Banque Cantonale de Fribourg
Freiburger Kantonalbank

Conditions d'utilisation BCF one

1. Conditions d'utilisation de one

1.1 Conditions d'utilisation des Services one et autres documents pertinents

Les présentes Conditions d'utilisation s'appliquent aux services en ligne désignés par le terme «one» (ci-après «**services**») et fournis par la Banque cantonale de Fribourg (la «**banque**») aux titulaires (les «**titulaires**») d'une carte Debit Mastercard de la banque (les «**cartes**»).

Viseca Payment Services SA (le «**sous-traitant**») agit en qualité de sous-traitant dans le cadre de la fourniture des services one et du traitement des opérations liées à la carte. Le titulaire autorise la banque à fournir au sous-traitant (et à ses éventuels prestataires de service) les données concernant le titulaire, la carte et le(s) compte(s) au(x)quel(s) la carte est rattachée. D'autres données (adresse et contact par ex.) peuvent également être transmises selon les fonctionnalités utilisées dans one. **En vue de ces communications, le titulaire délie la banque du respect du secret bancaire et professionnel (article 47 de la loi fédérale sur les banques et dispositions similaires).**

one est accessible par:
- le site Internet «one» (le «**site Internet**») et
- l'application «one» (l'«**application**»).

Des informations additionnelles sur le traitement des données personnelles des titulaires figurent dans la Déclaration de protection des données de la banque, la protection des données et conditions d'utilisation du sous-traitant ainsi que sur le site-Internet même.

Les présentes Conditions d'utilisation sont applicables en sus des Conditions d'utilisation des cartes Debit Mastercard de la banque (les Conditions d'utilisation DMC»). En cas de contradiction, les présentes Conditions d'utilisation priment sur les Conditions d'utilisation DMC.

Les présentes Conditions sont établies en langue française et en langue allemande. En cas de divergence, seule la version française fait foi, nonobstant d'éventuelles traductions des Conditions dans une autre langue.

1.2 Qu'est-ce-que one et comment est-ce développé?

one comprend des services de la banque, dispensés par le sous-traitant pour le compte de la banque. L'utilisation de one requiert une inscription préalable. Les nouveaux services introduits sont mis à disposition du titulaire moyennant des mises à jour (updates). La banque informe le titulaire de manière adéquate sur les développements et, le cas échéant, sur les changements des présentes conditions qui y sont liés.

1.3 Quelles fonctions propose one?

one peut – actuellement ou à l'avenir – comprendre en particulier les fonctions suivantes:
- Compte d'utilisateur pour l'administration de données personnelles;
- Contrôle et confirmation de paiements p. ex moyennant 3-D Secure (Mastercard Identity Check ou Visa Secure) avec l'application ou en entrant un code-SMS (cf. ch. 5);
- Contrôle et confirmation de certaines opérations (par ex. Logins, communications échangées avec la banque) avec l'application ou en entrant un code-SMS;
- Activation de cartes pour l'utilisation de moyens de paiement mobile (cf. ch. 6);
- Activation de la carte pour le service Click to Pay (cf. ch. 7);
- Echanges de messages et notifications de tout genre entre le titulaire et la banque (par ex. aussi communication d'une modification des dispositions), sous réserve d'une forme particulière de message ou de notification (par ex. contestation par écrit d'une facture mensuelle);
- Aperçu des transactions ou des cartes et affichage électronique des factures;
- Aperçu du compte du programme bonus et de la possibilité d'utiliser des points;
- Informations en lien avec l'utilisation de la carte.

2. Utilisation de one

2.1 Droit d'usage

Le titulaire n'est autorisé à utiliser one qu'aux conditions suivantes:
- Il est en mesure de mettre en œuvre les présentes conditions et les exigences qui s'y rattachent (en particulier ch. 3.2) et
- Il est autorisé à utiliser une carte de la banque en tant que titulaire d'une carte principale ou d'une carte supplémentaire de la banque.

