CONDITIONS GENERALES D'ADHESION AUX SYSTÈMES D'ACCEPTATION DE PAIEMENT PAR CARTES

Vos conditions d'adhésion aux Systèmes d'Acceptation de paiement par cartes sont régies par

- Les Conditions Particulières que vous devez régulariser
- Les présentes Conditions Générales d'Adhésion aux Systèmes d'Acceptation de paiement par cartes et leurs Annexes (ci-après « Conditions Générales »)

Nous vous informons que vos opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité, en particulier celles visées dans les présentes Conditions Générales.

ARTICLE 1 : DÉFINITIONS

- «Accepteur» : Vous êtes qualifié d'Accepteur lorsque vous acceptez un paiement par carte de type CB, Visa, Mastercard, JCB ou Discover ou dans l'activité de Quasicash lorsque vous délivrez des espèces ou des « quasi-espèces » dans le respect de la législation applicable (Casinos, Cercles de jeux privés référencés au Ministère de l'intérieur, Changeurs manuels et Prestataires de paiement).

- «Acquéreur» : Nous sommes qualifiés d'Acquéreur lorsque nous collectons vos transactions cartes en vue de leur règlement.

- Par «Automate», il faut entendre tout Équipement Électronique permettant la distribution automatique de biens et services payables par carte. Il doit être agréé selon des exigences définies par les Schémas de cartes.

- Par «Carte», il faut entendre Carte portant une Marque CB, Visa, MasterCard, Maestro, Electron, VPay, JCB, Discover ou Diners Club International. Une Carte est une solution de paiement que nous acceptons. Elle peut être matérialisée par tout support physique ou dématérialisé.

  Lorsqu'elles sont émises dans l'Espace Économique Européen (EEE), les Cartes portent au moins l'une des mentions suivantes :
  - crédit ou carte de crédit,
  - débit,
  - prépayée,
  - commerciale

  ou l'équivalent dans une langue étrangère.

  Les cartes prépayées sans puce ne portant pas les Marques CB, MasterCard, Maestro, Visa, Vpay, Electron, JCB,Discover ou Diners Club International ne sont pas acceptées dans le Schéma CB. L'acceptation de ce type de carte doit faire l'objet d'un contrat spécifique avec l'émetteur de ces Cartes. Cette liste est valable à la date de signature des présentes et elle est évolutive. Vous serez informé de toute modification par tout moyen, sans que ce changement ne donne lieu à l'établissement d'un avenant. bancaire).

- "Émetteur" : Il s'agit d'un organisme financier ou assimilé qui met une Carte à la disposition de son client, le Titulaire de Carte.

- Par «Équipement Électronique», il faut entendre tout dispositif de paiement qui comporte un système permettant l'acceptation d'un paiement par carte comme par exemple un Terminal de Paiement Électronique (ci-après «TPE»), un Automate ou une page de paiement sécurisée. Il doit être agréé selon des exigences définies par les Schémas de cartes.

- Par «Marque», il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptible de désigner le Schéma. Les marques des Schémas pouvant être acceptées entrant dans le champ d'application du présent contrat sont : CB, Visa, MasterCard, Maestro, Electron, VPay, JCB, Discover et Diners Club International.

- Par « Paiement de Proximité », il faut entendre tout paiement réalisé au moyen d'un Équipement Électronique avec la présence physique du Titulaire de Carte.

- Par « Paiement pour la Location de Biens et Services », il faut entendre un paiement comportant deux étapes :

  - L'acceptation initiale par le Titulaire de Carte de n'être débité qu'à l'issue de la location, du montant des frais réels de celle-ci dans les conditions définies aux présentes Conditions Générales,
  - L'exécution de l'opération de paiement intervenant après détermination de son montant.

  L'opération réalisée dans le cadre d'un Paiement pour la Location de Biens et Services doit respecter les conditions décrites dans les Conditions Générales, qui sont spécifiques aux Paiements de Proximité lorsqu'elle est réalisée dans ce contexte, ou bien celles de Vente à Distance Sécurisée lorsqu'elle se produit dans ce contexte.

- Par "Point d'Acception", il faut entendre le lieu physique ou digital où l'Équipement Électronique est situé et où le paiement par Carte est réalisé.

- Par « Quasicash », il faut entendre toute opération de délivrance d'espèces ou de «quasi-espèces» réalisée en contrepartie d'une opération de paiement par Carte.

  Par délivrance « d'espèces », il faut entendre :
  - l'achat de devises étrangères auprès d'un changeur manuel,
  - la mise à disposition aux Titulaires de Cartes, contre une opération de paiement par Carte, de monnaie fiduciaire par un Établissement de crédit et de paiement.

  Par délivrance de «quasi-espèces» il faut entendre :
  - l'achat de chèques de voyage auprès des changeurs manuels,
  - l'achat de jetons dans les casinos ou dans les cercles de jeux privés autorisés par la Loi.

  L'opération de Quasicash doit respecter les conditions décrites dans les Conditions Générales, qui sont spécifiques aux Paiements de Proximité lorsqu'elle est réalisée dans ce contexte, ou bien celles de Vente à Distance Sécurisée lorsqu'elle se produit dans ce contexte.

- Par «Schéma», il faut entendre un Schéma de cartes de paiement ou encore un réseau qui pose un ensemble de règles régissant l'opération de paiement par carte tel que défini à l'article 2 du Règlement UE n°2015/751 du 29 avril 2015 (ci-après le « Règlement »).

  Les Schémas CB, Visa, MasterCard, JCB et Discover reposent sur l'utilisation de Cartes CB, Visa, MasterCard, JCB et Discover auprès des Accepteurs et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits réseaux.

- Par «Système d'Acceptation», il faut entendre tout dispositif permettant la réalisation et le dénouement complet d'une opération de paiement par carte. Le Système d'Acceptation comprend l'ensemble des réseaux et systèmes informatiques conformes aux règles d'un Schéma qui assurent le transport et le traitement sécurisés des données entre l'Accepteur, l'Acquéreur, les entités de traitement et l'Emetteur de la carte. Le Système d'Acceptation englobe notamment les fonctions de validation de la Carte, d'authentification du Titulaire de Carte ou de l'utilisateur de l'application de paiement, ainsi que celles d'autorisation, de compensation et de règlement de l'opération de paiement par Carte.

- Par « Titulaire de Carte », il faut entendre la personne dont le nom est mentionné sur la Carte.

- Par "Vente à distance", il faut entendre tout paiement réalisé au moyen d'un Équipement Électronique sans la présence physique du Titulaire de Carte et faisant suite au recueil par l'Accepteur des données Carte par courrier, téléphone, fax...

- Par «Vente à Distance Sécurisée », il faut entendre tout paiement réalisé sans la présence physique du Titulaire de Carte et pour la réalisation duquel ce dernier saisit lui même ses données Carte sur l'Equipement Electronique.

ARTICLE 2 : LES SCHÉMAS DE CARTES

Les Schémas de cartes reposent sur l'utilisation de Cartes pour la réalisation d'un paiement.

Lorsque vous adhérez aux Schémas de cartes, vous vous engagez à respecter les dispositions et procédures définies ou homologuées par lesdits Schémas.
Notre rôle se limite à appliquer les conditions techniques d'acceptation des Cartes et de remise des opérations à l'Acquéreur, et ne s'étend pas à la mise en jeu de la garantie du paiement (telle que visée à l'article « Garantie du Paiement » des présentes Conditions Générales).

ARTICLE 3 : INFORMATION

Vous avez la possibilité d'installer sur l'Équipement Électronique, des mécanismes automatiques qui effectuent la sélection prioritaire d'une Marque de carte ou d'un Schéma. Cependant, vous ne pouvez pas vous opposer à ce que votre client passe outre cette sélection.

ARTICLE 4 : OBLIGATIONS DE L'ACCEPTEUR

Vous vous engagez à :

4.1 Assumer seul la responsabilité pleine et entière de vos services, de vos biens et produits et du respect de la loi applicable à votre activité (notamment fiscales).

4.2 Respecter vous-même et faire respecter à vos prestataires installant votre solution de paiement l'ensemble des contraintes techniques et sécuritaires prévues aux présentes (notamment les Annexes « Référentiel sécuritaire accepteur » et « PCI DSS et risques acquéreurs »), et obtenir leur accord pour que nous puissions diligenter des audits chez eux.

4.3 Accepter que nous procédions à des audits conformément à la clause d'audit de l'annexe « PCI DSS et risques acquéreurs ».

4.4 Utiliser un Équipement Électronique agréé par les Schémas de cartes et vous assurer de sa conformité notamment dans le temps en nous interrogeant.

4.5 Recueillir l'autorisation des Schémas de cartes ou notre autorisation avant de modifier les paramètres de fonctionnement de l'Équipement Électronique ou d'y installer de nouvelles applications.

4.6 Nous informer de tout changement impactant vos déclarations initiales (notamment type d'activité, sociétés prestataires, responsable sécurité…).

4.7 Ne pas exercer une activité de « Membre Service Provider (MSP) – Agrégateurs » qui consiste à assurer la collecte et le recouvrement des paiements effectués par Cartes pour des tiers, professionnels ou particuliers louant ou vendant des biens ou services sur Internet, vendant des espèces ou des quasi-espèces; ou encore, à réaliser la gestion de leurs moyens de paiement. Le non-respect de cette obligation vous rendrait pleinement responsable des conséquences dommageables liées à ces activités.

4.8 Vous devez afficher visiblement les informations suivantes :
- Les catégories et Marques de cartes que vous acceptez ou refusez, en apposant les panonceaux, vitrophanies et enseignes fournis de façon apparente à votre Point d'Acceptation.
- Le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Titulaire de Carte en soit préalablement informé.
- Les contraintes spécifiques figurant en Annexe et imposées par type de paiement.

4.9 Informer les Titulaires de Cartes des conditions imposées pour l'utilisation de leur Carte et recueillir leur acceptation explicite.

4.10 Vous devez vous identifier clairement par votre numéro d'identifiant commerçant et par votre code activité (NAF/APE) que l'INSEE vous a attribué. Si votre activité a changé depuis l'attribution de ce code NAF/APE, vous nous autorisez à vous enregistrer sous un code correspondant à votre activité actuelle principale ou secondaire. Si vous n'êtes pas immatriculable, vous pourrez dans certains cas utiliser un numéro d'identification spécifique, que nous vous fournirons vous permettant l'accès aux Schémas de cartes. Vous devrez vous faire immatriculer dans un délai maximum de six (6) semaines, sauf cas particulier ci-après :
- Accepteur situé à Monaco, Collectivités d'Outre-Mer, Accepteur situé hors de France,
- Accepteur exerçant une activité secondaire (exemple : garage exerçant à titre d'activité secondaire la location de voitures…),
- Certaines activités spécifiques (distributeur automatique de carburant, armée, artiste).

4.11 Vous devez vous assurer que votre client pourra sans difficulté vérifier et identifier, suite à un paiement, les opérations de paiement qu'il a effectuées à votre Point d'Acceptation (votre dénomination commerciale connue du client) et le mode de paiement. Vous devrez vérifier auprès de nous la conformité des informations transmises à votre client. En cas d'achat de devises étrangères ou de chèques de voyage, vous devez également vous assurer que votre client pourra identifier le montant éventuel des commissions de change perçues et le montant de l'opération d'achat de «quasi-espèces».

4.12 N'accepter les paiements par carte qu'en contrepartie de prestations réelles ou de dons, de la remise d'espèces ou de quasi-espèces, et respecter le choix du Titulaire de Carte en ce qui concerne tant la Marque, que la catégorie de Carte, que le Schéma de cartes lors du paiement par Carte.

4.13 En cas de Paiement pour la Location de Biens et Services, ne pas faire usage de la Carte pour vous octroyer une caution ou un dépôt de garantie.

4.14 Attribuer à l'occasion de l'initialisation de l'opération de Paiement pour la Location de Biens et Services, un numéro de dossier indépendant du numéro de carte.

4.15 Ne pas réaliser une opération de paiement pour laquelle vous n'avez pas reçu le consentement du Titulaire de Carte

4.16 Nous transmettre les enregistrements des opérations de paiement, dans les délais prévus dans les Conditions Particulières. Le délai maximum pour transmettre les enregistrements est de 6 (six) mois pour l'encaissement des opérations de paiement du Schéma de cartes CB.

