Conditions générales et spécifiques du Contrat d'acceptation en paiement à distance sécurisé (VADS) par Carte

PARTIE I. Conditions Générales communes à tous les Schémas

Avertissement et pré-requis indispensable pour recevoir des paiements à distance sécurisés

Pour éviter, dans le commerce électronique (vente ou location) à distance ou pour le règlement à distance de dons ou cotisations, que tout tiers non autorisé accède aux données liées à la Carte et afin de limiter l'utilisation du seul numéro de Carte pour donner un ordre de paiement, les Schémas ont mis en place des procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Carte tel que le protocole 3D Secure, ainsi qu'un Référentiel de sécurité PCI DSS et un Référentiel Sécuritaire Accepteur.

Les procédures de sécurisation de paiement à distance consistent en l'authentification 3D Secure du titulaire de la Carte conformément aux spécifications établies par les Schémas (« *Protocole 3D Secure* »).

L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que sa plateforme de service technique e-commerce inclut l'authentification 3D Secure du titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

L'Accepteur est également informé que les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité qu'il doit respecter et en particulier celles visées à l'article 7 des Conditions Générales.

ARTICLE 1 : Définitions

"Accepteur"
L' "Accepteur" peut être tout commerçant, tout prestataire de services, toute personne, physique ou morale, exerçant une profession libérale, toute association, toute collectivité publique 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.

"Acquéreur"
Par "Acquéreur", il faut entendre tout établissement de crédit ou de paiement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) d'un (des) Schéma(s).

"Authentification Forte"
Par "Authentification Forte", il faut entendre une authentification basée sur l'utilisation de deux éléments d'authentification, ou plus, qui sont indépendants, de sorte que si un élément est compromis, la fiabilité des autres ne l'est pas, ces éléments faisant partie de deux des catégories suivantes au moins ; (i) un élément connu uniquement du titulaire de la Carte, (ii) un élément détenu uniquement par le titulaire de la Carte, et (iii) un élément inhérent au titulaire de la Carte.

"Carte(s)"
Par "Carte(s)", on entend un instrument de paiement qui permet à son titulaire d'initier une opération de paiement liée à une Carte. Elle porte une ou plusieurs Marques.

Lorsque la Carte est émise dans l'EEE, elle porte la mention de sa Catégorie, selon la classification indiquée ci-après ou l'équivalent dans une langue étrangère.

"Catégories de Carte"
Par "Catégories de Carte", on entend les catégories de Carte suivantes :
- crédit ou Carte de crédit,
- débit,
- prépayée,
- commerciale (Carte soumise aux règles commerciales du Chapitre III du Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015).

"Contrat" ou "Présent Contrat"
Par "Contrat" ou "Présent Contrat", il faut entendre ensemble les Conditions Générales et Spécifiques du Contrat d'acceptation en paiement à distance sécurisé (VADS) par Carte, ainsi que les Conditions Particulières des contrats d'acceptation en paiement par Carte (« **Condition Particulières** ») convenues entre l'Acquéreur et l'Accepteur, ainsi que leurs Annexes.

En cas de contradiction entre ces différents éléments, les Conditions Particulières prévalent sur les Conditions Spécifiques, qui elles-mêmes prévalent sur les Conditions Générales.

"EEE"
Par "EEE", il faut entendre l'Espace Economique Européen, soit, à la date des présentes, les Etats membres de l'Union Européenne, l'Islande, le Lichtenstein et la Norvège.

"Marque"
Par "Marque", il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptibles de désigner le Schéma.

Les Marques pouvant être acceptées dans le cadre du Présent Contrat sont celles indiquées dans les Conditions Particulières selon le(s) choix exprimé(s) par l'Accepteur.

Les règles spécifiques d'acceptation en paiement de proximité propres à chaque Schéma de Carte dont la(les) Marque(s) figure(nt) sur la Carte sont précisées dans le Conditions Spécifiques en Partie II du Présent Contrat.

"Partie(s)"
Par "Partie(s)", il faut entendre l'Acquéreur et l'Accepteur.

"Règlementation Relative à la Protection des Données à Caractère Personnel"
Par "Règlementation Relative à la Protection des Données à Caractère Personnel", il faut entendre les lois et règlementations applicables en matière de protection des données personnelles et de la vie privée, en particulier le Règlement (UE) 2016/679 du 27 avril 2016 dit « Règlement Général sur le Protection des Données » (RGPD), ainsi que toutes les lois et règlementations nationales, délibérations et recommandations de la CNIL ou de toute autorité de contrôle ou de supervision compétente au titre du Contrat ou d'une des Parties.

"Schéma"
Par "Schéma", il faut entendre un schéma de Cartes, soit un ensemble unique de règles et pratiques régissant l'exécution d'opérations de paiement liées à une Carte tel que défini à l'article 2 du Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015.

Les Schémas reposent sur l'utilisation de Cartes portant leur Marque auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

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

"UE"
Par "UE", il faut entendre l'Union Européenne, soit les Etats membres de l'Union Européenne.

ARTICLE 2 : Marques et Catégories de Cartes acceptées

L'Accepteur choisit librement les Marques et Catégories de Cartes qu'il souhaite accepter comme moyen de paiement, dans la limite des Marques et Catégories de Cartes dont l'Acquéreur propose l'acceptation.

Les Marques et Catégories de Cartes acceptées au titre du Présent Contrat sont celles qui ont été choisies par l'Accepteur dans les Conditions Particulières.

Dans le cas où l'Accepteur décide de ne pas accepter l'ensemble des Marques et/ou des Catégories de Cartes, ce dernier doit en informer clairement et sans ambiguïté le titulaire de la Carte, selon les modalités précisées à l'article 4.4 des présentes Conditions Générales.

ARTICLE 3 : Souscription du Contrat et convention de preuve

3.1 - Modalités de souscription du Contrat

L'Accepteur souscrit le Présent Contrat après avoir pris connaissance des Conditions Particulières, des Conditions Générales, des Conditions Spécifiques ainsi que de leurs Annexes.

La souscription du Contrat peut être réalisée, soit en agence, en présence d'un conseiller, soit à distance si cette possibilité est offerte, notamment par internet *via* l'espace client de la banque en ligne de l'Acquéreur.

