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

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 sous la dénomination **«one»** par la Banque Migros SA (ci-après dénommée **«banque»**) au demandeur / à la demandeuse et au / à la titulaire (ci-après collectivement dénommés **«personne ayant droit à 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)»**. one est exploité par Viseca Payment Services SA (ci-après **«processeur»**) pour le compte de la banque. La banque fait appel au processeur pour l'accomplissement dans l'accomplissement de certaines tâches dans le domaine des cartes. Dans ce cadre, le processeur traite les données (des clients et clientes de la banque) pour le compte de la banque.

one est accessible:
- sur le site internet one (ci-après dénommé **«site internet»**) et
- via l'app one (ci-après dénommée **«app»**)

Concernant l'utilisation de one, il convient de respecter également – selon le produit de carte choisi – les **Informations générales concernant la protection des données à la Banque Migros SA** (disponibles sur migrosbank.ch/fr/a-propos-de-nous/informations-legales) et les **Informations concernant la protection des données pour la carte de crédit Cumulus de la Banque Migros SA** (disponibles sur cumulus.banquemigros.ch/documents).

Les présentes Dispositions relatives à l'utilisation de one s'appliquent en sus des dispositions applicables à l'utilisation de cartes de la banque en fonction du produit choisi (Conditions générales de la Banque Migros SA, conditions d'utilisation des cartes de débit ou des cartes de crédit pour particuliers ou de Business Cards de la Banque Migros SA ou conditions d'utilisation de la carte de crédit Cumulus, ci-après dénommées collectivement **dispositions de la Banque Migros**).

L'utilisation de one suppose l'enregistrement de la personne ayant droit à la carte. Les présentes Dispositions relatives à l'utilisation de one sont réputées acceptées dès que la personne ayant droit à la carte s'enregistre sur l'app one ou sur le site internet one et confirme ces dispositions directement ou indirectement (en lançant ou en poursuivant le processus d'inscription ou de demande).

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 à la personne ayant droit à la carte (par exemple via one ou par e-mail). Si la personne ayant droit à la carte n'accepte pas les modifications apportées aux Dispositions relatives à l'utilisation de one, l'app ou le site internet ou certains services liés à la carte ne pourront pas ou plus être utilisés, selon les circonstances.

1.2 Qu'est-ce que one et comment le développe-t-on?
one comprend un processus d'onboarding numérique pour les nouveaux clients et clientes ainsi que des 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 de la personne ayant droit à la carte enregistré(e) au moyen de mises à jour. La banque informera la personne ayant droit à la carte de manière appropriée (p. ex. via one ou par e-mail) 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?
En fonction du produit de carte choisi, one peut notamment comprendre les fonctions suivantes, actuelles ou futures:

- onboarding numérique pour les nouveaux clients et clientes (voir chiffre 5);
- compte utilisateur pour la gestion des données personnelles;
- contrôle et confirmation de paiements, p. ex. via 3-D Secure (Mastercard SecureCode ou Verified by Visa) dans l'app ou par saisie d'un code SMS (voir chiffre 6.2);
- contrôle et confirmation de certaines opérations (p. ex. connexion, contacts avec la banque) dans l'app ou en saisissant un code SMS;
- activation de cartes pour l'utilisation de possibilités de paiement (voir chiffre 7);
- activation de cartes pour Click to Pay (voir chiffre 8);
- échange de communications et de notifications de toute nature entre la personne ayant droit à la carte et la banque (y compris communication d'une modification des dispositions), à moins qu'une forme particulière de communication ou de notification ne soit réservée (p. ex. contestation écrite d'une facture mensuelle);
- aperçu des transactions ou des cartes et affichage électronique des factures;
- aperçu du compte du programme de bonus et possibilité d'encaisser des points (actuellement compte surprize);
- informations relatives à l'utilisation de la carte (actuellement services SMS).

1.4 Avantages de one
one est censé offrir plusieurs avantages aux personnes ayant droit à la carte:

- one rend l'accès aux services de cartes plus sûr: une procédure moderne d'authentification de la personne ayant droit à la carte permet de vérifier et de confirmer que les actions ont effectivement été effectuées par celui-ci/celle-ci – en utilisant le téléphone mobile comme deuxième facteur (en plus du login) et par un canal de communication sécurisé entre le/la personne ayant droit à la carte et la banque;
- one regroupe les services de cartes de la banque sur une plateforme uniforme, ce qui rend leur présentation plus claire;
- one facilite l'accès aux différents services de cartes de la banque: l'identifiant 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/la personne ayant droit à la carte n'est autorisé(e) à utiliser one que dans les conditions suivantes:

- il/elle 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 (voir en particulier chiffres 3.2.1 et 3.2.3), et
- il/elle souhaite demander une carte dans le cadre du parcours numérique de demande, ou est autorisé(e) à en utiliser une.

2.2 Autorisations donnés lors de l'enregistrement de one
En acceptant les présentes Dispositions relatives à l'utilisation de one ou en utilisant one, le/la personne ayant droit à la carte donne expressément les consentements suivants à la banque (pour les consentements du parcours de demande numérique, voir en complément chiffre 5):

- consentement au traitement des données collectées 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. communication de changement 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, injonctions officielles 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, la personne ayant droit à la carte libère la banque du secret bancaire.

Le consentement de la personne ayant droit à 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/celle-ci par communication écrite à la banque avec effet à l'avenir (droit d'opt-out). Les coordonnées sont fournies dans les Informations concernant la protection des données à la Banque Migros SA.

