BANQUE POPULAIRE
AUVERGNE RHÔNE ALPES

CONDITIONS GENERALES

CONTRAT ACCEPTEUR CB – PAIEMENT VENTE A DISTANCE INTERNET HORS CYBERPLUS PAIEMENT

Société Anonyme Coopérative de Banque Populaire à capital variable, régie par les articles L512-2 et suivants et du Code Monétaire et Financier et l'ensemble des textes relatifs aux Banques Populaires et aux établissements de crédit – Siren 605 520 071 RCS Lyon - Intermédiaire d'assurance N° ORIAS : 07 006 015- Siège social : 4, boulevard Eugène Deruelle – 69003 LYON N° TVA intracommunautaire : FR 00605520071

BANQUE POPULAIRE
AUVERGNE RHÔNE ALPES

CONDITIONS GÉNÉRALES D'ADHÉSION AU SYSTÈME DE PAIEMENT A DISTANCE SECURISE PAR CARTES "CB" OU AGRÉÉES "CB"

Préambule

Le GIE "CB"

Compte tenu de l'essor économique du commerce électronique et plus généralement de la vente à distance, de la nécessité de ne pas laisser les risques de fraude entraver cet essor et de la législation visant à faciliter cet essor notamment en prévoyant des obligations d'informations au profit des consommateurs et en facilitant l'administration de la preuve sur support électronique, le GIE "CB" a souhaité proposer un mode de paiement à distance sécurisé par carte "CB" et agréées "CB".

Pour éviter, dans la mesure du possible, que des tiers non autorisés accèdent aux données relatives aux paiements, des précautions particulières de sécurisation méritent d'être prises. Le GIE "CB", conscient de ces besoins de sécurisation, a souhaité limiter les hypothèses de communication à un tiers par le porteur de son seul numéro de carte bancaire que ce soit par téléphone, par fax, par courrier postal ou par l'utilisation de moyens électroniques de communication, et a autorisé la mise en place de procédures de sécurisation des ordres de paiement donné à distance par les porteurs de cartes "CB" ou agréées "CB" telle que 3Dsecure.

Le GIE "CB" établit les présentes Conditions Générales, la Banque Acquéreur "CB" définissant les Conditions Particulières visées en Annexe 2 et les conditions spécifiques relatives à l'utilisation du dispositif technique qu'elle a proposé et convenu avec son client.

Lorsque la Banque Acquéreur "CB" représente le GIE "CB", le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation d'une carte "CB" et de cartes agréées "CB" et de remise des transactions à la Banque Acquéreur "CB", et non la mise en jeu de la garantie visée à l'article 4 des Conditions Générales.

L'Accepteur "CB"

L'Accepteur "CB" utilisant des moyens électroniques OU NON pour vendre à distance des biens et des services et notamment en utilisant Internet, souhaite recevoir des paiements à distance sécurisés en contrepartie d'actes de vente ou de fournitures de prestation de service qu'il réalise lui même.

L'Accepteur "CB" a été 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 4 des Conditions Générales.

Il déclare connaître les lois et règlements applicables aux ventes et achats à distance et notamment aux échanges utilisant les réseaux électroniques et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…). Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et qu'il doit commercialiser les produits ou services faisant l'objet d'un paiement à distance sécurisé en respectant les lois et règlements applicables, notamment fiscaux.

A la lumière de ces éléments, l'Accepteur "CB" a souhaité adhérer et être soumis au présent Contrat.

ARTICLE 1 - OBJET

Les présentes ont pour objet de déterminer les conditions d'adhésion au mode de paiement sécurisé à distance "CB".

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR "CB"

L'Accepteur "CB" s'engage à :

2.1. Utiliser les procédures de sécurisation des ordres de paiement donnés à distance par les porteurs de cartes "CB" et agréés "CB" , dans le respect des dispositions légales, réglementaires et professionnelles applicables, notamment et sans limitation des dispositions relatives aux ventes et prestations réalisées à distance et au commerce électronique (informations des utilisateurs, délais d'exécution des prestations…) ainsi que des bonnes pratiques commerciales telles que définies notamment par les codes de Conduite que la Banque Acquéreur a portés à la connaissance de l'Accepteur "CB".

Utiliser le Système de Paiement à Distance Sécurisé en s'abstenant de toute activité qui pourrait être pénalement sanctionnée option : (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 de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non respect des dispositions relatives aux jeux de hasard, aux courses de chevaux, aux loteries et des dispositions relatives aux conditions d'exercice de professions réglementées …).

