CONTRAT D'ACCEPTATION EN PAIEMENT DE PROXIMITE PAR CARTES DE PAIEMENT- CONDITIONS GENERALES

PREAMBULE

Le **Contrat d'Acceptation en paiement de proximité par cartes de paiement** (ci-après désigné le « Contrat ») est composé des documents suivants :

- les présentes Conditions Générales, comportant deux parties :
  - une partie I « Conditions Générales communes à tous les schémas de cartes de paiement »,
  - une partie II « Conditions Générales spécifiques à chaque schéma de cartes de paiement »,
- leur annexe 1 « Référentiel Sécuritaire Accepteur »,
- leur annexe 2 « Référentiel Sécuritaire PCI-DSS »,
- leur annexe 3 « conditions de fonctionnement du Service « Différé Santé »,
- les Conditions Particulières,
- le barème tarifaire.

Le présent Contrat définit, dans la présente partie I, les règles communes de fonctionnement et les conditions de l'acceptation en paiement de proximité et, dans la partie II, les règles spécifiques à chaque Schéma de cartes de paiement.

PARTIE I - CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS DE CARTES DE PAIEMENT

ARTICLE 1 : DEFINITIONS

Les termes dotés d'une majuscule ont la signification qui leur est attribuée ci-dessous ou dans les Conditions Particulières.

« Accepteur » : désigne tout commerçant, toute association, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) schéma(s) de cartes de paiement (ci-après « Schéma(s) ») dûment convenu(s) avec l'Acquéreur dans le cadre du présent Contrat. **Dans le cadre du présent Contrat, l'Accepteur est le Client**.

« Acquéreur » : désigne tout établissement de crédit ou tout autre établissement habilité à organiser l'acceptation des cartes portant la(les) Marque(s) du ou des Schéma(s) visé(s) en partie II des présentes Conditions, **l'Acquéreur est la Banque**.

« Application de paiement » : désigne tout logiciel informatique ou équivalent chargé sur un appareil, qui permet d'initier des opérations de paiement liées à une carte et donne au titulaire de la Carte la possibilité d'émettre des ordres de paiement.

« Carte » : désigne un instrument de paiement, équipé ou non de la technologie « sans contact », qui permet au payeur d'initier une opération de paiement. La Carte porte une ou plusieurs Marques. Lorsqu'elle est émise dans l'Espace Economique Européen (ci-après l'« EEE » - Il comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), la Carte porte au moin l'une des mentions suivantes :

- crédit ou carte de crédit,
- débit,
- prépayé,
- commercial,

ou, l'équivalent dans une langue étrangère.

« Catégorie de carte » : désigne les catégories de Cartes suivantes :

- crédit ou Carte de crédit,
- Carte de débit,
- Carte prépayée,
- Carte commerciale.

« Données de sécurité personnalisées » : désignent des données personnalisées fournies à un titulaire de carte de paiement (ci-après le « Titulaire de la carte ») par la Banque à des fins d'authentification (exemple : le code confidentiel).

« Equipement Electronique » : désigne tout dispositif de paiement capable de lire une Carte (par exemple, un terminal de paiement électronique ou un smartphone) équipée d'une puce au standard EMV ou d'une piste magnétique permettant l'authentification du Titulaire de la carte. L'Equipement Electronique est soit agréé, soit approuvé, par l'entité responsable du ou des Schéma(s) dont la ou les Marque(s) figure(nt) sur les Cartes acceptées sur cet Equipement.

L'agrément ou l'approbation de l'Equipement Electronique est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par le(s) Schéma(s) concerné(s), qui dispose(nt) de la liste des Equipements Electroniques agréés ou approuvés.

« Instrument de paiement « sans contact » » : désigne un instrument de paiement (par exemple, un smartphone, une tablette ou une montre connectée) disposant de la technologie « sans contact » et doté d'une application de portefeuille numérique dans laquelle la Carte est dématérialisée. Le logiciel de paiement mobile en mode « sans contact » peut être intégré pour partie dans l'élément sécurisé d'un terminal mobile, pour partie dans le terminal mobile lui-même, et permettant de réaliser des opérations de paiement quelle qu'en soit la Marque.

« Marque » : désigne tout nom, terme, sigle, symbole, matériel ou numérique, ou la combinaison de ces éléments susceptible de désigner un Schéma. Les conditions de fonctionnement spécifiques à chaque Marque figurent en partie II des présentes Conditions Générales.

« Partie(s) » : désigne collectivement ou individuellement, d'une part, le Client et/ou d'autre part, la Banque.

« Point d'acceptation » : désigne le lieu physique où est initié l'ordre de paiement.

« Règlement » : désigne le Règlement UE n°2015/751 du 29 avril 2015.

« Schéma » : désigne un ensemble unique de règles, de pratiques, de normes et/ou de lignes directrices de mise en œuvre régissant l'exécution d'opérations de paiement liées à une Carte tel que défini à l'article 2 du Règlement.

Les Schémas (tels que, par exemple CB, Visa, Mastercard, UnionPay, Discover, Diners ou JCB) reposent sur l'utilisation de Cartes auprès des Clients acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

« Système d'Acceptation » : désigne les logiciels, protocoles et équipements conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant l'une des Marques dudit Schéma. Le Client doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

ARTICLE 2 : ELIGIBILITE / DECLARATIONS

2.1 Condition d'éligibilité :

Le Client doit être Titulaire d'un compte ouvert dans les livres de la Banque.

2.2 Déclarations :

Le Client déclare :

- commercialiser ses produits ou prestations de services en respectant les lois et règlements applicables, notamment fiscaux ;
- faire son affaire personnelle de l'obtention de toutes les autorisations légales, réglementaires ou administratives ou de la réalisation de toutes formalités qui pourraient être nécessaires à son activité ;
- s'abstenir de toute activité qui pourrait être pénalement sanctionnée, telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et/ ou d'instruments de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries et le non-respect des dispositions relatives aux conditions d'exercice de professions réglementées ;
- s'engager à signaler sans délai à la Banque toute modification relative à son activité (nature des biens et des services proposés) ;
- que l'ensemble des informations et pièces fournies lors de son entrée en relation avec la Banque ainsi que toutes celles fournies tout au long de la durée du Contrat sont exactes, complètes et actualisées ;
- s'engager à communiquer à la Banque, sur demande de celle-ci, tout document constatant son inscription au Registre du Commerce et des Sociétés ou au Répertoire des Métiers, la dénomination, la forme juridique, le siège social et le type d'activité de l'entreprise (extrait K-Bis de moins de trois

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

mois, pouvoirs des dirigeants, statuts), ainsi qu'une copie de son assurance responsabilité civile. La Banque se réserve le droit de demander tout autre document (indice de cotation Banque de France, trois derniers bilans, …) qu'elle jugerait utile.

ARTICLE 3 : OBLIGATIONS DU CLIENT :

Le Client s'engage à :

3.1 Afficher visiblement chaque Marque qu'il accepte, notamment en apposant de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation des panonceaux, vitrophanies et enseignes qui lui sont fournis par la Banque ou le(s) Schéma(s).

Pour la ou les Marques qu'il accepte, le Client doit accepter toutes les Cartes émises hors de l' « EEE » sur lesquelles figurent cette ou ces Marques quelle qu'en soit la Catégorie de Carte.

3.2 Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation.

3.3 Afficher visiblement le montant minimum éventuel à partir duquel la Carte ou la Catégorie de carte est acceptée afin que le Titulaire de la Carte en soit préalablement informé.

3.4 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le Titulaire de la Carte pour donner l'ordre de paiement.

3.5 Dans le cas où le terminal de paiement ou le smartphone permet un envoi du Ticket (tel que défini à l'article 6.3.4 ci-dessous) par courriel ou par SMS (par exemple, Up2pay Mobile) :

- à informer le Titulaire de la Carte que, pour pouvoir recevoir par courriel ou par SMS le Ticket (tel que défini à l'article 6.3.4 ci-dessous) qui lui est destiné, ce dernier devra lui indiquer respectivement son adresse électronique personnelle ou son numéro de téléphone portable personnel. A défaut et en l'absence d'imprimante connectée au terminal de paiement ou le smartphone, un Ticket manuscrit lui sera remis.
- à communiquer au Titulaire de la Carte préalablement à la collecte de son adresse courriel ou numéro de téléphone portable pour l'envoi du Ticket, les informations légales sur le traitement qu'il met en œuvre à cette occasion conformément à la loi Informatique et libertés. Ces informations sont fournies par la Banque au Client au moyen d'un bouton « information client » présent dans l'application au moment du choix du mode de paiement, qu'il doit activer pour faire apparaître la mention légale et la transmettre au Titulaire de la Carte pour qu'il en prenne connaissance.