4.17 Remettre au Titulaire de Carte ou lui transmettre un justificatif de l'opération de paiement par Carte comportant notamment le montant final de l'opération.

4.18 Dans le cas où vous proposez des opérations de paiements récurrentes ou échelonnées vous vous engagez à respecter les règles relatives au stockage des données cartes, à informer clairement votre client des modalités de paiement et à ne plus réaliser de paiements récurrents ou échelonnés dès lors que ce dernier a retiré son consentement.

4.19 Faire votre affaire personnelle des litiges avec les Titulaires de Cartes concernant les achats, les réservations ou les locations de biens et services, la remise d'espèces ou de « quasi-espèces » dont l'achat a été réglé par Carte.

4.20 Nous régler les frais et commissions prévues aux Conditions Particulières.

4.21 Vous vous engagez à effectuer des travaux de maintenance et de mise à niveau de votre Système d'Acceptation conformément aux Conditions convenues avec nous. Ces travaux seront effectués dans le respect des règles définies dans l'annexe « PCI DSS et risques acquéreurs » et « l'annexe Référentiel sécuritaire accepteur ».

4.22 Vous vous engagez à prendre toutes mesures propres à assurer la garde de votre Équipement Électronique et/ou Automate et être vigilant quant à l'utilisation qui en est faite. Quels que soient vos modes de commercialisation, vous devez respecter les règles définies dans l'annexe « PCI DSS et risques acquéreurs » et l'annexe « Référentiel sécuritaire accepteur » qui vous ont été communiquées.

4.23 Vous vous engagez à nous informer immédiatement en cas de fonctionnement anormal de votre solution de paiement et de toutes autres anomalies (comme l'absence d'application des procédures de sécurisation des ordres de paiement, le dysfonctionnement du Système d'Acceptation, l'absence de reçu ou de mise à jour de la liste noire, l'impossibilité de réparer rapidement...).

ARTICLE 5 : CONDITIONS D'UTILISATION DE L'ÉQUIPEMENT ÉLECTRONIQUE

Les Schémas de cartes informent tous les constructeurs connus et référencés par eux des mises à jour de logiciels jugées indispensables. Vous devez assurer l'installation, le fonctionnement, la maintenance et la mise à niveau de l'Équipement Électronique.

5.1 Équipement Électronique vous appartenant ou loué à un tiers

Dans le cadre de l'acceptation des Cartes, vous devez :

5.1.1 Veiller à ce que votre police d'assurance couvre bien :
- les risques inhérents à la garde de cet Équipement Électronique ou des équipements annexes, dont nous ne saurons être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération,
- les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu vous être confiés.

5.1.2 Nous garantir un libre accès à l'Équipement Électronique, tout comme au constructeur ou à toute personne désignée par nos soins pour les différents travaux à effectuer sur l'appareil.

5.1.3 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées et n'y apporter aucune modification de logiciel ayant un impact sur les Schémas de cartes sans notre accord préalable. L'Equipement Électronique doit toujours être utilisé dans le respect des présentes Conditions générales.

5.1.4 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Équipements Électroniques.

5.2 Équipement Électronique nous appartenant

Dans le cadre de l'acceptation des Cartes, vous devez :

5.2.1 Réserver dans le Point d'Acceptation, l'emplacement nécessaire à l'installation de l'Équipement Électronique.

5.2.2 Faire votre affaire des travaux préalables à la mise en place des Équipements Électroniques (mise à disposition des prises électriques, téléphoniques, etc).

5.2.3 Nous garantir un libre accès à l'Équipement Électronique, tout comme au constructeur ou à toute personne désignée par nos soins pour intervenir sur l'Équipement Électronique afin d'en assurer la maintenance, notamment lorsque la mise à jour de logiciels s'avère nécessaire.

5.2.4 Signer, à réception de l'Équipement Électronique, qu'il s'agisse d'une première installation ou d'un remplacement, le bordereau de prise en charge qui vous sera présenté. Ce document reprend les caractéristiques indispensables à l'identification de l'Equipement Electronique.

5.2.5 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées, n'y apporter aucune modification si ce n'est dans le respect des dispositions des présentes Conditions générales.

5.2.6 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Équipements Électroniques dont vous avez la garde.

5.2.7 Veiller à ce que votre police d'assurance couvre bien les risques inhérents à la garde des Equipements Electroniques ou des équipements annexes et dont nous ne saurions être responsables, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération.

5.2.8 Assumer toutes les obligations du dépositaire, conformément aux dispositions des articles 1927 et suivants du Code Civil.

5.2.9 Payer les frais de location ou de dépôt vente selon les présentes Conditions Particulières convenues avec nous. En outre, cette mise à disposition peut faire l'objet d'un contrat spécifique.

ARTICLE 6 : GESTION DE SITUATIONS SPÉCIFIQUES

6.1 Retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition
Si conformément à nos procédures, vous êtes conduit à retirer une Carte à son titulaire (le retrait ayant eu lieu notamment sur instruction du serveur d'autorisation en raison de la présence de la Carte sur la liste des Cartes faisant l'objet d'un blocage ou en opposition et/ou contrefaites, vous devrez utiliser la procédure de gestion et de renvoi des Cartes oubliées ou capturées disponible auprès de votre conseiller.

6.2 Oubli d'une Carte par son titulaire
En cas d'oubli de sa Carte par le Titulaire de Carte, vous pouvez 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 de gestion et de renvoi des Cartes oubliées ou capturées qui vous est communiquée sur demande. Au-delà de ce délai, vous devez nous renvoyer la Carte en utilisant la procédure de gestion et de restitution des Cartes oubliées ou capturées.

6.3 Transaction crédit
Le remboursement partiel ou total d'une transaction réglée par Carte doit, avec l'accord du Titulaire de Carte, être effectué au moyen de la Carte utilisée pour l'opération initiale.

6.4 Carte non signée
En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, vous devez demander au Titulaire de 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 sa pièce d'identité. Si le Titulaire de Carte refuse de signer sa Carte, vous devez refuser le paiement par Carte.

ARTICLE 7 : NOS OBLIGATIONS EN TANT QU ACQUÉREUR

Nous nous engageons à :

7.1 Respecter votre choix et celui du Titulaire de la Carte en ce qui concerne tant la Marque, que la catégorie de Carte, que le Schéma de cartes lors du paiement par Carte.

7.2 Vous inscrire sur la liste des points d'acceptation habilités à recevoir des paiements par Cartes.

7.3 Vous préciser la liste et les caractéristiques des Cartes (Marques et catégories) pouvant être acceptées et vous fournir à votre demande le fichier des codes émetteurs (BIN).

7.4 Vous indiquez les frais applicables aux Cartes acceptées, y compris les commissions d'interchange et les frais versés aux Schémas de cartes.

7.5 Créditer votre compte des sommes qui vous sont dues selon les modalités prévues entre nous.

7.6 Ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté à votre compte, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

7.7 Nous vous adresserons un relevé mensuel des frais d'encaissement carte mentionnant :
- les références vous permettant d'identifier les opérations de paiement,
- les montants des opérations de paiement exprimés dans la devise dans laquelle votre compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement, et le montant de la commission de service commerçant ainsi que celui de la commission d'interchange.

Vous pouvez demander que les informations soient regroupées par Marque de carte, application de paiement, catégorie de Carte et par taux de commission d'interchange.

7.8 Vous indiquez les commissions de services à acquitter indiquées séparément pour chaque catégorie de Carte selon les différents niveaux de commission d'interchange.

ARTICLE 8 : PAIEMENT «SANS CONTACT»

8.1 Lorsque vous disposez d'un Équipement Électronique disposant de la technologie «sans contact», ledit Équipement Électronique permet le paiement rapide « sans contact » par des Titulaires de Cartes avec une lecture à distance de la Carte ou du support sur lequel la Carte est enregistré, et sans frappe du code confidentiel.

8.2 Vous vous engagez à signaler au public que votre point d'acceptation permet les paiements « sans contact » par l'apposition de façon apparente sur l'Équipement Électronique, au niveau du lecteur «sans contact», d'un pictogramme.

8.3 En toutes circonstances, vous devez vous conformer aux directives qui apparaissent sur l'Équipement Électronique comme lorsqu'il vous est demandé de faire composer au Titulaire de Carte son code confidentiel ou mettre en œuvre la méthode d'authentification prévue et adaptée à la technologie applicable dans les meilleures conditions de confidentialité.

8.4 Le paiement en mode « sans contact » n'est pas accepté pour les Cartes des Schémas JCB et Discover.

8.5 Lorsque le « sans contact » est réalisé par l'utilisation de la Carte physique, le montant unitaire maximum de chaque opération de paiement par Carte en mode «sans contact» est limité (à ce jour à 50 euros, ce plafond étant susceptible d'évoluer). Au-delà de ce montant unitaire maximum, la validation de l'opération par le Titulaire de Carte reste nécessaire. Lorsqu'il est réalisé par l'utilisation d'un autre support intégrant la Carte dématérialisée, le paiement est seulement soumis aux plafonds propres à la Carte.

8.6 Lorsqu'un certain nombre de paiements successifs par Carte en mode « sans contact » est atteint, la composition du code confidentiel sera exigée quel que soit le montant du paiement.

8.7 En cas d'opération « sans contact» permise par l'Équipement Électronique, l'opération de paiement est garantie dans les conditions visées à l'article « Garantie du paiement ».

8.8 Nous ne pouvons être tenus pour responsable de l'impossibilité d'utiliser la fonctionnalité « sans contact » en cas de dysfonctionnement du téléphone mobile et/ou de la carte SIM, de la carte micro SD ou de l'application de paiement.

ARTICLE 9 : RESPONSABILITÉS DE L'ACQUÉREUR

9.1 Nous ne serons tenus en cas de sinistre de notre fait qu'à la réparation des préjudices et dommages directs à l'exclusion de tout autre dommage tels que les dommages indirects, incidents ou immatériels et notamment les pertes de profits, les pertes ou les dommages causés aux données (dont les données clients), la perte d'une chance quelles qu'en soient les conséquences, la perte d'image ou l'atteinte à la réputation, que ces dommages soient prévisibles ou non.

9.2 Entre outre, les dommages et intérêts que nous pourrions vous devoir par année pour quelque cause que ce soit, ne pourront jamais excéder le montant total que vous nous payez au terme du présent contrat pendant l'année civile précédant le sinistre (ou pour la première année du contrat, l'année du sinistre).

ARTICLE 10 : GARANTIE DU PAIEMENT

En cas de contestation du Titulaire de Carte pendant le délai légal, nous pourrons débiter votre compte sans préavis et vous devrez en assumer les conséquences.

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 lorsqu'il est demandé.

En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement et en l'absence de contestation.

Par ailleurs, l'Emetteur devra aussi authentifier le Titulaire de Carte et autoriser la transaction.

Pour les opérations de paiement réalisées à l'aide d'une Carte émise hors de l'Espace Economique Européen, la garantie de paiement n'est pas acquise en cas de contestation du Titulaire de Carte liée à la relation sous-jacente.

ARTICLE 11 : INFORMATION SUR LES CONDITIONS COMPTABLES ET FINANCIÈRES

Les conditions comptables et financières n'incluent pas les coûts inhérents aux communications téléphoniques (ou électroniques) liées au fonctionnement de l'Équipement Électronique nécessaire à l'exécution des présentes ; ces frais restant par ailleurs à votre charge.

ARTICLE 12 : DROIT D'UTILISATION DES LOGOS, MARQUES...

Vous concédez au groupe Crédit Mutuel Arkéa (Crédit Mutuel Arkéa, Fédérations du Crédit Mutuel de Bretagne, du Crédit Mutuel du Sud-Ouest et leurs filiales) un droit d'usage non exclusif de votre nom, votre marque, votre logo ou de tout graphisme vous représentant, pour l'exécution du contrat et pour des actions promotionnelles (ex: insertion de vos marques et logos sur le site Citelis...).

Vous autorisez le groupe Crédit Mutuel Arkéa à les faire figurer sur ses supports commerciaux vous présentant comme client (Sites internet, réseaux sociaux, supports papier ou numériques, presse, radios…) pendant toute la durée du présent contrat. Cette autorisation étant donnée notamment pour internet, elle vaut pour le monde entier.
Vous nous garantissez contre toute action en contrefaçon, réclamation ou revendication relative à l'utilisation de ces éléments.

