CONTRAT VADS

Le contrat VADS permettant l'acceptation en paiement à distance sécurisé de cartes de paiement (ci-après dénommé le « Contrat ») est composé :

- des conditions particulières convenues ci-dessus entre la Banque et l'Accepteur (ci-après dénommées « Conditions Particulières ») ;
- et des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement.

CONDITIONS GENERALES DU CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PAR CARTES DE PAIEMENT (VADS)

PREAMBULE

Les présentes Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement comportent deux parties :

- Une Partie I : Conditions Générales communes à tous les Schémas de cartes de paiement,
- Une Partie II : Dispositions spécifiques à chaque Schéma de cartes de paiement.

PARTIE 1
CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

ARTICLE 1 – DEFINITIONS

1) L'"Accepteur" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens et/ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou à percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec l'Acquéreur.

2) 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 pouvant être acceptées entrant dans le champ d'application du présent Contrat sont visées en Partie 2.

3) Par "Acquéreur" il faut entendre tout établissement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) en Partie 2 du présent Contrat.

4) Par "Système d'Acceptation", il faut entendre les logiciels et protocoles, conformes aux spécifications définies par chaque Schéma, et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant la (l'une des) Marque(s) dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément ou d'une approbation par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

5) Par « Règlement », il faut entendre le Règlement UE n°2015/751 du 29 avril 2015.

6) Par "Schéma", il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.

Les Schémas CB/Visa/Mastercard reposent sur l'utilisation de Cartes auprès des Accepteurs acceptant la (l'une des) Marque(s) desdits Schémas et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

7) Par « Carte », on entend une catégorie d'instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marque(s).

Lorsque la Carte est émise dans l'Espace Economique Européen (ci-après l'"EEE" qui comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :

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

ou l'équivalent dans une langue étrangère.

8) Par « Catégorie de carte », on entend les catégories de Carte suivantes :
- carte de crédit,
- carte de débit,
- carte prépayée,
- carte commerciale.

9) Par "Paiements récurrents et/ou échelonnés" (ci-après les "Paiements Récurrents"), il faut entendre plusieurs opérations de paiement successives et distinctes (série d'opérations) ayant des montants et des dates déterminés ou déterminables et/ou à des échéances convenues entre l'Accepteur et le titulaire de la Carte.

10) Par « Parties », il faut entendre l'Acquéreur et l'Accepteur.

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

2.1 Afficher visiblement la (les) Marque(s) qu'il accepte et la (les) Catégorie(s) de carte qu'il accepte ou refuse pour chaque Marque notamment en apposant ces informations de façon apparente sur l'écran du dispositif technique ou /et sur tout autre support de communication.

Pour la(les) Marque(s) qu'il accepte, l'Accepteur doit accepter toutes les Cartes émises hors de l'EEE sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de carte .

2.2 Afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que le titulaire de la Carte en soit préalablement informé.

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

2.4 Respecter les lois et règlements (y compris en matière fiscale), les dispositions professionnelles ainsi que les bonnes pratiques 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 (ex : mobile et ordinateur).
A cet effet l'Accepteur organise la traçabilité adéquate des informations liées au paiement en ligne.

2.5 Utiliser le Système d'Acceptation en s'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 et de moyens ou instruments de paiement, le non-respect de la protection des données à caractère personnel, des atteintes aux systèmes de traitement automatisé desdites 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.

2.6 Garantir l'Acquéreur, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 2.5.

2.7 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a initiées, vérifier avec l'Acquéreur la conformité des informations transmises pour identifier son point de vente en ligne.

Les informations doivent indiquer une dénomination commerciale connue des titulaires de Carte et permettre de dissocier ce mode de paiement des autres modes de paiement (ex : automate et règlement en présence physique du titulaire de la Carte).

2.8 Accepter les paiements à distance sécurisés effectués avec la (les) Marque(s) et Catégorie(s) de carte qu'il a choisies d'accepter ou qu'il doit accepter en contrepartie d'actes de vente et/ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ou à titre de dons ou pour le règlement du montant de cotisations,

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

2.10 Afficher visiblement sur tout support, et notamment à l'écran du dispositif technique, le montant à payer ainsi que la devise dans laquelle ce montant est libellé.

2.11 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications du Schéma et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes (en ce compris la procédure d'authentification) proposées par l'Acquéreur.

2.12 – Ne pas stocker sous quelque forme que ce soit le cryptogramme visuel (trois derniers chiffres du numéro figurant au verso de la Carte).

