Bank
Banque
Banca
CLER

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

I. Généralités

1. Dispositions générales relatives à l'utilisation de one

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

Les présentes dispositions s'appliquent aux services en ligne (ci-après dénommés «services») baptisés «one» et fournis par la Banque Cler (ci-après dénommée «banque») au titulaire (ci-après dénommé «ayant droit à la carte») d'une carte principale ou supplémentaire délivrée par la Banque Cler ou une Business Card de la banque, ci-après dénommé(s) «carte» ou «cartes». One est exploité par Viseca Payment Services SA, ci-après dénommé «processeur». La banque fait appel au processeur pour exécuter des tâches relatives aux opérations par carte. Les présentes dispositions peuvent évoquer des cartes ou des fonctionnalités qui ne sont pas proposés par la banque, que ce soit de façon définitive ou temporaire, ou qui ne le seront qu'à l'avenir. Une simple évocation ne donne lieu à aucun droit à la mise à disposition des services correspondants pour le client ou l'ayant droit à la carte.

One est disponible sur le site Internet one («site Internet») et sur l'application one («app»).

Il convient de respecter les autres informations relatives à one – notamment celles qui concernent le traitement et la sécurité des données – disponibles dans les dispositions relatives à la protection des données visées au point III ci-dessous et dans les dispositions d'utilisation de One Digital Services du processeur («dispositions d'utilisation one»). La déclaration de protection des données de la banque disponible sur www.cler.ch s'applique également.

Les présentes dispositions s'appliquent en outre aux autres conditions ou dispositions relatives à l'utilisation de cartes de la banque. En cas de clauses différentes, les présentes dispositions priment les autres. La banque se réserve le droit de modifier à tout moment les présentes dispositions. Les modifications sont communiquées à l'ayant droit à la carte de façon appropriée.

1.2 Contenu de one et développement

One comprend les services de la banque fournis par le processeur pour le compte de la banque. L'utilisation de one nécessite un enregistrement. Les nouveaux services proposés sont mis à disposition de l'ayant droit à la carte enregistré par le biais des actualisations (updates). La banque informe ensuite de façon appropriée

801.0005 VP72 7.21

l'ayant droit à la carte des développements et, le cas échéant, des modifications des présentes dispositions qui en résultent.

1.3 Fonctions de one
One peut inclure, actuellement ou à l'avenir, les fonctionnalités suivantes:
- un compte utilisateur destiné à l'administration des données personnelles;
- la vérification et la confirmation de paiements, par ex. via 3-D Secure dans l'application ou par la saisie d'un code SMS (voir point II 1);
- la vérification et la confirmation de certaines actions (par ex. login, contacts avec la banque) dans l'application ou par la saisie d'un code SMS;
- l'activation de cartes pour utiliser les possibilités de paiement;
- l'échange de messages et de déclarations entre l'ayant droit à la carte et la banque (dont les messages relatifs aux modifications des présentes dispositions), sous réserve d'une autre forme convenue pour l'échange de messages et de déclarations;
- une vue d'ensemble des transactions ou des cartes et un affichage électronique des factures;
- un aperçu du compte des programmes de bonus et la possibilité d'utiliser les points;
- des informations liées à l'utilisation de la carte (actuellement services SMS).

2. Utilisation de one

2.1 Droits d'utilisation
L'ayant droit à la carte est autorisé à utiliser one dans les conditions suivantes:
- il est en mesure d'appliquer les présentes dispositions et les exigences correspondantes, et
- il est autorisé à utiliser l'une des cartes émises par la banque en qualité de titulaire d'une carte principale ou supplémentaire ou d'une Business Card de la banque.

2.2 Consentements dans le cadre de l'enregistrement et du développement de one
En utilisant one, l'ayant droit à la carte donne à la banque son consentement explicite dans les cas de figures suivants:
- Consentement au traitement des données collectées dans le cadre de l'utilisation de one. Cela inclut notamment aussi le consentement à leur mise en relation avec les données déjà en possession de la banque et à la création de profils, à des fins de gestion des risques et de marketing de la banque ou du processeur et de tiers, conformément à la déclaration de protection des données de one;
- Consentement à la réception de messages et d'informations au sujet des produits et services de la banque et de tiers à des fins de marketing (publicité). Ces informations peuvent être mises à disposition de la banque par e-mail, directement via l'application 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'application pour les échanges électroniques avec la banque (par ex. notification de changement d'adresse, communication de la modification des dispositions ou messages liés à la lutte contre l'utilisation frauduleuse des cartes);
- Le consentement à la réception de messages au sujet des produits et services et/ou au traitement des données à des fins de marketing peut être révoqué à tout moment par notification à la banque, avec effet pour l'avenir. La déclaration de protection des données de la banque s'applique aux coordonnées correspondantes.

