valiant

Conditions d'utilisation
de la Banque Valiant SA concernant

l'utilisation de one

A Partie générale

1. Conditions générales d'utilisation de one

1.1 Conditions d'utilisation de one et autres documents pertinents
Les présentes Conditions Générales sont applicables pour les services en ligne (ci-après « services ») fournis par la Banque Valiant SA (ci-après « banque ») au titulaire (ci-après « ayant droit de la carte ») d'une carte principale ou supplémentaire ou business de la banque (ci-après «carte(s) ») sous le nom « one ». Viseca Payment Services SA (ci-après « responsable du traitement ») assure le traitement de one. La banque a recours au responsable du traitement pour remplir ses obligations découlant des opérations liées à la carte.

one est accessible moyennant :
- Le site Internet one («site Internet») et
- L'application one («application»)

Il convient de tenir compte des informations complémentaires concernant one – particulièrement relatives au traitement des données et à la sécurité des données – dans la déclaration de protection des données de la banque (« Déclaration de protection des données de la banque »), les dispositions relatives à la protection des données sous le point C et les conditions d'utilisation des services numériques one du responsable du traitement («Conditions d'utilisation one»)

Les présentes Conditions sont applicables en plus des dispositions applicables pour l'utilisation de cartes de la banque (ci-après « CG-cartes-Valiant »). En cas de règles divergentes, les présentes conditions priment sur les CG-cartes-Valiant.

La banque se réserve le droit de modifier ces dispositions à tout moment. Les modifications seront communiquées aux ayants droit à la carte de manière appropriée.

1.2 Qu'est-ce-que one et comment est-ce développé ?
one comprend des services de la banque, dispensés par le responsable du traitement pour le compte de la banque. L'utilisation de one requiert une inscription préalable. Les nouveaux services introduits sont mis à disposition de l'ayant droit de la carte moyennant des mises à jour (updates). La banque informe l'ayant droit de la carte 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 (p. 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 (cf. ch. 5, ch. 6 et 7) ;
- Echanges de messages et notifications de tout genre entre l'ayant droit de la carte et la banque (p. ex. aussi communication d'une modification des dispositions), sous réserve d'une forme particulière de message ou de notification (p. ex. contestation par écrit d'une facture mensuelle) ;
- Blocage de cartes et commande de cartes de remplacement et affichage de codes PIN ;
- Aperçu des transactions ou des cartes et affichage électronique des factures (actuellement sous MyAccount) ;
- Aperçu du compte du programme bonus et de la possibilité d'utiliser des points (actuellement sous compte-surprize) ;
- Notifications push, services SMS ;
- Informations en lien avec l'utilisation de la carte (actuellement services SMS).

2. Utilisation de one

2.1 Droit d'usage
L'ayant droit de la carte n'est autorisé d'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. 3.2.1. et ch. 3.2.3) et
- Il est autorisé d'utiliser une carte de la banque en tant que titulaire d'une carte principale ou d'une carte supplémentaire ou d'une carte business de la banque.

2.2 Consentement lors de l'inscription et dans le cadre du développement de one

De par l'utilisation de one, l'ayant droit de la carte donne à la banque expressément les consentements suivants :

- Consentement au traitement de données qui sont ou seront prélevées lors de l'utilisation de one. Cela comprend en particulier également le consentement au rattachement par la banque de ces données avec les données déjà existantes et à la création de profils, respectivement à des fins de gestion des risques et de marketing par la banque ou le responsable du traitement et de tiers conformément à la déclaration de protection des données de one.
- Consentement à la réception de messages et informations concernant des produits et services de la banque et de tiers à des fins de marketing (publicité). Ceux-ci peuvent être distribués par la banque par e-mail ou directement dans l'application ou sur le site Internet.
- Consentement à l'utilisation de l'adresse e-mail et du numéro de téléphone indiqués lors de l'inscription ainsi qu'à la communication électronique avec la banque par e-mail ainsi que moyennant l'application (p. ex. notification de changements d'adresse, notification de modifications des conditions (Conditions Générales) ou de notifications en lien avec la lutte contre l'utilisation frauduleuse de cartes).
- Le consentement à la réception de messages et de produits et services et/ou au traitement des données à des fins de marketing peut être révoqué à tout moment avec effet pour l'avenir en informant la banque par écrit (droit « opt-out »). Les coordonnées se trouvent dans la declaration de confidentialité de la banque.