3.2 - Convention de preuve en cas de souscription au Contrat par internet

De convention expresse entre les Parties, en cas de souscription à distance par internet, les enregistrements électroniques constituent la preuve de la souscription au Présent Contrat. En cas de conflit, les enregistrements électroniques produits par l'Acquéreur prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur.

ARTICLE 4 : Obligations de l'Accepteur

L'Accepteur s'engage à :

4.1 - Connaître et respecter les lois et règlements, les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance, au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux

de communication (TV, téléphonie mobile, ordinateur…), et, le cas échéant, aux jeux d'argent et de hasard et/ou de paris, et aux réceptions de dons et règlements de cotisations.

Il reconnaît qu'il doit commercialiser les produits ou prestations de services faisant l'objet d'un paiement à distance sécurisé en se conformant à ces dispositions, notamment fiscales, et à celles qui pourront intervenir.

Lorsque son activité implique des jeux d'argent, de hasard et/ou de paris, il s'engage à obtenir toute autorisation et/ou agrément de l'autorité compétente, à respecter les limites autorisées par la loi, et à refuser d'une personne légalement incapable une prise d'enjeux et/ou de paris et/ou une Carte de crédit.

4.2 - Utiliser le(s) Système(s) d'Acceptation en s'abstenant de toute activité illicite, et notamment pénalement sanctionnée telle que, et sans que la liste soit limitative :
- la mise en péril de mineurs, d'actes de pédophilie ;
- les actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle ;
- les actes de contrefaçon de moyens ou d'instruments de paiements ;
- le non-respect de l'utilisation des données personnelles collectées ;
- les atteintes aux systèmes de traitement automatisé des données ;
- les actes de blanchiment et de fraude ;
- le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries ;
- le non-respect des dispositions relatives à l'exercice des professions règlementées.

4.3 - Signaler immédiatement à l'Acquéreur :
- toute modification affectant sa forme juridique ou concernant ses représentants légaux ;
- toute modification de son activité, notamment de l'ajout d'une ou plusieurs branches d'activité, la cessation d'une ou plusieurs branches d'activités et plus généralement de tout événement modifiant les conditions d'exercice de son activité.

4.4 - Signaler au public l'acceptation des Marques, Catégories de Cartes qu'il accepte ou qu'il refuse, par l'apposition 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'UE sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de Carte.

4.5 - Accepter les paiements à distance sécurisés effectués avec les Cartes telles que listées dans les Conditions Particulières en contrepartie d'actes de vente ou de fournitures de prestations de services offerts à sa clientèle et qu'il fournit ou qu'il réalise lui-même.

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

4.6 - Dans le cas d'une opération de paiement effectuée avec une Carte co-badgée, c'est-à-dire portant le logo de deux ou plusieurs Marques, permettre au titulaire de la Carte de choisir la Marque. Il est rappelé à l'Accepteur qu'il peut sélectionner prioritairement la Marque indiquée à l'article 1 des Conditions Particulières, sous réserve de laisser la possibilité au titulaire de la Carte de passer outre, et de sélectionner une autre Marque.

4.7- 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.

Respecter les montants maximum indiqués par l'Acquéreur pour l'acceptation d'une opération de paiement par Carte, et précisés dans les Conditions Particulières.

4.8 - S'identifier clairement dans la transmission de ses enregistrements à l'Acquéreur par le numéro d'immatriculation (pour la France le SIRET et le code activité NAF/APE) que l'INSEE lui a attribués ou comme entité dûment habilitée à recevoir des dons ou percevoir des cotisations. Si l'Accepteur n'est pas immatriculable, notamment lorsqu'il s'agit d'une personne physique, il doit utiliser un numéro d'identification spécifique, fourni par l'Acquéreur.

4.9 - Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec l'Acquéreur la conformité des informations transmises pour identifier son point d'acceptation. Ces informations doivent indiquer une dénomination commerciale ou sociale (pour les dons et cotisations) connue des titulaires de Carte et permettre d'identifier le point d'acceptation concerné et de dissocier ce type de paiement des autres types de paiement (ex : automate et règlement en présence physique du titulaire de la Carte).

4.10 - Transmettre les enregistrements des opérations de paiement à l'Acquéreur, dans le délai maximum précisé à l'article 7 "Mesures de sécurité", sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.

Le délai de remise de la "transaction crédit" ne peut excéder trente (30) jours calendaires à compter de la date de l'opération de paiement initiale, sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.

Au-delà d'un délai maximum indiqué dans les Conditions Spécifiques à chaque Schéma, après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable.

4.11 - Régler, selon les Conditions Particulières convenues avec l'Acquéreur et selon les Conditions Générales, les commissions, frais, pénalités éventuelles et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes et du fonctionnement du Schéma concerné.

4.12 - Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications du Schéma concerné par l'opération de paiement et les procédures de sécurisation des ordres de paiement, donnés à distance par les titulaires de Cartes, proposées par l'Acquéreur.

A cet effet, l'Accepteur organise la traçabilité adéquate des informations liées au paiement à distance.

4.13 - Respecter le Référentiel Sécuritaire Accepteur figurant en annexe des Conditions Particulières et le Référentiel Sécuritaire PCI DSS consultable sur le site pcisecuritystandards.org, dont une présentation générale figure également en annexe des Conditions Particulières.

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 liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter les mêmes exigences et règles sécuritaires et acceptent que les audits visés à l'article 4.14 ci-après soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.

Déclarer à l'Acquéreur, annuellement, à compter de la date d'entrée en vigueur du Présent Contrat, et immédiatement en cas de changements de prestataire technique ou de correspondant au sein d'un prestataire technique, lesdits prestataires techniques ou sous-traitants. A défaut, l'Accepteur s'expose à des pénalités telles qu'indiquées aux Conditions Particulières.

4.14 - Permettre à l'Acquéreur et/ou au(x) Schéma(s) concerné(s) de faire procéder aux frais de l'Accepteur dans ses locaux ou ceux de ses prestataires, à la vérification et/ou au contrôle périodique par un tiers indépendant du respect tant des clauses du Présent Contrat et ses Annexes, que des exigences et règles sécuritaires visées à l'article 4.13 ci-dessus. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du Présent Contrat et/ou pendant sa durée et s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.