2.3 Refus de consentement dans le cadre du développement de one
Si l'ayant droit à la carte refuse de donner son consentement aux dispositions dans le cadre du développement de one (par ex. lors des mises à jour), il est possible qu'il ne puisse pas ou plus avoir recours à l'application, au site Internet ou à certains services.

2.4 Effet des confirmations
Toute confirmation effectuée via l'application ou la saisie d'un code SMS est considérée comme une action de l'ayant droit à la carte. L'ayant droit à la carte est en droit d'apporter la preuve du contraire. L'ayant droit à la carte s'engage à répondre des débits résultant des confirmations imputées sur sa carte et autorise la banque à exécuter les ordres et à effectuer les actions correspondantes.

2.5 Disponibilité/blocage/modifications
La banque peut interrompre, restreindre, adapter ou compléter par d'autres prestations la possibilité d'utilisation de one, entièrement ou en partie. La banque est notamment en droit de bloquer temporairement ou définitivement l'accès de l'ayant droit à la carte à one (par ex. en cas de suspicion de fraude).

2.6 Droits de propriété intellectuelle et licence
Tous les droits (notamment les droits de propriété intellectuelle et les droits de marque) relatifs aux logiciels, aux textes, aux images, aux vidéos, aux noms, aux logos et à d'autres données ou informations accessibles via one ou accessibles au fil du temps appartiennent exclusivement à la banque ou aux partenaires et tiers correspondants (par ex. processeur, Visa, Mastercard®), sauf clause contraire spécifiée dans les présentes dispositions. Les noms et les logos visibles sur one sont des marques protégées.

La banque octroie à l'ayant droit à la carte une licence non exclusive, non cessible, illimitée, révocable et

801.0005 VP72 7.21

gratuite pour l'utilisation de l'application, lui permettant de télécharger cette dernière, de l'installer sur un appareil de l'ayant droit à la carte et de l'utiliser dans le cadre des fonctions prévues.

L'utilisation du site Internet et des canaux électroniques est en outre régie par les dispositions correspondantes sur le site Internet de la banque.

3. Risques, exclusion de garanties et obligations de diligence et de déclaration

3.1 Risques lors de l'utilisation de one

L'ayant droit à la carte prend connaissance des risques liés à l'utilisation de one et les accepte.

Il est notamment possible que les appareils ou les données personnelles de l'ayant droit à la carte liés à l'utilisation des cartes, du nom d'utilisateur et du mot de passe one fassent l'objet d'abus. L'ayant droit à la carte s'expose ainsi à l'éventualité de dommages financiers (par débit de sa carte) et personnels (par utilisation frauduleuse de ses données personnelles). Il existe en outre le risque que one ou l'un des services proposés sur one ne puisse pas être utilisé (par ex. lorsque l'identification sur one n'est pas possible).

Les abus sont notamment rendus possibles ou favorisés par les facteurs suivants:

- le non-respect des obligations de diligence ou de déclaration par l'ayant droit à la carte (par ex. par une utilisation imprudente du nom d'utilisateur / mot de passe ou en ne signalant pas une perte de carte);
- le paramétrage choisi par l'ayant droit à la carte ou le manque d'entretien des appareils et systèmes destinés à l'utilisation de one (par ex. ordinateur, téléphone portable, tablette, etc.), par ex. absence de verrouillage de l'écran, pare-feu inexistant ou insuffisant, protection antivirus insuffisante ou versions de logiciels obsolètes;
- l'accès de tiers ou erreurs lors de la transmission de données par Internet (par ex. hacking, phishing ou perte de données);
- les confirmations erronées dans l'application ou lors de la saisie d'un code SMS (par ex. en l'absence de contrôle d'une demande de confirmation);
- des paramètres de sécurité faibles choisis par l'ayant droit à la carte – notamment pour l'application (par ex. enregistrement du login).

Si l'ayant droit à la carte respecte les obligations de diligence et de déclaration dans le cadre de son utilisation des appareils et du mot de passe, ainsi que son obligation de contrôle des demandes de confirmation, il peut réduire le risque d'abus.

La banque n'assure et ne garantit en aucun cas que le site Internet et l'application soient accessibles durablement, fonctionnent parfaitement ou que les abus puissent être identifiés et évités de façon sûre.

3.2 Obligations de diligence générales de l'ayant droit à la carte

3.2.1 Obligations de diligence générales liées à l'utilisation d'appareils et de systèmes, notamment des appareils mobiles

Pour l'authentification, one recourt notamment aux appareils mobiles (par ex. téléphone portable, tablette, ci-après dénommés «appareil mobile») de l'ayant droit à la carte. La préservation de ces appareils mobiles à tout moment est par conséquent un facteur de sécurité essentiel. L'ayant droit à la carte doit manipuler avec précaution les appareils mobiles et assurer leur protection appropriée.