3.6 Afin que le Titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a initiées, vérifier avec la Banque la conformité des informations transmises pour identifier son Point d'acceptation. Les informations doivent indiquer une dénomination commerciale ou sociale connue du Titulaire de la Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, vente à distance, etc.) dans ce Point d'acceptation.

3.7 Accepter, en contrepartie d'actes de vente ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ou à titre de dons ou pour le règlement du montant de cotisations, les paiements effectués avec les Cartes (Catégories de carte et Marques) qu'il a choisies d'accepter ou qu'il doit accepter.

3.8 Ne pas collecter au titre du présent Contrat une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement du Titulaire de la Carte.

3.9 Transmettre les enregistrements des opérations de paiement à la Banque, dans les délais prévus dans les Conditions Particulières convenues avec lui.

3.10 Régler, conformément aux Conditions Particulières et au barème tarifaire portant les principales Conditions Générales de Banque ou tout autre document convenu entre les Parties, les commissions, frais et d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

3.11 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le Titulaire de la Carte et de leurs conséquences financières.

3.12 Utiliser obligatoirement l'Equipement Electronique et ne pas modifier les paramètres de son fonctionnement sauf s'il s'agit d'un smartphone et pour lequel une modification de ses paramètres serait nécessaire et à la main du Client.

3.13 Prendre toutes les mesures propres à assurer la garde de son Equipement Electronique et être vigilant quant à l'utilisation qui en est faite.

3.14 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données de paiement sensibles liées à l'utilisation des Cartes ou des Instruments de paiements « sans contact », que ces derniers :

- s'engagent à respecter tant le Référentiel Sécuritaire PCI DSS que le Référentiel Sécuritaire Accepteur et ses mises à jour et,
- acceptent que des audits soient réalisés dans leurs locaux et que les rapports puissent être communiqués, comme précisé à l'article 3.15 ci-dessous.

3.15 Permettre à la Banque de faire procéder, aux frais du Client, dans ses locaux ou ceux des tiers visés à l'article 3.14, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou de celles du Référentiel Sécuritaire PCI DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et pendant toute sa durée.

Le Client autorise la communication du rapport à la Banque et au(x) Schéma(s) concerné(s).

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou au Référentiel Sécuritaire PCI DSS, la Banque pourra procéder, le cas échéant à la demande d'un Schéma, à une suspension de l'acceptation des Cartes par le Client dans les conditions de l'article « Suspension de l'acceptation », voire à une demande de résiliation du présent Contrat, dans les conditions prévues à l'article « Durée et résiliation du contrat » ci-après.

3.16 A la demande de la Banque, selon les volumes d'opérations cartes acceptées, respecter les exigences du référentiel de sécurité PCI DSS figurant en annexe du présent contrat.

Respecter les exigences du Référentiel Sécuritaire Accepteur annexé aux présentes ainsi que les exigences du Référentiel Sécuritaire PCI DSS annexé aux présentes et dont il peut prendre connaissance des mises à jour à l'adresse suivante : https://fr.pcisecuritystandards.org/minisite/env2/

3.17 Respecter, pendant toute la durée du Contrat, les engagements pris à l'article « Eligibilité / Déclarations » ci-dessus.

ARTICLE 4 : OBLIGATIONS DE LA BANQUE :

La Banque s'engage à :

4.1 Fournir au Client les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la partie II des présentes Conditions Générales et son/leur évolution, les Catégories de cartes et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de cartes et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

4.2 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement effectué au Point d'acceptation, conformément au choix du Client ou du Titulaire de la Carte.

4.3 Mettre à la disposition du Client, toutes les informations relatives à la sécurité des opérations de paiement.

4.4 Indiquer au Client la liste et les caractéristiques des Cartes (Marques, Catégories de carte) pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

4.5 Créditer le compte du Client des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

4.6 Ne pas débiter, au-delà du délai maximum de quinze (15) mois à partir de la date du crédit initial porté au compte du Client, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

4.7 Selon les modalités convenues avec le Client, communiquer à celui-ci au moins une fois par mois les informations suivantes :

- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement, exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par le Client et de la commission d'interchange.

Le Client peut demander à ce que ces informations soient regroupées par Marque, Application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

4.8 Indiquer et facturer au Client les commissions de services à acquitter, séparément pour chaque Catégorie de carte et chaque Marque, selon les différents niveaux de commission d'interchange.

Le Client peut demander à ce que les commissions de services soient regroupées par Marque, Application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 5 : GARANTIE DE PAIEMENT :

5.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article « Mesures de sécurité » que dans la partie II du présent Contrat, ainsi qu'aux Conditions Particulières.

5.2 Toutes les mesures de sécurité sont indépendantes les unes des autres.

Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel et/ou des Données de sécurité personnalisées.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

5.3 En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement.
5.4 La Banque pourra contrepasser le montant des opérations non garanties qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 6 : MESURES DE SECURITE :

Le Client s'engage à :
6.1 Informer immédiatement la Banque en cas de fonctionnement anormal de l'Equipement Electronique (sauf pour le cas où l'Equipement Electronique est le smartphone du client) et/ou de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation, etc.).
6.2 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données, coopérer avec la Banque et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de la part du Client pourra conduire la Banque à mettre fin au présent Contrat conformément à l'article « Durée et résiliation du Contrat » ci-après.
6.3 **Lors du paiement, le Client s'engage à :**
6.3.1 Vérifier l'acceptabilité de la Carte, c'est-à-dire :
- la Marque, la Catégorie de carte du Schéma concerné par l'acceptation,
- le cas échéant, l'hologramme, sauf pour les Cartes ne le prévoyant pas,
- la puce sur les Cartes lorsqu'elle y est prévue par le Schéma,
- la Marque et Catégorie de carte définies dans les conditions spécifiques au Schéma concerné figurant dans la partie II des présentes Conditions Générales,
- le cas échéant, la période de validité (fin et éventuellement début).

6.3.2 Utiliser l'Equipement Electronique, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées.
L'Equipement Electronique doit notamment :
(i) Après la lecture de la puce de la Carte lorsqu'elle est présente :
- permettre le contrôle du code confidentiel ou des Données de sécurité personnalisées lorsque la puce le lui demande, et vérifier :
  - le code émetteur de la Carte (BIN),
  - le code service,
  - le cas échéant, la date de fin de validité de la Carte.

(ii) Lorsque la puce n'est pas présente sur une Carte, après lecture de la piste ISO 2, vérifier :
- le code émetteur de la Carte (BIN),
- le code service,
- le cas échéant, la date de fin de validité de la Carte.

6.3.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par la Banque, pour le Point d'acceptation concerné.
6.3.4 Lorsque la puce le demande à l'Equipement Electronique, faire composer ou apposer par le Titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel et/ou ses Données de sécurité personnalisées. La preuve de la frappe du code confidentiel ou de la vérification des Données de sécurité personnalisées est apportée par le certificat qui doit figurer sur le ticket émis par l'Equipement Electronique et conservé par le Client (ci-après « Ticket »).
Lorsque le code confidentiel n'est pas vérifié et/ou qu'une autre Donnée de sécurité personnalisée n'est pas utilisée, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.
6.3.5 Obtenir une autorisation, d'un montant identique à l'opération :
- lorsque le montant de l'opération en cause, ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée et pour le même Point d'acceptation, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières, et ceci quelle que soit la méthode d'acquisition des données de la Carte,
- lorsque l'Equipement Electronique ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières.