2.3 Refus de consentement dans le cadre du développement de one

Si l'ayant droit de la carte 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 l'ayant droit de la carte. L'ayant droit de la carte 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 de l'ayant droit de la carte à one (p. 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. responsable du traitement, Mastercard, Visa), sauf disposition contraire des présentes conditions. Les noms et logos visibles sur one sont des marques protégées.

La banque octroie à l'ayant droit de la carte une licence non exclusive, non transmissible, de durée indéterminée, révocable et gratuite pour télécharger l'application, l'installer sur un appareil que l'ayant droit de la carte 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 (sous le titre de « Propriété intellectuelle du site web, droit des marques et droits d'auteur »).

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

3.1 Risques lors de l'utilisation de one

L'ayant droit de la carte 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 de l'ayant droit de la carte. Ce faisant, l'ayant droit de la carte 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 peut 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 l'ayant droit de la carte 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 l'ayant droit de la carte 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 l'ayant droit de la carte de paramètres de sécurité faibles pour one, particulièrement pour l'application (p. ex. sauvegarde du login).

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 de l'ayant droit de la carte

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 ») de l'ayant droit de la carte. De ce fait, la conservation soigneuse en permanence de ces appareils est un facteur de sécurité essentiel. L'ayant droit de la carte doit employer les appareils mobiles avec la diligence appropriée et assurer leur protection adéquate.

Ainsi, l'ayant droit de la carte 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 (p. 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 à la banque sur l'appareil mobile (p. 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 de l'ayant droit de la carte.

L'ayant droit de la carte est tenu de respecter notamment les obligations de diligences générales suivantes en lien avec le mot de passe :

- l'ayant droit de la carte 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 de l'ayant droit de la carte 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. L'ayant droit de la carte prend acte que la banque ne demandera jamais à l'ayant droit de la carte de divulguer son mot de passe ;
- le mot de passe ne doit pas être noté ou être enregistré de manière non sécurisée ;
- l'ayant droit de la carte 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

Toute confirmation effectuée via l'application ou la saisie d'un code SMS est considérée comme une action de la part de l'utilisateur.

De ce fait, l'ayant droit de la carte 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 :

- l'ayant droit de la carte ne peut confirmer que si la demande de confirmation est directement liée à une opération ou une démarche spécifique (p. ex.

le paiement, login, contact avec l'émettrice) de l'ayant droit de la carte ;
- avant de confirmer, l'ayant droit de la carte 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 de l'ayant droit de la carte

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 l'ayant droit de la carte, 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).

D'éventuels abus ou la perte d'un appareil mobile sont à signaler immédiatement par téléphone au centre des cartes de la Banque Valiant SA (24 heures sur 24) : +41 (0)31 952 20 50.

4. Responsabilité

4.1 Responsabilité générale en cas de dommage

Sous réserve du ch. 4.2., la banque prend en charge les dommages (sans aucune franchise) qui ne sont pas pris en charge par une assurance,

- lorsque ces dommages :
  - ont été causés par une intervention illégale avérée dans les installations des opérateurs de réseau et/ou de télécommunication ou dans les appareils et/ou systèmes utilisés par l'ayant droit de la carte (p. ex. ordinateurs, appareils mobiles et autre infrastructure électronique) et
  - que l'ayant droit de la carte a respecté les obligations générales et particulières de diligence et de communiquer indiquées ci-dessus sous ch. 3.2 et 3.3, en particulier l'obligation de vérification des demandes de confirmation et l'obligation figurant dans les CG-cartes-Valiant de vérification des factures mensuelles et de contestation de transactions abusives en temps utile, et
  - qu'aucune autre faute en lien avec la survenance des dommages n'est imputable à l'ayant droit de la carte ;
- lorsque ces dommages ont été causés exclusivement par une violation du devoir de diligence usuel dans la profession de la banque.

La banque décline toute responsabilité pour les éventuels dommages indirects ou consécutifs de l'ayant droit de la carte sous quelque forme que ce soit, sous réserve des cas de vol ou de négligence grave.

4.2 Exceptions

L'ayant droit de la carte est responsable et la banque décline toute responsabilité pour les dommages dans les cas suivants :

- Lorsque ces dommages ne sont pas pris en charge par la banque conformément au ch. 4.1 (ainsi en particulier lors de la violation des obligations de diligence et de communiquer de l'ayant droit de la carte), ou
- Lorsque l'ayant droit de la carte, son/sa conjoint(e), la parenté directe (en particulier les enfants et les parents), les autres personnes proches de l'ayant droit de la carte, les représentants et/ou toute personne vivant dans le même ménage ont effectué une action (p. ex. confirmation dans l'application ou par saisie du code SMS).