L'Accepteur autorise la communication du rapport en résultant à l'Acquéreur et au(x) Schéma(s) concerné(s).

Au cas où le rapport d'audit révélerait un ou plusieurs manquements aux Contrat ou exigences et règles sécuritaires, le Schéma peut demander à l'Acquéreur de procéder à une résiliation du Contrat.

4.15 - En cas de compromission et si la non-conformité aux exigences et règles sécuritaires est confirmée par le Schéma ou un tiers indépendant**,** des frais forfaitaires à l'ouverture du dossier de compromission ainsi qu'un montant par Carte compromise seront applicables à l'Accepteur. Ces frais et montants sont indiqués dans les Conditions Particulières.

4.16 - Mettre en œuvre dans le délai imparti par l'Acquéreur les mesures destinées à résorber un taux d'impayés anormalement élevé ou une utilisation anormale de Cartes perdues, volées ou contrefaites ou pour remédier à tout autre manquement au regard du Présent Contrat.

A défaut, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et dans les conditions prévues à l'article 8.2 des Conditions Générales, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur.

En cas de taux de fraude anormalement élevé, notamment au regard du volume d'affaires réalisé par l'Accepteur, de l'augmentation des opérations mises en impayés suite à réclamation du titulaire de la Carte, d'utilisation anormalement élevée de Cartes perdues, volées ou contrefaites ou dont les données ont été usurpées, l'Acquéreur est fondé à ne créditer le compte de l'Accepteur qu'après l'encaissement définitif des opérations de paiement.

L'Acquéreur est également autorisé à ne créditer le compte de l'Accepteur qu'après encaissement définitif en cas d'opérations présentant un caractère inhabituel ou exceptionnel.

L'Acquéreur en informe l'Accepteur par tout moyen à sa convenance, ladite mesure prenant effet immédiatement. Les opérations de paiement seront alors portées sur un compte d'attente spécialement ouvert à cet effet, distinct et autonome du compte de l'Accepteur, pour n'être portées au crédit de ce dernier qu'après encaissement définitif par l'Acquéreur. Les fonds portés au crédit du compte d'attente demeurent indisponibles.

Dans les mêmes hypothèses, l'Acquéreur peut après avoir dans un premier temps inscrit une ou plusieurs opérations au compte de l'Accepteur, dès lors que le paiement n'est pas encore définitif et selon les mêmes modalités que celles définies aux alinéas précédents, procéder à la contrepassation desdites opérations afin de les inscrire sur le compte d'attente.

4.17 - Les Schémas peuvent appliquer des pénalités aux Acquéreurs, calculées sur des bases identiques quel que soit l'Acquéreur, notamment :

- en cas de dépassement d'un certain nombre et/ou taux d'impayés généré(s) chez l'Accepteur, des pénalités mensuelles peuvent être appliquées après mise en demeure restée infructueuse,

- en cas de dépassement d'un certain nombre et/ou taux de fraude généré(s) chez l'Accepteur. A titre d'exemple, des pénalités allant jusqu'à 50% du montant de la fraude cumulée des 6 derniers mois peuvent être appliquées,
- lorsque l'Accepteur dépasse un certain nombre de factures crédits,
- en cas de non-respect des obligations d'information de l'Acquéreur relatives à l'activité de l'Accepteur (ajout, modification, arrêt),
- en cas d'exercice par l'Accepteur d'une activité illicite comme précisé à l'article 4.2 des présentes Conditions Générales ou non-conforme avec les règles édictées par les Schémas,
- en cas d'utilisation d'un Système d'Acceptation non certifié par les Schémas.

L'Accepteur accepte expressément de prendre en charge ces pénalités et autorise l'Acquéreur à les prélever sur le compte désigné aux Conditions Particulières.

L'Accepteur reconnait avoir été informé que l'exercice de certaines activités peut être interdit, ou soumis à restrictions ou autorisations par les Schémas.

4.18 - Connaître et mettre en place des systèmes compatibles avec les dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte lors d'une opération de paiements.

Dans le cas où, lors d'une opération de paiement, l'Accepteur n'appliquerait pas, le cas échéant, un dispositif d'Authentification Forte du titulaire de la Carte dans les conditions et selon les modalités prévues par l'émetteur de la Carte, l'Accepteur accepte expressément de rembourser les sommes relatives à l'opération de paiement litigieuse débitées à l'émetteur de la Carte, l'Acquéreur étant alors déchargé de toute responsabilité en cas de non-respect des dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte par l'Accepteur.

4.19.1 - Dans le cas où il propose des paiements récurrents, à savoir des 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, l'Accepteur s'engage à :
- respecter les règles relatives au traitement des données à caractère personnel ou liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2018-303 du 6 septembre 2018,
- transmettre à l'acquéreur dans l'autorisation et l'opération la donnée permettant d'identifier qu'il s'agit d'un paiement récurrent (indicateur *credential on file*),
- s'assurer que le titulaire de la Carte a consenti à ce que les données liées à sa Carte soient conservées par l'Accepteur aux fins d'être 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 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,

4.19.2 - Dans le cas où l'Accepteur souhaite proposer au titulaire de la Carte une option en vue de faciliter des paiements ultérieurs (ex : achat en « un clic »), l'Accepteur s'engage à :
- respecter les règles relatives au traitement des données à caractère personnel liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2018-303 du 6 septembre 2018,
- recueillir le consentement explicite, libre et spécifique pour cette finalité du titulaire de la Carte pour la conservation des données précitées en vue de cet usage, en veillant à ce que ce dernier reçoive une information préalable et exhaustive à cet effet,
- 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 spécifique à cet usage ou, de façon générale, à la conservation de ses données.

4.19.3 - Dans le cas d'un paiement unique, l'Accepteur s'engage à :
- respecter les règles relatives au traitement des données à caractère personnel liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2018-303 du 6 septembre 2018,
- ne pas conserver des données à caractère personnel ou liées à l'utilisation de la Carte au-delà du temps nécessaire à la transaction commerciale.