2.3 Rejet des autorisations dans le cadre de la poursuite du développement de one
Si la personne ayant droit à la carte refuse de donner son consentement aux Dispositions relatives à l'utilisation de one dans le cadre du développement de l'app (p. ex. en cas de mises à jour), l'app ou le site internet ou certains services de cartes de ces derniers ne pourront pas ou plus être utilisés selon les circonstances.

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 de la personne ayant droit à la carte. La personne ayant droit à la carte s'engage ainsi de manière contraignante pour les achats, transactions ou autres opérations effectuées et pour les débits de sa carte en résultant. Il/elle autorise la banque à exécuter les ordres correspondants et à effectuer les actes correspondants.

2.5 Disponibilité/blocage/modifications
La banque peut à tout moment interrompre, restreindre, 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 de la personne ayant droit à la carte à one de manière temporaire ou définitive (p. ex. en cas de soupçon d'utilisation abusive ou de non-respect des obligations de diligence par la personne ayant droit à 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 relatives à l'utilisation de one. Les noms et logos visibles sur one sont des marques protégées.

Pour l'utilisation de l'app, la banque accorde à la personne ayant droit à la carte une licence non exclusive, non transférable, indéterminée, révocable et gratuite pour télécharger l'app, l'installer sur un appareil détenu en permanence par la personne ayant droit à la carteet l'utiliser dans le cadre des fonctions prévues.

Pour l'utilisation du site internet du processeur, les **dispositions relatives aux licences** (disponible sur https://viseca.ch/fr/app-pages/licensing-fr) conformément aux **conditions d'utilisation** (disponible sur https://viseca.ch/fr/conditions-utilisation/viseca) de son site internet (sous le titre «Propriété du site internet, droits de marque et droits d'auteur») s'appliquent en outre.

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

3.1 Risques liés à l'utilisation de one
La personne ayant droit à la carte prend acte et accepte que l'utilisation de one comporte des risques.

Il est notamment possible que des tiers non autorisés abusent lors de l'utilisation de cartes one, de l'identifiant et du mot de passe, des appareils utilisés ou des données personnelles de la personne ayant droit à la carte. Cela peut entraîner un préjudice financier pour la personne ayant droit à la carte (en raison du débit de la carte) ainsi qu'un préjudice moral (dû à une utilisation abusive des données personnelles). De plus, le risque existe que one ou l'un des services de cartes offerts sur one ne puissent pas être utilisés (p. ex. pas de connexion sur one possible).

Les utilisations abusives sont rendues possibles ou favorisées notamment par:

- le non-respect des obligations de diligence ou de déclaration par la personne ayant droit à la carte (par exemple, en raison d'une utilisation imprudente de l'identifiant et du mot de passe ou de la non-déclaration de perte de la carte);
- les paramètres choisis par la personne ayant droit à 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), par exemple en raison d'absence 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);
- des paramètres de sécurité plus faibles choisis par la personne ayant droit à la carte pour one – en particulier pour l'app – (p. ex. enregistrement du login).

En respectant 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, la personne ayant droit à la carte peut réduire ces risques d'utilisation abusive.

La banque ne garantit pas que le site internet et l'app soient accessibles en permanence ou fonctionnent sans problème, ou que des utilisations abusives puissent être détectées et évitées avec certitude.

3.2 Obligations générales de diligence de la personne ayant droit à 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») de la personne ayant droit à la carte à des fins d'authentification. La détention de ces appareils mobiles à tout moment est donc un facteur de sécurité essentiel. La

personne ayant droit à la carte doit traiter les appareils mobiles avec un soin approprié et veiller à leur protection.

Par conséquent, la personne ayant droit à 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 transmis 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 sécurité 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 les données notamment via «Rechercher mon iPhone» ou «Gestionnaire des appareils Android», en réinitialisant ou en faisant réinitialiser le compte utilisateur). La perte doit être signalée à la banque (voir chiffre 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 one
Outre la possession de l'appareil mobile, l'identifiant et le mot de passe servent également de facteurs d'authentification de la personne ayant droit à la carte.

La personne ayant droit à la carte doit notamment respecter les obligations générales de diligence suivantes en rapport avec le mot de passe:

- la personne ayant droit à la carte doit définir un mot de passe qu'il/elle n'a pas déjà utilisé pour d'autres services et qui n'est pas constitué de combinaisons facilement identifiables (sont p. ex. interdits le numéro de téléphone, la date de naissance, la plaque d'immatriculation, le nom de la personne ayant droit à la carte ou de ses proches, les répétitions ou suites de chiffres ou de lettres comme «123456» ou «aabbcc»);
- le mot de passe doit être tenu secret. Il ne peut être divulgué ou mis à la disposition de tiers. La personne ayant droit à la carte prend acte du fait que la banque ne lui demandera jamais de lui communiquer son mot de passe;
- le mot de passe ne doit pas être écrit ni enregistré de manière non sécurisée;
- la „personne ayant droit à la carte doit modifier son mot de passe ou réinitialiser son compte utilisateur ou le faire réinitialiser par la banque s'il / si elle soupçonne 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
La confirmation dans l'app ou par la saisie d'un code SMS engage la personne ayant droit à la carte.

La personne ayant droit à la carte doit donc respecter les obligations générales de diligence suivantes en rapport avec les confirmations réalisées dans l'app ou par la saisie d'un code SMS:

- la personne ayant droit à 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) de la personne ayant droit à la carte;
- la personne ayant droit à 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 et Click to Pay, les détails de paiement affichés, en particulier, doivent être contrôlés.