ARTICLE 13 : RÉCLAMATION ET CONVENTION DE PREUVE

13.1 Réclamation

Toute réclamation concernant le contrat doit nous être transmise par écrit dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion (perte de vos droits).

Ce délai est réduit à quinze (15) jours calendaires à compter de la date de débit de votre compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

13.2 Convention de preuve

De convention expresse les enregistrements électroniques émanant notamment de notre système d'information (ou de celui des Schémas CB, Visa, MasterCard, JCB et Discover) font foi à moins que vous démontriez l'absence de fiabilité ou d'authenticité des documents produits.

ARTICLE 14 : MODIFICATIONS

14.1 Nous pouvons, selon les modalités prévues aux Conditions Particulières, modifier les dispositions du présent contrat.

Nous pouvons 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 du Système d'Acceptation suite à un dysfonctionnement etc.
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptation des Cartes portant certaines Marques,
  - la modification du seuil d'autorisation,
  - la désactivation de la fonctionnalité transaction crédit.

14.2 Les nouvelles conditions entrent en vigueur au terme d'un délai de trente (30) jours à compter de l'information qui vous est faite concernant ces évolutions. Si vous les refusez, vous pouvez résilier le contrat dans ce délai de trente (30) jours. Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque nous constatons dans votre point de vente, une utilisation anormale de Cartes perdues, volées ou contrefaites.

Passé ces délais, vous êtes réputé avoir accepté les modifications.

14.3 Si vous ne respectez pas les nouvelles conditions techniques et sécuritaires, dans les délais requis, nous pourrons résilier ou suspendre l'adhésion dans les conditions des articles ci-après.

14.4 Nous pouvons à tout moment, et notamment en fonction de l'évolution du montant effectif du panier moyen que nous aurons constaté, faire évoluer notre tarification figurant à l'article 4 des Conditions Particulières.

Vous en serez informé par tout moyen, au moins trente (30) jours avant la date d'entrée en vigueur des nouvelles dispositions. Si vous les refusez, vous pouvez résilier le contrat dans ce délai de trente (30) jours. A défaut, votre silence vaudra acceptation de ces nouvelles dispositions.

ARTICLE 15 : DUREE ET RESILIATION DU CONTRAT

15.1 Le présent contrat est conclu pour une durée indéterminée. Il peut être résilié sans justification ni préavis selon les modalités prévues aux présentes et aux Conditions Particulières.

15.2 Toute cessation d'activité, cession ou mutation de votre fonds de commerce, nous autorise à résilier immédiatement le présent contrat sous réserve du dénouement des opérations en cours.

Dans le cas où, après résiliation du présent contrat, il se révélerait des impayés, ceux-ci seront à votre charge et pourront faire l'objet d'une déclaration de créances.

15.3 Après résiliation du présent contrat, vous pourrez souscrire un nouveau contrat avec un autre Acquéreur de votre choix.

15.4 Vous vous engagez lors de la résiliation à nous restituer les dispositifs techniques et sécuritaires nous appartenant et plus généralement tout document nous appartenant. Sauf si vous avez conclu d'autres contrats d'adhésion avec des Schémas de cartes, vous devrez retirer immédiatement de vos supports de communication tout signe d'acceptation des Cartes du Schéma concerné.

ARTICLES 16 : MESURES DE PRÉVENTION ET DE SANCTION

16.1 En cas de « transaction crédit » abusive, par exemple sans vérifier l'existence préalable d'un paiement par carte bancaire, nous pouvons rendre indisponible la fonction Crédit sur l'Equipement Electronique.

En cas de manquement 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 perdues, volées ou contrefaites, nous pourrons prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

16.2 Si dans un délai de trente (30) jours, vous n'avez pas remédié au manquement ayant justifié l'avertissement ou n'avez pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, nous pourrons soit procéder à une suspension, dans les conditions précisées à l'article ci-dessous, 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.

16.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, vous êtes toujours confronté à un taux d'impayés anormalement élevé, nous pourrons résilier le présent contrat de plein droit avec effet immédiat, sous réserve des opérations en cours, en vous le notifiant par lettre recommandée avec demande d'avis de réception.

ARTICLE 17 : SUSPENSION ET RADIATION

Nous pouvons (ou par représentation des Schémas) procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes. Elle est précédée, le cas échéant, d'un avertissement, voire d'une réduction de votre seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut également intervenir à l'issu de la procédure d'audit visée à l'article 3 de l'annexe « PCI DSS et risques acquéreurs » au cas où le rapport révélerait un ou plusieurs manquements aux clauses du présent contrat.

En outre, à la demande du Schéma de cartes, nous pouvons procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une radiation de votre adhésion au Système d'Acceptation dudit Schéma. La radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat.

La suspension ou radiation peut être décidée en raison notamment :

- du non-respect répété des obligations du présent contrat et du refus d'y remédier, notamment d'une utilisation non agréée de l'Equipement Electronique vous permettant d'accéder au Système d'Acceptation et d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma ;
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites ;
- d'un refus d'acceptation répété et non motivé des Cartes du Schéma que vous avez choisi d'accepter ou que vous devez accepter ;
- de plaintes répétées d'autres membres ou partenaires du Schéma 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 de vos activités,
- d'une utilisation anormale ou détournée de l'Equipement Electronique ou du Système d'Acceptation.

Vous vous engagez alors à nous restituer les dispositifs techniques et sécuritaires nous appartenant et plus généralement tout document nous appartenant. Sauf si vous avez conclu d'autres contrats d'adhésion avec des Schémas de cartes, vous devrez retirer immédiatement de vos supports de communication tout signe d'acceptation des Cartes du Schéma concerné.

La période de suspension est au minimum de six (6) mois, éventuellement renouvelable.
A l'expiration de ce délai, vous pouvez nous demander la reprise d'effet de votre contrat ou souscrire un nouveau contrat avec un autre Acquéreur de votre choix.
En cas de comportement frauduleux de votre part ou de risque élevé de fraude, vous pouvez être immédiatement radié ou votre suspension pourra être convertie en radiation.

18 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

18.1 Secret bancaire

Nous nous engageons à prendre toutes les précautions utiles pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel traitées dans le cadre du présent contrat.
Nous nous assurons de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques pour protéger ces données.
De convention expresse, vous nous autorisez à stocker le cas échéant des données secrètes ou confidentielles vous concernant et à les communiquer à des entités impliquées dans le fonctionnement des Systèmes de paiement aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations, qu'elles émanent des Titulaires de Cartes ou d'autres entités.

18.2 Protection des données à caractère personnel

Lors de la signature ou de l'exécution des présentes, l'Accepteur et l'Acquéreur peuvent avoir accès à des données à caractère personnel.

Ainsi, en application de la réglementation 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 :

- Nous collecterons vos données à caractère personnel nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation. Ces données ne seront utilisées que pour les finalités suivantes :
  - Le traitement des opérations de paiement par Carte. Ce traitement est nécessaire à la bonne exécution du présent contrat et à défaut le contrat ne pourra être exécuté.
  - La poursuite de nos intérêts légitimes que constituent la lutte contre la fraude à la carte de paiement et la gestion des éventuels recours en justice.
  - La réponse aux obligations légales et réglementaires.

- Les données à caractère personnel que nous traitons sont conservées pour les durées suivantes :
  - Les données nécessaires à l'exécution des opérations de paiement par Carte sont conservées pour une durée de 10 ans à compter de l'opération.
  - Les données nécessaires à la lutte contre la fraude sont conservées pour une durée maximale de 5 ans à compter de la clôture du dossier de fraude.
  - Les données nécessaires à la gestion d'un éventuel recours en justice sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées selon les durées légales de prescription applicables.

- Pour satisfaire les finalités précisées ci-dessus, vos données à caractère personnel pourront notamment être communiquées à toutes les entités du groupe Crédit Mutuel Arkéa, à tous ses partenaires qui interviennent dans le cadre du présent contrat, aux autorités administratives et judiciaires compétentes, ainsi qu'aux Schémas de cartes de paiement dont les marques que vous acceptez.

Conformément à la règlementation applicable et notamment le chapitre III du Règlement (UE) 2016/679 du 27 avril 2016, vous pouvez :
- Demander à accéder aux données à caractère personnel vous concernant et / ou en demander la rectification ou l'effacement ;
- Définir des directives relatives au sort des données à caractère personnel vous concernant en cas de décès ou en cas de dissolution de la personne morale ;
- Vous opposer au traitement de données à caractère personnel vous concernant réalisé aux fins de lutte contre la fraude et / ou de gestion des éventuels recours en justice, sous réserve que nous n'invoquons pas de motifs légitimes et impérieux ;
- Demander des limitations au traitement des données à caractère personnel vous 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 vous 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 prenant connaissance de notre politique de données personnelles accessible sur notre site web.

Pour toute question en lien avec la protection des données à caractère personnel, vous pouvez joindre notre Délégué à la protection des données :

- Par e-mail : protectiondesdonnees@arkea.com
- Par voie postale : M. le Délégué à la Protection des Données - Crédit Mutuel Arkéa - 29808 Brest Cedex 9

A l'occasion de l'exécution des ordres de paiement donnés par Carte, vous pouvez avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de Cartes.

Vous vous engagez à respecter la réglementation française et européenne applicable en matière de protection des données à caractère personnel et notamment le Règlement (UE) 2016/679 du 27 avril 2016.

Vous ne pouvez utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte et le traitement des réclamations dont les Titulaires de Cartes peuvent être l'objet. Sauf obligations légales et réglementaires, vous ne pouvez ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent contrat.

Vous vous engagez 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 Carte que vous êtes amené à recueillir à l'occasion de votre 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.

Les Titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès de vous, de l'intégralité des droits prévus par la réglementation 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, vous vous engagez d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 19 : NON RENONCIATION

Même si l'une ou l'autre Partie n'exige pas à un moment quelconque l'exécution stricte d'une disposition du présent contrat ceci ne peut en aucun cas être considéré comme constituant de sa part une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

ARTICLE 20 : LOI APPLICABLE/TRIBUNAUX COMPETENTS

Le présent contrat et toutes les questions qui s'y rapportent sont 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 21 : LANGUE DU PRÉSENT CONTRAT

Le présent contrat est le contrat original rédigé en langue française qui est le seul qui fait foi.

ANNEXE : Spécificités du schéma de Cartes CB

ARTICLE 1 : DISPOSITIONS RELATIVES AUX CARTES CB ET APPLICATION DE PAIEMENT CB

Sont utilisables dans le Schéma de cartes CB et dans le cadre du présent contrat :

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

ARTICLE 2 : TRANSMISSION DES ENREGISTREMENTS

Vous devez nous transmettre les enregistrements des opérations de paiement, dans les délais prévus dans les Conditions Particulières. 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 de cartes CB.

ARTICLE 3 : ÉQUIPEMENT ÉLECTRONIQUE AGRÉÉ

Vous devez utiliser obligatoirement un Équipement Électronique agréé CB et vous assurer à cette occasion qu'il est en cours de validité (qu'il n'a pas atteint ou dépassé la date de fin de vie telle que définie dans la notification d'agrément adressée par GIE CB). A cet effet, vous pouvez prendre information de la date de fin de vie auprès de la documentation du GIE CB (notamment en consultant son site internet).

ARTICLE 4 : MESURE DE PRÉVENTION ET DE SANCTION DANS LE CADRE DE LA VENTE À DISTANCE SÉCURISÉE

4.1 Mesures de prévention et de sanction que nous pouvons mettre en œuvre

En cas de manquement aux dispositions relatives au Schéma CB 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 perdues, volées ou contrefaites, nous pourrons prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

Si dans un délai de trente (30) jours, vous n'avez 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, nous pourrons soit procéder à une suspension de l'adhésion, dans les conditions précisées à l'article "Suspension et Radiation" des Conditions Générales, 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.

De même, si dans un délai de trois (3) mois à compter de l'avertissement, vous êtes toujours confronté à un taux d'impayés anormalement élevé, nous pourrons résilier le présent contrat de plein droit avec effet immédiat, sous réserve des opérations en cours, en vous le notifiant par lettre recommandée avec demande d'avis de réception.