L'Accepteur s'engage à respecter ces dispositions ainsi que l'ensemble de la Règlementation Relative à la Protection des Données à Caractère Personnel, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ses obligations légales et réglementaires par l'Accepteur.

4.19.4 - Le titulaire de la Carte peut enregistrer les données liées à sa Carte dans des environnements digitaux marchands (exemples : sites de e-commerce, applications mobiles) en particulier pour des paiements récurrents et/ou échelonnés. Ces données liées à la Carte se substituent aux données sensibles de la Carte et sont conservées sous la forme de jetons, liés à des appareils et à un domaine d'usage spécifique, qui sont utilisés à des fins de paiement (le ou les "Token(s)"). Chaque Token a un numéro unique, et peut être activé ou désactivé indépendamment de la Carte.

Si l'Accepteur conserve les données liées à la Carte sous forme d'un Token et sous réserve de disponibilité du service auprès de l'Acquéreur, ce Token peut être mis à jour automatiquement en cas de renouvellement de la Carte physique. Des paiements par Carte pourront ainsi continuer à être effectués chez l'Accepteur, sans que le titulaire de la Carte n'ait à renseigner les données de sa nouvelle Carte physique au lieu et place des données de la Carte physique qu'il avait initialement enregistrées.

Dans le cas où l'Accepteur souhaite bénéficier via l'Acquéreur auprès du Schéma concerné de la mise à jour des données liées à la Carte de ses clients ou des Tokens associés (alias des données liées à la carte précitées) par exemple en cas de renouvellement de la Carte, il s'engage à :
- recueillir le consentement explicite, libre et spécifique du titulaire de la Carte pour la mise à jour des données précitées, en veillant à ce que ce dernier reçoive une information préalable et exhaustive à cet effet,
- 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,
- respecter les règles relatives au traitement des données à caractère personnel liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2018-303 du 6 septembre 2018,
- ne plus procéder à cette mise à jour dès lors que le titulaire de la Carte a retiré son consentement spécifique à cet usage ou, de façon générale, à la conservation de ses données.

L'Accepteur s'engage à respecter ces dispositions ainsi que l'ensemble de la Règlementation Relative à la Protection des Données à Caractère Personnel, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ses obligations légales et réglementaires par l'Accepteur.

4.20 - Informer dans les meilleurs délais l'Acquéreur en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies.

4.21 - 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 10 des Conditions Générales.

4.22 - Garantir l'Acquéreur, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées au présent article.

ARTICLE 5 - Obligations de l'Acquéreur

L'Acquéreur s'engage à :

5.1 - Fournir à l'Accepteur, selon les choix qu'il exprime, les informations le concernant directement sur le fonctionnement du(des) Schéma(s) sélectionné(s) dans les Conditions Particulières et son (leur) évolution, les Catégories de Cartes et les Marques acceptées par lui, les frais applicables à chacune des Catégories de Cartes et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

5.2 - Mettre à la disposition de l'Accepteur les informations relatives aux procédures de sécurisation des opérations de paiement.

Dans le cas où l'Accepteur a souscrit à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, fournir à l'Accepteur les informations sur les procédures applicables à l'acceptation des paiements à distance sécurisés référencées par les Schémas, que l'Accepteur doit utiliser obligatoirement, ainsi que leurs évolutions éventuelles. Ces informations figurent dans le contrat de service relatif à cette offre.

5.3 - Respecter le choix de la Marque et de la Catégorie de Carte utilisés pour le paiement au point d'acceptation conformément au choix de l'Accepteur, sauf avis contraire du titulaire de la Carte.

5.4 - Fournir à l'Accepteur la liste et les caractéristiques des Cartes (Marques et Catégories de Carte) pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

5.5 - Indiquer et facturer à l'Accepteur les commissions à acquitter, séparément pour chaque Catégorie de Carte et chaque Marque selon les différents niveaux d'interchange.

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

5.6 - Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les conditions du Présent Contrat.

5.7 - 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 de dépôt auquel la Carte est rattachée.

5.8 - Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois, les informations suivantes pour la période écoulée :
- 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 le montant de la commission d'interchange.

L'Accepteur peut demander que ces informations relatives aux opérations exécutées soient regroupées par Marque, application de paiement, Catégorie de Carte et par taux de commission d'interchange applicable à l'opération de paiement.

5.9 - Communiquer chaque début d'année un relevé dit Relevé Annuel des Frais d'Encaissement par Carte (RAFEC), qui récapitule pour l'année écoulée les frais du (des) Schéma(s), les commissions de service payées par l'Accepteur et les commissions d'interchange par Marque et Catégorie de Carte.

ARTICLE 6 : Garantie de paiement

6.1 - Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité, visées dans les Conditions Particulières et leurs annexes, aux articles 4 et 7 des présentes Conditions Générales ainsi qu'aux Conditions Spécifiques à chaque Schéma, sauf en cas :
- de réclamation du titulaire de la Carte qui conteste la réalité même ou le montant de l'opération de paiement,
- d'opération de paiement réalisée au moyen d'une Carte non valide, périmée ou bloquée.

A ce titre, l'Accepteur autorise expressément l'Acquéreur à débiter d'office son compte du montant de toute opération de paiement dont la réalité même ou le montant serait contesté par le titulaire de la Carte.

6.2 - Toutes les mesures de sécurité sont indépendantes les unes des autres. Ainsi, l'autorisation donnée par le système Acquéreur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité.

6.3 - 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 ce, en l'absence de contestation.

6.4 - L'Accepteur autorise expressément l'Acquéreur à débiter d'office son compte du montant de toute opération de paiement non garantie.

ARTICLE 7 : Mesures de sécurité

7.1 - La procédure de sécurisation de paiement à distance consiste en l'authentification 3D Secure du titulaire de la Carte conformément aux spécifications établies par les Schémas (« *Protocole 3D Secure* »).

L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme techniques e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que son offre de plateforme de services techniques e-commerce inclut l'authentification 3D Secure du titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

7.2 - L'Accepteur doit informer immédiatement 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, dysfonctionnements du Système d'Acceptation...).