2.13 Régler, selon les Conditions Particulières convenues avec l'Acquéreur, les commissions, frais et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

2.14 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données de paiement sensibles liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter le Référentiel Sécuritaire Accepteur et le Référentiel Sécuritaire PCI DSS et acceptent que les audits visés à l'article 2.15 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé à cet article.

2.15 Respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat ainsi que celles du Référentiel Sécuritaire PCI DSS dont il peut prendre connaissance à l'adresse suivante : http//fr.pcisecuritystandards.org/minisite/en/ ou qui lui sera communiqué par l'Acquéreur à première demande,

2.16 Permettre à l'Acquéreur et/ou au(x) Schéma(s) concerné(s) de faire procéder dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.13 ci-dessus, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement sur Internet en fonction des risques de sécurité liés au Système d'Acceptation utilisé. Cette vérification, appelée "procédure d'audit", s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, l'Acquéreur peut procéder, le cas échéant à la demande du(des) Schéma(s) concerné(s), à une suspension de l'acceptation des Cartes portant la (les) Marques du(des) Schémas concerné(s) par l'Accepteur, voire à la résiliation du présent Contrat, dans les conditions prévues aux articles 8 et 9 de la présente Partie 1.L'Accepteur autorise la communication du rapport à l'Acquéreur et au(x) Schéma(s) concerné(s).

2.17 Dans le cas où il propose des Paiements Récurrents, l'Accepteur s'engage à :

- respecter les règles relatives au stockage des données à caractère personnel ou des données de paiement sensibles liées à l'utilisation de la Carte définies par la délibération de la CNIL n° 2018-303 du 6 septembre 2018,
- s'assurer que le titulaire de la Carte a consenti à ce que les données de paiement sensibles liées à sa Carte soient utilisées pour effectuer des Paiements Récurrents et, à ce titre, recueillir du titulaire de la Carte les autorisations et/ou mandats nécessaires à l'exécution des Paiements Récurrents et en conserver la preuve pendant quinze (15) mois à compter de la date du dernier paiement,
- donner une information claire au titulaire de la Carte sur les droits dont il dispose et notamment sur la possibilité de retirer à tout moment son consentement,
- ne plus initier de paiements dès lors que le titulaire de la Carte a retiré son consentement à l'exécution de la série d'opérations de paiement considérée.

2.18 Faire son affaire personnelle des litiges liés à la relation sous-jacente (ex : contrat de vente) qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.

2.19 Informer dans les meilleurs délais l'Acquéreur en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement dysfonctionnement du Système d'Acceptation)...

2.20 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données liées au paiement, coopérer avec l'Acquéreur et, le cas échéant, les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire l'Acquéreur à résilier le présent Contrat conformément à l'article 8 de la présente Partie 1.

ARTICLE 3 - OBLIGATIONS DE L'ACQUEREUR

L'Acquéreur s'engage à :

3.1 Mettre à la disposition de l'Accepteur les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.

3.2 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie 2 du présent Contrat et son/leur évolution, la (les) Marque(s) et Catégorie(s) de carte dont il assure l'acceptation, ainsi que les frais applicables à chaque Marque et Catégorie de carte acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

3.3 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement conformément au choix de l'Accepteur ou du titulaire de la Carte.

3.4 Inscrire l'Accepteur dans la liste des accepteurs habilités à recevoir des paiements à distance sécurisés par Cartes.

3.5 Indiquer à l'Accepteur la liste et les caractéristiques des Cartes pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation et lui fournir à sa demande le fichier des codes émetteurs (BIN).

3.6 Créditer le compte de l'Accepteur des sommes qui lui sont dues, dues, au plus tard le jour ouvrable (un jour ouvrable est un jour au cours duquel l'ensemble des personnes impliquées dans l'exécution d'une opération de paiement exerce une activité permettant d'exécuter l'opération de paiement concernée) suivant le moment de réception des enregistrements des opérations de paiement.
Les Parties conviennent que le moment de réception est le jour ouvrable au cours duquel l'Acquéreur reçoit les enregistrements. Toutefois, les enregistrements reçus après 10 h 00 sont réputés avoir été reçus le jour ouvrable suivant.

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

3.8 Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois les informations suivantes :
- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par l'Accepteur et de la commission d'interchange.

L'Accepteur peut demander à ce que les informations soient regroupées par Marque, par Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

3.9 Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

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

ARTICLE 4 : GARANTIE DE PAIEMENT

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 qu'en Partie 2 des présentes, ainsi que 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, ou lorsque l'opération ne fait pas l'objet d'une authentification forte sur demande de l'Accepteur conformément aux modalités prévues dans les Conditions Particulières, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestations.