4.2 Mesures de prévention et de sanction mises en œuvre par le GIE CB

En cas de manquement aux dispositions du présent contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où vous ventilez les remises en paiement entre plusieurs Acquéreurs CB de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE CB peut prendre des mesures de sauvegarde et de sécurité consistant en :

- la suspension de votre acceptation des Cartes CB. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de trois (3) mois suivant la mise en demeure d'y remédier.
  Ce délai peut être ramené à quelques jours en cas d'urgence et à un (1) mois au cas où vous auriez déjà fait l'objet d'une mesure de suspension dans les vingt-quatre (24) mois précédant l'avertissement.
  La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la réception de la notification.

- la radiation de votre adhésion au Système d'Acceptation du Schéma CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception.

4.3 Vous vous engagez alors à nous restituer les dispositifs techniques et sécuritaires et les documents en votre possession dont nous sommes propriétaire et à retirer immédiatement de votre établissement tout signe d'acceptation des Cartes du Schéma CB.

4.4 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable.
A l'expiration de ce délai, vous pouvez nous demander la reprise d'effet de votre contrat ou souscrire un nouveau contrat d'adhésion avec un autre Acquéreur de votre choix.

Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par nous ou par le GIE CB et portant sur le respect des bonnes pratiques en matière de vente ou de prestations réalisées à distance et des mesures de sécurité visées dans l'annexe «Vente à distance sécurisée ».

ARTICLE 5 : PROTECTION DES DONNEES A CARACTERE PERSONNEL

Au titre de l'acceptation en paiement par Carte CB, nous vous informons que le GIE CB traite vos données à caractère personnel (qui concernent notamment votre identité et vos fonctions).
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.

Vous pouvez exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés à l'article « Secret bancaire et protection des données à caractère personnel » des Conditions Générales par courriel à l'adresse : protegezvosdonnees@cartes-bancaires.com.

Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, vous pouvez :

- 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.

ANNEXE : Vente à distance sécurisée

1. Vos obligations

Vous déclarez connaître les lois et règlements applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…).
Vous reconnaissez devoir vous conformer à ces dispositions ou à celles qui pourront intervenir et que vous devez commercialiser les produits ou prestations de services faisant l'objet d'une vente à distance en respectant les lois et règlements applicables.

Dans le cadre d'une Vente à Distance Sécurisée, vous vous engagez à :

1.1. Utiliser les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes dans le respect des dispositions légales, réglementaires et professionnelles applicables, notamment et sans limitation, les dispositions relatives aux ventes et prestations réalisées à distance et au commerce électronique (informations des utilisateurs, délais d'exécution des prestations…) ainsi que les bonnes pratiques commerciales telles que définies notamment par les codes de conduite applicables à votre activité.

1.2. Utiliser le Système d'Acceptation en vous abstenant 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, 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 des dispositions relatives aux conditions d'exercice de professions réglementées et de façon plus générale l'ensemble des textes applicables à votre activité et toute vente illicite.

1.3. Nous garantir, ainsi que les Schémas de cartes le cas échéant, contre toute conséquence dommageable pouvant résulter du manquement de vos obligations contractées au titre des présentes.

1.4. Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas de cartes et les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes.

1.5. Faire votre affaire des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des Titulaires de Cartes notamment lors de l'exercice par ces derniers de leur droit de rétractation et concernant des biens et des services dont l'achat a été réglé par Carte au titre du présent contrat.

1.6. Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas de cartes, au Référentiel sécuritaire accepteur figurant en annexe et au Protocole 3D Secure dans le cadre d'un paiement transmis par internet.

1.7. Présenter sur votre site internet les informations suivantes :
- la description détaillée des biens et / ou des services que vous proposez à la vente,
- le pays de localisation de votre activité,
- la devise de paiement,
- des conditions générales d'utilisation informant les Titulaires de Cartes notamment :
    - du dispositif prévu pour la livraison des biens et / ou des services et les restrictions d'exportations,
    - du dispositif prévu pour le retour des biens et / ou des services et le remboursement aux Titulaires de Cartes associé,
    - d'un contact pouvant répondre aux questions des Titulaires de Cartes et ses coordonnées par mail ou par téléphone,
    - dans le cas où vous proposez un mode de facturation par des paiements récurrents par Cartes, le site doit expliquer comment le Titulaire de Carte peut faire cesser la vente des biens et / ou des services et la facturation associée.

2. Les mesures de sécurité

2.1. Lors du paiement, vous vous engagez à :
2.1.1 Appliquer la procédure décrite dans les Conditions Particulières,
2.1.2 Obtenir un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.
2.1.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la période de validité (fin et éventuellement début),
- la catégorie et la marque de la Carte utilisée qui doivent être indiquées dans les Conditions Particulières ou dans les Conditions Générales.

2.1.4. Obtenir une autorisation d'un montant identique à l'opération.

2.2. Suivre et respecter la procédure d'authentification demandée par l'Emetteur.

Après une opération de paiement, vous devez :
2.3. Nous transmettre dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations et vous assurer qu'ils ont bien été portés au crédit de votre compte dans les délais et selon les modalités prévus aux Conditions Particulières. Vous ne devez transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à votre profit. Toute opération ayant fait l'objet d'une autorisation doit nous être obligatoirement remise.

2.4. Envoyer au Titulaire de Carte, lorsqu'il le demande, un ticket précisant, entre autres, le mode de paiement par Carte utilisée.

2.5. Vous devez également :
- Demander obligatoirement une autorisation en cas d'acceptation d'un ordre de paiement transmis par Internet,
- Contrôler (ou faire contrôler) le cryptogramme visuel donné par le Titulaire de Carte.
- Suivre et respecter la procédure d'authentification demandée par le teneur du compte du Titulaire de Carte.

ANNEXE : Paiement pour la location de biens et services

1. Suite à la conclusion de la convention de location, vous vous engagez à :

1.1. Recueillir l'acceptation du Titulaire de Carte d'être débité du montant des frais réels de la location dont le montant estimé lui est précisé. Vous associez un numéro de dossier à l'opération de paiement de la location ainsi initialisée.

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

- la présence de la Marque sur la Carte ou de la Marque des cartes acceptées conformément à l'article 1 des Conditions Générales,
- le cas échéant l'hologramme sauf pour les Cartes portant la Marque V Pay,
- la présence de la puce sur les cartes CB,
- la Marque et catégorie de Carte définies à l'article 1 des Conditions Générales,
- le cas échéant, la période de validité (fin et éventuellement début).

1.2 Utiliser l'Equipement Electronique muni de l'extension de service Paiement de proximité pour la location de biens et services conforme aux spécifications des Schémas de cartes en vigueur, respecter les indications affichées à l'écran et suivre les procédures dont les modalités techniques vous ont été indiquées.

L'Equipement Electronique doit notamment :

- après la lecture de la puce de la Carte lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  - vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - la date de fin de validité de 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 date de fin de validité de la Carte.

1.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition que nous avons diffusée, pour le Point d'Acceptation concerné et selon les Conditions Particulières convenues avec nous.1.5
Lorsque la puce le demande à l'Équipement Électronique, faire composer par le Titulaire de 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 émis par le Terminal de Paiement Électronique (ci-après «Ticket TPE»).
Lorsque le code confidentiel n'est pas vérifié, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

1.4 Obtenir systématiquement une autorisation d'un montant identique à celui connu et accepté par le Titulaire de Carte :

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.

1.5 Faire signer le Ticket TPE dans tous les cas où l'Équipement Électronique le demande.

1.6 Lorsque la signature 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 Carte.

1.7 Remettre au Titulaire de Carte l'exemplaire du Ticket TPE qui lui est destiné sur lequel doit figurer notamment :

- le montant des frais estimés de la prestation de location,
- le numéro de dossier,
- la mention de : «ticket provisoire» ou «pré-autorisation».

2 Lors de l'exécution de l'opération de paiement, vous vous engagez à :

2.1 Clôturer l'opération de paiement en recherchant via le numéro de dossier, l'opération de paiement initialisée lors de la mise à disposition du bien et la finaliser pour le montant final des frais réels connu et accepté par le Titulaire de Carte qui ne doit pas excéder la valeur du montant autorisé par ce dernier.

2.2 Archiver et conserver, à titre de justificatif, pendant quinze (15) mois après la date de l'opération :

- un exemplaire du Ticket TPE comportant, lorsqu'elle est requise, la signature du Titulaire de Carte,
- l'enregistrement magnétique représentatif de l'opération ou le journal de fond lui-même.

2.3 Communiquer, à notre demande et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

2.4 Nous transmettre dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations, et vous assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation doit obligatoirement nous être remise.

2.5 Vous vous engagez à ne stocker, sous quelque forme que ce soit, aucune des données cartes ci-après :
- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- le code confidentiel

ANNEXE : Paiement par automate en libre service

Vous devez afficher visiblement le montant maximum de mille cinq cents (1500) euros au-delà duquel aucune opération sur Automate ne peut être réalisée.

1. Mesures de sécurité directement à votre charge

1.1 L'Automate doit être clairement identifié par le numéro d'identification spécifique que nous vous avons fourni, vous permettant l'accès aux Schémas CB, Visa ou MasterCard.

1.2 Vous devez suivre les procédures dont les modalités techniques vous ont été indiquées et nous informer immédiatement en cas de fonctionnement anormal de l'Automate, et pour toutes autres anomalies (absence de reçu ou de mise à jour de la liste noire, impossibilité de réparer rapidement, etc).

1.3 Vous devez procéder à une inspection visuelle externe approfondie des Automates afin de détecter l'éventuelle présence de matériels de capture de données placés à l'extérieur de ceux-ci. En cas de présence anormale d'un matériel, vous devez immédiatement nous le signaler.

1.4 Lors d'un paiement par Automate, vous vous engagez à utiliser l'Automate, respecter ou faire respecter les indications techniques affichées sur son écran et suivre les procédures dont les modalités techniques vous ont été indiquées.

1.5 Après un paiement par Automate, vous vous engagez à :

1.5.1 Nous transmettre, dans les délais et selon les modalités convenues avec nous, les enregistrements électroniques des opérations. Vous devez également vous assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités convenus avec nous. Toute opération ayant fait l'objet d'une autorisation doit nous être obligatoirement remise.

1.5.2 Archiver et conserver, à titre de justificatif, pendant quinze (15) mois après la date de l'opération, l'enregistrement magnétique représentatif de chaque opération comprenant l'image du ticket fourni par l'Automate et notamment les numéros de certificat et s'il y a lieu d'autorisation ainsi que les éléments servant à leur calcul.

1.5.3 Communiquer, à notre demande et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

2. Mesures de sécurité à votre charge et assurées directement par l'Automate

2.1 L'Automate doit notamment, après lecture de la puce de la Carte, assurer automatiquement les opérations suivantes :

2.1.1. Interdire une opération de plus de mille cinq cents (1500) euros.

2.1.2. Afficher le montant réel de l'opération dès que l'Automate peut le définir ou l'estimer et, au plus tard, à la délivrance complète du bien ou du service.

2.1.3. Traiter la puce et, en cas d'impossibilité de traitement de la puce ou en cas d'absence de puce, l'Automate doit traiter l'opération selon les règles que nous avons édictées, notamment abandonner l'opération :
- pour une Carte MasterCard, lorsque le montant de l'opération est supérieur à cinquante (50) euros et que l'Automate ne permet pas de mettre en œuvre une identification du Titulaire de la Carte par l'Émetteur conforme aux règles de l'Émetteur,
- pour une Carte Visa, lorsque le montant de l'opération est supérieur à l'équivalent en euros de quarante (40) dollars et que l'Automate ne permet pas de mettre en œuvre une identification du Titulaire de la Carte par l'Emetteur conforme aux règles de ce dernier.

2.1.4. Pour les Cartes CB, Visa et MasterCard, lorsque la Carte le demande, mettre en œuvre le contrôle du code confidentiel de la Carte. La preuve de ce contrôle est apportée par le certificat qui doit être enregistré par l'Automate et imprimé sur le Ticket.

2.2.1. Obtenir une autorisation au moment de l'opération sous-jacente et pour un montant défini dans les Conditions Particulières :
- 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 pour le même point de vente et pour le même type de paiement (Automate), dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec nous, et ceci, quelle que soit la méthode d'acquisition des informations,
- lorsque l'Automate ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation de l'Automate fixé dans les Conditions Particulières convenues avec nous.

A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.
Une opération interdite, refusée ou interrompue par le serveur d'autorisation doit être abandonnée par l'Automate.

2.2.2 Proposer au client l'émission d'un Ticket. Si l'Automate ne peut pas délivrer temporairement de Ticket, il doit en informer le client avant l'opération et lui proposer d'arrêter l'opération.