2.12 Utiliser obligatoirement les procédures de sécurisation des ordres de paiement donnés à distance par les porteurs de cartes « CB » et agréées « CB »

2.2 Garantir la Banque Acquéreur "CB" et le GIE "CB" le cas échéant, contre toute incidence dommageable pouvant résulter pour elle du manquement aux obligations visées à l'article 2.1.

2.3 Indiquer clairement ses coordonnées (dénomination commerciale, RCS, représentant légal…), de telle sorte que le Porteur "CB" n'ait pas de difficulté à vérifier les opérations de paiement qu'il a effectuées,

2.4 Vérifier avec la Banque Acquéreur "CB" la conformité des informations transmises pour identifier son point de vente lors de son adhésion au Système de Paiement à Distance Sécurisé et distinguer les modes de paiement utilisé (automate, vente à distance, vente de proximité) dans ce point de vente et isoler le Paiement à Distance Sécurisé.

2.5 Accepter les Cartes "CB" et les cartes agréées "CB" pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toutes délivrances d'espèces ou de tous titres convertibles en espèces pour leur valeur faciale), auquel le porteur a effectivement et expressément consenti, même lorsqu'il s'agit d'articles vendus ou de prestations fournies à titre de promotion ou de soldes. En outre l'Accepteur s'interdit de collecter des paiements dus à raison de ventes ou de prestations réalisées par d'autres commerçants ou prestataires avec leur propre clientèle.

2.6 Appliquer aux titulaires de Cartes "CB" et de cartes agréées "CB", les mêmes prix qu'à l'ensemble de sa clientèle. En tout état de cause, ne faire supporter, directement ou indirectement, aucun frais supplémentaire au Porteur "CB", du seul fait qu'il utilise sa Carte "CB" comme mode de paiement.

2.7 Afficher visiblement, sur le dispositif permettant la transaction notamment à l'écran du dispositif technique utilisé par le porteur "CB" et sur ses supports de communication, le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Porteur "CB" en soit préalablement informé. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes "CB".

2.8 Signaler au public l'acceptation des Cartes "CB" et des cartes agréées "CB" de façon apparente par affichage, notamment sur l'écran du dispositif technique utilisé par le porteur "CB" et sur ses supports de communication conformément à la charte graphique "CB" en vigueur.

Afficher visiblement sur tout support de l'offre de vente à distance et notamment à l'écran du dispositif technique utilisé par le porteur "CB" le prix du produit et/ou du service fourni, ainsi que la devise dans laquelle ce prix est libellé, et ce, notamment de façon à ce que le porteur "CB" ne soit pas en mesure de croire que le prix était autre.

Régler, selon les Conditions Particulières, les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du mode de paiement sécurisé à distance par carte "CB" et agréée "CB".

Faire son affaire personnelle des litiges commerciaux avec les Porteurs "CB", notamment lors de l'exercice par le porteur de son droit de rétractation.

2.12 Utiliser obligatoirement les moyens techniques proposés par la Banque Acquéreur « CB ».

2.13 Adhérer aux bons usages de la profession de la vente à distance correspondant à minima aux principes figurant en annexe du présent Contrat et les mettre en œuvre, comme notamment Paiement Card Industry (PCI), Data Security Standard (DSS).

Le GIE "CB" et/ou la Banque Acquéreur se réserve(nt) le droit de faire procéder aux frais de l'Accepteur "CB" dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect des bons usages de la profession (ci-après "l'Audit"), à tout moment lors de la conclusion du Contrat et/ou pendant la durée du Contrat.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'Audit révélerait un ou plusieurs manquements aux bons usages de la profession, le GIE "CB" et/ou la Banque Acquéreur peuvent mettre en œuvre les mesures prévues à l'article 8.

ARTICLE 3 - OBLIGATIONS DE LA BANQUE ACQUÉREUR "CB"

La Banque Acquéreur "CB" s'engage à :

3.1 Fournir, à l'accepteur "CB" les informations sur le ou les moyens sécurisés d'Acceptation des Paiements à Distance référencés par le GIE "CB" que l'Accepteur doit utiliser obligatoirement. Ces informations figurent en annexe 3.

Inscrire l'Accepteur "CB" dans la liste des points de vente habilités à recevoir des paiements par cartes de porteurs "CB" et agréés "CB" dûment authentifiés.