2.2 Traitement de données personnelles dans le cadre des services one

En utilisant les services one, le titulaire prend acte que la banque (et le sous-traitant) procède(nt) aux traitements de données personnelles listés ci-dessous (en sus de ceux listés dans la Déclaration de protection des données de la banque) lesquels traitements sont fondés sur l'exécution du contrat conclu entre la banque et le titulaire dans le cadre de l'utilisation de one:
- **Traitement des données personnelles qui sont ou seront collectées lors de l'utilisation de one (soit les données d'identification du titulaire, les données relatives au compte auquel la carte est rattachée et les transactions opérées à travers la carte et/ou one).**
- **Communication électronique par e-mail (en utilisant l'adresse e-mail indiquée lors de l'inscription) ainsi qu'à travers l'application (par exemple notification de changements d'adresse, notification de modifications des Conditions d'utilisation ou notifications en lien avec la lutte contre l'utilisation frauduleuse de cartes).**

Par ailleurs, le titulaire prend acte que la banque (respectivement le sous-traitant lorsque le traitement est délégué) procède(nt) aux traitements de données personnelles suivants, sur la base de l'intérêt légitime de la banque à la promotion de ses produits et services:
- Réception de messages et informations concernant des produits et services de la banque à des fins de *marketing* (publicité). Ces messages peuvent être distribués par la banque par e-mail ou directement dans l'application ou sur le site Internet. Ces traitements de données personnelles comprennent en particulier le rattachement par la banque de données collectées dans le cadre de one avec les données déjà existantes dans le cadre de la relation-client pour la création de profils à des fins de *marketing* (mais également à des fins de gestion des risques).

Le titulaire peut indiquer en tout temps à la banque qu'il ne souhaite pas que la banque procède à des traitements de données personnelles le concernant en vue de proposer des produits et services et/ou à d'autres fins de marketing (droit «opt-out»). Une telle indication doit être communiquée par écrit à la banque en utilisant les coordonnées qui se trouvent dans la Déclaration de protection des données de la banque, avec effet pour l'avenir.

2.3 Refus de consentements dans le cadre du développement de one

Si le titulaire refuse de donner son consentement à des dispositions dans le cadre du développement de one (p. ex. lors de mises à jour), l'application ou le site Internet ou certains de leurs services individuels ne pourront, selon les circonstances, pas ou plus être utilisés.

2.4 Effet des confirmations

Chaque confirmation effectuée moyennant l'application ou la saisie d'un code-SMS est considérée comme une opération effectuée par le titulaire. Le titulaire a le droit d'apporter la preuve du contraire. Le titulaire s'engage à prendre à sa charge les débits de sa carte résultants de ces confirmations et autorise la banque à exécuter les ordres et démarches respectifs.

2.5 Disponibilité / blocage / modifications

La banque peut en tout temps, pour des raisons suffisantes, totalement ou partiellement et même sans préavis interrompre, limiter, suspendre ou remplacer par une autre prestation la possibilité d'utiliser one. La banque a en particulier le droit de bloquer temporairement ou définitivement l'accès du titulaire à one (par ex. en cas de soupçon d'abus).

2.6 Droits de propriété intellectuelle et licence

Tous les droits (en particulier droits d'auteur et droit des marques) sur les logiciels, textes, images, vidéos, noms, logos et autres données et informations, accessibles par one ou qui seront accessibles au cours du temps, appartiennent exclusivement à la banque ou aux partenaires et tiers respectifs (p. ex. Mastercard, Visa), sauf disposition contraire des présentes conditions. Les noms et logos visibles sur one sont des marques protégées.
La banque octroie au titulaire une licence non exclusive, non transmissible, de durée indéterminée, révocable et gratuite pour télécharger l'application, l'installer sur un appareil que le titulaire possède durablement et l'utiliser dans le cadre des fonctions prévues.
Sont en plus applicables à l'utilisation du site Internet, les Conditions de licence selon les Conditions d'utilisation du site Internet.

3. Risques, exclusion de garantie et obligation générale de diligence et de communiquer

3.1 Risques lors de l'utilisation de one

Le titulaire prend acte et accepte que l'utilisation de one comporte des risques.

En particulier, il est possible que lors de l'utilisation de one, des tiers non autorisés utilisent frauduleusement les cartes, le nom d'utilisateur et mot de passe, les appareils employés ou données personnelles. Ce faisant, le titulaire peut subir un préjudice financier (lorsque la carte est débitée) et une violation de ses droits de la personnalité (de par l'utilisation abusive de ses données personnelles). En outre, il existe un risque que one ou l'un des services proposés par one ne puisse pas être utilisé (p. ex. le login n'est pas possible sur one).