3.3 Obligations générales de déclaration de la personne ayant droit à la carte
Les événements suivants doivent être immédiatement signalés à la banque:

- la perte d'un appareil mobile, mais pas le fait de ne pas le trouver durant un court moment;
- les demandes de confirmation qui ne sont pas liées à un paiement en ligne, à une connexion par la personne ayant droit à la carte, à un contact avec la banque ou à des opérations similaires (soupçon d'utilisation abusive);
- tout autre soupçon que les demandes de confirmation dans l'app ou le code SMS ne proviennent pas de la banque;
- le soupçon d'utilisation abusive d'identifiant, 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 d'appareil mobile utilisé pour one (dans ce cas, l'app doit être réenregistrée).

Les éventuelles utilisations abusives ou la perte d'un appareil mobile doivent être immédiatement signalées par téléphone à la hotline de la banque chargée du blocage des cartes (24 h / 24): +41 800 811 820.

4. Responsabilité

Sous réserve de ce qui suit, la banque rembourse les dommages liés à l'utilisation de one (sans franchise) qui ne sont pas couverts par une assurance de la personne ayant droit à 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 la personne ayant droit à la carte (p. ex. ordinateurs, appareils mobiles et autres infrastructures informatiques), et
  - la personne ayant droit à la carte a respecté les obligations générales et particulières de diligence et de déclaration énoncées aux chiffres 3.2, 3.3 et 7.5, en particulier les obligations de contrôle des demandes de confirmation et l'obligation de vérification de la facture mensuelle prévues dans les dispositions de la Banque Migros ainsi que la contestation en temps utile de transactions abusives, et
  - la personne ayant droit à la carte ne commet, par ailleurs, aucune faute imputable à 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 décline toute responsabilité quant aux éventuels dommages indirects, perte de gain, perte de données ou dommages consécutifs de quelque nature que ce soit subis par la personne ayant droit à la carte, dans la mesure où la banque n'a pas agi par négligence grave ou de manière intentionnelle. Ni la banque ni le processeur ne sont responsables des dommages résultant de l'utilisation illégale ou contraire au contrat de l'app one par la personne ayant droit à la carte.

La responsabilité de la banque est également exclue si le/la conjoint(e), les membres de la famille proche (en particulier les enfants et les parents) ou d'autres proches de la personne ayant droit à la carte, les mandataires et/ou les personnes vivant sous le même toit ont accompli une action (p. ex. confirmation dans l'app ou par code SMS).

B Partie spéciale

5. Processus de commande numérique et service d'identification numérique

5.1 Commande numérique d'une carte de crédit Cumulus et utilisation du service d'identification
La banque offre aux personnes physiques domiciliées en Suisse ainsi qu'à certaines personnes domiciliées dans quelques pays frontaliers, en tant que personnes ayant droit à la carte, la possibilité de commander en ligne une carte de crédit Cumulus et d'utiliser pour cela le service d'identification numérique de la société Intrum SA (ci-après dénommée **«Intrum»**) mandatée par le processeur.

En demandant une carte de crédit Cumulus et en participant au processus de demande numérique, les personnes ayant droit à la carte prennent connaissance du fait que les données personnelles (des titulaires de la carte principale et des cartes supplémentaires, p. ex. nom et prénom, sexe, date de naissance, lieu de naissance, nationalité, numéro de pièce d'identité, autorité émettrice, adresse e-mail, numéro de téléphone) sont traitées, enregistrées et transmises par la banque à des tiers (p. ex. processeur, Intrum, Fédération des coopératives Migros [FCM] et les services d'analyse en ligne mentionnés ci-dessous) dans le cadre du processus de demande, et l'acceptent. Ces données seront également transmises à des tiers (p. ex. processeur, Centrale d'information de crédit [ZEK], autorités [p. ex. offices des poursuites et administrations fiscales, contrôle des habitants, autorités de protection de l'adulte], à des sociétés de renseignements économiques (comme notamment CRIF SA), à l'employeur, à d'autres sociétés de la Fédération des coopératives Migros ou à d'autres organes d'information et de renseignement prévus par la loi [Centre de renseignements sur le crédit à la consommation, IKO] en vue de l'examen des indications fournies ci-dessus et en particulier dans le cadre de l'examen de solvabilité exigé avant toute émission de carte).

La FCM traite ces données ainsi que d'autres données de la FCM sous sa propre responsabilité, conformément à la **Déclaration de protection des données Migros** (disponible sur privacy.migros.ch/fr). La FCM traite ces données notamment afin de pouvoir attribuer des cartes à des comptes Migros existants et pour optimiser le processus de demande (analyse des interruptions de demande). Pour de plus amples informations sur la divulgation des données, voir les **Informations concernant la protection des données pour la carte de crédit Cumulus de la Banque Migros SA** (disponibles sur cumulus.banquemigros.ch/documents).

Lors de l'utilisation de l'app one et du site internet cumulus.banquemigros.ch, les prestataires tiers suivants sont associés (par le processeur, la banque et/ou la FCM) aux activités d'analyse en ligne destinées à optimiser le parcours de demande:

Google Analytics et Google Firebase
Sur les pages de son propre site internet, la Banque Migros SA utilise Google Analytics, un service d'analyse fourni par Google LLC (1600 Amphitheatre Parkway, Mountain View, CA, USA) et Google Ireland Ltd. (Google Building Gordon House, Barrow St, Dublin 4, Irlande; tous deux dénommés «Google», Google Ireland Ltd. étant responsable du traitement des données personnelles). Google utilise des cookies et des technologies similaires pour recueillir certaines informations sur le comportement des utilisateurs et utilisatrices sur le site internet concerné et sur le terminal utilisé (tablette, PC, smartphone, etc.) (par exemple, le nombre d'ouvertures de la page internet, le nombre d'achats effectués, les centres d'intérêt ainsi que des données sur le terminal utilisé, p. ex. le système d'exploitation). De plus amples informations figurent sur ce **lien**.