Indiquer à l'accepteur "CB" la liste et les caractéristiques de toutes les cartes "CB" ou agréées "CB" par le GIE "CB" pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation.

3.4 Créditer le compte de l'accepteur "CB" des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

3.5 Ne pas débiter, au delà du délai maximum de 6 mois à partir de la date du crédit initial porté au compte de l'Accepteur "CB" les opérations non garanties et qui n'ont pu être imputées au compte du Porteur.

ARTICLE 4 - GARANTIE DU PAIEMENT

4.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées à l'article 4.

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

4.2 L'Accepteur "CB" doit être clairement identifié par le numéro SIRET et le Code NAF que l'INSEE lui a attribués. Le numéro SIRET, identifiant le point de vente, sera celui du siège social de l'Accepteur "CB" ou de celui de l'un de ses établissements qui est habilité par les présentes à recevoir les paiements auquel les clauses du présent Contrat sont opposables.

4.3 Lors du paiement

L'Accepteur "CB" s'engage à :

Appliquer la procédure décrite dans les Conditions Particulières.

4.3.2 Obtenir de la Banque Acquéreur "CB" un justificatif d'Acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.

4.3.3. L'Accepteur "CB" doit informer immédiatement la Banque Acquéreur "CB" en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence de Justificatif d'Acceptation, dysfonctionnement de la relation avec le Gestionnaire de Télépaiement...).

4.4. Après le paiement

L'Accepteur "CB" s'engage à :
4.4.1. Communiquer à la demande de la Banque Acquéreur "CB" et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

4.4.2. Envoyer au Porteur, à sa demande, une facture précisant, entre autres, le mode de paiement par carte "CB".

4.5 Les Mesures de sécurité énumérées aux articles 4.3. et 4.4. ci-dessus, pourront être modifiées et complétées pendant toute la durée du Contrat, selon la procédure prévue à l'article 6.

ARTICLE 5 - Réclamation et convention de preuve

5.1. Réclamation

Toute réclamation de l'Accepteur "CB" doit être formulée par écrit à la Banque Acquéreur "CB" dans un délai maximum de 6 mois à compter de la date de l'opération contestée. Ce délai est réduit à 15 jours calendaires à compter de la date de restitution de l'impayé, dans le cas d'une réclamation relative à un impayé.

5.2. Convention de preuve

De convention expresse entre les parties, les supports électroniques sont réputés constituer au moins des commencements de preuve par écrit. En cas de conflit, les documents électroniques produits par la Banque Acquéreur "CB" ou le GIE "CB" prévaudront sur ceux produits par l'Accepteur "CB", à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par le GIE "CB" ou la Banque Acquéreur "CB".

5.3 Secret bancaire et protection des données à caractère personnel

De convention expresse l'Accepteur "CB" autorise la Banque Acquéreur à communiquer et stocker le cas échéant des données secrètes ou confidentielles portant sur lui à des entités impliquées dans le fonctionnement du système "CB" aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations qu'elles émanent des porteurs de cartes "CB" ou agréées "CB" ou d'autres entités.

ARTICLE 6 - MODIFICATIONS DES DISPOSITIONS DU CONTRAT

6.1 La Banque Acquéreur "CB" peut modifier à tout moment le Contrat, pour des raisons techniques, commerciales ou juridiques.

Les modifications autres que les travaux d'installation et de maintenance si elles n'ont pas de raisons sécuritaires, doivent être mises en œuvre par l'Accepteur "CB" un mois après l'envoi de la lettre de notification par la Banque Acquéreur.
Les modifications sécuritaires concernent notamment :

la modification du seuil de demande d'autorisation
la suppression de l'acceptabilité de certaines Cartes

La Banque Acquéreur "CB" peut modifier à tout moment le contrat pour des raisons liées à l'absence de sécurité présentée par le ou les moyens sécuritaires d'acceptation appliquée par l'Accepteur "CB" notamment en cas de retrait de l'autorisation donnée par le GIE "CB" pour l'utilisation de ce ou ces moyens ou pour la mise en œuvre de nouvelles dispositions sécuritaires.

6.3. Le délai dans lequel les modifications sécuritaires doivent être mises en œuvre par l'Accepteur "CB" est exceptionnellement réduit à cinq jours calendaires notamment lorsqu'il est constaté une utilisation anormale de Cartes "CB" perdues, volées ou contrefaites, exigeant une mesure sécuritaire rapide et motivée telle que notamment la réduction du montant du seuil de demande d'autorisation.