Pour ce qui a trait aux appareils et systèmes utilisés, notamment les appareils mobiles, l'ayant droit à la carte doit notamment respecter les obligations de diligence générales suivantes:

- le verrouillage de l'écran doit être activé pour les appareils mobiles et des mesures de sécurité supplémentaires doivent être mises en place pour éviter le déverrouillage par des personnes non autorisées;
- les appareils mobiles doivent être conservés en lieu sûr, protégés de tout accès par des tiers et ne doivent pas être prêtés à des tiers pour une utilisation durable ou sans surveillance;
- les logiciels doivent être régulièrement actualisés (par ex. systèmes d'exploitation et navigateurs Internet);
- les intrusions dans les systèmes d'exploitation (par ex. «jailbreaking» ou «rooting») ne sont pas souhaitables;
- des programmes de protection contre les virus et de sécurité Internet doivent être installés sur l'ordinateur portable ou de bureau et régulièrement actualisés;
- l'application doit être téléchargée uniquement depuis les stores officiels (par ex. Apple Store et Google Play Store);
- les mises à jour (updates) de l'application doivent être installées sans tarder;
- en cas de perte d'un appareil mobile, il convient de tout mettre en œuvre pour empêcher l'accès de personnes non autorisées aux données transmises par la banque à l'appareil mobile (par ex. par verrouillage de la carte SIM, verrouillage de l'appareil, suppression des données en utilisant par ex. la fonction «Localiser mon iPhone» ou «Gestionnaire d'appareils Android», réinitialisation ou demande de réinitialisation du compte utilisateur). La perte doit être notifiée à la banque (voir point I 3.3);
- l'application doit être supprimée avant toute vente ou tout prêt longue durée de l'appareil mobile à des tiers.

801.0005 VP72 7.21

3.2.2 Obligations de diligence générales liées au mot de passe

Outre la possession de l'appareil mobile, le nom d'utilisateur et le mot de passe sont des facteurs d'authentification de l'ayant droit à la carte. Pour ce qui a trait au mot de passe, l'ayant droit à la carte doit notamment respecter les obligations de diligences générales suivantes:

- l'ayant droit à la carte doit définir un mot de passe qu'il n'utilise pas déjà pour d'autres services et qui n'est pas composé de combinaisons faciles à deviner (par ex. numéro de téléphone, date de naissance, plaque d'immatriculation, nom de l'ayant droit à la carte ou de l'un de ses proches, suite de chiffres ou de lettres répétés ou se suivant directement, tels que de «123456» ou «aabbcc»);
- le mot de passe doit être tenu secret. Il ne doit pas être communiqué ou rendu accessible à des tiers. L'ayant droit à la carte prend note du fait que la banque n'exigera jamais qu'il lui communique son mot de passe;
- le mot de passe ne doit pas être noté ni enregistré de façon non sécurisée;
- l'ayant droit à la carte doit modifier le mot de passe ou réinitialiser le compte utilisateur (par lui-même ou par la banque) lorsqu'il soupçonne que des tiers sont entrés en possession de son mot de passe ou d'autres données;
- la saisie du mot de passe doit être effectuée uniquement à l'abri du regard de tiers.

3.2.3 Obligations de diligence liées aux demandes de confirmation

Les confirmations constituent un engagement obligatoire pour l'ayant droit de la carte. Pour ce qui a trait aux confirmations dans l'application ou par la saisie d'un code SMS, l'ayant droit à la carte doit par conséquent respecter les obligations générales de diligence suivantes:

- l'ayant droit à la carte ne peut procéder à une confirmation que si la demande correspondante est directement liée à une action ou à une opération spécifique (par ex. paiement, login, contact avec la banque) de l'ayant droit à la carte;
- l'ayant droit à la carte doit vérifier avant la confirmation si l'objet de la demande de confirmation correspond à l'opération concernée. Il convient notamment de vérifier les détails de paiement indiqués lors des demandes de confirmation avec 3-D Secure.

3.3 Obligations de déclaration de l'ayant droit à la carte

Les événements suivants doivent être immédiatement notifiés à la banque:

- perte d'un appareil mobile;
- demandes de confirmation sans lien avec un paiement en ligne, un login par l'ayant droit à la carte, un contact avec la banque ou toute opération similaire (soupçon d'abus);
- tout autre élément laissant soupçonner que la demande de confirmation dans l'application ou via le code SMS ne provient pas de la banque;
- soupçon d'utilisation abusive du nom d'utilisateur, du mot de passe, des appareils mobiles, du site Internet, de l'application, etc. ou soupçon d'entrée en possession de ces derniers par des tiers non autorisés;
- modification du numéro de téléphone et des autres données personnelles pertinentes;
- changement d'appareil mobile utilisé pour one (dans ce cas, l'application doit être à nouveau enregistrée).