Les abus sont rendus possibles ou facilités en particulier par:
- la violation par le titulaire des obligations de diligence ou de communiquer (p. ex. lors du traitement négligent de son nom d'utilisateur / mot de passe ou l'absence d'annoncer une perte de la carte);
- les réglages sélectionnés par le titulaire ou le manque d'entretien des appareils et systèmes employés pour l'utilisation de one (p. ex. ordinateurs, téléphones portables, tablette, et autre infrastructure informatique), par exemple par l'absence d'un verrouillage d'écran, par l'absence ou l'insuffisance d'un pare-feu ou d'une protection anti-virus ou par un logiciel obsolète;
- des interventions de tiers ou d'erreurs dans la transmission de données sur Internet (tels que le piratage, le phishing ou la perte de données);
- des confirmations erronées dans l'application ou par l'insertion d'un code-SMS (p. ex. en cas de vérification manquante d'une demande de confirmation);
- la sélection effectuée par le titulaire de paramètres de sécurité faibles pour one, particulièrement pour l'application (p. ex. sauvegarde du login).

Si le titulaire respecte les obligations de diligence et de communiquer ci-dessous lors de l'utilisation des appareils mobiles et du mot de passe ainsi que les obligations de vérification des demandes de confirmation, il peut réduire ces risques d'utilisation abusive. De plus amples informations sur la réduction de risques lors de l'utilisation de one sont disponibles sur le site Internet.

La banque ne fournit aucune garantie et ne donne aucune assurance que le site Internet et l'application soient accessibles en permanence ou fonctionnent sans interruption ou que des abus peuvent être reconnus et évités avec certitude.

3.2 Obligation générale de diligence du titulaire

3.2.1 Obligation générale de diligence en lien avec les appareils et systèmes employés, en particulier les appareils mobiles

one emploie pour l'authentification, entre autres, des appareils mobiles (p. ex. téléphone mobile, tablette; ci-après «appareil mobile») du titulaire. De ce fait, la conservation soigneuse en permanence de ces appareils est un facteur de sécurité essentiel. Le titulaire doit employer les appareils mobiles avec la diligence appropriée et assurer leur protection adéquate.

Ainsi, le titulaire est tenu de respecter notamment les obligations de diligence suivantes en lien avec l'emploi des appareils et systèmes, en particulier des appareils mobiles:
- Pour les appareils mobiles, le titulaire doit activer un **verrouillage d'écran** et prendre d'autres mesures de sécurité afin d'éviter un déverrouillage par des tiers non autorisés;
- Les appareils mobiles doivent être conservés dans un lieu sécurisé de façon à être protégés contre l'accès d'un tiers, et ne doivent pas être remis à des tiers pour une utilisation permanente ou non contrôlée;
- Les logiciels (p. ex. les systèmes d'exploitation et le navigateur Internet) doivent être régulièrement mis à jour;
- Les interventions dans les systèmes d'exploitation (p. ex. «Jailbreaking» ou «Rooting») sont interdites;
- Une protection anti-virus et des logiciels «Internet-Security» doivent être installés sur les ordinateurs/ordinateurs portables et mis à jour régulièrement;
- L'application doit être téléchargée exclusivement depuis les Stores officiels (par ex. Apple Store et Google Play Store);
- Les mises à jour (Updates) de l'application doivent être immédiatement installées;
- Lors de la perte d'un appareil mobile, toute mesure possible doit être prise afin d'empêcher un accès par un tiers non autorisé des données transférées sur l'appareil mobile (par ex. en bloquant la carte-SIM, en bloquant l'appareil, en supprimant les données à distance par exemple moyennant ««Find My iPhone» ou «Gestionnaire d'appareils Android», en réinitialisant ou faisant réinitialiser le compte d'utilisateur). La perte doit être annoncée à la banque (cf. ch. 3.3);
- L'application doit être supprimée avant une vente ou un autre transfert permanent à des tiers.

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

Outre la possession de l'appareil mobile, le nom d'utilisateur et le mot de passe servent d'éléments supplémentaires à l'authentification du titulaire.

Le titulaire est tenu de respecter notamment les obligations de diligences générales suivantes en lien avec le mot de passe :

- le titulaire doit choisir un mot de passe qui n'est pas déjà employé pour d'autres services et qui ne doit pas être constitué de combinaisons facilement déchiffrables (telles que numéros de téléphone, dates de naissance, plaques minéralogiques, noms du titulaire ou de personnes proches, des suites de chiffres ou de lettres répétées ou qui se suivent directement telles que « 123456 » ou « aabbcc ») ;
- le mot de passe doit rester confidentiel. Il ne doit pas être divulgué ou rendu accessible à des tiers. Le titulaire prend acte que la banque ne demandera jamais au titulaire de divulguer son mot de passe ;
- Le mot de passe ne doit pas être noté ou être enregistré de manière non sécurisée ;
- Le titulaire doit modifier le mot de passe ou réinitialiser le compte d'utilisateur ou le faire réinitialiser par la banque lorsqu'il y a un soupçon qu'un tiers ait connaissance du mot de passe ou pris possession d'autres données ;
- La saisie du mot de passe doit être effectuée seulement de façon à ne pas être visible pour des tiers.