6.4. En cas de suppression de l'acceptabilité de certaines Cartes "CB" ou de suspension de tout ou partie de l'activité de fourniture de moyens sécurisés d'acceptation, les nouvelles dispositions entrent immédiatement en vigueur, à compter de leur date de communication à l'Accepteur "CB", faite par tout moyen, par la Banque Acquéreur "CB".

6.5. Passés les délais visés aux articles 6.1. et 6.3, et après diffusion de l'information visée à l'article 6.4, les modifications sont opposables à l'Accepteur "CB". L'Accepteur "CB" peut résilier le Contrat s'il s'oppose à l'application des nouvelles dispositions.

6.6. Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner outre la suspension de la garantie de paiement, la résiliation du Contrat, voire la suspension de l'adhésion au Système de Paiement à Distance Sécurisé dans les conditions prévues à l'article 8 du Contrat.

ARTICLE 7 - DUREE - RESILIATION DU CONTRAT

7.1. Les présentes sont conclues pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

L'Accepteur "CB" d'une part, la Banque Acquéreur "CB" d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux parties), sous réserve du dénouement des opérations en cours, 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 "CB" garde alors la faculté de continuer à adhérer au mode de paiement à distance sécurisé par carte "CB" ou agrées "CB", en utilisant des moyens sécurisés d'acceptation avec toute autre Banque Acquéreur "CB" de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications des conditions contractuelles, elle ne peut intervenir qu'au-delà du délai prévu dans l'article précédent pour l'entrée en vigueur de ces modifications ou immédiatement en cas d'application de l'article 6.4.

7.2. Toute cessation d'activité de l'Accepteur "CB", 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 Contrat, des impayés apparaîtraient, ils seront à la charge de l'Accepteur "CB".

7.3. En fin de Contrat, l'Accepteur "CB" est tenu de restituer à la Banque Acquéreur "CB" les matériels, dispositifs de sécurité et documents en sa possession dont la Banque Acquéreur "CB" est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'adhésion, l'Accepteur s'engage à supprimer immédiatement de son serveur et de ses supports de communication tout signe d'acceptation des Cartes "CB".

ARTICLE 8 - MESURES DE PREVENTION ET DE SANCTION

8.1 Mesures de prévention et de sanction mises en œuvre par la Banque Acquéreur "CB".

En cas de manquement de l'Accepteur "CB" aux dispositions du Contrat ou aux lois en vigueur ou en cas de constat d'un Taux d'Impayés anormalement élevé ou d'utilisation anormalement élevée de Cartes "CB" perdues, volées ou contrefaites, la Banque Acquéreur "CB" peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur "CB" valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le Taux d'Impayés constaté. Si dans un délai de trente jours, l'Accepteur "CB" n' a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le Taux d'Impayés constaté, la Banque Acquéreur "CB" peut résilier de plein droit avec effet immédiat le Contrat par lettre recommandée avec demande d'avis de réception. De même, si dans un délai de trois mois à compter de l'avertissement, l'Accepteur "CB" est toujours confronté à un Taux d'Impayés anormalement élevé, la Banque Acquéreur "CB" peut décider la résiliation de plein droit avec effet immédiat du Contrat notifiée par lettre recommandée avec demande d'avis de réception.

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

En cas de manquement de l'Accepteur "CB" aux dispositions du Contrat concernant les mesures de sécurité ou en cas de Taux d'Impayés constaté anormalement élevé (notamment dans les hypothèses où l'Accepteur "CB" ventile ses remises en paiement entre plusieurs Banques Acquéreurs de sorte qu'aucune de ces dernières n'est en mesure d'avoir une vision globale du Taux d'Impayés), le GIE "CB" pourra prendre des mesures de sauvegarde et de sécurité consistant en :

la suspension de l'adhésion au Système de Paiement à Distance sécurisé. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de 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 mois au cas où l'Accepteur "CB" aurait déjà fait l'objet d'une mesure de suspension dans les 24 mois précédant l'avertissement ;

- La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux jours francs à compter de la réception de la notification ;

La radiation de l'adhésion au Système de Paiement à Distance Sécurisé 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 "CB" concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception.

8.3. En cas de suspension ou de radiation, l'Accepteur "CB" s'engage alors à restituer à la Banque Acquéreur "CB" les matériels, dispositifs de sécurité et documents en sa possession dont la Banque Acquéreur "CB" est propriétaire et à retirer immédiatement du Serveur Accepteur et de ses supports de vente tout signe d'acceptation des Cartes "CB" ou Agréées "CB".