L'Accepteur doit coopérer avec l'Acquéreur lorsqu'il stocke, traite ou transmet des données de paiement sensibles, en cas d'incident de sécurité de paiement majeur ou de compromission de données.

7.3 - Lors du paiement, l'Accepteur s'engage à :

7.3.1 - Appliquer la procédure de sécurisation des ordres de paiement à distance évoquée en avertissement ainsi qu'à l'article 7.1 des présentes Conditions Générales.

7.3.2 - Obtenir de l'Acquéreur un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.

7.3.3 - Vérifier l'acceptabilité de la Carte c'est-à-dire :
- le cas échéant, la période de validité (fin et éventuellement début),
- la Marque du Schéma qui doit être l'une de celles choisies dans les Conditions Particulières.

7.3.4 - Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par l'Acquéreur.

7.3.5 - Obtenir une autorisation d'un montant identique à l'opération. Une opération pour laquelle l'autorisation a été refusée par le système Acquéreur d'autorisation n'est jamais garantie.

7.4 - Après le paiement, l'Accepteur s'engage à :

7.4.1 - Transmettre les enregistrements des opérations de paiement à l'Acquéreur dans le délai maximum de trois (3) jours calendaires à compter de la date de l'opération de paiement. Au-delà de ce délai, les opérations de paiement ne seront réglées que sous réserve de bonne fin d'encaissement.

S'assurer que les opérations de paiement ont bien été imputées au compte dans les délais et selon les modalités prévus dans les Conditions Particulières.

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 signataire du Présent Contrat doit être obligatoirement remise à ce dernier.

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

7.4.3 - Communiquer, à la demande de l'Acquéreur, tout justificatif des opérations de paiement dans les huit (8) jours calendaires à compter de la date de la demande présentée par l'Acquéreur. Si l'Accepteur ne communique pas le justificatif, ou le communique au-delà du délai ci-dessus, il s'expose à un impayé.

7.4.4 - Ne pas stocker, sous quelque forme que ce soit, le cryptogramme visuel des Cartes.

7.4.5 - Prendre toutes les précautions utiles 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 de paiement par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux prescriptions de la Règlementation relative à la protection des données à caractère personnel.

7.4.6 - Les mesures de sécurité et de prévention des risques énumérées au présent article pourront être modifiées et complétées pendant toute la durée du Présent Contrat, selon la procédure prévue à l'article 9.

ARTICLE 8 - Mesures de prévention et de sanction prises par l'Acquéreur

8.1. Avertissement

8.1.1 - 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 un avertissement valant mise en demeure précisant les mesures à prendre pour remédier au manquement constaté ou résorber le taux d'impayés anormalement élevé.

8.1.2 - Si 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, soit résilier de plein droit avec effet immédiat le Présent Contrat dans les conditions précisées aux articles 8.2 et 10 des présentes Conditions Générales.

8.2. - Suspension de l'acceptation

8.2.1 - 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. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut s'accompagner d'un avertissement, voire d'une réduction du seuil de demande d'autorisation de l'Accepteur.

La suspension ne porte pas préjudice à la faculté des Parties de résilier le Contrat conformément à la procédure visée à l'article 10 des présentes Conditions Générales. Notamment, l'Accepteur pourra, en cas de suspension, résilier le Contrat avec effet immédiat.

8.2.2 - La suspension peut être décidée en raison notamment :

- d'un ou plusieurs manquement(s) aux clauses du Contrat et notamment aux exigences sécuritaires, qui serait(ent) révélé(s) au terme de la procédure d'audit visée à l'article 4 des présentes Conditions Générales ;
- 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,
- 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 de la (des) Marque(s) et/ou Catégorie(s) de Carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,
- de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
- du retard volontaire ou non motivé de transmission des justificatifs,
- d'un risque aggravé en raison des activités de l'Accepteur,
- du non-respect, le cas échéant, des dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte.

8.2.3 - L'Accepteur s'engage alors à restituer à l'Acquéreur, le cas échéant, 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 concernées.

8.2.4 - La période de suspension peut s'étendre sur une période de six (6) mois, 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 en paiement de proximité par Cartes avec un autre acquéreur de son choix.

8.2.5 - A tout moment, l'Accepteur peut présenter ses observations sur la suspension.

ARTICLE 9 : Modifications du Contrat

9.1 - L'Acquéreur peut modifier à tout moment les dispositions du Contrat, après en avoir informé l'Accepteur avant la date d'entrée en vigueur des nouvelles dispositions.

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, si celui-ci est mis à disposition par l'Acquéreur, suite à un dysfonctionnement.
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptabilité de Cartes portant certaines Marques.

9.2 - Les nouvelles conditions entrent en principe 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 tout autre support durable.

9.3 - Ce délai peut exceptionnellement être réduit en cas de modification(s) motivée(s) par des raisons sécuritaires, notamment lorsque l'Acquéreur constate dans le point d'acceptation une utilisation anormale de Cartes perdues, volées ou contrefaites.

9.4 - Dans les délais visés au présent article, l'Accepteur peut résilier le Présent Contrat s'il refuse les modifications opérées, dans les conditions prévues à l'article 10 des présentes Conditions Générales. A défaut de résiliation dans ces délais, les modifications lui seront opposables.

9.5 - Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la suspension de l'acceptation des Cartes du Schéma concerné voire la résiliation du pPésent Contrat par l'Acquéreur, selon les dispositions prévues à cet effet aux articles 8.2 et 10 des présentes Conditions Générales, et aux Conditions Spécifiques du Schéma concerné.

ARTICLE 10 : Durée et résiliation du Contrat

10.1 - Le présent Contrat est conclu pour une durée indéterminée, sauf accord contraire des Parties.

10.2 - L'Accepteur ou l'Acquéreur peuvent chacun, et à tout moment, sans justificatif, 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 à l'autre Partie d'une lettre recommandée avec demande d'avis de réception.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 9 des présentes Conditions Générales, elle prendra effet à l'issue du délai visé à cet article pour l'entrée en vigueur des modifications.

Lorsque cette résiliation fait suite à une cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, elle prend effet immédiatement.