A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.
Lorsque la puce n'est pas présente sur la Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.
Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.
Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations faites postérieurement le même jour et avec la même Carte, dans le même Point d'acceptation.
6.3.6 Faire signer le Ticket dans tous les cas où l'Equipement Electronique le demande.
6.3.7 Lorsque la signature sur le Ticket est requise et que la Carte comporte un panonceau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur ledit panonceau.
Pour une Carte sur laquelle ne figure pas le panonceau de signature, vérifier la conformité de la signature utilisée avec celle qui figure sur la pièce d'identité présentée par le Titulaire de la Carte.
6.3.8 Dans tous les cas où l'Equipement Electronique édite un Ticket, remettre au Titulaire de la Carte l'exemplaire qui lui est destiné.
Dans le cas où le terminal de paiement ou le smartphone permet un envoi du Ticket, par courriel ou par SMS (par exemple, un Up2pay Mobile), remettre celui-ci :
(i) soit, par courriel exclusivement à sa propre adresse courriel qui aura été collectée par le Client au moment du paiement dans le respect des règles relatives à la protection des données à caractère personnel,
(ii) soit, par SMS exclusivement envoyé au numéro de téléphone qui aura été collecté par le Client au moment du paiement dans le respect des règles relatives à la protection des données à caractère personnel,
(iii) soit, en cas de refus par le Titulaire de la Carte de communiquer son adresse courriel et/ou son numéro de téléphone mobile, sous la forme d'un Ticket papier manuscrit ou imprimé reprenant toutes les mentions obligatoires telles que figurant sur le modèle disponible dans l'onglet dédié de l'application (bouton « établir un ticket manuel »).

6.3.9 Mode « sans contact » : en cas d'opération en mode « sans contact » permise par l'Equipement Electronique, l'opération de paiement est garantie même dans le cas où les Données de sécurité personnalisées n'ont pas à être vérifiées, sous réserve du respect de toutes les autres mesures de sécurité.
6.4 **Après le paiement, le Client s'engage à :**
6.4.1 Transmettre à la Banque dans les délais et selon les modalités prévues dans les Conditions Particulières, les enregistrements électroniques des opérations et s'assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévues dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation transmise par la Banque doit être obligatoirement remise à cette dernière.
6.4.2 Archiver et conserver, à titre de justificatif, pendant la durée requise par les règles du Schéma concerné après la date de l'opération :
- un exemplaire du Ticket comportant, lorsqu'elle est requise, la signature du Titulaire de la Carte,
- l'enregistrement électronique représentatif de l'opération ou le journal de fond lui-même.

6.4.3 Communiquer, à la demande de la Banque et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.
6.4.4 Le Client s'engage à ne stocker, sous quelque forme que ce soit, aucune des données de paiement sensibles liées à la Carte suivantes :
- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- les Données de sécurité personnalisées, notamment, le code confidentiel.

6.4.5 Le Client s'engage à prendre toutes les précautions utiles pour que soit assuré la confidentialité et l'intégrité des données à caractère personnel du Titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte, ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de la loi Informatique et Libertés.

ARTICLE 7 : PAIEMENT « SANS CONTACT » :

7.1 Le présent article s'applique lorsque le Client utilise un Equipement Electronique disposant de la technologie « sans contact ». Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables aux opérations de paiement réalisées avec une Carte équipée de la technologie « sans contact », ou un Instrument de paiement « sans contact ».
7.2 Lorsque le Client dispose d'un Equipement Electronique disposant de la technologie dite « sans contact », ledit Equipement Electronique permet le règlement rapide par la Carte équipée de la technologie « sans contact », ou par l'Instrument de paiement « sans contact » grâce à une lecture à distance.
7.3 Le Client s'engage à signaler au public l'acceptation du paiement « sans contact » par l'apposition sur l'Equipement Electronique, au niveau du lecteur « sans contact », de façon apparente, d'un pictogramme permettant d'identifier le paiement « sans contact ».
7.4 En toutes circonstances, le Client doit se conformer aux directives qui apparaissent sur

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

l'Equipement Electronique, notamment la frappe du code confidentiel ou l'utilisation de tout autre Donnée de sécurité personnalisée dans les meilleures conditions de confidentialité.

7.5 Lorsqu'un certain nombre de règlements successifs en mode « sans contact » est atteint, le Client peut être amené à passer en mode contact même pour une opération d'un montant inférieur au montant unitaire maximum d'une opération en mode « sans contact ».

7.6 Lorsque l'opération de paiement est réalisée à l'aide d'une Carte équipée de la technologie « sans contact » ou d'un Instrument de paiement « sans contact », les articles 6.3.1, 9.3, 9.4 et 9. 6 de la présente partie I des Conditions Générales ne sont pas applicables.

ARTICLE 8 : PAIEMENT AVEC PREAUTORISATION (HORS AUTOMATE) :

Le présent article s'applique lorsque le Client (i) utilise un Equipement Electronique muni de l'extension de service « Paiement avec Préautorisation » conforme aux spécifications en vigueur et, (ii) a choisi cette option dans les Conditions Particulières ou dans tout autre document convenu entre les Parties.

Lors d'une opération de paiement avec préautorisation, le Titulaire d'une Carte ou d'un Instrument de paiement « sans contact » donne son consentement à une opération de paiement en début de prestation pour un montant maximum convenu avec le Client et dont le montant définitif est déterminé à l'issue de la prestation.

Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables.

8.1 Au moment du consentement du Titulaire de la Carte à l'opération de paiement, le Client s'engage à :

- Recueillir l'acceptation du Titulaire de la Carte d'être débité du montant final de la vente dont le montant maximal estimé lui est précisé.
- Ne pas faire usage de la Carte pour s'octroyer une caution ou un dépôt de garantie.
- Fournir au Titulaire de la Carte toutes les informations nécessaires lui permettant de raisonnablement déterminer le montant final de l'opération de paiement.
- Attribuer à l'occasion de l'initialisation de l'opération de paiement un numéro de dossier indépendant du numéro de carte.
- Obtenir systématiquement une autorisation d'un montant identique à celui connu et accepté par le Titulaire de la Carte.

A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.

Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.

Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations faites postérieurement le même jour et avec la même Carte dans le même Point d'acceptation.

8.2 Dans tous les cas où l'Equipement Electronique édite un Ticket (y compris sous la forme présentée à l'article 3.5 des présentes Conditions Générales), remettre au Titulaire de la Carte l'exemplaire qui lui est destiné sur lequel doit figurer notamment :

- le montant maximal estimé de la vente,
- le numéro de dossier,
- la mention de : « ticket provisoire » ou « préautorisation ».

En toutes circonstances, le Client doit se conformer aux directives qui apparaissent sur l'Equipement Electronique, notamment l'utilisation des Données de sécurité personnalisées (par exemple, le code confidentiel) dans les meilleures conditions de confidentialité.

8.3 A l'exécution de l'opération de paiement, le Client s'engage à clôturer l'opération de paiement en recherchant via le numéro de dossier, l'opération de paiement initialisée lors du consentement et la finaliser pour le montant final de la vente connu et accepté par le Titulaire de la Carte qui ne doit pas excéder la valeur du montant maximum autorisé par ce dernier.

Lorsqu'une opération de paiement avec préautorisation est réalisée, l'article 6.3.5 de la présente partie I n'est pas applicable.

ARTICLE 9 : MODALITES ANNEXES DE FONCTIONNEMENT :

9.1 Réclamation

9.1.1 Toute réclamation doit être formulée par écrit à la Banque, dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion.

9.1.2 Ce délai est réduit à une durée de quinze (15) jours calendaires à compter de la date de débit en compte d'une opération non garantie.

9.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à la Banque. En cas de conflit, les enregistrements électroniques produits par la Banque ou le Schéma, dont les règles s'appliquent à l'opération de paiement concernée, prévaudront sur ceux produits par le Client, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des enregistrements produits par la Banque ou le Schéma.

9.3 Retrait à son Titulaire d'une Carte faisant l'objet d'un blocage ou en opposition

9.3.1 En cas de retrait à son Titulaire d'une Carte faisant l'objet d'un blocage ou en opposition (le retrait ayant eu lieu sur instruction de l'Equipement Electronique), le Client utilise la procédure de gestion et de renvoi des Cartes capturées (disponible sur demande auprès de la Banque).

9.3.2 Pour toute capture de Carte, une prime pourra être versée au Client ou à toute personne indiquée par lui et exerçant une activité au sein de son Point d'acceptation.

9.4 Oubli d'une Carte par son Titulaire

En cas d'oubli de sa Carte par le Titulaire, le Client peut la lui restituer dans un délai maximum de deux (2) jours ouvrables après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord, demandé selon la procédure communiquée par la Banque. Au-delà de ce délai, le Client utilise la procédure de gestion et de restitution des Cartes oubliées (disponible sur demande auprès de la Banque).