4. Responsabilité

4.1 Responsabilité en cas de dommages en général

Sous réserve du point I 4.2, la banque indemnise les dommages qui ne sont pas couverts par une assurance dans les cas de figure suivants:

- lorsque ces dommages sont survenus à la suite d'intrusions manifestement illégales dans les installations des opérateurs de réseaux et/ou de télécommunications ou dans les appareils et/ou les systèmes utilisés par l'ayant droit à la carte (par ex. ordinateurs, appareils mobiles et autres infrastructures informatiques) et
- lorsque l'ayant droit à la carte a respecté les obligations de diligence et de déclaration visées aux points I 3.2 et 3.3, notamment les obligations de contrôle des demandes de confirmation et l'obligation de vérification du décompte mensuel, ainsi que de contestation en temps utile des transactions abusives, lorsque l'ayant droit à la carte n'est en aucun cas coupable de la survenance des dommages;
- lorsque les dommages concernés résultent exclusivement du non-respect de la diligence usuelle de la banque.

La responsabilité pour tous dommages indirects ou consécutifs éventuels de l'ayant droit à la carte, de quelque nature que ce soit, est exclue par la banque, sous réserve de faute intentionnelle ou de négligence grave.

4.2 Exceptions

L'ayant droit à la carte assume le risque de dommage et la banque exclut toute responsabilité dans les cas suivants:

- lorsque les dommages concernés ne sont pas imputables à la banque selon les modalités visées au point I 4.1 (notamment en cas de non-respect des obligations de diligence et de déclaration par l'ayant droit à la carte), ou
- lorsque l'ayant droit à la carte, son conjoint, un membre direct de sa famille (notamment ses enfants et ses parents) ou toute autre personne proche de l'ayant droit à la carte, mandataire et/ou personnes

801.0005 VP72 7.21

vivant sous le même toit effectue une action (par ex. confirmation dans l'application ou par code SMS).

II. Dispositions spécifiques

1. 3-D Secure

1.1 Qu'est-ce que 3-D Secure?
3-D Secure est un protocole de paiement sécurisé sur Internet reconnu à l'international. Il est appelé «Verified by VISA» chez VISA et «SecureCode» chez Mastercard®. L'ayant droit à la carte est tenu d'utiliser ce protocole de paiement sécurisé lors des paiements, si celui-ci est proposé par le point d'acceptation (le commerçant).

1.2 Comment fonctionne 3-D Secure?
Les paiements effectués par 3-D Secure peuvent être confirmés (autorisés) de différentes manières:
- dans l'application ou
- par la saisie d'un code transmis par la banque à l'ayant droit à la carte par message (code SMS), dans la fenêtre correspondante du navigateur pendant la procédure de paiement. Toute utilisation de la carte autorisée avec 3-D Secure est considérée comme effectuée par l'ayant droit à la carte.

1.3 Activation de cartes pour 3-D Secure
3-D Secure est activé lors de l'enregistrement dans one, pour toutes les cartes au nom de l'ayant droit et liées à une relation commerciale enregistrée de l'ayant droit à la carte ou d'un tiers avec la banque.

1.4 Désactivation de cartes pour 3-D Secure
Pour des raisons de sécurité, 3-D Secure ne peut pas être désactivé après l'activation réussie.

2. Mobile Payment

2.1 Qu'est-ce que Mobile Payment?
Mobile Payment désigne des solutions pour l'utilisation de cartes via un appareil mobile.

Mobile Payment permet à l'ayant droit à la carte possédant un appareil mobile compatible d'utiliser les cartes autorisées via une application mobile de la banque (voir point II 2.7) ou d'un fournisseur tiers pour le paiement sans contact ainsi que pour le paiement sur les boutiques en ligne et les applications. Pour des raisons de sécurité, le numéro de carte est remplacé par un numéro (jeton numérique) différent, généré à chaque fois et faisant office de «carte virtuelle». Les cartes virtuelles peuvent être utilisées comme les cartes physiques via Mobile Payment. Lors du paiement avec une carte virtuelle, ce n'est pas le numéro de la carte, mais uniquement le numéro généré (jeton numérique) qui est transmis au commerçant.

2.2 Quels sont les appareils mobiles compatibles et quelles sont les cartes autorisées?
Les appareils mobiles compatibles sont par ex. les ordinateurs portables, les téléphones portables, les montres connectées, les fitness trackers, dans la mesure où ces derniers sont compatibles avec l'utilisation de cartes virtuelles et sont autorisés par la banque. La banque décide en outre des cartes autorisées en fonction des fournisseurs.

2.3 Activation et désactivation
Pour des raisons de sécurité, l'activation d'une carte nécessite que l'ayant droit à la carte accepte les conditions d'utilisation du fournisseur de Mobile Payment concerné et prenne connaissance des dispositions de ce dernier relatives à la protection des données. L'ayant droit à la carte est tenu d'indemniser la banque en cas de dommages survenant suite au non-respect de ces conditions / dispositions.