2.2.3 Stocker les enregistrements des opérations, identifiées comme opérations par l'Automate, effectuées au Point d'Acceptation en vue de nous les remettre.

Annexe : Spécificités du schéma de cartes DISCOVER

ARTICLE 1 : ACCEPTATION DES CARTES

Vous vous engagez à ce que la fonctionnalité d'acceptation des Cartes Discover et Diners Club International soit active sur les Équipements Électroniques[2] et/ou les Systèmes d'Acceptation utilisés.
Vous vous engagez également à former tous les collaborateurs concernés par l'acceptation de Carte Discover ou Diners Club International dans vos Points d'Acceptation.
Vous devez respecter le choix du Titulaire de Carte en ce qui concerne l'utilisation du Schéma de cartes Discover pour effectuer une transaction par Carte. A ce titre, vous devez accepter les Cartes du Schéma Discover avec une parité identique aux autres Schémas de cartes.

ARTICLE 2 : VALIDITE DE L'AUTORISATION

Dans le Schéma de cartes Discover, l'autorisation afférente à une transaction par Carte doit être obtenue à la date de facturation et pour le montant total de la facturation, sauf dans les cas particuliers suivants :
2.1 Hôtel - Une autorisation est considérée comme valide si elle est obtenue: a) à tout moment entre la date d'arrivée et la date de départ, jusqu'à un maximum de trente (30) jours calendaires; et b) le montant du paiement est inférieur ou égal à 115 % du ou des montants autorisés. Les autorisations peuvent être cumulées et considérées comme valables pour la durée du séjour du Titulaire de Carte.
2.2 Location de voitures - Une autorisation est considérée comme valide si elle est obtenue: a) à tout moment entre la location de la voiture et les dates de retour, jusqu'à un maximum de trente (30) jours civils; et b) le montant du paiement est inférieur ou égal à 115 % du ou des montants autorisés.
2.3 Restaurant - Une autorisation est considérée comme valide si elle est obtenue: a) à la date de mise en charge; et b) le montant du paiement est inférieur ou égal à 120 % du ou des montants autorisés.
2.4 Commande par mail ou par téléphone (en anglais : mail order telephone order -MOTO) - Une autorisation est considérée comme valide si elle est obtenue: a) dans les sept (7) jours calendaires précédant la date de facturation; (b) à la date de la commande; et c) le montant du paiement est inférieur ou égal à 115 % du montant autorisé.
2.5 Taxi - Une autorisation est considérée comme valide si elle est obtenue: (a) à la date de facturation; et b) le montant du paiement est inférieur ou égal à 120 % du ou des montants autorisés.
2.7 Distributeur automatique de carburant - Une autorisation ne pourra pas être considérée comme valide pour un montant supérieur à 10 000 euros.

ARTICLE 3 : TRANSACTION SANS PIN ET SANS SIGNATURE

Les transactions par carte à puce du Schéma de cartes Discover, y compris les transactions avec un dispositif de paiement avec contact ou à puce sans contact, pour un montant inférieur ou égal à cinquante (50) dollars, (y compris les taxes, les frais supplémentaires et / ou les pourboires) n'exigent pas la signature du Titulaire de Carte et / ou la saisie du code PIN avec la demande d'autorisation.

Annexe : Spécificités du schéma de cartes JCB

ARTICLE 1 : ACCEPTATION DES CARTES

Vous vous engagez à ce que la fonctionnalité d'acceptation des Cartes JCB soit active sur les Systèmes d'Acceptation utilisés.

Vous vous engagez également à former tous les collaborateurs concernés par l'acceptation de Carte JCB dans vos Points d'Acceptation.

Vous devez respecter le choix du Titulaire de Carte en ce qui concerne l'utilisation du Schéma de cartes JCB pour effectuer une transaction par Cartes. A ce titre, vous devez accepter les Cartes du Schéma JCB avec une parité identique aux autres Schémas de cartes.

ARTICLE 2 : IDENTIFICATION DU TITULAIRE

Quand le Terminal de Paiement Électronique demande une authentification par la signature du Titulaire de Carte, vous devez refuser de réaliser un paiement si la signature apparaissant sur la facture n'est pas identique à celle figurant au verso de la Carte JCB.

ARTICLE 3 : TRANSACTION CRÉDIT

Vous pouvez réaliser une transaction de remboursement (relative à une transaction déjà traitée) quand :
vous souhaitez annuler la transaction et le Titulaire de Carte vous a restitué les produits achetés.
Cette exigence ne vous est pas applicable si votre activité consiste à fournir un service de remboursement de la TVA.

En cas de remboursement partiel ou total d'une transaction réglée par carte JCB, ce remboursement doit exclusivement être effectué à la Carte JCB utilisée pour l'opération initiale et pas au Titulaire de cette Carte ou d'une autre carte.

ARTICLE 4 : VALIDITE DE L'AUTORISATION

Dans le Schéma de cartes JCB, l'autorisation afférente à une transaction par Cartes doit être obtenue à la date de facturation et pour le montant total de la facturation, sauf dans les cas particuliers suivants :

a. Hôtel
   - Afin de garantir à l'avance la limite de paiement du Titulaire de Carte, l'hôtelier doit estimer le montant de la transaction en fonction de :
     - la durée prévue du séjour du titulaire,
     - le prix de la chambre,
     - les taxes applicables,
     - tout autre frais liés au séjour réservé par le Titulaire de Carte.
   - Après avoir terminé les estimations, vous devez traiter l'autorisation correspondant au montant estimé de la transaction de la même manière que la procédure d'autorisation habituelle.
   - A la date de départ du Titulaire de Carte, si le montant réel de la transaction dépasse de 15 % le montant estimé déjà autorisé, vous devez demander une autorisation supplémentaire. Le montant de cette seconde autorisation doit être égal à la différence entre le montant réel et le montant déjà autorisé.

b. Location de voitures
   - Afin de garantir à l'avance la limite de paiement du Titulaire de Carte, le loueur doit estimer le montant de la transaction en fonction de :
     - Le coût de la location,
     - la durée prévue de la location,
     - le kilométrage,
     - les taxes applicables,
     - tout autre frais liés à la location réservée par le Titulaire de Carte.
   - Après avoir terminé les estimations, vous devez traiter l'autorisation correspondante au montant estimé de la transaction de la même manière que la procédure d'autorisation habituelle.
   - A la date de retour de la location de la voiture, si le montant réel de la transaction dépasse de 15 % le montant déjà autorisé, vous devez demander une autorisation supplémentaire. Le montant de cette seconde autorisation doit être égal à la différence entre le montant réel et le montant déjà autorisé.

ARTICLE 5 : PROGRAMMES DE SERVICES HÔTELIERS, DE CROISIÈRES ET DE LOCATION DE VOITURES

Les programmes Guaranteed Reservation, Express Check-Out et Advance Deposit ne sont pas disponibles et vous ne devez pas délivrer les services associés aux Titulaires de Cartes.

ANNEXE : Référentiel sécuritaire accepteur

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

Exigence 1 (E1)
Gérer la sécurité du Système d'Acceptation au sein de l'entreprise

Pour assurer la sécurité des données des opérations de paiement et notamment, des données des Titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.
En particulier, un responsable de la sécurité du Système 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 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)
Gérer l'activité 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 d'Acceptation.

Exigence 3 (E3)
Gérer les accès 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 du Titulaire de 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.
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 Système d'Acceptation

Les règles de sécurité relatives aux accès et sorties depuis et vers le Système 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)
Contrôler l'accès au Système 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 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)
Gérer les accès autorisés au Système 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 d'Acceptation 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 accès au Système 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)
Contrôler 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 d'Acceptation.
La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

Exigence 9 (E9)
Appliquer les correctifs de sécurité (patches de sécurité) 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.
Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

Exigence 10 (E10)
Gérer 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'intégrité des logiciels applicatifs relatifs au Système 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 traçabilité des opérations 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'intégrité des informations relatives au Système d'Acceptation

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurés 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 d'Acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14)
Protéger la confidentialité des données bancaires

Les données du Titulaire de 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 du Titulaire de 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 d'Acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15)
Protéger la confidentialité des identifiants - authentifiants des utilisateurs et des 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.

ANNEXE : PCI DSS et risques acquéreurs

1. Règles à respecter

Vous devez respecter les dispositions du « Référentiel Sécuritaire Accepteur » figurant en Annexe et les exigences de sécurité PCI DSS (vous pouvez vous référer également au site officiel : http://fr.pcisecuritystandards.org/minisite/en/).
Vous devez vous conformer aux obligations, règles et directives applicables émises par les Schémas de cartes.
En conséquence, vous vous interdisez notamment de stocker ou communiquer, sous quelque forme que ce soit, les données d'authentification du Titulaire de Carte (numéro de carte, cryptogramme visuel, date d'échéance, code confidentiel, la piste magnétique dans son intégralité, ainsi que toute autre donnée qui serait considérée comme sensible et sujette à l'application des mesures du « Référentiel Sécuritaire Accepteur »).
Vous devez justifier, auprès de nous, la bonne réalisation de vos obligations et en fournir les documents associés sur notre simple demande.

2. Recours à des tiers

Dans vos relations contractuelles avec les tiers, tels que les prestataires de services techniques ou les sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des cartes, vous devez vous assurer que ces derniers s'engagent à respecter le référentiel de sécurité PCI DSS et les mesures du « Référentiel Sécuritaire Accepteur ».
Vous devez nous tenir informé du nom et des coordonnées des sous-traitants auxquels vous faites appel dans le cadre de la mise en œuvre de votre solution de paiement.

3. Clause d'audit

Nous pourrons procéder dans vos locaux ou ceux de vos prestataires, tout comme les Schémas de cartes, à la vérification par un tiers indépendant du respect tant des clauses du présent contrat que des exigences figurant en annexe ainsi que des exigences de sécurité PCI DSS. Cette vérification, appelée «procédure d'audit», peut intervenir à tout moment dès la conclusion du présent contrat.
Vous autorisez que ces rapports nous soient communiqués, ainsi qu'aux Schémas de cartes.
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 vos engagements, chacun de ces Schémas pourra procéder à une suspension de l'adhésion, voire à une radiation du Schéma telle que prévue dans les Conditions Générales.
Vous êtes tenus de nous informer immédiatement et de suivre intégralement nos instructions si vous avez connaissance ou si vous soupçonnez que des données de transactions sont (ou ont été) accessibles à des tiers ou sont (ou peuvent être) utilisées abusivement par des tiers. Vous nous fournissez dans ce cas sans délai, de votre propre initiative ou à notre demande, toutes les informations (telles que les données de transaction) en vue du traitement du dossier.
Vous êtes tenus d'apporter tout votre concours à l'enquête et de suivre intégralement toutes les instructions si nous soupçonnons ou constatons que des données de transaction erronées, falsifiées ou volées ont été utilisées dans votre commerce, ou l'utilisation de données compromises ou d'autres actes et/ou transactions frauduleux. Vous nous autorisez à partager les résultats de l'enquête avec des tiers tels que les Schémas de cartes.
Vous êtes tenu de ne commettre aucun acte pouvant nuire à une enquête éventuelle ou influencer négativement les résultats d'une telle enquête. Par « actes », on entend notamment l'extinction de systèmes ou la suppression de fichiers.
Nous pourrons aussi bloquer les fonds « suspects ».
Vous acceptez d'être facturé des éventuelles pénalités qui pourraient vous être appliquées par les Schémas de cartes en cas de compromission de données du fait de manquements ou d'actes et de faits relevant de votre responsabilité notamment après un audit.

4. Inventaire des Terminaux de Paiement Électronique

Vous devez établir un inventaire des Terminaux de Paiement Électronique et de leurs caractéristiques. L'inventaire doit au minimum lister la marque, le modèle, le numéro de série, l'emplacement physique de chaque TPE. La mise à jour de ces informations est requise dès lors qu'un changement intervient.
Vous devez vérifier périodiquement (une revue mensuelle est préconisée) l'exactitude de ces informations.
En cas de présence anormale d'un TPE vous devez nous le signaler immédiatement.