9.5 Transaction crédit

Le remboursement partiel ou total d'un achat d'un bien ou d'un service ou d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord de son Titulaire, être effectué au Titulaire de la Carte utilisée pour l'opération initiale. Le Client doit alors utiliser la procédure dite de « transaction crédit », et, dans un délai maximal de cinq (5) jours ouvrés, effectuer la remise correspondante à la Banque à qui il avait remis l'opération initiale. Le montant de la « transaction crédit » ne doit pas dépasser le montant de l'opération initiale.

9.6 Carte non signée

En cas de Carte non signée, et si le panonceau de signature est présent sur la Carte, le Client doit demander au Titulaire de la Carte de justifier de son identité et d'apposer sa signature sur le panonceau de signature prévu à cet effet au verso de la Carte et enfin vérifier la conformité de cette signature avec celle figurant sur la pièce d'identité présentée par le Titulaire de la Carte. Si le Titulaire de la Carte refuse de signer sa Carte, le Client doit refuser le paiement par Carte.

9.7 Dysfonctionnement

Ni la Banque, ni le Client ne peut être tenu pour responsable de l'impossibilité d'effectuer un paiement en cas de dysfonctionnement de la Carte et/ou de son support.

ARTICLE 10 : MODIFICATIONS :

10.1 La Banque peut modifier à tout moment le présent Contrat.

10.2 La Banque peut notamment apporter :

- des modifications techniques telles que l'acceptation de nouvelles Cartes, des modifications de logiciel, le changement de certains paramètres, la remise en état de l'Equipement Electronique suite à un dysfonctionnement, etc.
- des modifications sécuritaires telles que :
  - la modification du seuil de demande d'autorisation,
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptation des Cartes portant certaines Marques.

10.3 Les nouvelles conditions entrent en vigueur au terme d'un délai minimum fixé à un (1) mois à compter de l'envoi par tout moyen d'une lettre d'information ou de notification. Les modifications imposées par les lois et/ou règlements prennent effet dès leur entrée en vigueur sans qu'une information ne soit obligatoirement envoyée par la Banque.

D'un commun accord, les Parties peuvent déroger à ce délai en cas de modifications importantes.

10.4 Le délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque la Banque ou le Schéma concerné constate, dans le Point d'acceptation, une utilisation anormale de Cartes ou d'Instrument de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s.

10.5 La Banque peut notamment proposer un nouveau Schéma et/ou une nouvelle Marque de Carte ou un nouvelle Application de paiement. A cette fin, la Banque fera parvenir par tout moyen les conditions spécifiques et tarifaires afférentes au nouveau Schéma et/ou la nouvelle Marque proposée. Au terme de ce délai d'un (1) mois, sauf désaccord du Client signifié par tout moyen à la Banque, cette dernière rendra compatible pour l'acceptation du nouveau Schéma ou de la nouvelle Marque l'Equipement Electronique dont elle est propriétaire.

10.6 Passés les délais visés au présent article, les modifications et/ou conditions spécifiques aux nouveaux Schémas ou nouvelles Marques proposées sont réputées acceptées par le Client s'il n'a pas résilié le présent Contrat. Elles lui sont dès lors opposables.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

10.7 Le non-respect des nouvelles conditions contractuelles (techniques, sécuritaires ou autres), dans les délais impartis, peut entraîner la résiliation du présent Contrat.

ARTICLE 11 : DUREE ET RESILIATION DU CONTRAT :

11.1 Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

Le Client d'une part, la Banque d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux Parties), sous réserve du dénouement des opérations en cours, résilier le présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. Le Client garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article « Modifications » ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

11.2 En outre, à la demande de tout Schéma, la Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 12.2 ci-dessous. Elle est notifiée par écrit. Son effet est immédiat.

11.3 Toute cessation d'activité du Client, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat sous réserve du dénouement des opérations en cours.

11.4 En cas de manquement aux conditions d'éligibilité et/ou aux déclarations stipulées à l'article « Eligibilité / Déclarations » ci-dessus et/ou aux obligations stipulées aux articles « Obligations du client » et « Mesures de sécurit » ci-dessus, la Banque se réserve le droit, sans aucune indemnité et sans préavis, de suspendre ou de mettre fin à tout ou partie du présent Contrat, sans préjudice de toutes autres actions de droit commun qui pourraient être engagées par la Banque. Le client en sera informé par tout moyen.

11.5 Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge du Client ou pourront faire l'objet d'une déclaration de créances.

11.6 Le Client sera tenu de restituer à la Banque l'Equipement Electronique (sauf dans le cas où l'Equipement Electronique est un smartphone appartenant au Client), les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation en paiement de proximité par cartes de paiement, le Client s'engage à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes, application de paiement ou Marques du (des) Schéma(s) concerné(s).

ARTICLE 12 : SUSPENSION DE L'ACCEPTATION

12.1 La Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation de tout ou partie des Cartes, ou Instruments de Paiement « sans contact » acceptés par le Client. La suspension est précédée, le cas échéant, d'un avertissement au Client, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

La suspension peut également intervenir à l'issue d'une procédure d'audit telle que visée à l'article 3.15 de la présente partie I des Conditions Générales, au cas où le rapport d'audit révélerait un ou plusieurs manquements tant aux clauses du présent Contrat qu'au Référentiel Sécuritaire Accepteur et/ou au Référentiel Sécuritaire PCI DSS, annexés au présent Contrat.

12.2 La suspension peut être décidée en raison notamment :

- du non-respect répété des obligations du présent Contrat et/ou du refus d'y remédier, notamment d'une utilisation non agréée de l'Equipement Electronique permettant au Client d'accéder au(x) Système(s) d'Acceptation et d'un risque de dysfonctionnement important du (des) Système(s) d'Acceptation du (des) Schéma(s) concerné(s),
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes/ d'Instruments de Paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,
- d'un refus d'acceptation répété et non motivé des Cartes/d'Instruments de Paiement « sans contact »/des Catégories de carte du (des) Schéma(s) concerné(s) qu'il a choisi d'accepter ou qu'il doit accepter,
- de plaintes répétées d'autres membres ou partenaires du (des) Schéma(s) concerné(s) et qui n'ont pu être résolues dans un délai raisonnable,
- de retard volontaire ou non motivé de transmission des justificatifs,
- d'un risque aggravé en raison des activités du Client,
- du non-respect d'une ou plusieurs obligations portées par l'article « éligibilité/déclaration » ci-dessus.

12.3 Le Client s'engage alors à restituer à la Banque l'Equipement Electronique (sauf dans le cas où l'Equipement Electronique est un smartphone appartenant au Client), les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes du (des) Schéma(s) concerné(s).

12.4 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, le Client peut demander la reprise du présent Contrat auprès de la Banque, ou souscrire un nouveau contrat d'acceptation en paiement de proximité par cartes de paiement avec un autre acquéreur de son choix.

ARTICLE 13 : MESURES DE PREVENTION ET DE SANCTION PRISES PAR LA BANQUE

13.1 En cas de manquement du Client aux stipulations du présent Contrat ou aux lois en vigueur ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes/d'Instruments de Paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s, la Banque peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement au Client valant mise en demeure, précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

13.2 Si dans un délai de trente (30) jours, le Client n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, la Banque peut soit procéder à une suspension de l'acceptation des Cartes/des Instruments de paiement « sans contact », dans les conditions précisées à l'article « Durée et résiliation du contrat » et « Suspension de l'acceptation » ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat, par lettre recommandée avec demande d'avis de réception.

13.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, le Client est toujours confronté à un taux d'impayés anormalement élevé, la Banque peut décider la résiliation de plein droit avec effet immédiat, sous réserve des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

ARTICLE 14 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

14.1 Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel ou couvertes par le secret bancaire.

14.2 Secret bancaire

Les informations relatives au Client, collectées par la Banque, nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des opérations de paiement par Carte ou Instrument de paiement « sans contact», ordonnées en exécution du présent Contrat, de réponses aux obligations légales et réglementaires, de prévention des fraudes et de traitement des réclamations, qu'elles émanent des Titulaires de Cartes ou d'Instruments de paiement « sans contact » ou d'autres entités, la Banque étant à cet effet, de convention expresse, déliée du secret bancaire.