B Partie spéciale

Par ailleurs, les dispositions suivantes s'appliquent aux personnes qui utilisent les services 3-D Secure, Mobile Payment et Click to Pay.

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 CG-cartes-Valiant, l'ayant droit de la carte est tenu d'utiliser ces standards de sécurité lors de paiements, dans la mesure où ceux-ci sont proposés par le point d'accep-
tation (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 à l'ayant droit de la carte par message (code SMS) dans la fenêtre du navigateur correspondant durant le processus de paiement.

Conformément aux CG-cartes-Valiant , chaque utilisation autorisée de la carte moyennant 3-D Secure est considéré comme ayant été effectuée par l'ayant droit de la carte.

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 de l'ayant droit de la carte qui sont en lien avec la relation d'affaires entre l'ayant droit de la carte 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. Mobile Payment

6.1 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 de la carte qui dispose d'un appareil mobile compatible d'utiliser des cartes éligibles via une application mobile de la banque (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'applications. 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 l'ayant droit de la carte accepte les conditions d'utilisation du fournisseur concerné et qu'il prenne connaissance de ses dispositions relatives à la protection des données. L'ayant droit de la carte 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 l'ayant droit de la carte à travers l'application. Les restrictions de l'utilisation des cartes conformément aux dispositions des CG-cartes-Valiant applicables restent réservées. L'ayant droit de la carte 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 de l'ayant droit de la carte.

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 l'ayant droit de la carte. L'ayant droit de la carte 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 PIN pour l'appareil, par empreintes digitales ou par reconnaissance faciale. L'ayant droit de la carte prend acte du fait que le choix d'une combinaison trop simple (p. 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

L'ayant droit de la carte 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, l'ayant droit de la carte 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).

L'ayant droit de la carte 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 CG-cartes-Valiant et des obligations générales de diligence et de signalement au sens des ch. 3.2.1 et 3.3, l'ayant droit de la carte 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 (p. 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'application
- 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, tels que des opérateurs Internet ou de téléphonie.

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

L'ayant droit de la carte qui dispose d'un appareil compatible peut activer sa/ses carte(s) dans l'application one de l'émettrice et l'utiliser comme carte virtuelle. Afin de garantir la sécurité du Mobile Pay, l'ayant droit de la carte 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 Mobile Payment

Le fournisseur tiers et la banque répondent de façon indépendante de leur traitement respectif de données personnelles. L'ayant droit de la carte 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. L'ayant droit de la carte 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 responsable du traitement, la déclaration relative à la protection des données ci-dessous (C), la déclaration de confidentialité de la banque ainsi que les conditions d'utilisation one s'appliquent.

7. Click to Pay

7.1 Qu'est-ce que 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. Au lieu de saisir manuellement les données de carte lors d'achats en ligne, l'utilisateur peut traiter le processus de paiement plus simplement avec Click to Pay, une fois l'enregistrement effectué.

7.2 Activation et désactivation

Pour l'activation de Click to Pay, il est nécessaire d'enregistrer la carte ainsi que l'adresse e-mail, le numéro de téléphone et l'adresse de livraison auprès

de l'organisme de carte. Une fois l'enregistrement effectué, l'utilisateur 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. L'utilisateur peut enregistrer la carte pour Click to Pay dans l'application. Cet enregistrement suppose que l'utilisateur a accepté les conditions d'utilisation de l'organisme de carte et qu'il a pris connaissance des dispositions en matière de protection des données.

Une fois la carte enregistrée, Viseca transmet, avec le consentement de l'utilisateur, les informations relatives à la carte, à l'adresse e-mail, au numéro de téléphone et à l'adresse de livraison à l'organisme de carte. Les informations relatives aux cartes, à l'adresse e-mail, au numéro de téléphone et à l'adresse de livraison qui sont enregistrées par les paiements peuvent être modifiées et effacées en tout temps dans le compte utilisateur de Click to Pay de l'organisme de carte.

Les utilisateurs peuvent en tout temps mettre fin à l'utilisation de Click to Pay en retirant la carte enregistrée dans le compte utilisateur Click to Pay de l'organisme de carte.

7.3 Devoirs de diligence particuliers

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, l'utilisateur 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 ni la modification de l'adresse de livraison principale enregistrée, ni celle de l'adresse de facturation enregistrée auprès de 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.