Les cartes virtuelles peuvent être utilisées via l'application par l'ayant droit sauf en cas de blocage ou de désactivation de la carte. Demeurent réservées les restrictions d'utilisation de la carte conformément aux conditions spécifiques applicables à certaines cartes. L'ayant droit à la carte peut mettre fin à tout moment à l'utilisation de Mobile Payment, en supprimant sa ou ses carte(s) virtuelle(s) auprès du fournisseur correspondant.

Les coûts liés à l'activation et à l'utilisation de cartes virtuelles (par ex. coûts résultant de l'utilisation de données mobiles à l'étranger) sont à la charge de l'ayant droit à la carte.

2.4 Utilisation de la carte virtuelle (autorisation)
L'utilisation d'une carte virtuelle correspond à une transaction par carte habituelle. Toute utilisation d'une carte virtuelle est considérée comme autorisée par l'ayant droit à la carte.

L'autorisation d'utilisation d'une carte virtuelle doit s'effectuer selon la procédure prévue par le prestataire ou par le commerçant (point d'acceptation), par ex. en saisissant le NIP de l'appareil ou en s'identifiant par empreinte digitale ou par reconnaissance faciale. L'ayant droit à la carte prend connaissance du fait que le risque d'utilisation de la carte par des personnes non autorisées s'accroît lorsque l'outil d'autorisation éventuellement requis en plus par le fournisseur ou le commerçant (NIP de l'appareil ou de la carte) est composé de combinaisons faciles à deviner. L'ayant droit à la carte est informé qu'aucune autorisation ne sera exigée par le fournisseur ou le commerçant, en deçà d'un certain montant fixé par celui-ci. Du reste, la responsabilité est régie par les clauses visées au point 4 des présentes dispositions.

801 0005 VP72 7.21

2.5 Obligations de diligence particulières
L'ayant droit à la carte reconnaît et accepte que l'utilisation de Mobile Payment comporte des risques, malgré toutes les mesures de sécurité. Il est notamment possible que les cartes virtuelles et les données personnelles fassent l'objet d'utilisations abusives ou de consultations par des personnes non autorisées. L'ayant droit à la carte peut ainsi encourir des dommages financiers, par imputation frauduleuse d'une carte, ainsi que des dommages personnels par l'utilisation abusive de ses données personnelles.

L'ayant droit à la carte doit manipuler avec précaution les appareils et les cartes virtuelles utilisés et assurer leur protection. En plus des obligations de diligence visées par les différentes conditions d'utilisation de la carte applicables, et des obligations de diligence et de déclaration visée aux points I 3.2.1 et I 3.3 des présentes dispositions, l'ayant droit à la carte est tenu de respecter les obligations suivantes:

- les appareils utilisés doivent faire l'objet d'un usage adéquat et doivent être protégés d'un accès par des tiers;
- comme les cartes physiques, les cartes virtuelles sont personnelles et ne peuvent être cédées. Il est interdit de les transmettre à des tiers pour utilisation (par ex. en enregistrant les empreintes digitales ou en scannant le visage de tiers pour débloquer l'appareil utilisé);
- en cas de changement ou cession d'un appareil mobile (par ex. en cas de vente), chaque carte virtuelle doit être supprimée dans l'application du fournisseur et dans l'appareil mobile;
- tout soupçon d'utilisation abusive d'une carte virtuelle ou d'un appareil mobile utilisé pour Mobile Payment doit être immédiatement notifié à la banque afin que la carte virtuelle correspondante puisse être bloquée.

2.6 Exclusion de garanties
Il n'est pas possible de faire valoir le droit à l'utilisation de Mobile Payment. La banque peut interrompre l'utilisation ou y mettre fin à tout moment, notamment pour des raisons de sécurité, en cas de modification de l'offre Mobile Payment ou de restriction des cartes autorisées ou des appareils compatibles. En outre, la banque ne peut être tenue responsable des actions et des offres du fournisseur ou d'autres tiers, comme les fournisseurs de services Internet et de téléphonie.

2.7 Utilisation de la carte par l'application one
L'ayant droit à la carte qui dispose d'un appareil compatible peut activer sa ou ses carte(s) dans l'application one et l'(les) utiliser ainsi comme carte(s) virtuelle(s). Pour garantir la sécurité lors de Mobile Payment, l'ayant droit à la carte doit définir un code secret au moment de l'activation. La banque peut en tout temps procéder à la modification de ce service. Pour le reste s'appliquent les présentes dispositions relatives à Mobile Payment, notamment les obligations de diligence particulières visées au point II 2.5.