5. Entrée en relation et suivi de la relation

Sur notre demande, vous devrez nous informer par le biais du formulaire « Fiche d'Identification Accepteur » :
- Des informations relatives aux types d'activités réalisées, aux coordonnées des sous-traitants auxquels il fait appel dans le cadre de la mise en œuvre de sa solution de paiement, aux applications de paiement utilisées,...
- De tout changement intervenant en cours d'exécution du présent contrat et pouvant impacter vos déclarations initiales.

6. Activités illégales ou interdites

Vous déclarez ne pas exercer une activité de type :
- pornographie infantile,
- vente illégale de drogues comprenant notamment les produits dérivés du cannabis (fleurs et graines de chanvre, produits ou e-liquides contenant du cannabidiol – CBD - à un taux supérieur à celui autorisé par la loi),
- sites Internet de jeux d'argent en fonction de la juridiction en cours dans le pays émetteur,
- vente de marchandises contrefaites ou en violation des droits de propriétés,
- pornographie «agressive» : bestialité, viol, mutilation, …
- agrégateur qui traite les transactions d'un autre commerçant et nous les communique sans l'indiquer dans l'opération de paiement,
- cyberlocker proposant des services d'hébergement ou de téléchargement de données,
- commerce en marketing direct de services pour adultes (sexshop, striptease, pornographie…) par téléphone,

- vente de tabac à distance ou par e-commerce,
- sites pour adultes (films, « streaming ») en Vente à distance et Vente à distance sécurisée,
- vente de crypto-monnaies (bitcoin et crypto actifs).

ou plus généralement toute autre activité punie par la loi.

7. Risques de fraude

En cas d'alerte de fraude, vous vous engagez à mettre en œuvre les solutions que nous vous proposerons, telle que l'activation du protocole 3D Secure, afin de réduire la fraude ainsi que le taux de fraude au sein de votre Point d'Acceptation.
Lorsqu'une activité frauduleuse est constatée, nous pourrons vous contacter, venir dans vos locaux ou vous communiquer des instructions à suivre. En cas de refus de votre part, vous supporterez d'emblée l'ensemble des frais liés à la fraude qui n'aura pu être évitée.

Les pénalités appliquées par les Schémas de cartes vous seront facturées et seront débitées directement sur votre compte.

8. Activités à hauts risques

Vous devez nous demander notre autorisation et obtenir notre accord préalable et écrit, avant d'exercer des activités notamment telles que définies à hauts risques par les Schémas de cartes dans les documents « Mastercard Security Rules » et « Visa Global Brand Protection Programme ».
Les domaines d'activités précisés ci-dessous sont donnés à titre indicatif et peuvent évoluer dans le temps :

- grossiste en produits pharmaceutiques en Vente à distance et Vente à distance sécurisée,
- détaillant de produits pharmaceutiques en Vente à distance et Vente à distance sécurisée ,
- agence de voyages en marketing direct par courriers, mails ou par téléphone,
- commerce en marketing direct hors services pour adultes et agences de voyages,
- vente de cigarettes électroniques en Vente à distance et Vente à distance sécurisée,
- sites pour adultes : sextoys, lingerie… en Vente à distance et Vente à distance sécurisée ,
- paris, vente de jetons de casino et jeux de hasard en Vente à distance et Vente à distance sécurisée ,
- vente d'armes,
- vente de titres à risque élevé en Vente à distance sécurisée ,
- vente de produits dérivés du cannabis (produits ou e-liquides contenant du cannabidiol – CBD - à un taux autorisé par la loi).

En cas de réponse favorable à votre demande, vous devrez nous fournir les documents et informations mentionnés dans l'Annexe « Activités à Haut Risques » que nous vous communiquerons et nous autoriser à débiter annuellement votre compte des frais correspondants à l'enregistrement de votre activité à hauts risques auprès des Schémas de cartes. Nous pourrons vous communiquer le montant de ces frais sur simple demande.

A noter qu'en cas de volume d'impayés trop important détecté par les programmes « Visa Chargeback Monitoring Program » et Mastercard « Excessive Chargeback Program », vous serez alors considéré comme exerçant une activité à Haut Risques et serez soumis à l'ensemble de ces obligations, notamment à un enregistrement de votre activité à Haut Risques auprès des Schémas de cartes ainsi qu'au paiement des frais correspondants.

9. Pénalités et résiliation

En cas de manquement à l'une de ces obligations, vous vous exposez à des pénalités en provenance des Schémas de cartes ainsi qu'à la résiliation du présent contrat.

En cas de survenance d'un incident de sécurité majeur, notamment en cas de violation des données, vous devrez coopérer avec nous et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de votre part pourra entraîner la résiliation du présent contrat.

La résiliation du contrat vous sera alors notifiée par l'envoi d'une lettre recommandée, avec demande d'avis de réception. Son effet est immédiat.

ANNEXE : Notice d'information et de sensibilisation

Introduction aux programmes de gestion de risques

L'augmentation des paiements par carte bancaire a vu augmenter de manière significative le vol de données électroniques et d'informations de paiement.
Pour maîtriser les taux de fraude et garantir la confiance des clients dans le système de paiement, les principaux Schémas de Cartes bancaires ont développé un ensemble de programmes de gestion de risques auxquels les banques Acquéreurs[1], les commerçants Accepteurs[2] sont parties prenantes. Ce guide a pour objectif d'expliquer aux Accepteurs la manière dont ils doivent appliquer les bonnes pratiques réglementaires.

Programmes de gestion de risques

1.1 Quels sont les objectifs du programme de bonnes pratiques PCI DSS ?

PCI DSS - Payment Card Industry Data Security Standard, est un ensemble de bonnes pratiques de sécurité qui visent à réduire les risques de vol ou d'usurpation de données de cartes de paiement. Le respect de ces bonnes pratiques réduit le risque d'être victime d'une compromission de données, protège votre activité, votre réputation et augmente la confiance que vos clients placent en vous.

1.2 Qui devez-vous informer en cas de changement de mode de vente, ou de nature des biens, produits et services vendus ?

Le contrat conclu avec votre Acquéreur identifie votre activité principale selon la classification « Code NAF » normalisée de l'INSEE, et selon votre type de mode de vente: Paiement de proximité ou Vente à distance sécurisée.
Toute évolution de votre mode de vente devra faire l'objet d'une déclaration préalable à votre Acquéreur. Par évolution du mode de vente, on entend :

- Modification du canal de vente (évolution de vente via TPE ou Automate vers Vente à distance sécurisée).
- Modification des biens, produits et services vendus.

1.3 Existe-il des catégories de produits, biens et services dont la vente est interdite ou limitée ?

Les activités suivantes sont interdites par les Schémas de Cartes ou par le Crédit Mutuel Arkéa et ne pourront pas faire l'objet d'un contrat d'acceptation de la part du Groupe Crédit Mutuel Arkéa :

- pornographie infantile,
- vente illégale de drogues comprenant notamment les produits dérivés du cannabis (fleurs et graines de chanvre, produits ou e-liquides contenant du cannabidiol – CBD - à un taux supérieur à celui autorisé par la loi),
- sites Internet de jeux d'argent en fonction de la juridiction en cours dans le pays émetteur,
- vente de marchandises contrefaites ou en violation des droits de propriétés,
- pornographie «agressive» : bestialité, viol, mutilation …
- agrégateur qui traite les transactions d'un autre commerçant et nous les communique sans l'indiquer dans l'opération de paiement,
- cyberlocker proposant des services d'hébergement ou de téléchargement de données,
- commerce en marketing direct de services pour adultes (sexshop, striptease, pornographie…) par téléphone,
- vente de tabac à distance ou par e-commerce,
- sites pour adultes (films, « streaming ») en Vente à distance et Vente à distance sécurisée,
- vente de crypto-monnaies (bitcoin et crypto actifs).

Toute autre activité punie par la loi est également interdite d'opération.

Par ailleurs, les activités suivantes sont jugées « à risques » car susceptibles de générer des montants d'impayés plus élevés :

- grossiste en produits pharmaceutiques en Vente à distance et Vente à distance sécurisée ,
- détaillant de produits pharmaceutiques en Vente à distance et Vente à distance sécurisée ,
- agence de voyages en marketing direct par courriers, mails ou par téléphone,
- commerce en marketing direct hors services pour adultes et agences de voyages,
- vente de cigarettes électroniques en Vente à distance et Vente à distance sécurisée ,
- sites pour adultes : sextoys, lingerie… en Vvente à distance et Vente à distance sécurisée ,
- paris, vente de jetons de casino et jeux de hasard en Vente à distance et Vente à distance sécurisée,
- vente d'armes,
- vente de titres à risque élevé en Vente à distance sécurisée ,
- vente de produits dérivés du cannabis (produits ou e-liquides contenant du cannabidiol – CBD - à un taux autorisé par la loi).

Sans être interdites, ces activités devront faire l'objet d'une déclaration préalable à l'Acquéreur et d'un suivi particulier par celui-ci.

Ces listes sont susceptibles d'évoluer selon la législation en vigueur.

[1] Les acquéreurs désignent les établissements bancaires
[2] Les accepteurs désignent les commerçants

1.4 Quels sont les différents niveaux d'exigences de la norme PCI-DSS ?

Les exigences définies par la norme PCI-DSS varient proportionnellement au nombre de transactions à traiter selon une classification comportant 4 niveaux (*voir le tableau ci-après*).

Niveau de Commerçant Accepteur PCI DSS	Volumes de transactions	Mesures requises pour être conforme
Niveau 1	Plus de 6 millions de transactions par an (tous canaux confondus).	- Audit sur-site chaque année par un auditeur QSA. - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 2	Entre 1 et 6 millions de transactions par an (tous canaux confondus).	- Audit sur-site chaque année par un auditeur QSA ou ISA. - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 3	Entre 20.000 et 1 million de transactions e-commerce par an.	- Questionnaire d'auto-évaluation annuel (SAQ). - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 4	Tous les autres commerçants Accepteurs.	- Questionnaire d'auto-évaluation annuel recommandé (SAQ).

1.5 Quelles sont les risques en cas compromission des données ?

Si vous détectez ou soupçonnez une intrusion non autorisée dans un réseau ou tout type de perte de données de titulaires de cartes, il est essentiel de signaler les détails de l'incident à votre Acquéreur dans les plus brefs délais.

En cas de non-respect de la réglementation en vigueur ou de compromission de données importantes, des mesures pouvant donner lieu à des pénalités financières ou à la fermeture du contrat pourraient être appliquées.

Paiement en Vente à distance sécurisée

L'ensemble des informations précisées ci-après ne concernent que les Accepteurs ayant souscrit un contrat de Vente à distance sécurisée.

1.6 Quelles sont vos obligations en tant qu'Accepteurs ?

Dès lors que vous manipulez, transmettez ou stockez des données de cartes bancaires (et ce, quel que soit votre canal de paiement : point de vente physique, e-commerce, téléphone …) ou qu'un Fournisseur de Services s'en charge pour vous, vous êtes soumis à une mise en conformité à PCI DSS.

Les données de cartes bancaires concernées par PCI DSS sont :

- le numéro de la carte,
- la date d'expiration et le nom du porteur,
- le cryptogramme visuel.

1.7 Qu'est-ce qu'un questionnaire SAQ ?

Le questionnaire d'auto-évaluation (Self Assessment Questionnaire - SAQ) est un outil de validation de la conformité PCI DSS utilisé et rempli par les Accepteurs eux-mêmes.

Il existe plusieurs types de SAQ qui dépendent de la nature de l'environnement de paiement (le SAQ applicable à une installation comportant un seul TPE, sera différent d'un SAQ applicable à un E-Commerçant).

Les Questionnaires SAQ sont disponibles en ligne à l'adresse suivante : https://www.pcisecuritystandards.org/security_standards/documents.php (section « SAQs »).