C Déclaration relative à la protection des données pour one

Les dispositions suivantes relatives à la protection des données vous informent sur la manière dont la banque traite vos données personnelles (ou « données ») en tant que responsable du traitement. Le traitement comprend toute utilisation de données personnelles, en particulier la collecte, l'enregistrement, l'utilisation, la divulgation ou la suppression de données. Vous trouverez les données de contact pour tout renseignement au sujet de la protection et du traitement des données dans la déclaration de protection des données de la banque.

Les ayants droit de la carte déclarent consentir expressément aux traitements de données figurant dans la présente déclaration de protection des données lors de leur inscription à one. Vous trouverez des informations sur d'autres traitements de données dans le cadre de la relation de carte dans les conditions générales des cartes Valiant et dans les conditions d'utilisation de one. Veuillez également tenir compte des Déclarations relatives à la protection des données au niveau mondial ainsi que des droits que vous pouvez exercer en tant que tiers bénéficiaires de Mastercard® et Visa.

8. Traitement des données personnelles

8.1. Quel est l'objet de la déclaration relative à la protection des données de one ?

Via le site Internet ou l'application, le programme bonus surprize, resp. en combinaison avec une Business Card ou Corporate Card, la banque met à disposition, sous la dénomination « one », différents services en ligne en lien avec l'utilisation des cartes que nous émettons (collectivement **« services numériques one »**). La mise à disposition des services requiert de la banque un traitement des données des ayants droit de la carte. La présente Déclaration relative à la protection des données informe les ayants droit de la carte de manière détaillée et transparente sur le traitement des données lors de l'utilisation des services numériques one.

8.2. Comment les données sont-elles recueillies ?

8.2.1 Quelles données relatives à l'ayant droit de la carte sont divulguées ?

Lors de l'enregistrement pour les services numériques one, lors de l'inscription et lors de l'administration du compte d'utilisateur, l'ayant droit de la carte peut être tenu d'indiquer l'adresse e-mail, la date de naissance, le numéro de téléphone mobile, l'adresse de livraison, le numéro de carte et le code d'activation.

8.2.2 Quelles données sont collectées automatiquement ?

- Les données concernant l'utilisation d'appareils mobiles par l'ayant droit de la carte, telles que le fabricant, le type d'appareil, le système d'exploitation avec numéro de version, l'identifiant de l'appareil, l'adresse IP
- Les données concernant l'utilisation d'ordinateurs et de navigateurs ainsi que l'accès à Internet, telles que le type d'appareil, le système d'exploitation, l'adresse IP
- Les données concernant l'utilisation du compte utilisateur, telles que le nombre de logins avec date et heure, les modifications du compte utilisateur, l'acceptation de conditions d'utilisation des services numériques one et de la Déclaration relative à la protection des données
- Les données concernant les paramètres choisis par l'ayant droit de la carte, telles que l'enregistrement du nom d'utilisateur ou du login
- Les données concernant les visites et le comportement d'utilisateur sur le site web, ainsi que
- Les données liées à l'utilisation de l'application, telles que les mises à jour ou informations sur l'appareil ainsi que le comportement d'utilisateur, p.ex. dans l'application ou par code SMS

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

- Les informations relatives à l'ayant droit et à ses cartes enregistrées pour one, sauvegardées dans le compte utilisateur
- L'information selon laquelle 3-D Secure est utilisé pour les cartes enregistrées par une confirmation dans l'application ou par la saisie d'un code SMS
- Adresse de livraison et numéro de téléphone mobile

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

- Informations sur l'utilisation de Mobile Payment, telles que l'activation ou la désactivation de cartes et l'utilisation des cartes pour Mobile Payment
- Informations sur le montant de la transaction
- Informations sur l'utilisation de la carte, le moment de la transaction, le mode d'authentification

Lors de l'utilisation d'une solution de paiement mobile d'un fournisseur tiers, ce dernier peut également collecter et traiter les données personnelles de l'ayant droit de la carte Selon l'offre, il peut s'agir, par exemple, du nom, du numéro de carte et, le cas échéant, des données de transaction. De plus, les dispositions d'utilisation ou de protection des données du fournisseur tiers doivent être respectées.

