BANQUE POPULAIRE
AUVERGNE RHÔNE ALPES

CONDITIONS GENERALES

CONTRAT VENTE A DISTANCE INTERNET CYBERPLUS PAIEMENT NET OU MIX AVEC 3D SECURE PROGRESSIF

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

Conditions générales d'adhésion au système de paiement à distance par cartes « CB » ou agréées « CB » à sécurité optionnelle et progressive

PREAMBULE

Le GIE "CB"

Pour éviter, dans le commerce électronique et la vente ou la location à distance 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, le GIE "CB" a mis en place des procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes "CB" ou agréées "CB" telles que le protocole 3D Secure, ainsi qu'un référentiel sécuritaire de protection des données sensibles.

Article préliminaire

1) L'"Accepteur "CB" " peut être un commerçant, tout prestataire de services, toute personne exerçant une profession libérale, susceptible d'utiliser le Système "CB", et d'une manière générale, tout professionnel vendant ou louant des biens ou des prestations de services.
L'Accepteur "CB "dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix, Membre du GIE "CB" ou Entité de Groupe au sens des Statuts du GIE "CB" et avec lequel il a passé un contrat d'acceptation.

2) Par "Acquéreur "CB"", il faut entendre tout établissement de crédit ou de paiement Membre du GIE "CB" ou Entité de Groupe au sens des Statuts du GIE "CB", avec lequel l'Accepteur "CB" a signé un contrat d'acceptation, et cela quel que soit son statut, (banque, etc).

3) Par "Système d'Acceptation", il faut entendre les logiciels, protocoles conformes aux spécifications définies par le GIE "CB" et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes "CB" et agréées "CB".

4) **Responsabilité de l'Accepteur "CB" de sa décision d'utiliser ou non la procédure de sécurisation 3DS**
L'Accepteur "CB" a été informé que les opérations de paiement effectuées avec le protocole 3DS 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 5 des Conditions Générales.

Cependant, l'Accepteur "CB" souhaite rester maître de sa stratégie commerciale et de sa politique de risque en matière d'encaissements à distance par carte bancaire et demande à l'Acquéreur "CB" de lui permettre de désactiver ponctuellement pour une opération de paiement la procédure de sécurisation du paiement à distance telle que le protocole 3DS.

L'Accepteur "CB" est seul responsable de sa décision de ne pas utiliser la procédure sécuritaire du protocole 3DS. C'est à sa demande expresse que l'Acquéreur "CB" lui offre la possibilité de paramétrer sur son formulaire de paiement géré par la plate-forme de paiement Systempay de l'Acquéreur "CB" la désactivation de ladite procédure sécuritaire.
Le paramétrage de la désactivation de la procédure sécuritaire est décrit en annexe 2.

De manière générale, l'Acquéreur "CB" recommande à l'Accepteur "CB" d'utiliser systématiquement le protocole 3DS pour ses encaissements à distance par carte bancaire et attire son attention sur le fait que lesdits encaissements réalisés sans le protocole 3DS ne peuvent pas bénéficier de la garantie de paiement visée à l'article 5 des Conditions Générales. Ces encaissements se font exclusivement sous réserve de bonne fin et en l'absence de contestation par les titulaires de carte.

En conséquence, l'Accepteur "CB" ne pourra pas rechercher la responsabilité de l'Acquéreur "CB" pour un quelconque défaut de conseil au titre du présent Contrat.

l'Accepteur "CB" reconnaît avoir été informé de l'augmentation croissante du risque de fraude en matière de paiements par carte bancaire sur Internet, ce risque étant exclusivement à sa charge lorsque l'ensemble des mesures de sécurité prévues à l'article 5 des Conditions Générales n'ont pas été respectées.
Lors de la signature du présent Contrat, l'Accepteur "CB" s'engage à utiliser la procédure sécuritaire du protocole 3DS à hauteur du pourcentage d'encaissements stipulé à l'article 3.1.1 des Conditions Générales.

Il déclare connaître les lois et règlements applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…). Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et qu'il doit commercialiser les produits ou prestations de 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 comprenant les Conditions Générales, les Conditions particulières et le Référentiel Sécuritaire.