Lors du paiement, l'Accepteur s'engage à obtenir de l'Acquéreur un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement. Les conditions d'obtention du justificatif d'acceptation sont décrites dans les Conditions Particulières.

ARTICLE 5 - MESURES DE SECURITE

5.1 Lors du paiement

L'Accepteur s'engage à :

5.1.1 Appliquer la procédure de sécurisation des ordres de paiement (en ce compris la procédure d'authentification) décrite dans les Conditions Particulières.

5.1.2 Obtenir de l'Acquéreur un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement. .Les conditions d'obtention du justificatif d'acceptation sont décrites dans les Conditions Particulières.

5.1.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la période de validité (fin et éventuellement début),

- que la Marque est indiquée dans les Conditions Particulières ou figure dans la Partie 2 des présentes.

5.1.4 Obtenir une autorisation d'un montant identique à l'opération sous- jacente. La demande d'autorisation doit obligatoirement mentionner le CVX2 (cryptogramme visuel). Une réponse de type « interdit », faite par le Système d'Acceptation, annule la garantie pour toutes les transactions faites postérieurement, le même jour avec la même Carte, dans le même point de vente en ligne.

5.2 Après le paiement

L'Accepteur s'engage à :

5.2.1 Transmettre à l'Acquéreur dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur, les enregistrements électroniques des opérations et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur.

L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur doit être obligatoirement remise à ce dernier.

5.2.2 Envoyer au titulaire de la Carte, à sa demande, un ticket précisant, entre autres, le mode de paiement utilisé.

5.2.3 Communiquer, à la demande de l'Acquéreur et dans les délais prévus dans les Conditions Particulières convenues avec lui, tout justificatif des opérations de paiement.

5.2.4 Les mesures de sécurité énumérées ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 7 de la présente Partie 1.

ARTICLE 6 : MODALITES ANNEXES DE FONCTIONNEMENT

6.1 Réclamation

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

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

En cas de mauvaise exécution, il appartient à l'Accepteur d'établir l'erreur imputable à l'Acquéreur. Si la preuve de l'erreur de l'Acquéreur est démontrée par l'Accepteur, l'Acquéreur remboursera immédiatement ce dernier et rétablira le compte débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu.

6.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur.

En cas de conflit, les enregistrements électroniques produits par l'Acquéreur ou le Schéma prévaudront sur ceux réalisés par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur ou le Schéma.

6.3. Transaction crédit

Le remboursement partiel ou total d'un achat d'un bien ou d'un service, d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord de son titulaire, être effectué au titulaire de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de « transaction crédit » selon les règles du Schéma qui s'appliquent à l'opération de paiement concernée ou dans les Conditions Particulières convenues avec l'Acquéreur, effectuer la remise correspondante à l'Acquéreur à qui il avait remis l'opération initiale. Le montant de la « transaction crédit » ne doit pas dépasser le montant de l'opération initiale.

6.4 Le remboursement partiel ou total d'un achat d'un bien, d'un service, d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord du titulaire de la Carte, être effectué avec les données de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de «transaction crédit» selon les règles du Schéma qui s'appliquent à l'opération de paiement concernée ou dans les Conditions Particulières convenues avec l'Acquéreur, effectuer la remise correspondante à l'acquéreur à qu'il avait remis l'opération initiale. Le montant de la «transaction crédit» ne doit pas dépasser le montant de l'opération initiale.

ARTICLE 7 : MODIFICATIONS

7.1 L'Acquéreur peut modifier à tout moment les dispositions du présent Contrat .

L'Acquéreur peut notamment apporter :

- des modifications techniques telles que l'acceptabilité de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'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'acceptabilité de Cartes portant certaines Marques.

7.2 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un (1) mois à compter de l'envoi de la notification sur support papier ou sur tout autre support durable.

D'un commun accord, précisé dans les Conditions Particulières convenues entre l'Acquéreur et l'Accepteur, les Parties peuvent déroger à ce délai en cas de modifications importantes.

7.3 Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque l'Acquéreur ou le Schéma constate une utilisation anormale de Cartes perdues, volées ou contrefaites.

7.4 En cas de désaccord, l'Accepteur a la possibilité de résilier son Contrat, selon les modalités prévues à l'article 8 de la présente Partie 1.

7.5. Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur s'il n'a pas résilié le présent Contrat, sans que l'Acquéreur ait à lui rappeler cette faculté.