3.2.3 Obligations de diligence générales en lien avec les demandes de confirmation, et en particulier des contrôles

Les confirmations obligent le titulaire.

De ce fait, le titulaire est tenu de respecter les devoirs de diligence généraux suivants en lien avec les confirmations dans l'application ou par la saisie du code-SMS :

- Le titulaire ne peut confirmer que si la demande de confirmation est directement liée à une opération ou une démarche spécifique (par ex. le paiement, login, contact avec la banque) du titulaire ;
- Avant de confirmer, le titulaire doit vérifier si l'objet de la demande de confirmation correspond au processus concerné. Lors de demandes de confirmation en lien avec 3-D Secure, il convient notamment de vérifier les détails de paiement affichés.

3.3 Obligations générales de communiquer du titulaire

Les événements suivants doivent être immédiatement communiqués à la banque :

- Perte d'un appareil mobile, mais non pas un égarement de courte durée ;
- Demandes de confirmations qui ne sont pas en relation avec un paiement en ligne, un login effectué par le titulaire, un contact avec la banque ou d'autres processus semblables (soupçon d'abus) ;
- Toute autre suspicion, qu'une demande de confirmation dans l'application ou le code-SMS ne proviennent pas de la banque ;
- Cas de soupçon d'abus du nom d'utilisateur, du mot de passe, des appareils mobiles, du site Internet, de l'application, etc. ou qu'un tiers non autorisé soit entré en possession de ces informations ou objets ;
- Changement du numéro de téléphone et d'autres données personnelles pertinentes ;
- Changement de l'appareil mobile qui est utilisé pour one (dans ce cas, l'application doit être enregistrée à nouveau).

Le titulaire doit signaler immédiatement les événements à la banque. Entre autres, d'éventuels abus ou la perte d'un appareil mobile sont à signaler immédiatement par téléphone à la banque (24 heures sur 24) : tél. +41 (0)848 223 223.

4. Responsabilité

Il appartient au titulaire de mettre en oeuvre les obligations de diligence afin de prévenir l'utilisation non autorisée de one. Il appartient au titulaire de prendre des mesures appropriées afin de prévenir le risque de fraude dans l'utilisation de one. Le titulaire supporte tout dommage résultant de la violation de ses devoirs de diligence.

Plus généralement, les dommages résultant de défauts de légitimation ou de fraudes non décelées sont à la charge du titulaire, sauf en cas de faute grave de la banque.

5. 3-D Secure

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

3-D Secure est un standard de sécurité reconnu internationalement pour les paiements par carte en ligne. Il est appelé « Mastercard Identity Check » par Mastercard et « Visa Secure » par Visa. Sur la base des Conditions utilisation DMC, le titulaire est tenu d'utiliser ces standards de sécurité lors de paiements, dans la mesure où ceux-ci sont proposés par le point d'acceptation (le commerçant).

L'utilisation de 3-D Secure est uniquement possible après l'inscription auprès de one.

5.2 Comment fonctionne 3-D Secure ?

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

- Dans l'application ou,
- Par la saisie du code que la banque envoie au titulaire par message (code-SMS) dans la fenêtre du navigateur correspondant durant le processus de paiement.

Conformément aux Conditions utilisation DMC, chaque utilisation autorisée de la carte moyennant 3-D Secure est considéré comme ayant été effectuée par le titulaire.

5.3 Activation de cartes pour 3-D Secure

Lors de l'inscription auprès de one, 3-D Secure est activé pour toutes les cartes au nom du titulaire qui sont en lien avec la relation d'affaires entre le titulaire et la banque.

5.4 Désactivation de cartes pour 3-D Secure

Pour des raisons de sécurité, 3-D Secure ne peut plus être désactivé après une activation.