14.3 Protection des données à caractère personnel du Client

Lors de la signature ou de l'exécution des présentes, chacune des Parties peut avoir accès à des données à caractère personnel. Ainsi, conformément à la règlementation française et européenne applicable en matière de protection des données à caractère personnel, et en particulier du Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel, il est précisé que :

14.3.1 Les données à caractère personnel relatives au Client, collectées par la Banque, nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées que pour les seules finalités suivantes :

- le traitement des opérations de paiement par Carte, y compris la gestion des réclamations et litiges. Ce traitement est nécessaire à la bonne exécution du présent contrat et à défaut le contrat ne pourra être exécuté ;
- la poursuite des intérêts légitimes de la Banque que constituent la lutte contre la fraude à la carte de paiement, la gestion des recouvrements et éventuels recours en justice, l'analyse à des fins statistiques et la prospection ainsi que l'animation commerciale pouvant s'appuyer sur un traitement automatisé ou non de profilage ;
- la réponse aux obligations légales et réglementaires ;

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

14.3.2 Les données à caractère personnel traitées par la Banque sont conservées pour une durée maximale correspondant à la durée de la relation contractuelle augmentée des délais légaux de conservation et de prescription auxquels la Banque est tenu.
14.3.3 Pour satisfaire les finalités précisées ci-dessus, les données à caractère personnel relatives au Client et leur mise à jour pourront être communiquées aux destinataires suivants :
a) l'organe central du Groupe Crédit Agricole, tel que défini par le Code monétaire et financier, afin que celui-ci puisse satisfaire, au bénéfice de l'ensemble du Groupe, à ses obligations légales et règlementaires, notamment en matière de déclarations prudentielles auprès de toute autorité ou tout régulateur compétent ;
b) toute entité du Groupe Crédit Agricole, à des fins de prospection commerciale ou de conclusion de contrats ;
c) les médiateurs, auxiliaires de justice et officiers ministériels dans le cadre de leurs missions de recouvrement de créances, ainsi que les personnes intervenant dans le cadre de la cession ou du transfert de créances ou de contrats, ainsi que tout autorité judiciaire ou administrative compétente ;
d) les bénéficiaires d'opération de paiement, par le biais des Schémas de cartes de paiement et à leur prestataire de service de paiement notamment à des fins de lutte contre le blanchiment des capitaux et le financement du terrorisme et dans le respect de la règlementation en matière d'embargos et de sanctions internationales ;
e) les partenaires de la Banque, pour permettre aux Clients de bénéficier des avantages du partenariat auquel elle a adhéré, le cas échéant, et ce dans le cadre exclusif des accords de partenariat
f) les sociétés du Groupe Crédit Agricole chargées de la gestion ou de la prévention de risques opérationnels (évaluation du risque, sécurité et prévention des impayés et de la fraude, lutte contre le blanchiment des capitaux…) au bénéfice de l'ensemble des entités du Groupe ;
g) toute entité du Groupe Crédit Agricole en cas de mise en commun de moyens ou de regroupement de sociétés afin de permettre à ces entités de réaliser les missions faisant l'objet de cette mise en commun ;
h) les sous-traitants de la Banque et notamment ceux participant à l'exécution des opérations de paiements, et ce pour les seuls besoins des travaux de sous-traitance ;
i) Crédit Agricole SA ou toute entité du Groupe, et leurs sous-traitants, dans le cadre de la mise en place de systèmes informatisés d'analyse des données des clients des entités du Groupe Crédit Agricole ayant pour objet l'élaboration de modèles algorithmiques prédictifs avec comme finalités (i) la passation, la gestion et l'exécution de contrats relatifs à des produits bancaires et/ ou assurantiels, (ii) l'amélioration des services rendus aux Clients et l'adéquation des produits bancaires et/ ou assurantiels proposés aux Clients, (iii) l'élaboration de statistiques et d'études actuarielles et simulations relatives aux contrats conclus avec la banque et (iv) la lutte contre la fraude.
La liste des destinataires susceptibles d'être bénéficiaires d'informations collectées dans le cadre du présent Contrat pourra être communiquée au Client sur simple demande adressée à la Banque.
14.3.4 Conformément à la règlementation applicable et notamment le chapitre III du Règlement (UE) 2016/679 du 27 avril 2016, le Client (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :
- demander à accéder aux données à caractère personnel le concernant et / ou en demander la rectification ou l'effacement ;
- définir des directives relatives au sort des données à caractère personnel le concernant après son décès ;
- s'opposer au traitement de données à caractère personnel le concernant réalisé aux fins de lutte contre la fraude et / ou de gestion des éventuels recours en justice, sous réserve que l'Acquéreur n'invoque pas de motifs légitimes et impérieux ;
- demander des limitations au traitement des données à caractère personnel le concernant dans les conditions prévues à l'article 18 du Règlement (UE) 2016/679 du 27 avril 2016 ;
- demander à recevoir et / ou transmettre à un autre responsable du traitement les données à caractère personnel le concernant sous une forme couramment utilisée et lisible par un appareil électronique ;
- introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés.
Ces droits peuvent être exercés en s'adressant au Service clients, 121 chemin de Devèzes, 64121 Serres-Castet, ou courriel : service.client@ca-pyrenees-gascogne.fr.
14.3.5 Pour toute question en lien avec la protection des données à caractère personnel, le Client (personne physique ou personne physique le représentant) peut :
- consulter la Politique de protection des données à caractère personnel de la Caisse Régionale accessible à https://www.credit-agricole.fr/ca-pyrenees-gascogne/particulier/informations/politique-de-protection-des-donnees-personnelles-de-la-caisse-regionale.html
- contacter le Délégué à la protection des données désigné par la Banque dpo@ca-pyrenees-gascogne.fr.
14.4 Protection des données à caractère personnel des titulaires de Cartes
14.4.1 A l'occasion de l'exécution des ordres de paiement donnés par Carte, le Client peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte.
14.4.2 Le Client s'engage à respecter la règlementation française et européenne applicable en matière de protection des données à caractère personnel et notamment le Règlement (UE) 2016/679 du 27 avril 2016.
14.4.3 Le Client ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte, le traitement des réclamations dont les Titulaires de la carte peuvent être l'objet, ou la gestion de toute offre impliquant le traitement des DCP des cartes de paiement par le Client dans le strict cadre d'un contrat de service avec une entité du Groupe Crédit Agricole. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat.
14.4.4 Le Client s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du Titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de l'article 32 du Règlement (UE) 2016/679 du 27 avril 2016.
14.4.5 Les Titulaires de Cartes pour lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès du Client, de l'intégralité des droits prévus par la règlementation française et européenne applicable en matière de protection des données à caractère personnel, et notamment de leurs droits d'accès, de rectification, d'effacement, d'opposition, de limitation ainsi que de leur droit à la portabilité. A cet égard, le Client s'engage d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 15 : REFERENCEMENT
Sauf convention contraire, la Banque est autorisée à citer à titre de référence, le nom du client et les prestations réalisées pour celui-ci.

ARTICLE 16 : NON RENONCIATION
Le fait pour le Client ou pour la Banque de ne pas exiger à un moment quelconque l'application d'une clause du présent Contrat, que ce soit de façon permanente ou temporaire, ne peut en aucun cas être considéré comme constituant une renonciation aux droits de cette partie découlant de ladite clause.

ARTICLE 17 : TITRE – PERMANENCE
17.1 En cas de difficulté d'interprétation entre les titres des articles et le texte de leur contenu, le texte des articles primera.
17.2 Si l'une quelconque des stipulations du présent Contrat est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle sera réputée non écrite, mais n'entraînera pas la nullité du présent Contrat.

ARTICLE 18 : LOI APPLICABLE ET TRIBUNAUX COMPETENTS
Le présent Contrat et toutes les questions qui s'y rapportent seront régis par le droit français et tout différend relatif à l'interprétation, la validité et/ ou l'exécution du présent Contrat est soumis à la compétence des tribunaux français, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

ARTICLE 19 : LANGUE DU CONTRAT
La langue utilisée dans le Contrat et pour toute communication effectuée en application des présentes est le français.

ARTICLE 20 : DOMICILIATION
Pour l'exécution du présent Contrat d'Acceptation ainsi que de ses suites, les Parties font respectivement élection de domicile en leurs sièges ou adresses indiqués dans les Conditions Particulières.