Lorsque la résiliation intervient à la demande d'un Schéma ou de l'Acquéreur lui-même, pour des raisons de sécurité ou de fraude, notamment pour l'une des raisons visées aux articles 4 et 7 des présentes Conditions Générales, elle pourra prendre effet immédiatement. Selon la gravité des faits concernés, cette résiliation immédiate peut intervenir à la suite d'un avertissement et d'une mesure de suspension de l'acceptation prévus à l'article 8 des présentes Conditions Générales.

10.3 - En cas de résiliation, l'Accepteur garde la faculté d'accepter les Cartes de tout Schéma avec tout autre Acquéreur de son choix.

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

10.4 - L'Accepteur sera tenu de restituer à l'Acquéreur les dispositifs techniques et sécuritaires, le Système d'Acceptation et les documents en sa possession dont l'Acquéreur est propriétaire.

Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation, l'Accepteur s'engage à retirer immédiatement de son point d'acceptation et de ses supports de communication tout signe d'acceptation des Cartes, ou Marques des Schémas concernés.

ARTICLE 11 - Modalités annexes de fonctionnement

11.1 - Réclamation

Toute réclamation de l'Accepteur doit être justifiée et 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.

Toutefois, ce délai est réduit à quinze (**15) jours calendaires** à compter de la date de débit en compte, en cas d'opération non garantie, notamment en cas d'impayé.

11.2 - 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 produits par l'Acquéreur ou le Schéma prévaudront sur ceux produits 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 dont les Cartes sont concernées.

11.3 - Remboursement ou Transaction crédit

Le remboursement partiel ou total d'un achat d'un bien ou d'un service réglé par Carte doit, avec l'accord de son titulaire, être effectué avec les données de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de "Transaction crédit" en effectuant, dans le délai prévu par l'article 4 des présentes Conditions Générales, la remise de la "Transaction crédit" 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.

ARTICLE 12 : Secret bancaire et protection des données à caractère 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 du Contrat, chacune des Parties peut avoir accès à des données à caractère personnel.

En application de la Règlementation Relative à la Protection des Données à Caractère Personnel, il est précisé que les informations relatives à l'Accepteur, collectées par l'Acquéreur nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des opérations de paiement par Carte, données en exécution du Présent Contrat, ou pour répondre aux obligations légales et réglementaires, l'Acquéreur étant à cet effet, de convention expresse, délié du secret bancaire.

Dans le cadre de la signature et de l'exécution du Présent Contrat, et plus généralement de la relation entre l'Acquéreur et l'Accepteur, personne physique, ou la personne physique le représentant, l'Acquéreur recueille et traite, en tant que responsable de traitement, des données à caractère personnel concernant l'Accepteur et/ou la personne physique le représentant.

Ces traitements ont pour finalités :
- la gestion de la relation commerciale pour l'exécution du Présent Contrat,
- la lutte contre la fraude, le blanchiment de capitaux et le financement du terrorisme.

Ces traitements sont obligatoires. A défaut, l'exécution du Contrat ne pourrait être assurée et l'Acquéreur ne serait en mesure de respecter ses obligations règlementaires.

Les informations expliquant pourquoi et comment ces données sont utilisées, combien de temps elles seront conservées, ainsi que les droits dont l'Accepteur et/ou son représentant disposent quant à leur usage par l'Acquéreur, figurent dans la notice d'information sur le traitement des données à caractère personnel de l'Acquéreur (la "Notice").

Cette Notice est portée à la connaissance de l'Accepteur lors de la première collecte de ses données et/ou de celles de son représentant.

L'Accepteur et/ou son représentant peuvent y accéder à tout moment sur le site internet de l'Acquéreur ou en obtenir un exemplaire auprès d'une agence de l'Acquéreur.

L'Accepteur s'engage à informer son représentant de cette collecte de données et des droits dont il dispose en vertu de la Règlementation Relative à la Protection des Données à Caractère Personnel et du présent article. Il s'engage également à l'informer de l'existence de la Notice et des modalités pour y accéder.

A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant les titulaires de Carte, à savoir notamment le numéro de la Carte, le cryptogramme visuel et le cas échéant, l'identité du Titulaire de la Carte, sa date de fin de validité sans que cette liste soit exhaustive, dont il doit garantir la sécurité et la confidentialité conformément aux dispositions du Présent Contrat et à la Règlementation Relative à la Protection des Données à Caractère Personnel.

Dans le cadre du Présent Contrat, 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 admises par la CNIL dans sa délibération de n°2018-303 du 6 septembre 2018 portant 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.

12.3 - Prospection commerciale

En tant que responsable de traitement au sens de la Règlementation Relative à la Protection des Données à Caractère Personnel lorsqu'il traite les données personnelles de ses clients et notamment des titulaires de Carte, l'Accepteur doit respecter les obligations prévues par la Règlementation Relative à la Protection des Données à Caractère Personnel, et notamment les principes de licéité, de loyauté et de transparence des traitements, les droits des personnes et la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer la confidentialité et l'intégrité des données à caractère personnel qu'il est amené à traiter dans le cadre de son activité et notamment, celles des titulaires de Carte, sous peine d'engager sa seule responsabilité.

12.3 - Les dispositions de l'article L.34-5 du Code des postes et des communications électroniques obligent l'Accepteur à recueillir le consentement exprès et préalable du titulaire de Carte lors de toute utilisation de ses données de contact (notamment, son adresse mail et de son numéro de mobile) à des fins de prospection commerciale.

L'Accepteur s'engage à chaque envoi d'une nouvelle proposition commerciale à informer le titulaire de la Carte de sa possibilité de se désabonner et des modalités y afférentes. L'Accepteur s'engage enfin à respecter ces dispositions et à supprimer de ses propres bases de données, les données personnelles du titulaire de la Carte relatives à la prospection commerciale si ce dernier en fait la demande auprès de l'Accepteur, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ces obligations légales et réglementaires par l'Accepteur.