ARTICLE 1 : DEFINITION DU SYSTEME

Le système de paiement à distance sécurisé par Carte "CB" repose sur l'utilisation de Cartes "CB" ou agréées "CB" pour le paiement d'achats de biens ou de prestations de services auprès des Accepteurs adhérant au Système "CB" et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE "CB".
Lorsque l'Acquéreur "CB" représente le GIE "CB", le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte "CB" ou de Cartes agréées "CB" et de remise des opérations à l'Acquéreur "CB", et non la mise en jeu de la garantie du paiement visée à l'article 5 des présentes Conditions Générales.

ARTICLE 2 : DISPOSITIONS RELATIVES AUX CARTES

Sont utilisables dans le Système "CB" :
● les cartes sur lesquelles figure la marque "CB"
● les cartes agréées "CB" c'est-à-dire :
- cartes portant uniquement la marque Visa ou MasterCard dont l'acceptation dans le Système "CB" a été agréée par le GIE "CB",
- cartes émises dans le cadre de réseaux étrangers ou internationaux homologuées par le GIE "CB" et dont l'Accepteur "CB" peut obtenir les signes de reconnaissance auprès de l'Acquéreur "CB".
L'ensemble de ces cartes précitées est désigné ci-après par le terme générique de "Carte".

ARTICLE 3 : OBLIGATIONS DE L'ACCEPTEUR "CB"

3.1 L'Accepteur "CB" s'engage à :

3.1.1 Augmenter progressivement le taux d'utilisation de la procédure de sécurisation 3DS des ordres de paiement donnés à distance par les Titulaires de Cartes dans le respect des dispositions légales, réglementaires et professionnelles applicables, notamment et sans limitation 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 applicables à son activité.
Lors de la signature du présent Contrat, l'Accepteur "CB" s'engage à réaliser mensuellement **35%** de ses encaissements à distance par Carte selon ladite procédure de sécurisation.
A l'issue d'un délai de six mois suivant la date de signature du présent Contrat, l'Accepteur "CB" s'engage à augmenter en accord avec l'Acquéreur "CB" le pourcentage de ses encaissements mensuels sécurisés 3DS à atteindre dans un nouveau délai de 12 mois.
Puis par la suite, ledit pourcentage sera révisé avec une périodicité annuelle et selon les modalités suivantes : le nouveau pourcentage sera déterminé de façon à réduire la fraude constatée. Ce nouvel engagement sera confirmé par courrier signé de l'Accepteur "CB" et réputé accepté par l'Acquéreur "CB" sauf opposition de sa part dans un délai de 2 mois : il vaudra ainsi avenant du présent Contrat.

3.1.2 Utiliser le système de paiement à distance sécurisé en s'abstenant de toute activité qui pourrait être pénalement sanctionnée telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'oeuvres protégées par un droit de propriété intellectuelle et de moyens ou instruments de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries et des dispositions relatives aux conditions d'exercice de professions réglementées.

3.2 Garantir l'Acquéreur "CB" et le GIE "CB" le cas échéant, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 3.1.

3.3 Afficher visiblement, notamment sur l'écran du dispositif technique utilisé par le Titulaire de la Carte et sur ses supports de communication :

● le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Titulaire de la Carte en soit préalablement informé. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.
● les différentes marques de Cartes acceptées.

3.4 S'identifier clairement par le numéro SIRET et le code activité (NAF/APE) que l'INSEE lui a attribués. Si l'Accepteur "CB" n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par l'Acquéreur "CB", lui permettant l'accès au système "CB".

3.5 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 "CB" la conformité des informations transmises pour identifier son point de vente en ligne, les informations doivent indiquer une dénomination commerciale connue des Titulaires de Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, règlement en présence physique de l'accepteur, etc) dans ce point de vente en ligne.

3.6 Recevoir des paiements à distance sécurisés en contrepartie d'actes de vente ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même.