ARTICLE 21 : RENSEIGNEMENT – RECLAMATION
L'agence est à la disposition du Client pour lui fournir tous les renseignements qu'il pourrait souhaiter sur le fonctionnement du Contrat et répondre à ses éventuelles réclamations.
Dans ce dernier cas, le Client a aussi la possibilité, en écrivant à l'adresse de la Caisse Régionale, de faire appel au Service clients, 121 chemin de Devèzes, 64121 Serres-Castet, ou courriel : service.client@ca-pyrenees-gascogne.fr qui s'efforcera de trouver la meilleure solution à son différend.
L'agence ou le service « Clients-Réclamations » répond au Client sur support papier ou sur un support durable convenu avec lui dans les 15 jours ouvrables suivant la réception de la réclamation. Si une réponse ne peut être exceptionnellement donnée dans ce délai de 15 jours pour des raisons échappant au

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

contrôle de la Caisse Régionale, celle-ci envoie une réponse d'attente motivant le délai complémentaire nécessaire et précisant la date ultime à laquelle le Client recevra une réponse définitive. Cette réponse définitive devra lui être adressée dans les trente-cinq jours ouvrables suivant la réception de la réclamation.
Si le Client n'a pas pu résoudre au préalable son différend auprès du service « Clients-Réclamations » par une réclamation écrite, il a également la possibilité, si la réglementation le prévoit, de s'adresser gratuitement à l'instance de règlement extrajudiciaire des litiges proposée par la Caisse Régionale, dont les coordonnées et les modalités de saisine sont disponibles sur le site Internet de la Caisse Régionale : www.ca-pg.com.
Aux fins de cette procédure, le Client autorise expressément la Caisse Régionale à communiquer à l'instance de règlement extrajudiciaire compétente tous les documents et informations utiles à l'accomplissement de sa mission. Le Client délie la Caisse Régionale du secret bancaire le concernant, pour les besoins de cette procédure.

ARTICLE 22 : DEMARCHAGE BANCAIRE ET FINANCIER

Lorsqu'un acte de démarchage précède la conclusion du présent Contrat, le Client dispose d'un délai de quatorze (14) jours calendaires révolus pour se rétracter sans frais ni pénalités et sans être tenu d'indiquer les motifs de sa décision. Ce délai court à compter de la conclusion du Contrat ou de la réception des conditions contractuelles et informations préalables si celle-ci est postérieure.
Le commencement d'exécution ne prive pas le Client du droit de rétractation.
La rétractation met fin au Contrat de plein droit. Le Client sera tenue au paiement du prix correspondant à l'utilisation du produit pour la période comprise entre la date de commencement d'exécution du Contrat et de la date de rétractation, à l'exclusion de toute autre somme.
Le Client peut exercer son droit de rétractation au moyen du formulaire joint ou d'une déclaration dénuée d'ambigüité (lettre, télécopie ou courrier électronique) envoyée à son agence.

ARTICLE 23 : LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX, LE FINANCEMENT DU TERRORISME, LA CORRUPTION ET LA FRAUDE – RESPECT DES SANCTIONS INTERNATIONALES

La Banque est tenue de respecter les dispositions légales et réglementaires relatives à la lutte contre le blanchiment des capitaux, le financement du terrorisme et plus généralement, à exercer une vigilance constante sur les opérations effectuées par ses clients.
La Banque est également tenue d'agir conformément aux lois et réglementations en vigueur dans diverses juridictions, en matière de sanctions économiques, financières ou commerciales, et de respecter toute mesure restrictive relative à un embargo, au gel des avoirs et des ressources économiques , à des restrictions pesant sur les transactions avec des individus ou entités ou portant sur des biens ou des territoires déterminés émises, administrées ou mises en application par le Conseil de sécurité de l'ONU, l'Union européenne, la France, les États-Unis d'Amérique (incluant notamment le bureau de contrôle des Actifs Etrangers rattaché au Département du Trésor, l'OFAC et le Département d'État) et par des autorités locales compétentes pour édicter de telles sanctions (ci-après les « Sanctions Internationales »).
La Banque peut être amenée à suspendre ou rejeter une opération de paiement ou de transfert émise et/ou reçue, qui pourrait être ou qui, selon son analyse, serait susceptible d'être, sanctionnée par toute autorité compétente, ou le cas échéant, à bloquer les fonds et les comptes du Client.
La Banque peut être amenée à demander au Client de lui fournir des informations concernant les circonstances et le contexte d'une opération tels que la nature, la destination et la provenance des mouvements des fonds, ainsi que des justificatifs nécessaires pour appuyer ces explications, notamment en cas d'opération particulière par rapport aux opérations habituellement enregistrées sur son compte.
Le Client est tenu de communiquer immédiatement les informations exigées. Tant que le Client n'a pas fourni les informations demandées par la Banque ou que les informations ne sont pas jugées suffisantes, la Banque se réserve le droit de ne pas exécuter ses instructions.
La Banque peut également être amenée à réaliser des investigations dans le cadre de la réalisation de toute opération qui pourrait être ou qui, selon son analyse, serait susceptible d'être, sanctionnée par toute autorité compétente, conduisant le cas échéant, à retarder l'exécution des instructions du Client.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

PARTIE II - CONDITIONS GENERALES SPECIFIQUES A CHAQUE SCHEMA DE CARTES DE PAIEMENT

DISPOSITIONS SPECIFIQUES AUX SCHEMAS INTERNATIONAUX

La présente partie II des Conditions Générales précise les conditions générales de fonctionnement spécifiques à chaque Schéma dont la (l'une des) marque(s) est apposée sur la Carte ; elles viennent compléter les Conditions Générales de fonctionnement précisées en partie I.

ARTICLE 1 – DEFINITION DES SCHEMAS DE CARTES DE PAIEMENT INTERNATIONAUX

1.1 Les schémas de cartes de paiement internationaux permettent la réalisation, dans les conditions prévues dans les Conditions Particulières et les présentes Conditions Générales (partie I et II), de réaliser des opérations de paiement en France ainsi qu'à l'étranger.

1.2 Les schémas internationaux inclus dans le périmètre du présent Contrat sont notamment :

(i) VISA Inc.
(ii) Mastercard International Inc.
(iii) UnionPay International Corporation Ltd.

1.3 Les schémas internationaux reposent sur l'utilisation des Cartes portant notamment les marques suivantes :

(i) Pour VISA Inc. : Visa, V PAY, Visa Electron
(ii) Pour Mastercard International Inc. : Mastercard, Maestro.
(iii) Pour UnionPay International Corporation Ltd : UnionPay

ARTICLE 2 – DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

2.1 Obligations de la Banque

Par dérogation à l'article 4.6 de la partie I des présentes Conditions Générales, la Banque s'engage à ne pas débiter, au-delà du délai maximum de 24 (vingt-quatre) mois à partir de la date du crédit initial porté au compte du Client les opérations de paiement non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

2.2 Garantie de paiement :

Une opération de paiement réalisée en lecture puce EMV est garantie, même s'il n'y a pas eu frappe du code confidentiel par le Titulaire de la Carte, à condition d'avoir obtenu une autorisation d'un montant identique à ladite opération.

Pour les opérations de paiement réalisées à l'aide d'une Carte/d'un Instrument de paiement « sans contact » émis(e) hors de l'EEE, la garantie de paiement n'est pas acquise en cas de contestation du Titulaire de la Carte liée à la relation sous-jacente.

ARTICLE 3 – DISPOSITIONS SPECIFIQUES AU SCHEMA UNIONPAY

3.1 Fonctionnement du Schéma

Le Schéma repose sur l'utilisation des Cartes portant la Marque UnionPay.

3.2 Garantie de paiement :

Une opération de paiement réalisée en lecture puce EMV est garantie, même s'il n'y a pas eu frappe du code confidentiel par le Titulaire de la Carte, à condition d'avoir obtenu une autorisation d'un montant identique à ladite opération.

Pour les opérations de paiement réalisées à l'aide d'une Carte/d'un Instrument de paiement « sans contact » émis(e) hors de l'EEE, la garantie de paiement n'est pas acquise en cas de contestation du Titulaire de la Carte liée à la relation sous-jacente.