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 compétents

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 Contrat

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

ARTICLE 16 : Confidentialité

Aucune des Parties ne communiquera d'information et ne publiera de communiqué en relation avec l'existence des Conditions Générales, Particulières et Spécifiques, et de leurs annexes ou leur contenu sans l'accord préalable de l'autre Partie, sauf si la communication de l'information ou la publication du communiqué est rendue obligatoire par une disposition légale ou règlementaire s'imposant à la Partie concernée, ou pour répondre à une demande d'une autorité judiciaire ou administrative (gouvernementale, bancaire, fiscale ou autre autorité réglementaire similaire).

PARTIE II. Conditions Spécifiques d'acceptation en paiement à distance sécurisé propres à chaque Schéma

PARTIE II. 1. Conditions spécifiques pour les opérations réalisées selon le Schéma "CB"

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles du Schéma "CB".

ARTICLE 1 : Conditions liées à la garantie de paiement des opérations de paiement "CB"

La garantie de paiement est conditionnée par le respect des conditions prévues au Présent Contrat.

Le montant du seuil de demande d'autorisation pour une opération de paiement "CB", par jour et par point d'acceptation, au jour de la signature du Contrat est fixé dans les Conditions Particulières. Ce montant peut être modifié ultérieurement.

Ce montant ne s'applique pas aux Cartes pour lesquelles une autorisation doit être demandée à chaque opération de paiement dès le 1er euro.

ARTICLE 2 : Délai maximum de transmission des opérations de paiement "CB" à l'Acquéreur

L'Accepteur s'engage à transmettre à l'Acquéreur les opérations de paiement réalisées selon les règles du Schéma "CB" dans un délai maximum de **6 mois**. Au-delà de ce délai maximum, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma "CB".

Ce délai de 6 mois est un délai distinct du délai conditionnant la Garantie de paiement prévu aux articles 6 et 7 des Conditions Générales.

ARTICLE 3 : Litiges commerciaux

L'Accepteur s'engage à faire son affaire personnelle de tous litiges de nature commerciale ou autre, ou/et de leurs conséquences financières, pouvant survenir avec des clients, adhérents ou donateurs, concernant des biens et services, cotisations ou dons ayant été réglés par Carte au titre du Présent Contrat.

ARTICLE 4 : Suspension et clôture du contrat pour le Schéma "CB"

4.1 - Le Schéma "CB" 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 du Schéma "CB". Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat. Elle peut être décidée en raison notamment :

- d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'une utilisation d'un Système d'Acceptation non agréé,
- d'un risque de dysfonctionnement important du Schéma "CB",
- en cas de comportement frauduleux de la part de l'Accepteur responsable du point d'acceptation.

4.2 - L'Accepteur s'engage alors à restituer, le cas échéant, à l'Acquéreur le Système d'Acceptation, les dispositifs techniques et sécuritaires du Schéma "CB" et les documents en sa possession dont l'Acquéreur est propriétaire, et à retirer immédiatement de son point d'acceptation tout signe d'acceptation des Cartes "CB" ou de la Marque "CB".

4.3 - La période de suspension est au minimum de 6 mois, éventuellement renouvelable.

4.4 - A l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du Schéma "CB", demander la reprise d'effet du Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation avec un autre Acquéreur de son choix.

4.5 - En cas de comportement frauduleux de la part de l'Accepteur, il peut être immédiatement radié du Schéma "CB" ou la suspension être convertie en radiation.

ARTICLE 5 : Communication des Commissions Interbancaires de Paiement (interchange) de "CB"

Les taux de commissions interbancaires pratiqués par le Schéma "CB" sont publics et consultables sur son site internet du Schéma "CB", http://www.cartes-bancaires.com/.

ARTICLE 6 : Protection des données à caractère 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" (intérêt légitime) ;
- de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte (obligation légale).

Le détail des données personnelles traitées par le GIE "CB", de leurs durées de conservation, des destinataires de ces données et des mesures de sécurités mises en œuvre pour les protéger, peut être consulté dans sa politique de protection des données personnelles accessible à www.cartes-bancaires.com/protegezvosdonnees.

Pour exercer les droits prévus en application de la Règlementation Relative à la Protection des Données à Caractère Personnel, et notamment les droits d'accès, de rectification et d'effacement des données ainsi que les droits d'opposition et de limitation du traitement, l'Accepteur (personne physique ou personne physique le représentant) peut contacter le Délégué à la protection des données du Schéma "CB" 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 également contacter son Délégué à la protection des données désigné par le GIE "CB" par courriel à protegezvosdonnees@cartes-bancaires.com.

PARTIE II.2 Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas "Visa"," Visa Electron" ou "VPAY"

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles des Schémas "Visa", "Visa Electron" ou "VPAY".

ARTICLE 1 : Conditions liées à la garantie de paiement des opérations de paiement "Visa", "Visa Electron" ou "VPAY"

La garantie de paiement est conditionnée par le respect des conditions du Présent Contrat.

Seuil d'autorisation : quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas "Visa", "Visa Electron" ou "VPAY", que ce soit une carte étrangère ou française, qu'elle soit co-badgée avec un autre Schéma ou non.

ARTICLE 2 : Suspension ou clôture du contrat à la demande des Schémas "Visa", "Visa Electron" ou "VPAY"

Les Schémas "Visa", "Visa Electron" ou "VPAY" peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas "Visa", "Visa Electron" ou "VPAY", faute de quoi l'Acquéreur sera dans l'obligation de résilier le Présent Contrat.

ARTICLE 3 : Acceptation des Cartes "Visa", "Visa Electron" ou "VPAY" émises hors UE

Les Cartes des Schémas "Visa", "Visa Electron" ou "VPAY" émises par un émetteur situé hors de l'UE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas Visa, "Visa", "Visa Electron" ou "VPAY".

ARTICLE 4 : Communication des Commissions Interbancaires de Paiement (interchange) de "Visa", "Visa Electron" ou "VPAY"

Les taux de commissions d'interchange pratiqués par les Schémas "Visa", "Visa Electron" ou "VPAY" sont publics et consultables sur le site internet : www.visa-europe.fr.

PARTIE II.3 Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas "Mastercard" ou "Maestro"

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles des Schémas "Mastercard" ou "Maestro".