6. Paiement Mobile

6.1 Qu'est-ce que le Paiement Mobile (ci après « Mobile Payment ») ?

Mobile Payment désigne des solutions pour l'utilisation de cartes via un appareil mobile. Mobile Payment permet au titulaire qui dispose d'un appareil mobile compatible d'utiliser des cartes éligibles via une application mobile (app) de Viseca (cf. ch. 6.7) ou d'un fournisseur tiers pour le paiement sans contact ainsi que pour le paiement dans des boutiques en ligne ou dans le cadre d'apps. Pour des raisons de sécurité, un numéro différent (token) est généré à la place du numéro de carte et stocké comme « carte virtuelle ». Les cartes virtuelles peuvent être utilisées comme une carte physique par Mobile Payment. Lors d'un paiement par carte virtuelle, ce n'est pas le numéro de carte, mais seulement le numéro généré (token) qui est transmis au commerçant.

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

Sont compatibles des appareils mobiles tels que p. ex. les ordinateurs, téléphones mobiles, smart watches et fitness trackers, pour autant qu'ils supportent l'utilisation de cartes virtuelles et soient approuvés par la banque. La banque décide en outre quelles cartes peuvent être activées pour quels fournisseurs.

6.3 Activation et désactivation

Pour des raisons de sécurité, l'activation d'une carte implique que le titulaire accepte les conditions d'utilisation du fournisseur concerné et qu'il prenne connaissance de ses dispositions relatives à la protection des données. Le titulaire répond envers la banque de tout dommage résultant de la violation de ces conditions.

Les cartes virtuelles peuvent être employées jusqu'au blocage ou à la désactivation par le titulaire à travers l'app. Les restrictions de l'utilisation des cartes conformément aux dispositions des Conditions utilisation DMC applicables restent réservées. Le titulaire peut à tout moment mettre fin à l'utilisation de Mobile Payment en retirant sa/ses carte(s) virtuelle(s) enregistrée(s) auprès du fournisseur concerné.

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

6.4 Utilisation de la carte virtuelle (autorisation)

L'utilisation d'une carte virtuelle correspond à une transaction par carte normale. **Toute utilisation d'une carte virtuelle est réputée autorisée par le titulaire.** Le titulaire a le droit d'apporter la preuve du contraire.

L'utilisation de cartes virtuelles doit conséquemment être autorisée de la façon prévue par le fournisseur ou le distributeur, p. ex. en entrant un code NIP pour l'appareil, par empreintes digitales ou par reconnaissance faciale. Le titulaire **prend acte du fait que le choix d'une combinaison trop simple (par ex. « 1234 ») comme moyen d'autorisation (code PIN de l'appareil ou de la carte) éventuellement requis par le fournisseur ou le commerçant augmente le risque qu'une carte virtuelle puisse être utilisée par une personne non autorisée**. Il prend également acte du fait que les fournisseurs et commerçants sont libres de définir un montant au-dessous duquel aucun moyen d'autorisation ne sera demandé. Pour le surplus, la responsabilité se détermine à l'aune du ch. 4 des présentes dispositions.

6.5 Obligations de diligence particulières

Le titulaire prend acte et accepte qu'en dépit de toutes les mesures de sécurité, l'utilisation de Mobile Payment comporte des risques. Il est notamment possible que la/les carte(s) virtuelle(s) et les données personnelles puissent faire l'objet d'une utilisation frauduleuse ou être consultées par des personnes non autorisées. Ce faisant, le titulaire peut subir un préjudice financier (lorsque la carte est débitée en raison d'une utilisation frauduleuse) et une violation de ses droits de la personnalité (de par l'utilisation abusive de ses données personnelles).

Le titulaire doit par conséquent manipuler les appareils et cartes virtuelles utilisés avec soin et veiller à les protéger. Au-delà des obligations de diligence selon les Conditions utilisation DMC et des obligations générales de diligence et de signalement au sens des ch. 3.2.1 et 3.3, le titulaire est notamment tenu au respect des obligations de diligence spéciales suivantes :

- Les appareils utilisés doivent l'être de façon conforme à leur destination et être stockés en toute sécurité **à l'abri de tout accès par des tiers**;
- **à l'instar des cartes physiques, les cartes virtuelles sont personnelles et non transmissibles.** Elles ne doivent pas être transmises à des tiers pour utilisation (par ex. en sauvegardant des empreintes digitales ou en scannant le visage de tiers pour déverrouiller l'appareil utilisé);
- en cas de changement ou de transmission d'un appareil mobile (p. ex. en cas de vente), chaque carte virtuelle devra être supprimée de l'app et de l'appareil mobile du fournisseur;
- **tout soupçon d'utilisation abusive d'une carte virtuelle ou d'un appareil utilisé à cette fin doit être immédiatement signalé à la banque afin que la carte virtuelle concernée puisse être bloquée.**

6.6 Exclusion de garantie

Il n'existe aucun droit à l'utilisation de Mobile Payment. La banque peut à tout moment interrompre ou mettre fin à l'utilisation – c.-à-d. la possibilité d'utiliser des cartes virtuelles –, notamment pour des raisons de sécurité ou en cas de modification de l'offre Mobile Payment ou de restriction des cartes ou appareils compatibles autorisés. La banque n'est en outre pas responsable des actes et des offres du fournisseur ou d'autres tiers, comme p. ex. des opérateurs Internet ou de téléphonie.