Les données sont également utilisées à la fin ou à l'interruption du processus de demande afin de recueillir des statistiques, d'améliorer le processus de demande et pour les échanges commerciaux avec vous (voir chiffre 9).

Le service d'identification sert à identifier les personnes physiques et à vérifier les documents d'identité officiels dans le cadre de la commande numérique de cartes de paiement.

En vertu de dispositions légales (notamment la loi sur le blanchiment d'argent et la loi fédérale sur la signature électronique), la banque est tenue d'établir l'identité de la personne ayant droit à la carte dans le processus de commande numérique. L'identification fait appel à un logiciel d'identification sous licence d'une société tierce. Le service d'identification est disponible à la fois sur le site internet et via l'app one.

5.2 Processus d'identification
Le service d'identification est géré par le système et le processus, la vérification des documents d'identité pouvant également s'effectuer manuellement. Les différentes étapes du processus d'identification sont les suivantes:

- avec l'utilisation du service d'identification, un numéro d'identification est attribué à la personne physique; au moyen d'un masque de saisie prédéfini, la banque (ou le processeur désigné par celle-ci) recueille directement auprès de la personne ayant droit à la carte des données personnelles (telles que nom et prénom, sexe, date de naissance, lieu de naissance, nationalité, numéro de pièce d'identité, autorité émettrice, adresse postale, adresse e-mail, numéro de téléphone) qui sont appropriées et nécessaires pour vérifier son identité. Les données ainsi recueillies sont transmises à Intrum. Sur mandat de la banque, les données recueillies peuvent être transmises à d'autres sous-traitants pour le traitement ultérieur;
- la personne ayant droit à la carte utilise un terminal (p. ex. un PC, une tablette ou un smartphone) pour prendre en photo le document d'identité à l'aide de la caméra intégrée. Intrum compare les données recueillies par la banque (ou par le processeur mandaté par elle) au document d'identité téléchargé (p. ex. carte d'identité, passeport, permis de conduire). Dans un second temps, en fonction de la configuration, des photos du visage de la personne ayant droit à la carte sont prises avec le logiciel sous licence et comparées au document d'identité. Ces comparaisons peuvent être automatisées ou manuelles.

La banque ne peut procéder à l'identification de la personne ayant droit à la carte que si tous les documents nécessaires à la vérification et demandés par Intrum dans le cadre du processus de commande sont mis à disposition par la personne ayant droit à la carte.

Les données recueillies lors du processus d'identification sont supprimées des serveurs d'Intrum dans les 90 jours.

5.3 Obligations du/de la personne ayant droit à la carte
La personne ayant droit à la carte est tenue de remettre à la banque tous les documents nécessaires à la prestation du service d'identification, conformément au chiffre 5 des présentes dispositions, et de saisir correctement toutes les informations contenues dans les champs de données mis à disposition.

L'utilisation du service d'identification nécessite un terminal approprié (par exemple un ordinateur, un smartphone ou une tablette) et une connexion internet. Si la personne ayant droit à la carte souhaite utiliser le service d'identification via un terminal mobile, cela n'est possible qu'en utilisant l'app one. Il incombe à la personne ayant droit à la carte de garantir l'efficacité et la compatibilité du terminal concerné.

La personne ayant droit à la carte doit garder secrètes les données mises à sa disposition (p. ex. numéro de procédure) et les protéger contre toute utilisation par des tiers non autorisés. La personne ayant droit à la carte doit informer sans délai la banque en cas de soupçon d'utilisation abusive de ses données.

5.4 Consentement à la collecte, à la transmission, au stockage et à la suppression des données dans le cadre du processus de commande numérique et du service d'identification numérique

Lors de la collecte, du traitement et de l'utilisation de données personnelles (telles que nom et prénom, sexe, date de naissance, lieu de naissance, nationalité, numéro de pièce d'identité, autorité émettrice, adresse postale, adresse e-mail, numéro de téléphone) à des fins d'identification, d'examen de la solvabilité et de conformité à la loi sur le blanchiment d'argent, la banque collabore avec des sous-traitants en Suisse et en Europe.

Lors du processus de vérification, la personne ayant droit à la carte utilise un terminal (PC, tablette ou smartphone) pour prendre une photo de son document d'identité à l'aide de la caméra intégrée. Le processus de vérification et d'identification ainsi que les étapes correspondantes et le traitement des données y afférent sont expliqués ci-après. Pour l'exécution de ces processus, la banque a besoin, en principe, des données suivantes de la personne ayant droit à la carte: nom et prénom, adresse, date de naissance, lieu de naissance, numéro de téléphone, adresse e-mail. Ces données sont saisies par la personne ayant droit à la carte sur le site internet **cumulus.banquemigros.ch** ou dans l'app one. Au cours du processus d'identification, des photos du document d'identité sont prises afin de comparer les données reçues précédemment à celles figurant sur le document d'identité. Les données recueillies par la banque diffèrent selon le document d'identité et le cas d'application de la personne ayant droit à la carte. En ce qui concerne les passeports et les cartes d'identité, le prénom et le nom, le sexe et la date de naissance sont notamment recueillis. Aux fins de l'identification au titre de la loi sur le blanchiment d'argent, l'autorité émettrice, le numéro de la pièce d'identité, la nationalité et l'adresse de la personne ayant droit à la carte sont également relevés. Outre les données de la personne ayant droit à la carte, la banque enregistre également les photographies des documents d'identité. Dans un second temps, en fonction de la configuration, des photos du visage de la personne ayant droit à la carte sont prises avec le logiciel sous licence et comparées au document d'identité.