7.6 Le non-respect des nouvelles conditions techniques et sécuritaires, dans les délais impartis, peut entraîner la suspension par l'Acquéreur de l'acceptation des Cartes portant la (les) Marque(s) du(des) Schéma(s) concerné(s), dans les conditions prévues à l'article 9 de la présente Partie 1, voire la résiliation du Contrat, dans les conditions prévues à l'article 8 de la présente Partie 1.

ARTICLE 8 : DUREE ET RESILIATION DU CONTRAT

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

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

8.2 En outre, à la demande de tout Schéma, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 9.2 ci-dessous. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

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

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

8.4. L'Accepteur est tenu de restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire.

Sauf dans le cas où il a conclu un ou plusieurs autre(s) contrat(s) d'acceptation, l'Accepteur s'engage à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes.

8.5. L'Acquéreur peut suspendre ou résilier le Contrat sans préavis, sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception, dès lors qu'il est informé de l'illicéité du contenu du site Internet de l'Accepteur.

ARTICLE 9 - SUSPENSION DE L'ACCEPTATION

9.1 L'Acquéreur peut 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 portant certaines Marques par l'Accepteur. La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut également intervenir à l'issue d'une procédure d'audit visée à l'article 2.15 ci-dessus au cas où le rapport révélerait un ou plusieurs manquement(s) tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS.

9.2 La suspension peut être décidée en raison notamment :

9.2.1 du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation d'un Schéma,

9.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,

9.2.3 d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,

9.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,

9.2.5 de retard volontaire ou non motivé de transmission des justificatifs,

9.2.6 d'un risque aggravé en raison des activités de l'Accepteur.

9.3 L'Accepteur s'engage alors à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire, et à retirer immédiatement de son point de vente en ligne tout signe d'acceptation des Cartes du Schéma concerné.

9.4 En cas de suspension, la période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur peut demander la reprise du présent Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son choix.

ARTICLE 10 - MESURES DE PREVENTION ET DE SANCTION PRISES PAR L'ACQUEREUR

10.1 En cas de manquement de l'Accepteur 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, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

10.2 Si dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut soit procéder à une suspension de l'acceptation des Cartes, dans les conditions précisées à l'article 9 ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat par lettre recommandée avec demande d'avis de réception.

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

10.4 En cas de suspension ou de résiliation, l'Accepteur s'engage à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire et, à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes, sauf dans le cas où il a conclu un ou plusieurs autre(s) contrat(s) d'acceptation.

ARTICLE 11 – PRESTATAIRE TECHNIQUE – RESPONSABILITÉ DE L'ACCEPTEUR

Aux fins de la bonne exécution du Contrat, l'Accepteur choisit, sous son entière responsabilité, un Prestataire technique chargé notamment de la sécurisation des paiements.

L'Accepteur s'engage à ce que ce prestataire choisi par ses soins soit en permanence conforme aux standards PCI DSS ayant pour objet la protection des données monétiques sensibles utilisées pour la réalisation des opérations de paiement contre les actes de piratage et de malveillance.

S'agissant des conditions de délivrance du Justificatif d'acceptation visé dans les Conditions Particulières, l'Acquéreur ne sera lié par aucune obligation résultant des informations transmises par l'Accepteur et son Prestataire technique. En cas d'impayé, seules les données authentifiées par le serveur d'autorisation de l'Acquéreur et restituées dans la chaîne de traitement des impayés feront foi. À défaut de concordance entre ces informations et celles délivrées par le Prestataire technique à l'Accepteur, l'Acquéreur se réserve la possibilité de ne pas délivrer la garantie de paiement visée à l'article 4 des présentes.
L'Accepteur s'engage à autoriser expressément son Prestataire technique à transmettre à l'Acquéreur, à première demande, le ou les adresse(s) réticulaire(s) (URL) utilisée(s).

ARTICLE 12 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

12.1 Secret bancaire

De convention expresse, l'Accepteur autorise l'Acquéreur à stocker le cas échéant des données secrètes ou confidentielles portant sur lui et les communiquer à des entités impliquées dans le fonctionnement du(des) Schéma(s) 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.

12.2 Protection des données à caractère personnel

Lors de la signature ou de l'exécution des présentes, chacune des Parties peut avoir accès à des données à caractère personnel.
Ainsi, en application de la réglementation française et européenne sur la 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 :

12.2.1 Les données à caractère personnel relatives à l'Accepteur, collectées par l'Acquéreur nécessaires à l'exécution des ordres de paiement transmis et leur sécurisation, 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 des intérêts légitimes de l'Acquéreur que constituent la prévention et la lutte contre la fraude à la carte de paiement, la gestion des éventuels recours en justice ;
- La réponse aux obligations légales et réglementaires.