8.4. La période de suspension est au minimum de 6 mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur "CB" peut, sous réserve de l'accord préalable du GIE "CB", demander la reprise d'effet de son Contrat auprès de la Banque Acquéreur "CB", ou souscrire un nouveau contrat d'adhésion avec une autre banque 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 la Banque Acquéreur et portant sur le respect des bonnes pratiques en matière de vente à distance et des mesures de sécurité visées à l'article 4.

BANQUE POPULAIRE
AUVERGNE RHÔNE ALPES

ARTICLE 9 - PROTECTION DES DONNEES A CARACTERE 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 des articles 32, 38, 39 et 40 de la loi du 6 janvier 1978 relative à la protection des données à caractère personnel, modifiée par la loi du 6 août 2004, il est précisé que :

a) Les informations collectées par la Banque Acquéreur "CB", nécessaires pour l'établissement et l'exécution des présentes, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules nécessités de la gestion des ordres de paiement par carte "CB" et agréées "CB" donnés en exécution du présent Contrat, ou pour répondre aux obligations légales et réglementaires.

La Banque Acquéreur "CB" étant à cet effet, de convention expresse, déliée du secret bancaire.

L'Accepteur "CB" peut avoir accès à différentes données à caractère personnel concernant notamment les porteurs "CB" lors de l'utilisation de moyens sécurisés d'acceptation. L'Accepteur "CB" ne peut utiliser ces données personnelles que pour l'exécution des ordres de paiement par carte "CB" ou agréées "CB". 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 ; il s'assure également de l'existence et de la mise en œuvre de dispositifs de contrôle des accès physiques et logiques à ces données.

Les personnes sur lesquelles portent les données à caractère personnel ci-dessus recueillies ont le droit d'en obtenir communication, le cas échéant d'en exiger la rectification et de s'opposer, pour des motifs légitimes, à ce qu'elles fassent l'objet d'un traitement ou à leur utilisation à d'autres fins que celles citées ci-dessus.

Les Porteurs de cartes "CB" et agrées "CB" sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer desdits droits d'accès, de rectification et d'opposition auprès de l'Accepteur "CB". A cet égard, l'Accepteur "CB" s'engage d'ores et déjà à leur permettre d'exercer ces droits.

Les Accepteurs, personnes physiques, sur lesquelles des données à caractère personnel ont été recueillies disposeront également desdits droits d'accès, de rectification et d'opposition auprès de la Banque acquéreur.

ARTICLE 10 - NON RENONCIATION

Le fait par l'Accepteur ou par la Banque Acquéreur de ne pas exiger à un moment quelconque l'exécution stricte par l'Accepteur ou par la Banque Acquéreur d'une disposition du présent Contrat n'est en aucun cas réputé constituer une renonciation, quelle qu'elle soit , à l'exécution de celle-ci.

ARTICLE 11 - LOI APPLICABLE/TRIBUNAUX COMPETENTS

Le présent Contrat et toutes les questions qui s'y rapportent seront régis par le droit français et tout différend relatif à l'interprétation, la validité, et/ou l'exécution du Contrat sera 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.

CONDITIONS PARTICULIÈRES AUX CONDITIONS GÉNÉRALES D'ADHÉSION AU SYSTÈME DE PAIEMENT À DISTANCE SÉCURISÉ PAR CARTES « CB » OU AGRÉÉES « CB »

Solutions de paiement sécurisé 3 DSecure homologuées PCI / DSS proposées par les prestataires OGONE ou PAY BOX

ANNEXE 2
PREAMBULE
L'Accepteur a signé avec la Banque Acquéreur un contrat d'adhésion au système de paiement à distance sécurisé par cartes bancaires « CB » ou agréées « CB »

Dans le cadre de ce contrat l'Accepteur utilise une solution de paiement sécurisé 3 DSecure proposée par les prestataires OGONE ou Pay BOX pour recevoir des paiements à distance sécurisés par cartes bancaires « CB » ou cartes agréées « CB » en contrepartie d'actes de vente ou de fourniture de service qu'il réalise lui-même. Cette solution doit être conforme PCI / DSS.

ARTICLE 1 : OBJET

Les présentes conditions particulières aux conditions générales d'adhésion au système de paiement à distance sécurisé - Version 2 du 02 juin 2006 - Amendée par décision extraordinaire du CMJR du 03/11/2008 - s'appliquent aux solutions de paiement sécurisé 3 DSecure proposées par les prestataires OGONE ou PAY BOX conformes PCI / DSS.