Les données sont supprimées du serveur d'Intrum 90 jours après la fin de leur examen et de l'identification. Conformément aux délais légaux de conservation (p. ex. dans le cadre de la loi sur le blanchiment d'argent), les données peuvent rester enregistrées à la banque pendant au moins 10 ans après la fin de la relation d'affaires entre la personne ayant droit à la carte et la banque.

6. 3-D Secure

6.1 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. La personne ayant droit à 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.

6.2 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 à la personne ayant droit à 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 la personne ayant droit à la carte.

6.3 Activation de cartes pour 3-D Secure

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

6.4 Pas de 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.

7. Paiement mobile

7.1 Qu'est-ce que le paiement mobile?

Le paiement mobile permet à la personne ayant droit à la carte disposant d'un appareil mobile compatible (ci-après «appareil mobile») d'utiliser les cartes autorisées via une app mobile (app) de la banque (voir chiffre 7.7) ou d'un prestataire tiers pour le paiement sans contact, ainsi que pour le paiement dans les boutiques en ligne et les apps.
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).

7.2 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.

7.3 Activation et désactivation

Pour des raisons de sécurité, l'activation d'une carte est conditionnée à l'acceptation des **dispositions de la Banque Migros** en vigueur et à la prise de connaissance des Dispositions relatives à la protection des données par la personne ayant droit à la carte (voir chiffre 1.1).

Les cartes virtuelles peuvent être utilisées jusqu'à leur blocage ou leur désactivation par le/la titulaire ou la banque. Les restrictions d'utilisation de la carte conformément aux dispositions applicables de la Banque Migros restent réservées. La personne ayant droit à la carte peut cesser d'utiliser le paiement mobile à tout moment en supprimant sa ou (ses) carte(s) virtuelle(s) sur les appareils compatibles.

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 de la personne ayant droit à la carte.

7.4 Utilisation de la carte virtuelle (autorisation)

L'utilisation d'une carte virtuelle correspond à une transaction habituelle par carte. Chaque utilisation de la carte virtuelle est réputée autorisée par la personne ayant droit à la carte.

L'utilisation de cartes virtuelles doit être autorisée selon les modalités prévues par le prestataire (p. ex. du système de paiement mobile choisi) ou par le commerçant, p. ex. en saisissant le code NIP de l'appareil ou en identifiant les empreintes digitales ou le visage. La personne ayant droit à 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 prestataire ou le commerçant (NIP de l'appareil ou de la carte) se compose de combinaisons faciles à deviner (comme «1234»). La personne ayant droit à 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. Du reste, la responsabilité est régie par le chiffre 4 des Dispositions relatives à l'utilisation de one.

7.5 Obligations de diligence particulières

La personne ayant droit à la carte prend acte du fait que l'utilisation du paiement mobile présente des risques malgré toutes les mesures de sécurité et l'accepte. 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 entraîner un préjudice financier pour la personne ayant droit à la carte (en raison de l'utilisation abusive de la carte) ainsi que subir une atteinte illicite à sa personnalité (due à une utilisation abusive des données personnelles).

La personne ayant droit à la carte doit donc traiter avec soin les appareils et cartes virtuelles utilisés, et veiller à leur protection. Outre les obligations de diligence énoncées dans les dispositions applicables de la Banque Migros et les obligations générales de diligence et de déclaration énoncées aux chiffres 3.2 et 3.3, la personne ayant droit à la carte est, en particulier, tenu(e) de se conformer aux obligations 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 compatible (p. ex. en cas de vente), toute carte virtuelle doit être supprimée de l'app du prestataire et de l'appareil compatible;
- 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.

7.6 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 prestataires d'accès à Internet et de téléphonie.

7.7 Utilisation de la carte via l'app one

La personne ayant droit à la carte disposant d'un appareil compatible peut activer sa ou ses carte(s) dans l'app one et l'utiliser comme carte virtuelle. Afin de garantir la sécurité du paiement mobile, la personne ayant droit à 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 les paiements mobiles, en particulier les obligations particulières de diligence selon le chiffre 7.5.

7.8 Protection des données en cas de paiement mobile

Le prestataire tiers (en particulier le prestataire du système de paiement mobile) et la banque sont responsables du traitement des données personnelles en toute indépendance. La personne ayant droit à 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 ou la titulaire et les cartes activées ainsi que les données de transaction issues de l'utilisation de cartes virtuelles) sont recueillies 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, la personne ayant droit à la carte confirme par chaque activation d'une carte qu'il/elle a lu et compris les dispositions relatives à la protection des données du prestataire tiers concerné et qu'il/elle accepte expressément le traitement des données du prestataire tiers. S'il / si elle refuse ce traitement, il lui incombe de renoncer à l'activation d'une carte ou de s'opposer au traitement auprès du prestataire tiers. Le traitement des données personnelles par la banque et le processeur est soumis aux Dispositions relatives à la protection des données énoncées au point C ci-dessous ainsi qu'aux **Informations générales concernant la protection des données à la Banque Migros SA** (disponibles sur migrosbank.ch/fr/a-propos-de-nous/informations-legales).