8.2.5 Quelles informations sont collectées lors de l'utilisation de Click to Pay ?

- Informations sur la carte
- Informations sur l'ayant droit de la carte (prénom, nom, numéro de téléphone mobile, adresse de livraison, adresse e-mail)

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

- Informations concernant le commerçant, la transaction et son exécution, ainsi que la confirmation de la transaction avec 3-D Secure
- Informations en lien avec les appareils qui sont utilisés pour la transaction et la confirmation
- Informations en lien avec l'accès à Internet ou au

réseau mobile, telles que l'adresse IP, le nom du fournisseur d'accès

8.2.7 Quelles données sont collectées lors de l'affichage de la section de carte correspondant à la localisation du commerçant?
- Données de localisation des commerçants établis en Suisse,
- telles que le nom du commerçant, la localité, le pays et le secteur
- Requête Google automatique périodique pour préciser la localisation du commerçant

8.3. Dans quel but la banque traite-t-elle mes données?

8.3.1 Fourniture des services et exécution du contrat de carte
- Permettre l'enregistrement, l'inscription et l'utilisation des services numériques one par l'ayant droit de la carte
- Mise en place d'une connexion sécurisée entre services numériques one et l'appareil mobile de l'ayant droit de la carte
- Transmission à l'ayant droit de demandes de confirmation, p. ex. confirmation de paiements en ligne via les services numériques one, par des notifications Push ou par code SMS
- Transmission de l'information sur les confirmations qui ont été faites à la banque
- Authentification de l'ayant droit par l'exécution d'actions. Lors de l'enregistrement sur one, l'application ou l'appareil mobile utilisés sont clairement attribués à l'ayant droit de la carte. 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 de la carte et transmission d'informations en lien avec la relation de cartes ou l'utilisation de cartes (p. ex. informations concernant de nouvelles factures, mises en garde contre des fraudes ou demandes lors de transactions inhabituelles) sur les services numériques one et le téléphone mobile
- Avis de transactions et factures
- Exécution du contrat de carte avec l'ayant droit de la carte et des transactions réalisées avec la carte. A cet effet, il est renvoyé à la déclaration de protection des données de la banque ainsi qu'aux conditions d'utilisation de one.
- Exploitation de la boutique de primes surprize et comptabilité des points
- Exploitations de transactions en ligne 3-D Secure

8.3.2 Mobile Payment
- Pour décider de l'autorisation de la carte pour Mobile Payment
- Pour l'activation, la désactivation et la mise à jour de cartes pour Mobile Payment
- Pour empêcher tout usage abusif des cartes ajoutées
- Le cas échéant, pour la communication avec tout fournisseur tiers d'une solution de paiement mobile dans le cadre des présentes dispositions et des dispositions d'utilisation ou de protection des données du fournisseur concerné, qui s'appliquent dans la relation entre l'ayant droit de la carte et le fournisseur tiers.

8.3.3 Click to Pay
- Pour l'enregistrement de la carte auprès des organismes de cartes
- Pour le traitement par les organismes de cartes dans le cadre de leurs propres dispositions d'utilisation et de protection des données

8.3.4 Marketing
- Pour associer ces données à des données déjà disponibles à la banque (également données de tiers)
- Pour créer des profils individuels de clients, des profils de consommation et de préférences qui permettent à la banque de développer et d'offrir des produits et services à l'ayant droit de la carte
- Pour la transmission d'informations concernant des produits et services existants ou nouveaux de la banque ainsi que de tiers (matériel publicitaire) à l'ayant droit de la carte
- Pour le traitement par le fournisseur tiers dans le cadre de ses propres dispositions d'utilisation ou de protection des données

8.3.5 Autres buts du traitement
- Évaluation des risques de crédit et de marché pertinents
- Améliorer la sécurité lors de l'utilisation des services, par exemple par la diminution du risque de transactions abusives ou d'abus d'appareils ou de moyens de légitimation par exemple par du phishing ou du hacking
- Preuve d'opérations et défense contre des prétentions à l'encontre de la banque
- Amélioration des prestations générales de la banque ainsi que des services numériques one
- Respect des exigences légales et réglementaires
- Traitement par le fournisseur tiers dans le cadre de ses propres dispositions d'utilisation ou de protection des données

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

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

Les tiers sont des personnes ou des sociétés qui traitent des données à leurs propres fins. Les prestataires mandatés par la banque ne sont pas des tiers. Dans le cadre des cartes auxquelles s'appliquent les Conditions générales de la banque et les Conditions générales d'utilisation des Business Cards et Corporate Cards, la banque ne donne aucune donnée – en particulier aucune donnée de transaction – à des tiers pour leurs propres fins, sous réserve des dispositions suivantes, à moins que l'ayant droit de la carte ne consente à une telle transmission ou ne le demande ou n'y fasse procéder lui-même. En particulier, la banque ne transmet à des tiers aucun profil individuel de client, profil consommation et profil préférence, créé par elle sans le consentement distinct et exprès de l'ayant droit de la carte.