2.8 Protection des données lors de Mobile Payment
Le fournisseur tiers et la banque sont responsables indépendamment du traitement des données personnelles qu'ils effectuent. L'ayant droit à la carte reconnaît que ses données personnelles sont collectées par le fournisseur tiers dans le cadre de l'offre et de l'utilisation de Mobile Payment (notamment les données relatives à l'ayant droit à la carte, ainsi qu'aux cartes activées et aux données de transaction liées à l'utilisation de cartes virtuelles) et qu'elles sont stockées et traitées en Suisse ou à l'étranger. Le traitement des données personnelles par le fournisseur tiers dans le cadre de Mobile Payment et de l'utilisation des offres et des prestations du fournisseur tiers, y compris de ses appareils et de ses logiciels, est régi par ses conditions en matière d'utilisation et de protection des données. Par conséquent, l'ayant droit à la carte confirme par chaque activation d'une carte qu'il a lu et compris les dispositions relatives à la protection des données du fournisseur tiers concerné, et qu'il consent expressément au traitement des données correspondant du fournisseur tiers. S'il s'oppose à ce traitement, il en va de la responsabilité de l'ayant droit à la carte de renoncer à l'activation d'une carte ou de s'opposer au traitement auprès du fournisseur tiers. Pour ce qui relève du traitement des données personnelles par la banque et le processeur, ce sont les dispositions relatives à la protection des données visées au point III ci-après, la déclaration de protection des données de la banque et les dispositions d'utilisation one qui s'appliquent.

III. Déclaration de protection des données de one

Les dispositions suivantes relatives à la protection des données livrent des informations sur la façon dont la banque traite les données personnelles (ci-après dénommées «données») en qualité de responsable. Le traitement inclut toute manipulation des données personnelles, notamment la collecte, l'enregistrement, l'utilisation, la communication ou la suppression de données. Pour toute information relative à la protection et au traitement des données, il convient de se reporter aux coordonnées indiquées dans la déclaration de protection des données de la banque.

Lors de l'enregistrement pour one, les ayants droit à des cartes déclarent accepter expressément le traitement de données mentionné dans cette déclaration de protection des données. Des informations relatives à d'autres types de traitement dans le cadre du contrat lié à la carte sont disponibles dans les conditions d'utilisation de la carte concernée, ainsi que dans les conditions

801.0005 VP72 7.21

générales et particulières d'utilisation de one. Il convient en outre de se référer aux déclarations de protection des données globales de Visa et de Mastercard®, ainsi qu'aux droits d'exécution de tiers bénéficiaires en la matière.

1. Traitement des données personnelles

1.1 De quoi traite la déclaration de protection des données de one?

Le terme «one» désigne la mise à disposition de différents services en ligne liés à l'utilisation des cartes éditées (ci-après dénommés «one digital services»). La mise à disposition des services nécessite le traitement des données de l'ayant droit à la carte par la banque. La présente déclaration de protection des données livre aux ayants droit de cartes des informations sur le traitement des données lors de l'utilisation des services numériques one.

1.2 Comment les données sont-elles collectées?

1.2.1 Quelles données de l'ayant droit de la carte sont communiquées?

Lors de l'enregistrement pour les services numériques one, lors de l'inscription et lors de l'administration du compte d'utilisateur, il peut être demandé à l'ayant droit à la carte de fournir son adresse e-mail, sa date de naissance, son numéro de téléphone, son numéro de carte et son code d'activation.

1.2.2 Quelles sont les données automatiquement collectées?

- Données relatives à l'utilisation d'appareils mobiles de l'ayant droit à la carte, par ex. fabricant, type d'appareil, système d'exploitation avec numéro de version, identifiant d'appareil, adresse IP;
- Données relatives à l'utilisation d'un ordinateur et d'un navigateur, ainsi que pour l'accès à Internet, par ex. type d'appareil, système d'exploitation, adresse IP;
- Données relatives à l'utilisation du compte utilisateur, par ex. nombre de logins avec date et heure, modifications entreprises dans le compte utilisateur, acceptation des dispositions relatives à l'utilisation des services numériques one et de la déclaration de protection des données;
- Données relatives aux paramètres souhaités par l'ayant droit à la carte, par ex. enregistrement du nom d'utilisateur ou du login;
- Données relatives aux visites et aux comportements d'utilisation sur le site Internet;
- Données produites lors de l'utilisation de l'application, par ex. mises à jour ou informations de l'appareil relatives aux comportements d'utilisation, par ex. dans l'application ou par code SMS.

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

- Informations relatives à l'ayant droit à la carte et à sa carte enregistrée pour one, qui sont sauvegardées dans le compte utilisateur;
- Informations utilisées par 3-D Secure pour les cartes enregistrées via une confirmation dans l'application ou la saisie d'un code SMS;
- Adresse de livraison et numéro de téléphone portable.

1.2.4 Quelles sont les informations collectées lors de l'utilisation de Mobile Payment?

- Informations relatives à l'utilisation de Mobile Payment, par ex. l'activation ou la désactivation de cartes et l'utilisation des cartes pour Mobile Payment;
- Informations relatives au montant de la transaction;
- Informations relatives à l'utilisation de la carte, à la date et à l'heure de la transaction, au type de vérification.