8. Click to Pay

8.1 Qu'est-ce que Click to Pay?

Click to Pay sert à faciliter le paiement des achats en ligne. Il s'agit d'une initiative des organisations de cartes internationales Mastercard et Visa (organisations de cartes). Pour pouvoir utiliser Click to Pay, il est nécessaire d'enregistrer la carte ainsi que l'adresse e-mail et l'adresse de livraison auprès de l'organisation de cartes. Une fois l'enregistrement accompli, la personne ayant droit à la carte peut effectuer l'achat en ligne avec l'adresse e-mail, dans la mesure où le symbole Click to Pay apparaît. Par la suite, il n'est plus nécessaire de saisir les détails de la carte.

8.2 Activation et désactivation

La personne ayant droit à la carte peut enregistrer des cartes pour Click to Pay dans l'app one. L'enregistrement suppose que la personne ayant droit à la carte a pris connaissance des dispositions relatives à l'utilisation et à la protection des données de l'organisation de cartes, et qu'elle les a acceptées.

Lors de l'enregistrement d'une carte, la personne ayant droit à la carte accepte que des informations relatives à sa carte, son nom et ses coordonnées telles que l'adresse de facturation et de livraison, l'adresse e-mail et le numéro de téléphone soient transmis à l'organisation de cartes. Les informations relatives aux cartes et les coordonnées enregistrées pour le paiement peuvent être modifiées et supprimées à tout moment dans le compte utilisateur de Click to Pay.

La personne ayant droit à la carte peut mettre fin à l'utilisation de Click to Pay à tout moment en supprimant les cartes enregistrées dans l'app one ou auprès de l'organisation de cartes.

Les frais liés à l'activation et à l'utilisation de Click to Pay sont à la charge de la personne ayant droit à la carte.

8.3 Utilisation de Click to Pay

Les dispositions relatives à l'utilisation et à la protection des données ainsi que les instructions de l'organisation de cartes concernée s'appliquent à l'utilisation de Click to Pay. Les organisations de cartes peuvent développer, limiter ou bloquer Click to Pay à tout moment.

La banque n'est pas responsable des dommages résultant de l'utilisation de Click to Pay. Chaque transaction déclenchée par Click to Pay est considérée comme autorisée par la personne ayant droit à la carte.

Étant donné que l'adresse de livraison enregistrée pour Click to Pay peut ne pas correspondre à l'adresse de livraison souhaitée, la personne ayant droit à la carte est tenue de vérifier l'adresse de livraison indiquée au commerçant dans le cadre du processus de paiement avec Click to Pay.

8.4 Exclusion de garantie
Il n'y a aucun droit à l'utilisation de Click to Pay. La banque et/ou les organisations de cartes peuvent interrompre ou empêcher l'utilisation – c'est-à-dire la possibilité de recourir à Click to Pay – à tout moment, notamment pour des raisons de sécurité ou en cas de modification de l'offre ou de limitation des cartes autorisées ou des appareils compatibles. En outre, la banque n'est pas responsable des actes et offres des organisations de cartes ou d'autres prestataires tiers, ni des dommages résultant de perturbations ou d'interruptions de Click to Pay.

8.5 Protection des données Click to Pay
Les prestataires tiers (en particulier les organisations de cartes) et la banque sont responsables du traitement respectif des données personnelles en toute indépendance. La personne ayant droit à la carte prend acte du fait que les données personnelles liées à l'offre et à l'utilisation de Click to Pay (notamment les informations sur la carte, le nom et les informations de contact telles que l'adresse de facturation et de livraison, l'adresse e-mail et le numéro de téléphone) sont recueillies par le prestataire tiers, et stockées et traitées en Suisse ou à l'étranger. Le traitement des données personnelles par un prestataire tiers en relation avec Click to Pay et l'utilisation d'offres et de prestations du prestataire tiers sont régis par les règles d'utilisation et de protection des données de ce dernier. Par conséquent, la personne ayant droit à la carte confirme, par l'activation via Click to Pay, avoir lu et compris les dispositions relatives à la protection des données du prestataire tiers concerné et accepter expressément le traitement des données du prestataire tiers. Si la personne ayant droit à la carte refuse ce traitement, il lui incombe de renoncer à l'activation de Click to Pay ou de s'opposer au traitement auprès du prestataire tiers. Le traitement des données personnelles par la banque et le processeur est soumis aux Dispositions relatives à la protection des données énoncées au point C ci-dessous ainsi qu'aux **Informations générales concernant la protection des données** (disponibles sur banquemigros.ch/bases) de la Banque Migros SA.

C Dispositions relatives à la protection des données pour l'utilisation de one

Les dispositions suivantes relatives à la protection des données indiquent comment la banque traite les données personnelles (ci-après dénommées «données») en tant que responsable de traitement dans le cadre de l'utilisation de one. 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 données de contact pour obtenir des renseignements sur la protection et le traitement des données dans les **Informations générales concernant la protection des données à la Banque Migros SA** (disponibles sur migrosbank.ch/fr/a-propos-de-nous/informations-legales).

En s'enregistrant à one, les personnes ayant droit à la carte acceptent expressément les traitements de données contenus dans la présente Déclaration relative à la protection des données. Des informations sur d'autres traitements de données dans le cadre de la relation de carte figurent dans les dispositions de la Banque Migros et dans les présentes Dispositions relatives à l'utilisation de one. 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**.