Elles déterminent :

Les procédures de paiement sécurisé 3 DSecure dans ce contexte d'utilisation,,
Les conditions d'application de la garantie telles que définies à l'article 4 des Conditions Générales du présent contrat qu'elles complètent,
Le délai de communication des justificatifs
Les conditions tarifaires de l'adhésion au système de paiement à distance sécurisé,
D'autres dispositions spécifiques susceptibles d'être fixées par la banque Acquéreur.

ARTICLE 2 : PROCEDURE DE PAIEMENT SÉCURISÉ 3 DSECURE

2.0 Enregistrement de l'Accepteur

La mise en œuvre du paiement sécurisé nécessite un enregistrement préalable 3 DSecure de l'Accepteur auprès des réseaux VISA et MASTERCARD.
L'acceptation des paiements sécurisés est conditionnée par la confirmation par l'Accepteur à la banque Acquéreur de son enregistrement 3 DSecure.
Cette confirmation se matérialise par l'envoi d'un courrier recommandé avec accusé de réception au service Monétique à la banque Acquéreur au plus tard 8 jours calendaires après la signature du présent contrat.

2.1 Solution de paiement sécurisé utilisée par l'Accepteur

Pour recevoir des paiements à distance sécurisés 3 DSecure par cartes bancaires « CB » ou cartes agréées « CB », l'Accepteur doit utiliser une solution de paiement sécurisé 3 DSecure proposée par les prestataires OGONE ou PAY
BOX. L'Accepteur doit s'assurer auprès du prestataire concerné de la conformité PCI/DSS de la solution dans le cadre de son environnement d'utilisation.

L'Accepteur doit, au plus tard dans les 8 jours calendaires suivant la signature des présentes conditions particulières, confirmer à la banque Acquéreur au moyen d'un courrier recommandé avec avis de réception :
Qu'il utilise la solution de paiement à distance sécurisée 3 DSecure / proposée par les prestataires OGONE ou PAY BOX,
Que cette solution est conforme PCI / DSS dans son environnement d'utilisation,
son enregistrement 3 DSecure dont il doit adresser une copie à la Banque Acquéreur.
En cas de changement de prestataire technique fournisseur d'une des deux solutions objet du présent contrat, l'Accepteur doit informer la banque Acquéreur de ce changement au moyen d' un courrier recommandé avec accusé de réception au plus tard 8 jours calendaires avant ce changement. Un nouveau contrat devra être signé par l'Accepteur.
L'utilisation de cette solution de paiement sécurisée transfère à la Banque Émettrice de la Carte le soin d'identifier son Porteur de Carte.

2.2 Identification du porteur de Carte par la Banque Emettrice de la Carte

La solution de paiement à distance sécurisée 3 DSecure proposée par les prestataires OGONE / PAY BOX repose notamment sur un système d'identification du Porteur de Carte par la Banque Emettrice de la Carte.
En cas d'échec ou d'absence d'identification, l'Accepteur doit abandonner la transaction, celle-ci ne répondant plus aux critères d'un paiement sécurisé 3 DSecure.

2.3 Demande d'autorisation

Une autorisation doit être demandée à chaque transaction de paiement sécurisé 3 DSecure quel que soit le montant et le type de carte bancaire « CB » ou agréée « CB ».
La demande d'autorisation doit comporter le cryptogramme visuel et les éléments relatifs à l'identification du Porteur de la Carte concernée.

La présence du cryptogramme visuel dans la demande d'autorisation est obligatoire pour tout paiement sécurisé 3 DSecure. Il doit donc être systématiquement transmis lors d'une demande d'autorisation à la Banque Emettrice de la Carte.

2.4 Délai de transmission des opérations
Le délai maximum de transmission des enregistrements au centre de traitement au-delà duquel la garantie cesse est égal au délais indiqué dans la grille détaillée en première page des présentes.

ARTICLE 3 : GARANTIE DU PAIEMENT

3.1 Conditions
Le strict respect des conditions définies à l'article 2 des présentes conditions particulières et de celles de l'article 4 des conditions générales du présent contrat conditionne l'obtention de la garantie du paiement.

3.2 Litige commercial
Ce litige est indépendant de l'opération de paiement. Il doit être réglé directement entre l'Accepteur et le Porteur de la Carte concernée.