Ces données à caractère personnel traitées par l'Acquéreur sont conservées pour les durées suivantes :
- Les données nécessaires à l'exécution des opérations de paiement par Carte sont conservées pour une durée de 5 ans à compter de l'exécution de l'opération étant précisé que cette durée est portée à 10 ans dès lors qu'il s'agit d'un document comptable ;
- Les données nécessaires à la lutte contre la fraude sont conservées pour une durée maximale de 10 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, les données à caractère personnel relatives à l'Accepteur pourront être communiquées aux émetteurs, partenaires, sous-traitants, prestataires de l'Acquéreur, ainsi qu'aux Schémas de cartes de paiement dont les marques sont acceptées par l'Accepteur.

Conformément à la réglementation applicable et notamment au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :
- demander à accéder aux données à caractère personnel le concernant et/ou en demander la rectification ou l'effacement ;
- définir des directives relatives au sort des données à caractère personnel le concernant après son décès ;
- s'opposer au traitement de données à caractère personnel le concernant réalisé aux fins de lutte contre la fraude - et/ou de gestion des éventuels recours en justice, sous réserve que l'Acquéreur n'invoque pas de motifs légitimes et impérieux ;
- demander des limitations au traitement des données à caractère personnel le concernant dans les conditions prévues à

l'article 18 du Règlement (UE) 2016/679 du 27 avril 2016 ;
- demander à recevoir et/ou transmettre à un autre responsable du traitement les données à caractère personnel le concernant, nécessaires à l'exécution des présentes, 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.

L'Accepteur peut exercer ses droits et contacter le délégué à la protection des données personnelles en s'adressant : auprès de l'agence dans laquelle est ouvert son compte, par courrier électronique à l'adresse suivante dpo.cdn@cdn.fr, aux coordonnées du service client indiquées dans les conditions générales du compte bancaire.

12.2.2 À l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les titulaires de Cartes.

L'Accepteur s'engage 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.

L'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte ainsi que pour les finalités prévues par la délibération n° 2018-303 du 6 septembre 2018 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance.Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat.

L'Accepteur s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de l'article 32 du Règlement (UE) 2016/679 du 27 avril 2016.

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès de l'Accepteur, 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. À cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 13 : NON RENONCIATION

Le fait pour l'Accepteur ou pour l'Acquéreur de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat 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 14 : 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 15 : LANGUE DU PRESENT CONTRAT

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

PARTIE 2
DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

I. DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

ARTICLE 1 – FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas sont :
- Visa Europe et VISA Inc,
- Mastercard Europe SA.

Ces Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes :
- Pour VISA Inc. et Visa Europe :
  - Visa,
  - V PAY,
  - ELECTRON.
- Pour Mastercard Europe SA. :
  - Mastercard,
  - Maestro.

ARTICLE 2 – OBLIGATION DE L'ACCEPTEUR

En complément de l'article 2.7 de la Partie 1, l'Accepteur s'engage à localiser son point de vente en ligne (en principe, pays de son établissement principal) et à faire en sorte que ce dernier porte mention de sa localisation.

ARTICLE 3 – OBLIGATION DE L'ACQUEREUR

Par dérogation à l'article 3.7 de la Partie 1 du Contrat, l'Acquéreur s'engage à ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 4 - GARANTIE DE PAIEMENT

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

II. DISPOSITIONS SPECIFIQUES AU SCHEMA CB

ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les "Cartes CB") pour le paiement d'achats de biens et/ou de prestations de services, le règlement de dons ou de cotisations auprès des Accepteurs adhérant au Schéma CB et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.
Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou solutions de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'acceptation, l'Acquéreur définissant certaines conditions spécifiques de fonctionnement.
Lorsque l'Acquéreur représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à l'Acquéreur , et non la mise en jeu de la garantie du paiement visée à l'article 4 de la Partie 1 du présent Contrat.

ARTICLE 2 - DISPOSITIONS RELATIVES AUX CARTES CB ET AUX SOLUTIONS DE PAIEMENT CB

Sont utilisables dans le Schéma CB et dans le cadre du présent Contrat :
- les Cartes sur lesquelles figure la Marque CB,
- les solutions de paiement CB.

ARTICLE 3 : DISPOSITIONS SUR L'ACCEPTATION DE CARTES CB

En complément des dispositions de l'article 2 de la Partie 1 du présent Contrat, l'Accepteur s'engage à :

3.1 Accepter les Cartes CB pour le paiement d'achats de biens et/ou de prestations de services offerts à sa clientèle et réellement effectués, même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, à titre de dons ou en contrepartie du règlement du montant de cotisations.