3.3 Mesures de sécurité

Par dérogation aux dispositions de l'article 6 de la partie 1, le Client s'engage lors du paiement à :

3.3.1 Vérifier l'acceptabilité de la Carte, c'est-à-dire :

- la présence de la Marque UnionPay sur la Carte
- la présence ou non de la puce électronique sur la Carte pour identifier le mode de lecture requis (lecture puce ou lecture piste magnétique),
- la période de validité (fin et éventuellement début) lorsqu'elle figure sur la Carte,
- l'absence des inscriptions « Sample Card », « Special Card » ou « VOID »,
- l'absence de dégradation ou d'altération de la Carte,
- si une photo est présente sur la Carte, qu'elle soit celle de la personne qui l'utilise,
- la présence d'une signature sur le panonceau de signature au dos de la Carte (lorsque la Carte dispose d'un tel panonceau),
- l'absence de dégradation ou d'altération du panonceau de signature,
- et la refuser en cas de non-conformité.

3.3.2 Utiliser l'Equipement Electronique, respecter les indications affichées sur l'écran et suivre les procédures dont les modalités techniques lui ont été indiquées.

L'Equipement Electronique doit notamment :

- après la lecture de la puce de la Carte lorsqu'elle est présente :
  (i) permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  (ii) vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - période de validité (fin et éventuellement début) lorsqu'elle est présente sur la Carte.
- lorsque la puce n'est pas présente sur une Carte, après lecture de la piste ISO 2, vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - la période de validité (fin et éventuellement début) lorsqu'elle est présente sur la Carte.

3.3.3 Lorsque la puce le demande à l'Equipement Electronique, faire composer par le Titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel. La preuve de la frappe du code confidentiel est apportée par le certificat qui doit figurer sur le Ticket.

3.3.4 Obtenir une autorisation d'un montant identique à l'opération lorsque l'Equipement Electronique ou la puce de la Carte déclenche une demande d'autorisation. A défaut, l'opération ne sera pas garantie.

Lorsque la puce n'est pas présente sur la Carte ou lorsqu'elle ne fonctionne pas, si l'Equipement Electronique le permet, l'autorisation doit être demandée en lecture piste en transmettant l'intégralité des données de la piste ISO 2.

Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation est annulée.

3.3.5 Faire signer le Ticket dès le premier euro pour toute opération de paiement.

3.3.6 Lorsque la Carte comporte un panonceau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur le Ticket.

Pour une Carte sur laquelle ne figure pas le panonceau de signature, vérifier la conformité de la signature qui figure sur le Ticket avec celle qui figure sur la pièce d'identité présentée par la personne qui utilise la Carte.

3.3.7 Remettre au Titulaire de la Carte l'exemplaire du Ticket qui lui est destiné.

3.3.8 En cas de suspension de l'acceptation des Cartes du Schéma UnionPay International, la période de suspension est au minimum de deux (2) ans. A l'expiration de ce délai, l'Accepteur peut demander la reprise du Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat avec un autre acquéreur de son choix.

3.4 Suspension de l'acceptation

Par dérogation à l'article 12.4 de la partie I du présent Contrat, la période de suspension de l'acceptation des Cartes du Schéma UnionPay International est de deux (2) ans minimum.

DISPOSITIONS SPECIFIQUES AUX SCHEMAS CB

1.1 Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les « Cartes CB ») auprès des Accepteurs adhérant au Schéma CB dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou application de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'adhésion, la Banque définissant certaines conditions spécifiques de fonctionnement.

Lorsque la Banque représente le GIE CB, le terme de « représentation » ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à l'Acquéreur, et non la mise en jeu de la garantie du paiement visée à l'article 5 de la partie I du présent Contrat.

1.2 Dispositions relatives aux Cartes CB et Solutions de paiement CB

Sont utilisables dans le Schéma CB et dans le cadre du présent Contrat :

- les cartes sur lesquelles figure la Marque CB,
- les solutions de paiement CB.

[FACULTATIF: 1.2 Bis - Dispositions relatives aux cartes prépayées sans puce.

Les obligations prévues aux articles 3.1 et 6.3.1 de la partie I et à l'article 1.2 ci-dessus ne sont pas applicables aux cartes prépayées sans puce ne portant pas la Marque CB qui peuvent être acceptées dans le Schéma CB par le Client ayant signé un contrat spécial pour ce faire avec l'émetteur de ces cartes.]

1.3 Dispositions sur l'acceptation de Cartes CB

En complément des dispositions de la partie I du présent Contrat, le Client s'engage :

- à accepter les Cartes CB pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués, même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, pour le paiement de dons et en contrepartie du règlement du montant de cotisations,
- à transmettre les enregistrements des opérations de paiement à la Banque dans

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

les délais prévus dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 (six) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma CB.

- en cas de demande d'audit par le GIE CB, à permettre à la Banque de faire procéder aux frais de l'Accepteur dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 3.14 de la partie I du présent Contrat, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'adhésion, voire à une radiation du Schéma CB telle que prévue à l'article 1.4 ci-après. Le Client autorise la communication du rapport à la Banque et au GIE CB.

1.4 Suspension de l'adhésion et radiation du Schéma CB

1.4.1 Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au Schéma CB. Elle est précédée, le cas échéant, d'un avertissement au Client, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen. Son effet est immédiat.

Elle peut être décidée en raison :

- d'une utilisation anormale de Cartes/d'Instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,
- d'une utilisation d'un Equipement Electronique non agréé,
- d'un risque de dysfonctionnement important du Schéma CB,
- d'une utilisation anormale ou détournée de l'Equipement Electronique.

1.4.2 Le Client s'engage alors à restituer à la Banque l'Equipement Electronique (sauf dans le cas où l'Equipement Electronique est un smartphone appartenant au Client), les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes CB.

1.4.3 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable.

1.4.4 A l'expiration de ce délai, le Client peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet du présent Contrat auprès de la Banque, ou souscrire un nouveau contrat d'adhésion avec un autre acquéreur de son choix.

1.4.5 En cas de comportement frauduleux de la part du Client, il peut être immédiatement radié du Schéma CB ou la suspension être convertie en radiation.

1.5 Protection des données à caractère personnel du Client

1.5.1 La Banque, au titre de l'acceptation en paiement par Carte dans le Système CB, informe que le GIE CB traite des données à caractère personnel du Client (personne physique ou personne physique le représentant) qui concernent notamment son identité et ses fonctions.

1.5.2 Ces données à caractère personnel font l'objet de traitements afin de permettre :

- la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB ;
- de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte.

1.5.3 Le Client (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés à l'article 14 des Conditions générales communes à tous les schémas de cartes de paiement par courriel à protegezvosdonnees@cartes-bancaires.com.

1.5.4 Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, le Client (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :

- Consulter la Politique de protection des données à caractère personnel du GIE CB accessible à www.cartes-bancaires.com/protegezvosdonnees ;
- Contacter le Délégué à la protection des données désigné par le GIE CB par courriel à protegezvosdonnees@cartes-bancaires.com.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

ANNEXE 1 : REFERENTIEL SECURITAIRE ACCEPTEUR

Les exigences constituant le Référentiel Sécuritaire Accepteur sont présentées ci-après :

EXIGENCE 1 (E1) : GERER LA SECURITE DU SYSTEME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE

Pour assurer la sécurité des données des opérations de paiement et notamment des données personnelles et des données de paiements sensibles liées à la Carte des Titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.
En particulier, un responsable de la sécurité du système commercial et d'acceptation doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et du secret bancaire dans le cadre de leur utilisation et de leur environnement.
Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.
Le contrôle du respect des exigences de sécurité relatives au système commercial et d'acceptation doit être assuré.
Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

EXIGENCE 2 (E2) : GERER L'ACTIVITE HUMAINE ET INTERNE

Les obligations et les responsabilités du personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.
Les obligations et les responsabilités du personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.
Le personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Le personnel doit être régulièrement sensibilisé aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.
Il convient que le personnel reçoive une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

EXIGENCE 3 (E3) : GERER LES ACCES AUX LOCAUX ET AUX INFORMATIONS

Tout dispositif (équipement réseau, serveur, …) qui stocke ou qui traite des données relatives à une opération de paiement et, notamment, des données de paiement sensibles liées à la Carte du Titulaire de la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.
Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre. Les sauvegardes peuvent se faire sur bande, disques ou tout autre support reconnu.
Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.
La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