6.7 Utilisation de la carte par le biais de l'app one

Le titulaire qui dispose d'un appareil compatible peut activer sa/ses carte(s) dans l'app one de la banque et l'utiliser comme carte virtuelle. Afin de garantir la sécurité du Mobile Pay, le titulaire doit définir un code secret lors de l'activation. La banque peut adapter ce service à tout moment. Pour le surplus, les présentes dispositions pour Mobile Payment sont applicables, notamment les obligations de diligence spéciales au sens du ch. 6.5.

6.8 Protection des données

Le fournisseur tiers et la banque répondent de façon indépendante de leur traitement respectif de données personnelles. Le titulaire prend acte du fait que les données personnelles sont collectées par le fournisseur tiers en rapport avec l'offre et l'utilisation de Mobile Payment (notamment les indications concernant le titulaire et les cartes activées ainsi que les données de transaction de l'utilisation de cartes virtuelles) et qu'elles sont sauvegardées et soumises à un traitement subséquent en Suisse ou à l'étranger. Le traitement des données personnelles par le fournisseur tiers dans le cadre de Mobile Payment et l'utilisation des offres et services du fournisseur tiers, y compris ses appareils et logiciels, sont régis par ses dispositions en matière d'utilisation et de protection des données. **Le titulaire confirme par conséquent par chaque activation de carte qu'il a lu les dispositions de protection des données pertinentes du fournisseur tiers concerné et qu'il consent expressément au traitement correspondant des données par le fournisseur tiers.** S'il ne souhaite pas le traitement en question, il appartient au titulaire de renoncer à l'activation d'une carte ou de s'opposer au traitement par le fournisseur tiers. Pour le traitement des données personnelles par la banque et le sous-traitant, la déclaration de protection des données de la banque ainsi que la Déclaration générale de protection des données de Viseca s'appliquent.

7. Click to Pay

Click to Pay est une initiative des organismes internationaux de carte Mastercard et Visa (« **organisme de carte** »), qui simplifie le paiement lors d'achats en ligne. Pour utiliser cette méthode de paiement, il est nécessaire d'enregistrer la carte ainsi que l'adresse e-mail et l'adresse de livraison auprès de l'organisme de carte. Une fois l'enregistrement effectué, le titulaire peut effectuer ses achats en ligne avec son adresse e-mail partout où le symbole Click to Pay est affiché, sans avoir à saisir les détails de la carte.

Le titulaire peut enregistrer la carte pour Click to Pay via one. Cet enregistrement suppose que le titulaire a accepté les conditions d'utilisation de l'organisme de carte et qu'il a pris connaissance de ses dispositions en matière de protection des données. Le titulaire accepte que, lors de l'enregistrement de la carte, **le sous-traitant transmette à l'organisme de carte des informations relatives à la carte, son nom et ses coordonnées telles que l'adresse de facturation et de livraison, son adresse e-mail et son numéro de téléphone**. Les informations relatives aux cartes et aux coordonnées qui sont enregistrées pour les paiements peuvent être traitées et effacées en tout temps dans le compte utilisateur Click to Pay.

L'utilisation de Click to Pay est soumise aux conditions d'utilisation et aux instructions de l'organisme de carte concerné. La banque ne répond pas des dommages résultant de l'utilisation de Click to Pay.

Etant donné que l'adresse de livraison enregistrée peut ne pas correspondre à l'adresse de livraison souhaitée, le titulaire est tenu de contrôler l'adresse de livraison transmise au commerçant dans le cadre du processus de paiement avec Click to Pay. La saisie d'adresses de livraison pendant le paiement n'entraîne pas la modification de l'adresse enregistrée à la banque.

L'organisme de carte peut en tout temps développer ou bloquer Click to Pay, notamment s'il y a des raisons de penser que Click to Pay est utilisé de manière abusive.

Les titulaires peuvent en tout temps mettre fin à Click to Pay en retirant la carte enregistrée auprès des organismes de carte.