Lors de l'utilisation d'une solution Mobile Payment d'un fournisseur tiers, ce dernier peut également collecter et traiter les données personnelles de l'ayant droit à la carte. En fonction de l'offre concernée, il peut par ex. s'agir du nom, du numéro de carte et éventuellement des données relatives à la transaction. Il convient à ce propos de se référer aux dispositions relatives à l'utilisation et la protection des données du fournisseur tiers.

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

- Informations relatives au commerçant, à la transaction et à son exécution, ainsi qu'à la confirmation de la transaction avec 3-D Secure;
- Informations liées aux appareils utilisés pour la transaction et la confirmation;
- Informations liées à l'accès à Internet ou au réseau mobile, par ex. l'adresse IP, le nom du fournisseur d'accès.

1.2.6 Quelles sont les données collectées lors de l'affichage de l'extrait de carte du site du commerçant?

- Données relatives au site du commerçant implanté en Suisse;
- Données relatives au site, telles que le nom du commerçant, la localité, le pays et le secteur;
- Recherches Google périodiques automatisées, afin de préciser le site du commerçant.

1.3 À quelles fins la banque traite-t-elle mes données?

1.3.1 Fourniture des services et exécution de la relation contractuelle relative à la carte

- Facilitation de l'enregistrement, de l'inscription et de l'utilisation des services numériques one par l'ayant droit à la carte;

801.0005 VP72 7.21

- Établissement d'une connexion sécurisée entre les services numériques one et l'appareil mobile de l'ayant droit à la carte;
- Transmission des demandes de confirmation, par ex. pour confirmer les paiements en ligne via les services numériques one, par message push ou code SMS à l'ayant droit à la carte;
- Transmission à la banque des informations relatives aux confirmations effectuées;
- Authentification de l'ayant droit à la carte lors de l'exécution d'actions. L'application ou l'appareil mobile sont associés uniquement aux ayants droit de la carte lors de l'enregistrement sur one. La banque peut ainsi s'assurer que la confirmation a été effectuée dans l'application enregistrée ou avec l'appareil mobile enregistré;
- Communication avec l'ayant droit à la carte et transmission d'informations liées à la relation contractuelle relative à la carte ou à l'utilisation de la carte, telle que les informations sur les nouvelles factures, les avis de fraude ou les demandes dans le cadre des transactions inhabituelles via les services numériques one et l'appareil mobile;
- Réception de messages de l'ayant droit à la carte
- Affichage des transactions et des factures;
- Exécution de la relation contractuelle relative à la carte avec l'ayant droit et des transactions effectuées à l'aide de la carte. À ce sujet, il convient de se référer à la déclaration de protection des données de la banque, ainsi qu'aux chiffres I et II des présentes dispositions d'utilisation.

1.3.2 Mobile Payment

- Pour la décision concernant l'autorisation de la carte liée à Mobile Payment;
- Pour l'activation, la désactivation et l'actualisation de cartes liées à Mobile Payment;
- Pour prévenir toute utilisation abusive des cartes enregistrées;
- Pour communiquer avec un éventuel fournisseur tiers d'une solution de Mobile Payment dans le cadre des présentes dispositions, ainsi que des conditions d'utilisation et de protection des données du fournisseur concerné, applicables dans la relation entre l'ayant droit à la carte et le fournisseur tiers.

1.3.3 Marketing

- Pour mettre en lien des données avec des informations déjà en possession de la banque (également issues de sources tierces);
- Pour établir des profils individuels de clientèle, de consommation et de préférence, qui permet à la banque de mettre au point des produits et des services pour les ayants droit de cartes et de les leur proposer;
- Pour transmettre à l'ayant droit à la carte des informations relatives à des produits et des services nouveaux ou existants de la banque ainsi que de tiers (matériel promotionnel);
- Pour le traitement par le fournisseur tiers dans le cadre de ses conditions d'utilisation et de protection des données.

1.3.4 Autres finalités du traitement

- Calcul des risques de crédit et de marché applicables;
- Amélioration de la sécurité lors de l'utilisation des services, par ex. en minimisant le risque de transactions frauduleuses ou d'utilisation abusive des appareils ou des moyens de validation, telles que le phishing ou le hacking;
- Justification des actions et rejet des prétentions envers la banque;
- Amélioration des prestations de la banque et des services numériques one;
- Respect des exigences juridiques et réglementaires;
- Traitement par le fournisseur tiers à ses propres fins dans le cadre de ses conditions d'utilisation et de protection des données.

1.4 Mes données sont-elles divulguées à d'autres destinataires?

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

Les tiers sont des personnes ou des entreprises qui traitent les données à leurs propres fins. Aucun tiers, au sens visé ci-dessus, n'est un prestataire mandaté par la banque. Sous réserve des dispositions suivantes, la banque ne divulgue en principe, aux tiers et à leurs propres fins, aucune donnée – notamment relative aux transactions – liée aux cartes auxquelles s'appliquent les conditions générales de la banque ou les conditions spécifiques applicables aux cartes, sauf si l'ayant droit à la carte a consenti à sa divulgation ou s'il l'a lui-même exigée ou occasionnée. Plus particulièrement, la banque ne transmet pas les profils individuels de clientèle, de consommation et de préférences établis par ses soins sans le consentement spécifique et explicite de l'ayant droit à la carte.