3.2 Régler, selon les Conditions Particulières convenues avec l'Acquéreur les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du Schéma CB.

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

3.4 En cas d'audit par le GIE CB, permettre à l'Acquéreur de faire procéder dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.13 de la Partie 1, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur joint et/ou du Référentiel Sécuritaire PCI DSS. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'acceptation des Cartes CB, voire à une radiation du Schéma CB tel que prévu à l'article 5 de la présente Partie.

L'Accepteur autorise la communication du rapport à l'Acquéreur et au GIE CB.

ARTICLE 4 : PROTECTION DES DONNEES A CARACTERE PERSONNEL

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

Les données à caractère personnel traitées par le GIE CB sont conservées pour les durées suivantes :

- En matière de lutte contre la fraude, les données utilisées pour l'émission d'alertes sont conservées pour une durée maximale de douze (12) mois à compter de l'émission des alertes. En cas de qualification de fraude avérée, les données relatives à la fraude sont conservées au maximum cinq (5) années, conformément à la réglementation de la CNIL.
- 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.

L'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés dans la Partie I à l'article 11 des présentes conditions générales par courriel à protegezvosdonnees@cartes-bancaires.com.

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

- Consulter la Charte 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.

ARTICLE 5 : MESURES de PREVENTION ET DE SANCTION

5.1 Mesures de prévention et de sanction mises en œuvre par l'Acquéreur.

En cas de manquement de l'Accepteur 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 CB perdues, volées ou contrefaites, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur 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, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut résilier de plein droit avec effet immédiat 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, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur peut décider la résiliation de plein droit avec effet immédiat du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

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

En cas de manquement de l'Accepteur 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 l'Accepteur ventile ses remises en paiement entre plusieurs acquéreurs 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 l'acceptation des Cartes CB par l'Accepteur. 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 l'Accepteur aurait déjà fait l'objet d'une mesure de suspension dans les vingt quatre (24) mois précédant l'avertissement.

  La suspension de l'adhésion au Système CB peut être immédiate lorsqu'elle est décidée en raison d'un des motifs suivants :
  - une utilisation anormale de Cartes perdues, volées ou contrefaites,
  - une utilisation d'un Système d'Acceptation non agréé,
  - un risque de dysfonctionnement important du Système CB,
  - une utilisation anormale ou détournée du Système d'Acceptation.

  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 l'adhésion de l'Accepteur au 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 vis-à-vis de l'Accepteur concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée avec demande d'avis de réception.

5.3 En cas de suspension ou de radiation, l'Accepteur s'engage alors à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire et à retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes CB.

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

A l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet du présent Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son 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 le GIE CB ou l'acquéreur concerné, et portant sur le respect des bonnes pratiques en matière de ventes et prestations réalisées à distance visées à l'article 2.4 de la Partie 1 et des mesures de sécurité visées à l'article 5 de la Partie 1.

Annexe 1 - REFERENTIEL SECURITAIRE ACCEPTEUR

Les exigences constituant le référentiel sécuritaire accepteur sont présentées ci-après :

Exigence 1 (E1)
Gérer la sécurité du système commercial et d'acceptation au sein de l'entreprise

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

Exigence 2 (E2)
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 applicatif commercial et 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 de paiement sensible liées à la Carte du Titulaire 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 commercial et d'acceptation

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation doivent être établies et leur respect doit être contrôlé.
Seul le serveur supportant l'application commerciale doit être accessible par les internautes.

Le serveur de base de données client ainsi que le serveur hébergeant le système d'acceptation ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu.

Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-

feu.

L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées.

Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.

Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.

Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

Exigence 5 (E5)

Contrôler l'accès au système commercial et d'acceptation

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés.

Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et d'acceptation.

Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

Exigence 6 (E6)

Gérer les accès autorisés au système commercial et d'acceptation

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.

Outre les accès clients, tout accès au système commercial et de paiement 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 commercial et d'acceptation

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.

L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.

Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées.

Les systèmes assurant l'enregistrement doivent au minimum avoir la fonction de pare-feu pour le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.

Les journaux d'audit doivent être protégées 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 commercial et 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 permettent 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 commercial et d'acceptation

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.
Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

La demande de modification doit être approuvée par le responsable fonctionnel du système.
Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

Exigence 12 (E12)
Assurer la 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 commercial et 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 commercial et 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 de paiement sensibles liées à la Carte du Titulaire 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 « CB ».
Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données de paiement sensibles liées à la Carte du Titulaire 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 « CB » et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15)

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.