Le tableau ci-après présente les questionnaires SAQ disponibles et leurs modalités d'utilisations :

Version du SAQ	Description	Proximité	Vente à distance sécurisée	Vente à distance (téléphone, courrier…)
A	Paiement carte non présente (e-commerce ou commerce par courrier ou téléphone), sous-traitance de toutes les fonctions de données des titulaires de carte auprès d'un fournisseur de services conforme à PCI DSS. Aucune manipulation/transmission/ stockage de données de cartes sur l'environnement du commerçant Accepteur. *Applicable seulement aux activités E-commerce.Exemple : Commerçant Accepteur exerçant une activité de E-commerce avec sous-traitance auprès d'un fournisseur certifié des fonctions de paiement, redirection vers le fournisseur par méthode Iframe ou HTTP Redirect.*		X	X

A-EP	Paiement E-commerce, sous-traitance de toutes les fonctions de données des titulaires de carte auprès d'un fournisseur de services conforme à PCI DSS, le site web ne reçoit pas directement des données de cartes mais il peut impacter la sécurité de la transaction de paiement. Aucune manipulation / transmission / stockage de données de cartes sur l'environnement du commerçant Accepteur. *Applicable seulement aux activités E-commerce.Exemple : Commerçant Accepteur exerçant une activité de E-commerce avec sous-traitance auprès d'un fournisseur certifié des fonctions de paiement, redirection vers le Fournisseur par méthode Direct Post ou Javascript.*		X	
D	Tous les autres commerçants Accepteurs non pris en compte dans les descriptions des SAQ précédentes.	X	X	X

1.8 Qu'est-ce qu'un scan de vulnérabilités?

Un scan de vulnérabilités est une revue de tous vos sites et systèmes accessibles depuis Internet, qui permet de vérifier que ceux-ci sont protégés contre les menaces externes telles que : accès illégitimes, hacking, virus, etc.
Le scan de vulnérabilités doit être réalisé chaque trimestre. Il est non intrusif et cible l'ensemble de vos équipements réseaux, systèmes et applicatifs. Il est mené par une entreprise certifiée en tant qu'Approved Scanning Vendor (ASV) et vous assurera que votre environnement offre un niveau de protection adéquat.
La liste des vendeurs ASV est accessible en ligne à l'adresse suivante :
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

1.9 Qu'est-ce qu'un audit sur-site mené par un QSA ?

Si vous êtes éligible à un audit sur-site, vous devrez recourir aux services d'une société accréditée en tant que Qualified Security Assessor (QSA) qui validera chaque année la conformité PCI DSS de votre environnement.
La liste des sociétés accréditées QSA est accessible en ligne à l'adresse suivante :
https://www.pcisecuritystandards. org/approved_companies_providers/qualified_security_assessors.php

1.10 Par où commencer ?

Le standard PCI DSS est accessible en ligne gratuitement sur le site suivant : http://fr.pcisecuritystandards.org/minisite/en/
Il est recommandé de démarrer une analyse d'écart PCI DSS à l'aide du questionnaire d'auto-évaluation (SAQ) qui correspond à votre environnement de paiement et de vous rapprocher d'un vendeur ASV pour démarrer les scans de vulnérabilité trimestriels. Vous obtiendrez alors de la visibilité sur votre niveau de conformité PCI DSS.
S'il s'avère que certaines exigences PCI DSS ne sont pas opérationnelles, vous devrez développer un plan de mise en conformité couvrant chaque élément non conforme. Ce plan comportera une indication du temps estimé pour chaque action. Les Accepteurs de niveaux 1, 2 et 3 devront transmettre chaque trimestre ce plan à leur Acquéreur en utilisant l'outil « Approche par Priorités » disponible sur le site ci-dessous, ce qui démontrera ainsi les progrès réalisés et réduira les risques de pénalités pour « non-conformité ».
https://www.pcisecuritystandards.org/documents/Prioritized_Approach_for_PCI_DSS_v20.xls

Lorsque vous aurez finalisé la mise en conformité, vous devrez valider votre conformité au standard PCI DSS par le biais de la méthode qui correspond à votre niveau de commerçant Accepteur (chaque année : audit annuel sur-site ou auto-évaluation et scan ASV trimestriel), transmettre ces éléments à votre Acquéreur et maintenir votre niveau de conformité dans le temps.

1.11 Quelles sont les actions que vous pouvez mener en urgence pour réduire les risques sur votre environnement et simplifier votre mise en conformité PCI ?

Le moyen le plus simple pour augmenter la sécurité des données de paiement de vos clients est de ne pas stocker ces données.
Si cela s'avérait indispensable, alors :

- Stockez les données de paiement sur des composants informatiques sécurisés et conformes aux exigences du standard PCI DSS.
- Ne conservez pas sous format électronique ou papier les données de paiement « très sensibles » comme le Cryptogramme Visuel.
- Recourez aux services de fournisseurs de services de paiement conformes au standard PCI DSS et utilisez des applications de paiement certifiées PA-DSS.

Paiement de proximité et par Automate

L'ensemble des informations précisées ci-après ne concernent que les Accepteurs équipés de TPE ou d'Automates.

1.12 Vous êtes un commerçant Accepteur de proximité. Etes-vous soumis à la conformité PCI DSS ?

Dès lors que vous manipulez, transmettez, ou êtes au contact de données de cartes bancaires, la conformité de votre environnement au Standard PCI DSS est requise.
Cependant, les menaces auxquelles vous êtes confrontés en tant que point de vente physique étant différentes de celles d'un marchand E-Commerce, le mécanisme de vérification de votre conformité PCI DSS est allégé. Vous n'aurez pas l'obligation de faire valider votre conformité PCI DSS chaque année par un auditeur externe ni à remonter l'état de conformité PCI DSS à votre Acquéreur.

1.13 Quelles précautions devez-vous prendre pour assurer la sécurité de mes Paiements de proximité ?

Les menaces qui touchent les points de vente physique ciblent avant tout les terminaux de paiement (TPE). Pour vous protéger, il est vivement recommandé d'appliquer les bonnes pratiques suivantes :

- Utilisez des TPE conformes à « PCI PED » (demandez à votre loueur, à votre mainteneur ou à votre Acquéreur si vos terminaux sont conformes).

- Faites appel à des prestataires certifiés par votre Acquéreur. Rapprochez-vous de votre centre d'affaires pour en connaître la liste.
- Rangez en lieu sûr (dans un tiroir sous le comptoir, dans une salle fermée à clé) les reçus commerçants sur lesquels le numéro de carte, le nom du porteur, la date d'expiration sont inscrits. Ces reçus sont à conserver sur une durée d'un an.
- Appliquez des autocollants (par exemple le nom de votre société) sur vos TPE pour détecter toute substitution de terminal.
- Ne laissez pas votre TPE facilement accessible et sans surveillance, pour éviter qu'ils ne soient manipulés, modifiés et piratés.
- Maintenez à jour un inventaire des numéros de série, marque, modèle, localisation physique de chacun de vos TPE.
- Inspectez périodiquement vos TPE, leurs connexions, et vérifiez que leurs caractéristiques correspondent à votre inventaire.
- N'autorisez l'accès physique aux TPE qu'aux mainteneurs préalablement autorisés et clairement identifiés par leur carte professionnelle.

D'une manière générale, il est vivement recommandé que vous utilisiez le questionnaire SAQ correspondant à votre environnement de paiement, pour auto-évaluer et améliorer vos pratiques opérationnelles le cas échéant.

1.14 Qu'est-ce qu'un questionnaire SAQ ?

Le questionnaire d'auto-évaluation (SAQ, Self Assessment Questionnaire) est un outil de validation de la conformité PCI DSS utilisé par les Accepteurs qui n'ont pas l'obligation de mener un audit sur-site chaque année.

Il existe plusieurs types de SAQ qui dépendent de la nature de l'environnement de paiement. Les versions de SAQ qui correspondent à des activités de proximité sont les suivants :

Version de SAQ	Description
B	Accepteur utilisant des périphériques d'impression uniquement, ou des terminaux autonomes à ligne directe, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant de TPE RTC.*
B-IP	Accepteur utilisant uniquement des terminaux de paiement autonomes certifiés PTS, avec une connexion IP vers le processeur de paiement, sans stockage électronique de données de cartes. *Exemple : Commerçant Accepteur disposant de TPE certifiés PTS avec liaison IP vers le processeur de paiement.*
C-VT	Accepteur qui saisit manuellement une transaction unitaire à travers un clavier dans une solution basée sur un terminal virtuel Web hébergée chez un Fournisseur de Services certifié PCI DSS, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant d'une interface de saisie des transactions hébergée chez un Fournisseur certifié.*
C	Accepteur possédant des systèmes d'application de paiement connectés à Internet, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant d'une application de paiement reliée au processeur par Internet.*
D	Tous les autres Accepteurs non décrits dans les descriptions des SAQ ci-dessus.

Les Questionnaires SAQ sont disponibles en ligne à l'adresse suivante :
https://www.pcisecuritystandards.org/security_standards/documents.php (section « SAQs »).

Régimes spécifiques : hôtels, compagnies aériennes

1.15 Vous êtes un hôtelier. Comment devez-vous valider votre conformité PCI DSS ?

Les hôteliers évoluent dans un paysage de risques spécifiques, ils sont soumis à un régime particulier. Les critères qu'ils doivent respecter s'ils acceptent exclusivement les paiements de proximité pour valider leur conformité sont les suivants :

- L'hôtel doit être de niveau 4.
- L'hôtel doit confirmer qu'il ne fait pas de stockage électronique de données d'authentification sensibles (Cryptogramme Visuel, Code PIN, données de la piste) avant ou après l'autorisation.
- L'hôtel confirme que les transactions « no-show[3] » sont conduites conformément à la réglementation - Visa Europe Operating Regulations, à savoir produire un reçu comportant les informations suivantes :
    - Montant de la nuitée facturée et des taxes applicables.
    - Nom du porteur débité.
    - Numéro de la carte (de préférence n'afficher que les six premiers et les quatre derniers chiffres du numéro)
    - La date d'expiration de la carte
    - La mention « No-Show » sur la ligne de signature du reçu.
- L'hôtel fournit chaque année à son acquéreur une liste des fournisseurs de services qui stockent, traitent ou transmettent des données de cartes.

[3] Le No-show s'applique quand un client ayant réservé une chambre ne se présente pas à l'hôtel le jour d'arrivée prévu sans avoir au préalable annulé sa réservation auprès de l'hôtel. Dans ce cas, la première nuit de la réservation est facturée par l'hôtel par une facture « no-show ».

- L'hôtel confirme qu'il n'utilise pas de mots de passe par défaut sur ses systèmes (en particulier sur les systèmes de gestion type PMS[4]).

L'hôtelier doit confirmer chaque année le respect de ces points à son acquéreur.

Les hôteliers qui ne s'inscrivent pas dans ces critères devront mettre leur environnement en conformité à PCI DSS.

1.16 Vous êtes une compagnie aérienne. Comment devez-vous valider votre conformité PCI DSS ?

Les compagnies aériennes, au titre de leur activité d'émission de billets, sont soumises elles aussi à la mise en conformité PCI DSS de leurs environnements. Toutefois, de par la complexité générale de leur système d'information, un régime dérogatoire leur est proposé.
Ainsi, les compagnies aériennes processant plus de 50.000 transactions cartes par an doivent fournir à leur banque Acquéreur un plan de mise en conformité à PCI DSS adressant la conformité au plus tard au 31/12/2017. La compagnie aérienne doit communiquer chaque année l'évolution de son plan d'action à son Acquéreur.

Les compagnies aériennes n'atteignant pas ce volume de transactions n'ont pas d'obligations spécifiques, elles doivent néanmoins appliquer les pratiques « de bon sens » pour sécuriser leurs environnements.