EXIGENCE 4 (E4) : ASSURER LA PROTECTION LOGIQUE DU SYSTEME COMMERCIAL ET D'ACCEPTATION

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation doivent être établies et leur respect doit être contrôlé.
Seul le serveur supportant l'application commerciale doit être accessible par les internautes.
Le serveur de base de données client ainsi que le serveur hébergeant le système d'acceptation ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu.
Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu.
L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées.
Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.
Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.
Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

EXIGENCE 5 (E5) : CONTROLER L'ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés.
Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et d'acceptation.
Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

EXIGENCE 6 (E6) : GERER LES ACCES AUTORISES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.
Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification.
L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.
L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.
Les changements de situation (changement de poste, départ, …) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.
La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.
Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.
Les tentatives d'accès doivent être limitées en nombre.
Les mots de passe doivent être changés régulièrement.
Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

EXIGENCE 7 (E7) : SURVEILLER LES ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.
L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.
Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées.
Les systèmes assurant l'enregistrement doivent au minimum avoir la fonction de pare-feu pour le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.
Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées.
Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

EXIGENCE 8 (E8) : CONTROLER L'INTRODUCTION DE LOGICIELS PERNICIEUX

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.
L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et d'acceptation.
La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

EXIGENCE 9 (E9) : APPLIQUER LES CORRECTIFS DE SECURITE (PATCHES DE SECURITE) SUR LES LOGICIELS D'EXPLOITATION

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

EXIGENCE 10 (E10) : GERER LES CHANGEMENTS DE VERSION DES LOGICIELS D'EXPLOITATION

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée.
Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

EXIGENCE 11 (E11) : MAINTENIR L'INTEGRITE DES LOGICIELS APPLICATIFS RELATIFS AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.
Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.
La demande de modification doit être approuvée par le responsable fonctionnel du système.
Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

EXIGENCE 12 (E12) : ASSURER LA TRAÇABILITE DES OPERATIONS TECHNIQUES (ADMINISTRATION ET MAINTENANCE)

Les opérations techniques effectuées doivent être enregistrées de manière chronologique, dans un cahier de bord pour permettre la reconstruction, la revue et l'analyse en temps voulu des séquences de traitement et des autres activités liées à ces opérations.

EXIGENCE 13 (E13) : MAINTENIR L'INTEGRITE DES INFORMATIONS RELATIVES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurées ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.
Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 14 (E14) : PROTEGER LA CONFIDENTIALITE DES DONNEES BANCAIRES

Les données de paiement sensibles liées à la Carte du Titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un Titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur.

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données de paiement sensibles liées à la Carte du Titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant de l'Accepteur et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 15 (E15) : PROTEGER LA CONFIDENTIALITE DES IDENTIFIANTS – AUTHENTIFIANTS DES UTILISATEURS ET ADMINISTRATEURS

La confidentialité des identifiants - authentifiants doit être protégée lors de leur stockage et de leur circulation.
Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.
Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

ANNEXE 2 : REFERENTIEL SECURITAIRE PCI-DSS

L'intégralité des exigences du Référentiel Sécuritaire PCI-DSS doivent être respectées dans la version en cours de validité disponible à l'adresse suivante : https://www.pcisecuritystandards.org/ (Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards).

Les exigences constituant le Référentiel Sécuritaire PCI-DSS sont organisées autour d'un ensemble de douze (12) familles d'exigences regroupant deux cent cinquante (250) règles réparties en six (6) grands domaines présentés ci-après :

1° *Mettre en place et gérer un réseau sécurisé*

1ère exigence	Installer et gérer une configuration de pare-feu afin de protéger les données des Titulaires des Cartes
2ème exigence	Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système

2° *Protéger les données des Titulaires de Cartes*

3ème exigence	Protéger les données des Titulaires de Cartes stockées
4ème exigence	Crypter la transmission des données des Titulaires de Cartes sur les réseaux publics ouverts

3° *Disposer d'un programme de gestion de la vulnérabilité*

5ème exigence	Utiliser et mettre à jour régulièrement un logiciel antivirus
6ème exigence	Développer et gérer des applications et systèmes sécurisés

4° *Mettre en œuvre des mesures de contrôle d'accès efficaces*

7ème exigence	Limiter l'accès aux données des Titulaires de Cartes aux cas de nécessité professionnelle absolue
8ème exigence	Attribuer une identité d'utilisateur à chaque personne disposant d'un accès informatique
9ème exigence	Limiter l'accès physique aux données des Titulaires de Cartes

5°*Surveiller et tester régulièrement les réseaux*

10ème exigence	Suivre et surveiller tous les accès aux ressources du réseau et aux données des Titulaires de Cartes
11ème exigence	Tester régulièrement les systèmes et procédures de sécurité

6° *Disposer d'une politique en matière de sécurité de l'information*

12ème exigence	Disposer d'une politique régissant la sécurité de l'information

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26

ANNEXE 3 : CONDITIONS DE FONCTIONNEMENT DU SERVICE « DIFFERE SANTE »

Préambule :

La présente annexe détaille les conditions de fonctionnement du service « Différé Santé », en complément des Conditions Générales et Conditions Particulières du présent Contrat. Ce service est destiné aux Clients (i) Professionnels de Santé listés ci-dessous, (ii) disposant d'un Equipement Electronique compatible avec l'accès au service « Différé Santé », et (iii) ayant choisi cette option aux Conditions Particulières du présent Contrat. Elle expose notamment les conditions dans lesquelles les Clients Professionnels de Santé peuvent bénéficier d'un délai prolongé de présentation en compensation des opérations leur permettant ainsi de proposer à leurs patients un délai supplémentaire avant que leur propre compte soit débité.

Les termes dotés d'une initiale majuscule non définis dans la présente annexe ont la signification qui leur est attribuée dans les Conditions Générales et/ou Particulières du Contrat.

Article 1 : Conditions préalables

Le service « Différé Santé » est soumis aux conditions préalables et suspensives suivantes :

- Cartes : le service « Différé Santé » n'est disponible que pour les Cartes sur lesquelles figurent la Marque « CB ». En conséquence, le Client s'engage à systématiquement refuser sur son TPE le « Différé Santé » pour les autres cartes.
- Professionnels de Santé : le service « Différé Santé » n'est disponible que pour les Professionnels de Santé identifiés par les codes APE (NAF) suivants, déclarés à l'INSEE :

SECTEURS	APE (NAF) 2008	APE (NAF) 2003
Commerce de détail de produits Pharmaceutiques	4773Z	523A
Activités hospitalières	8610Z	851A
Pratique médicale	8621Z-8622A / 8622B-8622C	851C
Pratique dentaire	8623Z	851E
Activités des auxiliaires médicaux	8690D-8690E / 8710A-8710B 8710C-8720A / 8720B-8730A / 8730B	851G
Ambulances	8690A	851J
Laboratoires analyse médicale	8690B	851K
Commerce de détail d'optique et de photographie[1]	4778A[1]	524T[1]

Le Client est informé que (a) le service « Différé Santé » ne sera activé/disponible que postérieurement à la réception d'une confirmation de l'INSEE de son enregistrement sous l'un des code APE (NAF) listé ci-dessus, et (b) cette procédure peut prendre quelques jours.

Le service « Différé Santé » sera résilié de plein droit en cas de changement de numéro SIRET du Client, sauf accord préalable de la Banque.

- Choix lors de l'opération de paiement : lors de l'opération de paiement, le TPE proposera systématiquement au Client de choisir l'option « Différé Santé ». Le service « Différé Santé » ne sera effectif, pour chaque opération, qu'en cas d'acceptation de l'option par le Client.

Article 2 : Obligation du Client

Le Client s'engage à informer systématiquement son patient de la possibilité de bénéficier du « Différé Santé » et du délai supplémentaire dont ce dernier bénéficiera en cas de choix de cette option.

Article 3 : Délais du « Différé Santé »

Des délais spécifiques sont fixés dans les Conditions Particulières pour le crédit du compte du Client et la remise en compensation.

Article 4 : Divers

Les stipulations des Conditions Générales et Conditions Particulières non modifiées par la présente annexe restent applicables.

[1] Activité d'optique uniquement, le Client doit fournir une déclaration sur l'honneur qu'il ne pratique que l'activité d'optique

Réf : CGL_CONTRAT_PAIEMENT_PROXIMITE_SE-CGLPAIEPROXSE-23_S16-2023.04.03.11.57.51.26