Exigence 16 (E16)

Respecter le standard « Payment Card Industry – Data Security System » PCI-DSS

En souscrivant le contrat VADS, vous adhérez également à ce standard intitulé PCI DSS dont le détail peut être obtenu sur le site internet www.pcisecuritystandards.org.

Les obligations ou recommandations qui incombent aux commerçants sont fonction du nombre de transactions annuelles effectuées sur le site marchand. Quatre niveaux ont été définis. Nous vous invitons à vous reporter au document « Programme PCI-DSS » ci-après afin de prendre connaissance du niveau de votre entreprise.

PROGRAMME PCI/DSS

Niveaux et actions à mener selon le nombre de transactions :

Sources : programmes PCI-DSS des Réseaux Visa Europe (AIS[1]) et Mastercard (SDP[2]). http://www.visaeurope.com/receiving-payments/security/merchants
http://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html

	Critères	Actions à mener par le commerçant	Périodicité
Niveau 1	Accepteur ayant un volume annuel de transactions Visa et/ou Mastercard supérieur à 6 000 000 ou ayant fait l'objet d'une compromission l'année précédente	✓ Rapport de conformité suite à un audit réalisé par un QSA 2 (Qualified Security Assessor) ou une ressource interne agréée auditeur PCI-DSS ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) ✓ Formulaire d'attestation de conformité Obligation	⇨ Annuelle ⇨ Trimestrielle
Niveau 2	Accepteur ayant un volume annuel de transactions Visa ou Mastercard compris entre 1 000 000 et 6 000 000	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) ✓ Formulaire d'attestation de conformité Obligation	⇨ Annuelle ⇨ Trimestrielle
Niveau 3	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard compris entre 20 000 et 1 000 000	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) Obligation	⇨ Annuelle ⇨ Trimestrielle
Niveau 4	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard inférieur à 20 000	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) Recommandation	⇨ Annuelle ⇨ Trimestrielle

- ASV (Approved Scan Vendor) : prestataire spécialisé dans la sécurité informatique agréé pour la réalisation de scan de vulnérabilité.

Liste des ASV agréés par PCI-DSS :
http://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

- QSA (Qualified Security Assessor) : prestataire spécialisé dans la sécurité informatique certifié pour la réalisation d'audits PCI-DSS.

Liste des QSA certifiés par PCI-DSS : http://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

– Questionnaire de self audit et formulaire d'attestation de conformité disponibles sur le site PCI-DSS : https://fr.pcisecuritystandards.org/minisite/env2/

(1) AIS : Account Information Security
(2) SDP : Site Data Protection
(3) Prestataires agréés ou certifiés par PCI-DSS (Conseil des normes de sécurité PSI — https://fr.pcisecuritystandards.org/minisite/en/)

ANNEXE 2 - PROGRAMME 3D SECURE

Le protocole 3D Secure (ci-après dénommée « 3DS » et, dans sa première version, « 3DS V1 ») a pour objet la mise en oeuvre, par l'émetteur de la Carte (ci-après dénommé « l'Émetteur »), de moyens techniques aux fins d'authentification forte du titulaire de la Carte.

Ce protocole a évolué (ci-après dénommé « 3DS V2 ») dans le but notamment de se conformer aux exigences de la Directive (UE) 2015/2366 dite « DSP2 » et des normes techniques en découlant (Règlement Délégué (UE) 2018/389)

dites « RTS SCA ».

Dans le cadre de 3DS V2, la décision d'authentification du titulaire de la Carte appartient à l'Émetteur. Cette authentification est réalisée soit en interaction avec le titulaire de la Carte (il y a alors authentification forte), soit sans interaction avec ce dernier (dans les cas où une exemption à l'authentification forte est possible), au moyen d'un certain nombre d'informations relatives au contexte de l'opération de paiement (a minima nom et adresse électronique du titulaire de la Carte ainsi que l'adresse de facturation).

Votre attention est attirée sur le fait que certaines opérations de paiement ne peuvent être réalisées dans le cadre de 3DS en raison notamment de la catégorie de la Carte avec laquelle l'opération de paiement est effectuée (ex : cartes prépayées anonymes) ou du mode de paiement utilisé (ex : paiement en l'absence du titulaire de la Carte comme le paiement récurrent).

Par ailleurs, vous vous interdisez de demander au titulaire de la Carte la communication du code d'authentification ou de sécurité que lui a transmis l'Émetteur, à l'exception du cryptogramme visuel.