ARTICLE 4 : DÉLAI DE COMMUNICATION DES JUSTIFICATIFS

Si la Banque Acquéreur en fait la demande, l'Accepteur s'engage à lui fournir tout justificatif des opérations de paiement dans un délai de 7 jours calendaires à compter de la demande de la Banque Acquéreur.

Passé ce délai, le compte de l'Accepteur pourrait être débité du montant de la transaction concernée.

Article 5 – REJETS TECHNIQUES
L'accepteur est tenu d'accepter les rejets techniques, pendant 3 mois à compter de la date de traitement de la transaction initiale, en cas de :
- N° de carte différent de 13, 16 ou 19 positions
- Code émetteur du n) de carte erroné
- N° de carte inexistant

Article 6 : OBLIGATIONS DE L'ACCEPTEUR – L'ACCEPTEUR S'ENGAGE A :

6-1 - N'utiliser le présent contrat que pour le seul et unique SIREN précisé ci dessus et les seuls et uniques sites Internet précisés ci dessus dans la grille figurant sur la première page des présentes. Toute modification devra être signalée et acceptée par la Banque qui se réserve le droit de ne pas accepter d'ouvrir ou de modifier le présent contrat ou de procéder à sa clôture, motivée par l'adresse, le contenu ou partie du contenu du site marchand.

6-2 - Informer préalablement et formellement la banque du souhait de toute modification de son objet social ou de toute extension de la nature des produits ou services vendus à distance (signalés sur la ligne **« Activités réelles détaillées »** indiquée dans la grille figurant sur la première page des présentes) et encaissés à l'aide du présent contrat.

6-3 - Suppression ou provisionnement des paiements reçus sans livraison complète des produits ou services payés
Pour des raisons de sécurité ou de disponibilité des produits, le client peut être amené à NE PAS LIVRER la commande de l'acheteur. Dans ce cas, le commerçant a l'obligation de supprimer le paiement CB AVANT qu'il ne passe en compensation. Il lui suffit de faire régler ou de faire régler par son développeur le paramètre de sa solution de paiement securisé à 3 jours AU MOINS afin de lui laisser le temps matériel de supprimer le paiement manuellement ou automatiquement. A DEFAUT : les sommes perçues indûment doivent être systématiquement et immédiatement provisionnées sur un compte BPA dédié.

6-4 - Impayés et Fraude

L'accepteur reconnaît qu'en cas d'impayé, la banque se réserve le droit de facturer des frais de gestion unitaires et forfaitaires, tels qu'indiqués dans les conditions tarifaires BPA.
Cette commission sera révisée annuellement à chaque renouvellement des conditions tarifaires de la Banque.
La Banque se réserve la possibilité de provisionner, si nécessaire et sans préavis, le montant des impayés potentiels détectés, ou des commandes encaissées non livrées, notamment si l'article 3 n'a pas été respecté.
L'accepteur s'engage à lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en oeuvre sans délais les mesures préconisées par le GIE Carte Bancaire, Visa, Mastercard ou la Banque.
Concernant les autres frais induits par les dossiers de fraude ou d'impayés, la Banque se réserve la possibilité de les imputer à l'accepteur, lorsque les recommandations ou instructions de la Banque ou du GIE CB n'ont pas été respectées. Selon la nature, le volume et la répétition des dossiers, ces montants peuvent être importants.

6-5 Le non respect de l'une de ces dispositions pourra entraîner la clôture immédiate et sans préavis du/des contrat(s) CB du client et pourra donner lieu à la facturation des éventuels frais engendrés par l'absence de respect des obligations de l'accepteur : notamment les pénalités du GIE, de VISA, de Mastercard et tout autres frais divers induits y compris les impayés et frais à venir sur les encaissements déjà réalisés « sauf bonne fin ».

Article 7 : La non utilisation de ce contrat sur une période de 12 mois glissants pourra entrainer sa clôture immédiate, à l'initiative de la banque et sans préavis.