ARTICLE 1 : Conditions liées à la garantie de paiement des opérations de paiement « Mastercard » ou « Maestro »

La garantie de paiement est conditionnée par le respect des conditions prévues au Présent Contrat.

Seuil d'autorisation : quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas "Mastercard" ou "Maestro".

ARTICLE 2 : Suspension ou clôture du contrat à la demande des Schémas "Mastercard" ou "Maestro"

Les Schémas "Mastercard" ou "Maestro" peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas "Mastercard" ou "Maestro", faute de quoi l'Acquéreur sera dans l'obligation de résilier le Présent Contrat.

ARTICLE 3 : Acceptation des Cartes "Mastercard" ou "Maestro" émises hors Union Européenne

Les Cartes des Schémas "Mastercard" ou "Maestro" émises par un émetteur situé hors de l'UE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas "Mastercard" ou "Maestro" émise dans l'Union Européenne.

ARTICLE 4 : Communication des Commissions Interbancaires de Paiement (interchange) de "Mastercard" ou "Maestro"

Les taux de commissions d'interchange pratiqués par les Schémas "Mastercard" ou "Maestro" sont publics et consultables sur le site internet : www.mastercard.com

ANNEXE 4 – Informations sur les commissions d'interchanges et frais de Schéma

** Hors UE, les interchanges restent inchangés (non impactés par le Règlement) ; les taux indiqués ici sont des taux moyens constatés.*

Canal d'acquisition	Schéma de paiement de la transaction	Marque de la transaction	Catégorie de carte ayant réaliséé la transaction	Interchange depuis le 08 Déc. 2016	Scheme Fee moyen du schéma de paiement de la transaction 2018
Paiement de proximité	CB	CB	Carte de débit	0,20%	0,00110 €
			Carte de crédit	0,30%	0,00110 €
			Carte commerciale	0,90%	0,00110 €
			Cartes hors UE *		
	VISA	VISA	Carte de débit UE	0,20%	0,0100%
			Carte de crédit UE	0,30%	0,0140%
			Carte commerciale UE / Business DD	1,30%	0,0140%
			Carte commerciale UE / Corporate DD	1,35%	0,0140%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,4600%
			Cartes de crédit hors UE * particulier	1,60%	0,4640%
			Cartes de débit hors UE * commerciale	2,00%	0,4600%
			Cartes de crédit hors UE * commerciale	2,00%	0,4640%
		VISA ELECTRON	Carte de débit UE	0,20%	0,0100%
			Carte de crédit UE	0,30%	0,0140%
			Carte commerciale UE	1,35%	0,0140%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,4600%
			Cartes de crédit hors UE * particulier	1,60%	0,4640%
			Cartes de débit hors UE * commerciale	2,00%	0,4600%
			Cartes de crédit hors UE * commerciale	2,00%	0,4640%
		VPAY	Carte de débit UE	0,15 €	0,0100%
			Carte non régulée UE		
	MASTERCARD	MASTERCARD	Carte de débit UE	0,20%	0,0164%
			Carte de crédit UE	0,30%	0,0164%
			Carte commerciale UE / Business	1,65%	0,0164%

			Carte commerciale UE / Corporate	1,90%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,3664%
			Cartes hors UE * commerciale	2,00%	0,3664%
		MAESTRO	Carte de débit	0,20%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,3664%
			Cartes hors UE * commerciale	2,00%	0,3664%
	DFS	DFS	Carte de débit UE (Diners' Club)	0,20%	0,15%
			Carte de crédit UE (Diners'Club)	0,30%	0,15%
			Carte Commerciale	1,75%	0,15%
			Carte hors UE *	1,50%	0,15%
	UP	UP	Carte de débit UE		
			Carte de crédit UE		
			Carte hors UE *	1,20%	

Canal d'acquisition	Schéma de paiement de la transaction	Marque de la transaction	Catégorie de carte ayant réalisé la transaction	Interchange depuis le 08 Déc. 2016	Scheme Fee moyen du schéma de paiement de la transaction
E-commerce	CB	CB	Carte de débit	0,20%	0,00110 €
			Carte de crédit	0,30%	0,00110 €
			Carte commerciale	0,90%	0,00110 €
			Carte non régulée		
			Cartes hors UE *		
	VISA	VISA	Carte de débit UE	0,20%	0,020%
			Carte de crédit UE	0,30%	0,024%
			Carte commerciale UE / Business DD	1,30%	0,024%
			Carte commerciale UE / Corporate DD	1,35%	0,024%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,5600%
			Cartes de crédit hors UE * particulier	1,60%	0,5640%
			Cartes de débit hors UE * commerciale	2,00%	0,5600%
			Cartes de crédit hors UE * commerciale	2,00%	0,5640%
		VISA ELECTRON	Carte de débit	0,20%	0,020%
			Carte de crédit UE	0,30%	0,024%
			Carte commerciale	1,35%	0,024%

			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,5600%
			Cartes de crédit hors UE * particulier	1,60%	0,5640%
			Cartes de débit hors UE * commerciale	2,00%	0,5600%
			Cartes de crédit hors UE * commerciale	2,00%	0,5640%
		VPAY	Carte de débit UE	0,15 €	0,020%
			Carte non régulée UE		
	MASTERCARD	MASTERCARD	Carte de débit	0,20%	0,0164%
			Carte de crédit UE	0,30%	0,0164%
			Carte commerciale UE / Business	1,65%	0,0164%
			Carte commerciale UE/ Corporate	1,90%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,3664%
			Cartes hors UE * commerciale	2,00%	0,3664%
		MAESTRO	Carte de débit	0,20%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,3664%
			Cartes hors UE * commerciale	2,00%	0,3664%

ANNEXE 5 - Référentiel Sécuritaire 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 des titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.

En particulier, un responsable de la sécurité du système commercial et d'acceptation doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et du secret bancaire dans le cadre de leur utilisation et de leur environnement.

Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.

Le contrôle du respect des exigences de sécurité relatives au système commercial et d'acceptation doit être assuré.

Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

Exigence 2 (E2)
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 du titulaire de la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.

Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.

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

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL.

Il en est de même pour l'authentifiant de l'Accepteur et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15)
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.