Mise en œuvre

La mise en oeuvre de 3DS V2, comme de 3DS V1 (possible en présence d'une opération de paiement VISA ou MASTERCARD), requiert votre enrôlement préalable par l'Acquéreur auprès des Schémas CB (Paiement sécurisé CB – seulement pour 3DS V2), VISA (VisaSecure©) et MASTERCARD (Mastercard Identity Check©).

Authentification du titulaire de la carte

Authentification forte

Lors de l'opération de paiement, le titulaire de la Carte est redirigé vers la page d'authentification de l'Émetteur. L'authentification est effectuée conformément à une des/la méthode(s) d'authentification que ce dernier a choisie(s).

Exemption à l'authentification forte dans le cadre de 3DS V2 (également dénommée « frictionless »)

L'exemption à l'authentification forte est mise en oeuvre à partir des informations que vous avez collectées et convoyées par votre Prestataire technique et des informations connues par la base de gestion de risque (ex : historique des transactions du titulaire de la Carte) sans interaction avec le titulaire de la Carte.

L'exemption à l'authentification forte est appliquée :

(i) soit sur votre demande expresse (uniquement dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30€ ou d'un paiement récurrent de rang supérieur à 1) validée par l'Émetteur (en présence d'une telle demande, l'Émetteur peut l'accueillir favorablement – outre la communication des informations obligatoires au service, la communication d'informations facultatives y concourt fortement - ou la refuser et décider d'appliquer une authentification forte).

(ii) soit à l'initiative de l'Émetteur.

Conséquences de l'authentification forte et de l'exemption à l'authentification forte du titulaire de la Carte

La réponse à la demande d'authentification forte ou à la demande d'exemption à l'authentification forte vous est systématiquement transmise dans le journal des transactions envoyé chaque matin. Elle est également disponible via le portail de gestion, onglet « Gestion des transactions », menu « Transactions ».

L'obtention du justificatif d'acceptation, visé à l'article 4 des Conditions Générales d'acceptation en paiement à distance sécurisé par cartes de paiement– Partie 1 –Conditions Générales communes à tous les schémas, se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement (le titulaire de la Carte peut contester ou répudier – c'est-à-dire nier être l'auteur – une transaction auprès de l'Émetteur, à tout moment, et ce, pendant les 13 (treize) mois qui suivent la date initiale de la transaction). Lorsque la Carte n'est pas émise par la Banque, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'Émetteur à la Banque.

La Banque pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

Demande d'autorisation

À la suite de l'authentification forte ou de l'exemption à l'authentification forte du titulaire de la Carte, une autorisation doit être demandée pour chaque opération de paiement.

La demande d'autorisation doit comporter le cryptogramme visuel (s'il est présent) et les éléments relatifs à la demande d'authentification du titulaire de la Carte concernée.

Justificatif d'acceptation

En adhérant au contrat d'acceptation en paiement à distance sécurisé par cartes de paiement (VADS), l'Accepteur demande à être inscrit dans le programme 3D Secure auprès des Schémas CB (Paiement sécurisé CB), Visa (VisaSecure©) et Mastercard (Mastercard Identity Check©).

Ce dernier génère, pour les paiements effectués au moyen de Cartes portant les marques CB, Visa, V PAY, Electron, Mastercard ou Maestro par un internaute à partir de la page de paiement de l'Accepteur, en complément de la demande d'autorisation, une demande d'authentification du titulaire de la Carte.

L'Accepteur peut toutefois demander à l'émetteur (uniquement au titre de 3D Secure V2 et dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30 € ou d'un Paiement Récurrent de rang supérieur à 1) de ne pas appliquer de procédure d'authentification forte du titulaire de la carte. L'émetteur est libre d'accepter ou non la demande.Les opérations réalisées sans authentification forte à la demande de l'émetteur sont effectuées sans justificatif d'acceptation.

L'Accepteur s'interdit de demander au titulaire de la Carte de lui communiquer le code d'authentification ou de sécurité que lui a transmis l'émetteur de la Carte, à l'exception du cryptogramme visuel.

L'obtention du justificatif d'acceptation, visé à l'article l'article 5.1.2 des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement (VADS), se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement. Lorsque la Carte n'est pas émise par l'Acquéreur, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'émetteur à l'Acquéreur.

L'Acquéreur pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

Matrice de responsabilité dans le cadre de 3DS V2

Dans le cadre de 3DS V2, les règles applicables en matière de responsabilité sont les suivantes :

		Votre Souhait		
		Pas de souhait	Frictionless	Authentification forte
Décision de l'Emetteur	Frictionless	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	**Impossibilité d'obtenir un justificatif d'acceptation (Opération de paiement non garantie)**	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)
	Authentification forte	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)