3.7 Accepter les Cartes telles que définies à l'article 2 ci-dessus pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués auquel le Titulaire de la Carte a effectivement et expressément consenti. En outre, l'Accepteur "CB" s'interdit de collecter au titre du présent Contrat toute opération de paiement pour laquelle il n'a pas reçu lui-même le consentement du Titulaire de la Carte.
Afficher visiblement sur tout support de l'offre de vente à distance et notamment à l'écran du dispositif technique utilisé par le Titulaire de la Carte 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 Titulaire de la Carte ne soit pas en mesure de croire que le prix était autre.
3.8 Transmettre les enregistrements des opérations de paiement à l'Acquéreur "CB", dans les délais prévus dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Système "CB".

3.9 Faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des clients, notamment lors de l'exercice par ces derniers de leur droit de rétractation, et concernant des biens et services dont l'achat a été réglé par Carte au titre du présent Contrat.

3.10 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par le GIE "CB" et les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes, proposées par l'Acquéreur "CB".

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

3.12 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 le référentiel de sécurité PCI DSS et acceptent que les audits visés à l'article 3.14 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.

3.13 A la demande de l'Acquéreur selon les volumes d'opérations cartes acceptées chez l'Accepteur, ce dernier doit respecter les exigences du référentiel de sécurité PCI DSS figurant en annexe du présent contrat.

3.14 Permettre à l'Acquéreur "CB" et au GIE "CB" 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 tant des clauses du présent Contrat que des exigences figurant en annexe, notamment des obligations du Référentiel Sécuritaire susvisé. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.
Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses, obligations ou exigences, le GIE "CB" et/ou l'Acquéreur "CB" peuvent mettre en oeuvre les mesures prévues à l'article 9. L'Accepteur "CB" autorise la communication du rapport à l'Acquéreur "CB" et aux réseaux étrangers ou internationaux mentionnés sur les Cartes acceptées par l'Accepteur "CB" et définies à l'article 2.

3.15 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 au Titulaire de la Carte utilisée pour l'opération initiale. L'Accepteur "CB" doit alors utiliser la procédure dite de "transaction crédit", et dans le délai prévu dans les Conditions Particulières convenues avec lui, effectuer la remise correspondante à l'Acquéreur "CB" à qui il avait remis l'opération initiale. Le montant de la "transaction crédit" ne doit pas dépasser le montant de l'opération initiale.

3.16 Laisser libre accès au Système d'Acceptation à l'Acquéreur "CB" et à toute personne désignée par ce dernier pour effectuer des travaux de maintenance et de mise à niveau dudit Système d'Acceptation pour répondre aux Conditions Générales et Particulières du présent Contrat.

ARTICLE 4 : OBLIGATIONS DE L'ACQUEREUR "CB"

L'Acquéreur "CB" s'engage à :

4.1 Fournir à l'Accepteur "CB" les informations sur les procédures applicables à l'Acceptation des paiements à distance sécurisé référencées par le GIE "CB" que l'Accepteur "CB" doit utiliser obligatoirement. Ces informations figurent dans les Conditions Particulières.

4.2 Inscrire l'Accepteur "CB" dans la liste des points de vente habilités à recevoir des paiements par Cartes de Titulaires de Cartes dûment authentifiés.

4.3 Indiquer à l'Accepteur "CB" la liste et les caractéristiques des Cartes pouvant être acceptées.

4.4 Créditer le compte de l'Accepteur "CB" des sommes qui lui sont dues, selon les Conditions Particulières convenues avec lui.

4.5 Ne pas débiter, au delà du délai maximum de 15 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 sur lequel fonctionne la Carte.

ARTICLE 5 : GARANTIE DU PAIEMENT

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

5.2 Informer immédiatement l'Acquéreur "CB" en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation...).

5.3 Lors du paiement
L'Accepteur "CB" s'engage à :
5.3.1 Appliquer la procédure de sécurisation 3DS des encaissements à distance par Carte décrite dans les Conditions Particulières.

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

5.3.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :
● la période de validité (fin et éventuellement début),
● que le type de carte utilisé figure à l'article 2.
● contrôler le numéro de Carte par rapport à la dernière liste de Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par l'Acquéreur "CB" pour le point de vente concerné et selon les Conditions Particulières convenues avec l'Acquéreur "CB".