9. Traitement des données personnelles

9.1 En quoi consistent les Dispositions relatives à l'utilisation de one?
Par l'intermédiaire du site internet ou de l'app, la banque met à disposition, sous la dénomination «one», un service d'onboarding pour les nouveaux clients et clientes ainsi que divers services de cartes liés à l'utilisation des cartes émises (collectivement «services numériques one»). La mise à disposition de l'onboarding numérique et des services liés aux cartes implique le traitement par la banque des données concernant les personnes ayant droit à la carte. Les présentes dispositions informent les personnes ayant droit à la carte de manière détaillée et transparente du traitement des données lors de l'utilisation des services numériques one. En ce qui concerne le parcours de demande en ligne pour les cartes de crédit Cumulus, reportez-vous également au chiffre 5 pour obtenir des compléments explicatifs. Il convient, en outre, de tenir compte des «Informations générales concernant la protection des données à la Banque Migros SA» et des «Informations concernant la protection des données pour la carte de crédit Cumulus de la Banque Migros» (voir également chiffre 1.1).

9.2 Comment les données sont-elles recueillies?
9.2.1 Quelles données de la personne ayant droit à la carte sont recueillies?
Lors de l'enregistrement en vue de l'utilisation des services numériques one, de l'inscription et de la gestion du compte utilisateur, la personne ayant droit à la carte peut être invitée à indiquer son adresse e-mail, sa date de naissance, son numéro de téléphone mobile, son numéro de carte et son code d'activation.

9.2.2 Quelles données sont recueillies automatiquement?
- Les données relatives à l'utilisation des appareils mobiles de la personne ayant droit à la carte, telles que le fabricant, le type d'appareil, le système d'exploitation et le numéro de version, l'ID de périphérique, l'adresse IP;
- les données relatives à l'utilisation d'un ordinateur et d'un navigateur 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 la personne ayant droit à la carte, telles que l'enregistrement de l'identifiant ou du login;
- les données relatives aux visites et au comportement d'utilisation du site internet et 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.

9.2.3 Quelles informations sont recueillies lors de l'enregistrement et de l'activation des services de cartes sur one?
- Les informations sur la personne ayant droit à la carte et sur ses cartes enregistrées pour one 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.

9.2.4 Quelles informations sont recueillies 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 de paiement mobile d'un prestataire tiers, celui-ci peut également recueillir et traiter des données personnelles de la personne ayant droit à 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.

9.2.5 Quelles informations sont collectées lors de l'utilisation de 3-D Secure?
- Les informations relatives au commerçant, 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 de téléphonie mobile, telles que l'adresse IP, le nom du prestataire d'accès.

9.2.6 Quelles informations sont recueillies lors de l'utilisation de Click to Pay?
- Des informations sur les cartes enregistrées et sur leur utilisation;
- le nom et les coordonnées, telles que l'adresse de facturation et l'adresse de livraison;
- l'adresse e-mail et le numéro de téléphone.

9.2.7 Quelles données sont collectées lors de l'affichage de la section de carte de l'emplacement du commerçant?
- Les données d'emplacement des commerçants établis en Suisse et à l'étranger, p. ex. nom du commerçant, lieu, pays et secteur d'activité;
- la consultation périodique automatisée de Google pour préciser l'emplacement du commerçant.

9.3 Dans quel but la banque traite-t-elle mes données?
9.3.1 Fourniture des services de cartes et traitement du rapport de carte
- Possibilité d'enregistrement, d'inscription et d'utilisation des services numériques one par la personne ayant droit à la carte;
- mise en place d'une connexion sécurisée entre les services numériques one et l'appareil mobile de la personne ayant droit à la carte;
- transmission de demandes de confirmation, p. ex. pour confirmation de paiements en ligne via les services numériques one, par message push ou par code SMS à la personne ayant droit à la carte;
- transmission à la banque de l'information sur les confirmations effectuées;
- authentification de la personne ayant droit à la carte lors de l'exécution d'actions. L'app ou l'appareil mobile utilisé sont clairement attribués à la personne ayant droit à 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 la personne ayant droit à 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 de la personne ayant droit à la carte;
- affichage des transactions et des factures;
- traitement de la relation contractuelle de carte avec le personne ayant droit à 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.

9.3.2 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 de paiement mobile dans le cadre des présentes Dispositions relatives à l'utilisation de one et de celles relatives à l'utilisation ou à la protection des données du prestataire concerné, qui s'appliquent au rapport entre la personne ayant droit à la carte et le prestataire tiers.

9.3.3 Click to Pay
- Pour décider de l'admission de la carte à Click to Pay;
- pour activer et désactiver Click to Pay;
- pour prévenir toute utilisation abusive des cartes enregistrées;
- pour communiquer avec des prestataires tiers (en particulier les organisations de cartes) 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 la personne ayant droit à la carte et le prestataire tiers.

9.3.4 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 client, de consommation et de préférences permettant à la banque de développer et de proposer des produits et des services à la personne ayant droit à la carte;
- pour transmettre des informations sur les produits et services existants ou nouveaux de la banque et de tiers (matériel publicitaire) à la personne ayant droit à la carte;
- pour le traitement par le prestataire tiers dans le cadre de ses propres dispositions d'utilisation ou de protection des données.

9.3.5 Autres objectifs de traitement
- Calcul des risques de crédit et de marché pertinents pour l'opération;
- amélioration de la sécurité de l'utilisation des services de cartes, par exemple en réduisant le risque de transactions abusives ou d'utilisation abusive d'appareils ou de moyens de légitimation tels que l'hameçonnage ou le piratage;
- preuve des actions et protection face aux reproches contre la banque;
- amélioration des prestations générales de la banque et des 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.