Lexique

Terme	Définition
ASV	Approved Scanning Vendor. Société habilitée par le Conseil PCI à réaliser des scans de vulnérabilité externes. La liste des solutions ASV référencées est maintenue à jour : https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
Donnée d'authentification sensible	Au sens PCI DSS ce terme couvre individuellement ou non : - La piste magnétique complète. - Le code PIN. - Le Cryptogramme Visuel (CVV).
Données porteurs	Les Données Porteurs sont constituées de l'un ou l'ensemble des éléments suivants : - Le numéro de la carte. - Le nom du porteur. - La date de validité. - Le code de service.
Environnement de données de carte(s) bancaire(s) Environnement porteur(s)	Ceci correspond aux individus, aux processus et aux technologies qui stockent, traitent ou transmettent les données de titulaires de cartes ou des données sensibles d'authentification, et comprend également tous les composants connectés du système.
ISA	Internal Security Assessor. Le registre du personnel certifié ISA est maintenu à jour par le Conseil PCI : https://www.pcisecuritystandards.org/approved_companies_providers/verify_isa.php
PA-DSS	Payment Application - Data Security Standard : Variante du standard PCI DSS qui s'applique aux applications de paiement
Prestataire de Services	Entité commerciale qui n'est pas une marque de carte de paiement, directement impliquée dans le traitement, le stockage et la transmission des données de titulaires de cartes. Ceci comprend notamment les sociétés qui assurent des services de contrôle ou susceptibles d'affecter la sécurité des données de titulaires de cartes. Les prestataires de services gérés qui mettent à disposition des pare-feu, des IDS et autres services, ainsi que les fournisseurs et autres entités d'hébergement en sont des exemples. Les entités telles que les sociétés de télécommunication fournissant uniquement des liens de communication sans accès à la couche application du lien de communication sont exclues.
SAQ	Questionnaire d'auto-évaluation de la conformité à PCI DSS. Il permet à toute entité d'auto évaluer le niveau de conformité de son système d'information à PCI DSS. Il est destiné aux entités qui n'ont pas l'obligation d'être évaluées par un auditeur QSA.
QSA	Qualified Security Assessor : entreprise indépendante et disposant de compétences en sécurité de l'information qui a été qualifiée par le PCI Security Standards Council pour évaluer la conformité d'une entité à la norme PCI DSS. Le registre du personnel certifié QSA est maintenu à jour : https://www.pcisecuritystandards.org/approved_companies_providers/verify_qsa_employee.php

[4] Le Property Management System (PMS) gère les activités opérationnelles de l'hôtel : réservation, facturation depuis les terminaux points de vente (restauration, bar, boutique, spa, et/ou depuis les systèmes de gestion de téléphonie/Internet/TV payante), gestion des débiteurs, gestion de la relation client …

ANNEXE : PAYLIB

1. Principes

Paylib est un service permettant de réaliser des paiements par Carte CB sur internet ou sur un téléphone mobile, avec une authentification sécurisée sans contraindre le client porteur de Carte à saisir son numéro de carte, la date de fin de validité et le cryptogramme visuel. Le parcours de paiement Paylib se substitue à la saisie de ces données et également au processus 3D Secure pour les Accepteurs enrôlés 3D Secure.

2. Conditions d'éligibilité et accès au service

Paylib est un mode de paiement et non un instrument de paiement. En conséquence, une opération de paiement effectuée via Paylib reste une opération de paiement par carte CB. Pour bénéficier du service Paylib, vous devez être titulaire d'un Contrat d'acceptation en paiement à distance sécurisé par cartes et d'un contrat de service Citelis (plateforme d'acceptation technique permettant le paiement à distance sécurisé). La résiliation/suspension de l'un de ces contrats entraînera la résiliation/suspension du service Paylib. En revanche, l'arrêt du service Paylib est sans incidence sur la poursuite de ces contrats.

3. Modalités de fonctionnement

Vous trouverez les modalités d'installation et d'utilisation de Paylib sur les sites : www.citelis.fr et www.paylib.fr.
Nous vous informons par ailleurs que certaines fonctionnalités prévues dans ce contrat ne sont pas applicables aux opérations de paiement effectuées via Paylib. La liste des fonctionnalités incompatibles peut vous être fournie par votre conseiller.

4. Garantie de paiement

Vous bénéficiez pour les opérations de paiement Paylib de la garantie de paiement sous réserve du respect de l'ensemble des règles de sécurité prévues au contrat.

5. Nos obligations

Vous bénéficiez d'un service d'assistance technique.
Vous bénéficiez également d'un reporting des transactions réalisées avec Paylib.

6. Vos obligations

Vous vous engagez à :

- respecter les conditions techniques et modalités prévues dans la documentation Paylib qui vous sont mises à disposition sur les sites www.citelis.fr et www.paylib.fr.
- mettre en œuvre les mises à jour de la plateforme technique Paylib et de ses conditions d'acceptation,
- respecter les règles et procédures relatives à l'acceptation des paiements par Cartes CB et notamment les procédures et protocoles de sécurisation des opérations de paiement prévues dans les Conditions générales d'adhésion aux Schémas de cartes et en annexes,
- ne pas faire de discrimination entre les différents instruments de paiement offerts sur votre site marchand avec ou sans utilisation du service Paylib,
- collaborer régulièrement et activement avec nous dans l'intérêt du bon fonctionnement du service,
- ne pas revendre, partager, louer ou mettre le service Paylib à la disposition de tout tiers.

7. Propriété intellectuelle

Dans le cadre du service Paylib, vous disposerez d'un droit d'usage non exclusif, non transférable et non cessible des moyens Paylib mis à votre disposition. Ce contrat n'emporte pas de cession de licence, ni un quelconque droit d'utilisation ou de reproduction des images, marques et logo du service Paylib, à l'exception de celui nécessaire à son chargement, son affichage et son exécution sur le site marchand. Vous nous autorisez, ainsi que la société Paylib Services, à vous citer en référence comme « Commerçant accepteur Paylib », et ainsi à utiliser votre marque et votre logo pour la promotion de ce service, vous en autorisez donc la reproduction et la diffusion par tout moyen et sur tout support.

8. Confidentialité et loi « informatique et liberté » données personnelles

Vous vous engagez à garder confidentiel l'ensemble des informations dont vous auriez connaissance liées au service Paylib.
La finalité de la collecte de vos données personnelles a pour objet la gestion du service Paylib. Les données seront communiquées à la société Paylib Services à des fins de gestion, de sécurité, d'animation, de promotion commerciale, de prévention notamment de la fraude et en vue d'études statistiques.

9. Interruption du service

Nous nous réservons la possibilité, tout comme la société Paylib Services, sans préavis et sans formalité particulière, de suspendre à tout moment l'accès au service ou à certaines fonctions du service pour des raisons de sécurité, de fraude, ou de manquement grave et répétés à vos engagements. Cette interruption n'ouvre droit à aucune pénalité ou indemnité à votre profit.
Nous nous engageons à vous en informer dans les plus brefs délais.

10. Durée et arrêt du service

Le service Paylib prend effet à la date de signature des Conditions Particulières. Vous pourrez utiliser ce service pour une durée indéterminée.

Le service Paylib pourra être arrêté à tout moment par l'une ou l'autre Partie par lettre recommandée avec accusé de réception moyennant un préavis d'un (1) mois sauf juste motif justifiant la réduction du préavis.

En cas d'arrêt de Paylib, vous serez informé des dates et conditions d'arrêt de Paylib.

Suite à la résiliation vous ne pourrez vous prévaloir de la dénomination distributeur Paylib et vous devrez supprimer toute référence à Paylib dans vos documents.

11. Evolution du service

Paylib est susceptible de faire l'objet d'évolutions, notamment par l'ajout de nouvelles fonctionnalités, ou d'être remplacé à tout moment, notamment en fonction des évolutions technologiques.

Nous vous informons que cette évolution pourra donner lieu à la facturation de frais additionnels dont nous vous communiquerons le tarif ou à la modification de la tarification existante.

ANNEXE : Paiement de Proximité

1. Nos obligations

Nous vous fournissons les informations sur les procédures applicables à l'acceptation des paiements de proximité que vous devez utiliser obligatoirement. Ces informations figurent notamment dans les Conditions Particulières et dans la présente annexe.

2. Garantie de paiement et mesures de sécurité

3.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées au présent article et dans les Conditions Particulières.
Toutes les mesures de sécurité sont indépendantes les unes des autres.
En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement et en l'absence de contestation.

3.2 Lors d'un paiement de proximité, vous vous engagez à :

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

- la présence de la Marque sur la Carte ou de la Marque des cartes acceptées conformément à l'article 1 des Conditions Générales d'adhésion aux Schémas de cartes,
- le cas échéant l'hologramme sauf pour les Cartes portant la Marque V Pay,
- la présence de la puce sur les cartes CB,
- la Marque et catégorie de Carte définies à l'article 1 des Conditions Générales d'adhésion aux Schémas de cartes,
- le cas échéant, la période de validité (fin et éventuellement début).

3.2.2 Utiliser l'Equipement Electronique, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques vous ont été indiquées.
L'Equipement Electronique doit notamment :

- après la lecture de la puce de la Carte lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  - vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - la date de fin de validité de 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 date de fin de validité de la Carte.

3.2.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition que nous avons diffusé, pour le point d'acceptation concerné et selon les Conditions Particulières convenues avec nous.

3.2.4 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 émis par le Terminal de Paiement Electronique (ci-après "Ticket TPE").
Lorsque le code confidentiel n'est pas vérifié, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

3.2.5 Obtenir une autorisation d'un montant identique à l'opération sous-jacente :

- 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 convenues avec nous, et ceci quelle que soit la méthode d'acquisition des informations,
- 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 convenues avec nous.

A défaut d'obtention d'une autorisation ou l'autorisation a été refusée par le serveur, l'opération ne sera pas garantie.
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.

3.2.6 Faire signer le Ticket TPE dans tous les cas où l'Equipement Electronique le demande.

3.2.7 Lorsque la signature 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.

3.2.8 Dans tous les cas où l'Equipement Electronique édite un Ticket TPE, remettre au Titulaire de la Carte l'exemplaire qui lui est destiné.

3.2.9 Dans tous les cas où l'Equipement Electronique émet un Ticket TPE dématérialisé, adresser au Titulaire de la Carte l'exemplaire qui lui est destiné.

3.3 Après un paiement, vous devrez :

3.3.1 Nous transmettre dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations, et vous assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation doit obligatoirement nous être remise.

3.3.2 Archiver et conserver, à titre de justificatif, pendant une durée de quinze (15) mois requise par les règles des Schémas de cartes de paiement après la date de l'opération :

- un exemplaire du Ticket TPE comportant, lorsqu'elle est requise, la signature du Titulaire de la Carte,
- l'enregistrement magnétique représentatif de l'opération ou le journal de fond lui-même.

3.3.3 Communiquer, à notre demande et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

3.3.4 Vous vous engagez à ne stocker, sous quelque forme que ce soit, aucune des données cartes ci-après :

- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- le code confidentiel.

3. Les conditions d'utilisations de l'Equipement Electronique

1ère OPTION : Equipement Electronique vous appartenant ou loué à un tiers

Le GIE CB, Visa, MasterCard, JCB et Discover informent tous les constructeurs connus et référencés par eux des mises à jour de logiciels jugées indispensables. Vous devez assurer l'installation, le fonctionnement, la maintenance et la mise à niveau de l'Equipement Electronique.

Dans le cadre de l'acceptation des Cartes, vous devez :

1 Veiller à ce que votre police d'assurance couvre bien :
- les risques inhérents à la garde de cet Equipement Electronique dont nous ne saurons être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération,
- les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu vous être confiés.

2 Nous garantir un libre accès à l'Equipement Electronique, tout comme au constructeur ou à toute personne désignée par nos soins pour les différents travaux à effectuer sur l'appareil.

3 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées et n'y apporter aucune modification de logiciel ayant un impact sur les Schémas CB, Visa, MasterCard, JCB ou Discover sans notre accord préalable et sans nouvelle procédure d'agrément dans le respect de l'article 4.19 des Conditions générales d'adhésion aux Schémas de cartes.

4 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Equipements Electroniques.

2ème OPTION : Equipement Electronique nous appartenant

Vous devez :

1 Réserver dans le point de vente, l'emplacement nécessaire à l'installation de l'Equipement Electronique.

2 Faire votre affaire des travaux préalables à la mise en place des Equipements Electroniques (mise à disposition des prises électriques, téléphoniques, etc).

3 Nous garantir un libre accès à l'Equipement Electronique, tout comme au constructeur ou à toute personne désignée par nos soins pour intervenir sur l'Equipement Electronique afin d'en assurer la maintenance, notamment lorsque la mise à jour de logiciels s'avère nécessaire.

4 Signer, à réception de l'Equipement Electronique, qu'il s'agisse d'une première installation ou d'un remplacement, le bordereau de prise en charge qui vous sera présenté. Ce document reprend les caractéristiques indispensables à l'identification de l'Equipement Electronique.

5 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées, n'y apporter aucune modification si ce n'est dans le respect des dispositions de l'article 4.18 des Conditions générales d'adhésion aux Schémas de cartes.

6 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Equipements Electroniques dont vous avez la garde.

7 Veiller à ce que votre police d'assurance couvre bien les risques inhérents à la garde des Equipements Electroniques et dont nous ne saurons être responsables, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération.

8 Assumer toutes les obligations du dépositaire, conformément aux dispositions des articles 1927 et suivants du Code Civil.

9 Payer les frais de location ou de dépôt vente selon les présentes Conditions Particulières convenues avec nous.

En outre, cette mise à disposition peut faire l'objet d'un contrat spécifique.