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

5.4 Après le paiement
L'Accepteur "CB" s'engage à :

5.4.1 Transmettre à l'Acquéreur "CB" dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur "CB", les enregistrements électroniques des opérations et s'assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur "CB". L'Accepteur "CB" 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 "CB" signataire du présent Contrat doit être obligatoirement remise à ce dernier.

5.4.2 Envoyer au Titulaire de la Carte, à sa demande, un ticket précisant, entre autres, le mode de paiement par Carte utilisé.

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

5.4.4 L'Accepteur "CB" s'engage à 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 par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux prescriptions de la loi "Informatique et Libertés" du 6 janvier 1978 et notamment de son article 34.
5.4.5 Les mesures de sécurité énumérées aux articles 5.3 et 5.4 ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 7.

ARTICLE 6 : RECLAMATION ET CONVENTION DE PREUVE

6.1 Réclamation
Toute réclamation doit être formulée par écrit et justifiée à l'Acquéreur "CB", dans un délai maximum de 6 mois à compter de la date de l'opération contestée, sous peine de forclusion.
Ce délai est réduit à 15 jours calendaires à compter de la date de débit en compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

6.2 Convention de preuve
De convention expresse entre les parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur "CB". En cas de conflit, les enregistrements électroniques produits par l'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 l'Acquéreur "CB" ou le GIE "CB" .

ARTICLE 7 : MODIFICATIONS

7.1 L'Acquéreur "CB" peut modifier à tout moment les présentes Conditions Générales ainsi que les Conditions Particulières.
L'Acquéreur "CB" peut notamment apporter :
● des modifications techniques telles que l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'état du Système d'Acceptation suite à un dysfonctionnement etc.
● des modifications sécuritaires telles que :
- la suppression de l'acceptabilité de certaines Cartes
- la suspension de l'adhésion au Système "CB".

7.2 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un mois à compter de l'envoi de la lettre d'information ou de notification.
D'un commun accord, précisé dans les Conditions Particulières convenues entre l'Acquéreur "CB" et l'Accepteur "CB", les parties peuvent déroger à ce délai en cas de modifications importantes.

7.3 Ce délai est exceptionnellement réduit à cinq jours calendaires lorsque l'Acquéreur "CB" ou le GIE "CB" constate, dans le point de vente en ligne, une utilisation anormale de Cartes perdues, volées ou contrefaites.

7.4 Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur "CB" s'il n'a pas résilié le présent Contrat.

7.5 Le non respect des nouvelles conditions techniques et sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat, voire la suspension par le GIE "CB" de l'adhésion au Système "CB" dans les conditions prévues à l'article 9 du présent Contrat.

ARTICLE 8 : DUREE ET RESILIATION DU CONTRAT

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

L'Accepteur "CB" d'une part, l'Acquéreur "CB" d'autre part, peuvent, à tout moment, sans justificatif et moyennant un préavis de trois mois (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 Système "CB" en utilisant des moyens sécurisés d'acceptation avec tout autre Acquéreur "CB" de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 7 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

8.2 Toute cessation d'activité de l'Accepteur "CB", cession ou mutation du fonds de commerce ainsi que tout comportement gravement répréhensible , 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" ou pourront faire l'objet d'une déclaration de créances.

8.3 L'Accepteur "CB" est tenu de restituer à l'Acquéreur "CB" les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur "CB" est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'adhésion, l'Accepteur "CB" s'engage à retirer immédiatement de son Système d'Acceptation et de ses supports de communication tout signe d'acceptation des Cartes.

ARTICLE 9 : MESURES DE PREVENTION ET DE SANCTION

9.1 Mesures de prévention et de sanction mises en oeuvre par l'Acquéreur "CB"
En cas de manquement de l'Accepteur "CB" aux dispositions 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 "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 anormalement élevé 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 oeuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur "CB" peut résilier de plein droit avec effet immédiat le présent Contrat par lettre recommandée avec demande d'avis de réception.
De même, si dans un délai de trois mois à compter de l'avertissement, l'Accepteur "CB" est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur "CB" peut décider la résiliation de plein droit avec effet immédiat du présent Contrat notifiée par lettre recommandée avec demande d'avis de réception.

