguées à d'autres destinataires?

7.4.1 Transmission à des tiers ou collecte de données par des tiers

Les tiers sont des personnes ou des entreprises qui traitent des données à leurs propres fins. Aucun tiers n'est un prestataire de services mandaté par la Banque. En ce qui concerne les cartes auxquelles s'appliquent les dispositions de la Banque Migros, la Banque ne transmet en principe aucune donnée – en particulier aucune donnée de transaction – à des tiers à des fins propres à moins que le titulaire de la carte n'ait consenti à une telle transmission ou qu'il ne l'ait demandée ou organisée lui-même. En particulier, la Banque ne transmet pas de profils individuels de clients, de consommation et de préférences qu'elle a établis sans le consentement séparé et exprès du titulaire de la carte à des tiers. Si et dans la mesure où une transmission de données est admissible au regard des présentes dispositions d'utilisation de one, notamment du présent chiffre 7.4., le titulaire de la carte dispense la Banque du secret bancaire à cet égard.

7.4.2 Autres catégories de tiers auxquels les données sont divulguées
- Les données (y compris les données de transaction) du titulaire de la carte supplémentaire peuvent être divulguées au titulaire de la carte principale
- Les données du titulaire d'une Business Card peuvent être communiquées à l'entreprise
- Personnes mandatées par le titulaire de la carte
- Sur ordre des autorités ou en vertu d'obligations légales, la Banque transmet des données à des organismes publics tels que les autorités de poursuite pénale ou de surveillance

7.4.3 Transmission des données de titulaires de cartes par l'utilisation du paiement mobile
- Les données relatives à la carte et aux transactions nécessaires au traitement de la transaction sont transmises via les serveurs des organisations de cartes durant le processus de paiement. Vous trouverez plus d'informations sur le traitement et la transmission de données ainsi que sur le recours à des tiers dans les dispositions de la Banque Migros.
- Lors de l'utilisation du paiement mobile par l'intermédiaire d'un tiers, le tiers collecte et traite des données conformément à ses propres conditions d'utilisation ou de protection des données.

7.4.4 Transmission électronique de données

Lors de l'utilisation du transfert électronique de données, les données du titulaire de la carte peuvent également parvenir à des tiers (en Suisse et à l'étranger) sans l'intervention de la Banque.

En particulier lors de l'utilisation de l'app et/ou des appareils mobiles, les fabricants d'appareils ou de logiciels (comme Apple ou Google) peuvent obtenir des données à caractère personnel. Ceux-ci peuvent traiter et transmettre les données conformément à leurs propres règles d'utilisation ou de protection des données. Par conséquent, ces tiers peuvent en déduire une relation entre le titulaire de la carte et la Banque. Les SMS sont soumis aux dispositions légales en vigueur en matière de surveillance des télécommunications et sont enregistrés sur le téléphone mobile. Cela permet à des tiers de détenir les informations correspondantes.

7.5. Comment protégeons-nous vos données?

La transmission d'informations entre la Banque, le processeur et l'app et/ou les appareils mobiles du titulaire de la carte (mais pas l'envoi de SMS) est cryptée. Toutefois, la communication avec le titulaire de la carte s'effectue par le bais des réseaux publics de communication. Ces données sont en principe accessibles à des tiers, peuvent être perdues pendant le transfert ou interceptées par des tiers non autorisés. Il n'est donc pas exclu que des tiers aient accès à la communication avec le titulaire de la carte lorsqu'ils utilisent one malgré toutes les mesures de sécurité. Lors de l'utilisation d'Internet, il est également possible de transmettre des données à des pays tiers qui peuvent ne pas offrir le même niveau de protection des données que la Suisse lorsque le propriétaire est en Suisse.

La sécurité des données dépend également de la participation du titulaire de la carte. Le titulaire de la carte doit donc utiliser les moyens dont il dispose pour protéger ses appareils et ses données. Les obligations de diligence et de déclaration à respecter au minimum sont énoncées au point A. Des mesures de sécurité appropriées accroissent la sécurité et réduisent encore les risques liés à l'utilisation de one.

7.6. Quels sont vos droits en rapport avec vos données?
- Renseignements sur les informations relatives à vos données personnelles et à la façon dont la Banque les traite
- Correction de données personnelles inexactes ou incomplètes
- Suppression de vos données personnelles
- Limitation du traitement de vos données
- Dépôt d'une plainte auprès de l'autorité compétente concernant la manière dont vos données personnelles sont traitées
- Opposition ou révocation de votre consentement au traitement de vos données personnelles

La Banque ne peut accorder vos droits que dans le respect des exigences légales. Même si vous révoquez par exemple votre consentement, vos données personnelles peuvent continuer à être traitées dans la mesure requise par la loi.

7.7. Combien de temps la Banque stocke-t-elle les données?

La Banque conserve vos données tant qu'elles sont nécessaires à l'objectif pour lequel elles ont été collectées. La Banque stocke également des données personnelles lorsqu'il existe un intérêt légitime à les stocker, p. ex. lorsque les données sont nécessaires pour faire valoir ou refuser des droits, pour garantir la sécurité informatique, ou lorsque des délais de prescription expirent ou qu'une suppression n'est pas encore possible sur le plan technique. Enfin, vos données sont stockées pour se conformer aux obligations légales et réglementaires.

Version 9/2021