9.4 Mes données seront-elles divulguées à d'autres destinataires?
9.4.1 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 pour leurs propres besoins, sous réserve des dispositions suivantes et en fonction du produit choisi (notamment d'autres réglementations pour la carte de crédit Cumulus), à moins que la personne ayant droit à la carte n'ait donné son accord à une telle transmission ou l'ait demandée ou encore en ait pris l'initiative. En particulier, la banque ne transmet à des tiers aucun profil individuel de client, de consommation ou de préférences qu'elle a établi sans le consentement explicite et séparé de la personne ayant droit à la carte. Si, et dans la mesure où, une transmission de données est admissible au regard des présentes Dispositions relatives à l'utilisation de one, notamment du présent chiffre 9.4, la personne ayant droit à la carte libère la banque du secret bancaire à cet égard. En ce qui concerne le parcours numérique de demande de carte de crédit Cumulus, il est également renvoyé au chiffre 5 pour des compléments explicatifs.

9.4.2 Autres catégories de tiers auxquels les données sont divulguées
- Les données (y compris les données de transaction) du/de la titulaire de la carte supplémentaire peuvent être communiquées au / à la titulaire de la carte principale;
- les données du/de la titulaire d'une Business Card peuvent être communiquées à l'entreprise;
- personnes mandatées par le/la titulaire de la carte;
- s'agissant de la carte de crédit Cumulus, des données personnelles (données de base), entre autres, peuvent aussi être communiquées à la Fédération des coopératives Migros (FCM), aux coopératives régionales et aux filiales concernées (toutes des «entreprises Migros») conformément aux **Informations concernant la protection des données pour la carte de crédit Cumulus de la Banque Migros** (disponibles à l'adresse cumulus.banquemigros.ch/documents), en vue d'établir le lien avec des comptes Migros existants, des crédits de points pour le programme Cumulus et des données de comportement et de transaction (y c. informations sur les retraits d'espèces), également pour le marketing direct personnalisé.
- 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.

9.4.3 Transmission des données de la personne ayant droit à la carte à des tiers via l'utilisation du paiement mobile ou de Click to Pay

- 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. De plus amples informations sur le traitement et la transmission de données ainsi que sur le recours à des tiers figurent dans les dispositions de la Banque Migros;
- Lors de l'utilisation du paiement mobile ou de Click to Pay par l'intermédiaire d'un prestataire tiers, ce dernier collecte et traite des données conformément à ses propres conditions d'utilisation ou de protection des données.

9.4.4 Transmission électronique de données

Lors de l'utilisation du transfert électronique de données, les données de la personne ayant droit à 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 la personne ayant droit à 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.

9.5 Comment protégeons-nous vos données?

La transmission d'informations entre la banque, le processeur et l'app et/ou les appareils mobiles de la personne ayant droit à la carte est cryptée (mais pas l'envoi de SMS, et seulement de manière limitée lors de l'envoi d'e-mails). Toutefois, la communication avec la personne ayant droit à 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. On ne peut donc exclure que des tiers aient accès à la communication avec la personne ayant droit à la carte lorsqu'ils utilisent one malgré toutes les mesures de sécurité. Lors de l'utilisation d'Internet, il est également possible que des données soient transmises à des pays tiers qui peuvent ne pas offrir le même niveau de protection des données que la Suisse lorsque la personne ayant droit à la carte est en Suisse.

La sécurité des données dépend également de la participation de la personne ayant droit à la carte. Celui-ci/celle-ci doit donc utiliser les moyens à sa disposition 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.

9.6 Quels sont vos droits en rapport avec vos données?

- Le droit de demander des informations sur vos données personnelles enregistrées chez nous;
- le droit de faire rectifier des données personnelles inexactes ou incomplètes;
- le droit de demander la suppression ou l'anonymisation de vos données personnelles;
- le droit de recevoir certaines données personnelles dans un format structuré, usuel et lisible par machine;
- le droit de révoquer un consentement avec effet pour l'avenir, dans la mesure où le traitement est sujet à un consentement;
- le droit de s'opposer au traitement de vos données personnelles;
- le droit de déposer plainte auprès de l'autorité de surveillance compétente contre la manière dont nous traitons vos données personnelles.

La banque ne peut vous accorder ces 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.

9.7 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 enregistre également des données personnelles lorsqu'il existe un intérêt légitime à les enregistrer, 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 enregistrées pour se conformer aux obligations légales et réglementaires.

D Libération du secret bancaire

10. Libération du secret bancaire

La banque prend les mesures appropriées pour assurer le respect du secret bancaire. Elle divulgue toutefois des données (p. ex. nom et prénom, sexe, date de naissance, lieu de naissance, nationalité, numéro de pièce d'identité, autorité émettrice, adresse postale, adresse e-mail, numéro de téléphone) de clients, comme ci-dessus en particulier aux chiffres 2.2, 5.1, 5.2 et 9, à différentes fins, notamment pour le traitement des demandes de carte en ligne (notamment par l'intermédiaire du processeur), pour l'exécution des obligations contractuelles, des ordonnances et obligations légales ou réglementaires nationales ou étrangères en matière d'information et de divulgation, ainsi que pour la protection des intérêts légitimes.

De plus amples informations sur l'étendue des divulgations et la libération du secret bancaire figurent dans les dispositions de la Banque Migros, dans les **Informations concernant la protection des données à la Banque Migros SA** (disponibles sur migrosbank.ch/fr/a-propos-de-nous/informations-legales) et les **Informations concernant la protection des données pour la carte de crédit Cumulus de la Banque Migros SA.** (disponibles sur cumulus.migrosbank.ch/documents).

Dans le cadre des divulgations susmentionnées, la personne ayant droit à la carte renonce consciemment et volontairement à la protection du secret bancaire. Dans cette mesure, elle libère la banque (et d'éventuels autres tiers impliqués) du secret bancaire et de toute autre obligation de confidentialité, notamment le secret de fonction et le secret professionnel.

Version 04/2025

mgb0051/2025_04