Article 8 : INFORMATIQUE ET LIBERTE

8.1 - Données personnelles :
Dans le cadre de la relation bancaire, la Banque est amenée à recueillir des données à caractère personnel concernant le client, le cas échéant, le représentant légal, le mandataire et à les traiter notamment en mémoire informatisée selon les dispositions de la loi « informatique et libertés » du 6 janvier 1978 modifiée. Les données à caractère personnel ainsi recueillies sont obligatoires et ont pour principales finalités la tenue et la gestion du (des) compte(s), ainsi que la gestion de la relation bancaire, la gestion du risque, la gestion et la prévention du surendettement, la gestion des incivilités, le respect de ses obligations légales ou réglementaires, les études statistiques et la fiabilisation des données, le contrôle et la surveillance lié au contrôle interne auquel est soumis la Banque, l'octroi de crédit, les analyses, les études, le pilotage de l'activité bancaire, le reporting, l'historisation des données pour garantir la piste d'audit, la sécurité et la prévention des impayés et de la fraude, le recouvrement, le contentieux, la lutte contre le blanchiment de capitaux et le financement du terrorisme, l'échange automatique d'informations relatif aux comptes en matière fiscale, la classification, la segmentation à des fins réglementaires et/ou commerciales, la sélection et le ciblage de la clientèle, la prospection et l'animation commerciale, la communication et le marketing.
Le refus par le titulaire/représentant légal/mandataire de communiquer tout ou partie de ses données peut entraîner le rejet de la demande.
Elles sont destinées, de même que celles qui seront recueillies ultérieurement, à la Banque responsable de traitement. Certaines données peuvent être adressées à des tiers pour satisfaire aux obligations légales et réglementaires.
La Banque est tenue au secret professionnel à l'égard de ces données. Toutefois, la Banque est autorisée par le titulaire/représentant légal/mandataire à communiquer les données le concernant dans les conditions prévues aux présentes Conditions Générales.
Les données à caractère personnel (informations nominatives) que le Client a transmises à la Banque conformément aux finalités convenues peuvent, à l'occasion de diverses opérations, faire l'objet d'un transfert dans un pays de l'Union Européenne ou hors Union Européenne.
Dans le cadre d'un transfert vers un pays hors Union Européenne, des règles assurant la protection et la sécurité de ces informations ont été mises en place. Le Client peut en prendre connaissance en consultant la notice d'information accessible sur le site Internet de la Fédération Bancaire Française : www.fbf.fr.
Ces données peuvent être communiquées, à leur requête, aux organismes officiels et aux autorités administratives ou judiciaires habilités, notamment dans le cadre de la lutte contre le blanchiment des capitaux ou de la lutte contre le financement du terrorisme. Pour ces mêmes raisons, en vertu du Règlement CE/1781 du 15 novembre 2006, en cas de virement de fonds, certaines des données doivent être transmises à la banque du bénéficiaire du virement située dans un pays de l'Union européenne ou hors Union européenne.
Le titulaire/représentant légal/mandataire disposent d'un droit d'accès et de rectification s'agissant de leurs données ainsi que d'un droit d'opposition au traitement de ces données pour motifs légitimes. Ils peuvent également s'opposer sans frais à ce que ces données fassent l'objet d'un traitement à des fins de prospection notamment commerciale.

Ces droits peuvent être exercés par courrier accompagné d'une copie de tout document d'identité signé par le demandeur auprès de La Banque Populaire Auvergne Rhône Alpes, en s'adressant au service réclamations 30 avenue Charles De Gaulle - 74 800 La Roche sur Foron.

8.2 - Communications auprès de la plateforme téléphonique Alodis

Le client est informé que lorsqu'il est en communication téléphonique auprès de la plateforme Alodis, les conversations entre le client et le téléconseiller peuvent faire l'objet d'une écoute ponctuelle par un superviseur du centre. Ces écoutes sont nécessitées par l'obtention ou le maintien d'une norme qualitative professionnelle. Le client autorise expressément ces écoutes.

REFERENTIEL SECURITAIRE ACCEPTEUR

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

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

Pour assurer la sécurité des données des transactions et notamment, des données des porteurs, une organisation, des procédures et des responsabilités doivent être établies.
En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données nominatives et des données bancaires 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 de paiement 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.
Les personnels doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Les personnels doivent être régulièrement sensibilisés 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 les personnels reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et de paiement.

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 transaction et notamment, des données du porteur doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les 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 de paiement

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement 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 de paiement 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 de paiement

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 de paiement.
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 de paiement

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 de paiement

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 être le pare-feu, 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 de paiement.
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 de paiement

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 de paiement

La protection et l'intégrité des éléments de la transaction 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 de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14)
Protéger la confidentialité des données bancaires

Les données du porteur ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations. Le cryptogramme visuel d'un porteur ne doit en aucun cas être stocké par le commerçant.

Les données bancaires et nominatives relatives à une transaction, et notamment les données du porteur doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux recommandations de la CNIL. Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et de paiement 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.