1.4.2 Autres catégories de tiers auxquels sont divulguées les données

- Les données (également celles relatives aux transactions) d'un l'ayant droit de carte supplémentaire peuvent être divulguées à l'ayant droit à la carte principale;
- Les données des ayants droit de cartes d'entreprise (Business Cards, etc.) peuvent être divulguées à l'entreprise concernée;
- Sur décision administrative ou pour se conformer aux obligations légales, la banque divulgue ou transmet des données à des organismes publics, tels que les autorités pénales ou de surveillance.

801.0005 VP72 7.21

1.4.3 Transmission des données des ayants droit à des tiers via l'utilisation de Mobile Payment

- Les données relatives à la carte et à la transaction nécessaires à l'exécution de celle-ci transitent par le serveur de l'organisme émetteur de la carte lors de la procédure de paiement. Des informations supplémentaires relatives au traitement des données, à la transmission de données et au recours à des tiers se trouvent dans les conditions d'utilisation des cartes, qui font l'objet d'un document à part;
- Lors de l'utilisation de Mobile Payment par le biais d'un fournisseur tiers, ce dernier collecte et traite des données conformément à ses propres conditions d'utilisation et de protection des données.

1.4.4 Transmission électronique de données

Les données des ayants droit à des cartes peuvent être transmises à des tiers (dans le pays ou à l'étranger) lors du recours à la transmission électronique de données, également sans intervention de la banque.

Les fabricants d'appareils ou de logiciels (par ex. Apple ou Google) peuvent notamment collecter des données personnelles lors de l'utilisation de l'application et/ou des appareils mobiles. Ils peuvent traiter et transmettre ces données conformément à leurs propres conditions d'utilisation et de protection des données. Cela peut leur permettre d'en déduire qu'il existe une relation entre l'ayant droit à la carte et la banque. Les SMS sont soumis aux dispositions légales applicables en matière de surveillance des télécommunications et sont enregistrés sur le téléphone portable. Des tiers peuvent ainsi entrer en possession des informations correspondantes.

1.5 Comment les données de l'ayant droit à la carte sont-elles protégées?

L'échange d'informations entre la banque, le processeur et l'application et/ou les appareils mobiles de l'ayant droit à la carte (hormis l'envoi de SMS) s'effectue de façon cryptée. Cette communication avec l'ayant droit à la carte se déroule cependant sur les réseaux de communication publics. Ces données sont en principe visibles par des tiers, elles peuvent être perdues lors du transfert ou interceptées par des tiers non autorisés. Il subsiste par conséquent la possibilité que, lors de l'utilisation de one, des tiers parviennent à accéder à la communication avec l'ayant droit à la carte, malgré toutes les mesures de sécurité. Le recours à Internet peut en outre impliquer le transfert de données via des pays tiers qui n'offrent parfois pas le même niveau de protection des données que la Suisse, si l'ayant droit à la carte se trouve en Suisse.

La sécurité des données dépend également du comportement de l'ayant droit à la carte. L'ayant droit à la carte est par conséquent tenu d'utiliser toutes les possibilités à sa disposition pour protéger ses appareils et ses données. Les obligations de diligence et de déclaration minimum qu'il convient de respecter à cet effet sont définies au chiffre I. Des mesures appropriées améliorent la sécurité et diminuent les risques liés à l'utilisation de one.

1.6 Quels sont les droits des ayants droit des cartes concernant leurs données?

- Renseignement sur les informations relatives aux données personnelles et sur le traitement de ces données par traitent ces dernières;
- Rectification des données personnelles incorrectes ou incomplètes;
- Suppression de données personnelles;
- Limitation du traitement des données;
- Dépôt d'une réclamation contre le mode de traitement des données personnelles auprès des autorités compétentes;
- Refus ou retrait des consentements relatifs au traitement des données personnelles.

Les droits des ayants droit de cartes ne peuvent être garantis par la banque que dans le respect des exigences réglementaires. Ainsi, même en cas de révocation d'un consentement, le traitement des données personnelles peut se poursuivre dans la mesure exigée par la loi.

1.7 Pendant combien de temps la banque conserve-t-elle les données?

La banque conserve les données aussi longtemps que cela est nécessaire pour les fins auxquelles elles ont été collectées. La banque conserve en outre les données personnelles parce que cela répond à un intérêt justifié, par ex. lorsque les données sont nécessaires pour faire valoir ou rejeter des droits, pour garantir la sécurité informatique ou à l'expiration des délais de prescription. Les données sont également conservées pour répondre aux obligations légales et réglementaires.

Version 08/2021

801 0005 VP72 7.21