8.4.2 Autres catégories de tiers auxquelles des données peuvent être divulguées
- Les données (également données de transaction) du titulaire de la carte supplémentaire peuvent être communiquées au titulaire de la carte principale
- Sur ordre d'une autorité ou en vertu d'une obligation légale, la banque communique les données à des autorités étatiques, telles que des autorités de poursuite pénale ou de surveillance.

8.4.3 Transmission des données de l'ayant droit à des tiers par l'utilisation de Mobile Payment
- Les données relatives aux cartes et aux transactions nécessaires à l'exécution de la transaction sont redirigées sur les serveurs des organisations de cartes pendant le processus de paiement. De plus amples informations sur le traitement, la transmission de données et le recours à des tiers sont disponibles dans les conditions générales des cartes Valiant.
- Lors de l'utilisation de Mobile Payment via un fournisseur tiers, ce dernier collecte et traite des données conformément à ses propres dispositions d'utilisation ou de protection des données.

8.4.4 Transmission de données par voie électronique
Les données de l'ayant droit de la carte peuvent, également sans intervention de la banque, parvenir à des tiers (en Suisse ou à l'étranger) par la transmission de données par voie électronique.

En particulier lors de l'utilisation de l'application et/ou d'appareils mobiles, les fabricants d'appareils ou de logiciels (p. ex. Apple ou Google) peuvent recevoir des données à caractère personnel. Ceux-ci peuvent traiter et transmettre les données conformément à leurs propres dispositions d'utilisation ou de protection des données. Cela peut conduire à ce que ces tiers concluent à l'existence d'une relation entre l'ayant droit de la carte et la banque. Les SMS sont soumis aux dispositions légales sur la surveillance des télécommunications applicables et sont enregistrés sur le téléphone mobile. Des tiers peuvent ainsi avoir accès aux informations en question.

8.5. Comment protégeons-nous vos données ?
La transmission d'informations entre la banque, le responsable du traitement et l'application et/ou les appareils mobiles de l'ayant droit de la carte (mais pas l'envoi de SMS) se fait de manière cryptée. Cette communication avec l'ayant droit a toutefois lieu sur les réseaux de com
munication publics. Ces données sont en principe visibles par des tiers, peuvent être perdues durant le transfert ou être interceptées par des tiers non autorisés. **Il ne peut dès lors être exclu que, malgré toutes les mesures de sécurité, des tiers se procurent un accès aux communications avec l'ayant droit de la carte lors de l'utilisation de one.** Avec l'utilisation d'Internet, des données peuvent également être transmises via des Etats tiers, qui, selon les circonstances, ne disposent pas du même niveau de protection de données que la Suisse, lorsque le titulaire se trouve en Suisse.

La sécurité des données dépend également du comportement de l'ayant droit. L'ayant droit doit dès lors utiliser les possibilités à sa disposition pour protéger son appareil et les données. Les obligations de diligence et de communication minimales à respecter sont contenues dans la section A.

8.6. De quels droits disposez-vous en lien avec vos données ?
- Renseignements sur les informations relatives à vos données personnelles et sur la manière dont la banque les traite,
- Rectification de données personnelles inexactes ou incomplètes
- Suppression de vos données personnelles
- Limitation du traitement de vos données
- Dépôt d'une réclamation auprès d'une autorité compétente par rapport à la manière dont sont traitées vos données personnelles
- Droit de vous opposer au traitement de vos données personnelles ou de retirer votre consentement

La banque ne peut accorder ces droits uniquement dans le respect des exigences légales. Même si vous retirez votre consentement, le traitement de vos données personnelles est susceptible d'être poursuivi dans la mesure exigée par la loi.

8.7. Combien de temps la banque conserve-t-elle les données ?
La banque conserve vos données aussi longtemps que cela est nécessaire au regard des finalités pour lesquelles elle les a collectées. La banque conserve en outre les données personnelles lorsqu'elle a un intérêt légitime à le faire, par exemple lorsque la banque en a besoin pour faire valoir ou se défendre contre des prétentions, pour garantir la sécurité informatique ou lorsque des délais de prescriptions expirent. Enfin, vos données sont conservées pour satisfaire à nos obligations légales et réglementaires.

Version 08/2023

08/2023

Banque Valiant SA
Bundesplatz 4
Case postale • 3001 Berne
Téléphone 031 952 20 50
info@valiant.ch
valiant.ch

votre banque en toute simplicité