9.2 Mesures de prévention et de sanction mises en oeuvre par le GIE "CB"

En cas de manquement de l'Accepteur "CB" aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où l'Accepteur "CB" ventile ses remises en paiement entre plusieurs Acquéreurs "CB" de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE "CB" peut prendre des mesures de sauvegarde et de sécurité consistant en :
● la suspension de l'adhésion au Système "CB". 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 "CB" en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis de l'Accepteur "CB" concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception.

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

9.4 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 l'Acquéreur "CB", ou souscrire un nouveau contrat d'adhésion avec un autre Acquéreur "CB" de son choix.
Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en oeuvre de recommandations d'un auditeur désigné par le GIE "CB" ou l'Acquéreur "CB" et portant sur le respect des bonnes pratiques en matière de vente à distance visées à l'article 3 et des mesures de sécurité visées à l'article 5.

ARTICLE 10 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

10.1 Secret bancaire
De convention expresse l'Accepteur "CB" autorise l'Acquéreur "CB" à stocker le cas échéant des données secrètes ou confidentielles portant sur lui et les communiquer 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 Titulaires de Cartes ou d'autres entités.

10.2 Protection des données à caractère personnel
Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel.

Ainsi, en application des articles 32, 38, 39 et 40 de la loi du 6 janvier 1978 relative à la loi "Informatique et Libertés" modifiée par la loi du 6 août 2004, il est précisé que :

10.2.1 Les informations relatives à l'Accepteur "CB", collectées par l'Acquéreur "CB" 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 "CB" étant à cet effet, de convention expresse, délié du secret bancaire.
L'Accepteur "CB", personne physique, ou la personne physique le représentant ou sur laquelle portent les données à caractère personnel ci-dessus recueillies, a le droit d'en obtenir communication, et 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, auprès de l'Acquéreur "CB".

10.2.2 A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur "CB" peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte. L'Accepteur "CB" ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte. 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 oeuvre de dispositifs de protection et de contrôle des accès physiques et logiques à ces données.
Les Titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer des 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.

ARTICLE 11 : NON RENONCIATION

Le fait pour l'Accepteur "CB" ou pour l'Acquéreur "CB" 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 12 : LOI APPLICABLE/TRIBUNAUX COMPETENTS

Le présent Contrat et toutes les questions qui s'y rapportent sont régis par le droit français et tout différend relatif à l'interprétation, la validité, et/ou l'exécution du présent Contrat est soumis à la compétence des Tribunaux français, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

ARTICLE 13 : LANGUE DU PRESENT CONTRAT

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

Conditions particulières convenues entre l'Acquéreur CB et l'Accepteur CB

L'Acquéreur "CB" met à disposition de l'Accepteur "CB" sa solution technique de sécurisation des ordres de paiement effectués à distance au profit de ce dernier pour recevoir des paiements sécurisés par Carte via Internet.
Les modalités de cette mise à disposition font l'objet de conditions spécifiques indiquées par ailleurs.

ARTICLE 1 : PROCEDURE DE PAIEMENT SÉCURISÉ 3DSECURE

1.1 **Enregistrement de l'Accepteur "CB"**
La mise en oeuvre du paiement sécurisé nécessite un enregistrement préalable 3DSecure de l'Accepteur "CB" auprès des réseaux VISA et MASTERCARD.
L'acceptation des paiements sécurisés est conditionnée par la confirmation de l'enregistrement 3D Secure de l'Accepteur "CB" par l'Acquéreur "CB". Cette confirmation se matérialise par l'envoi d'un courriel à l'adresse communiquée par l'Accepteur "CB", ce dernier s'engageant à informer sans délai l'Acquéreur "CB" de toute modification de cette adresse, ainsi que de toute indisponibilité de cette dernière.

1.2 **Moyen technique mis à disposition de l'Accepteur "CB" par l'Acquéreur "CB"**

L'Accepteur "CB" doit utiliser la solution technique – 3DSecure – mise à sa disposition par l'Acquéreur "CB" pour recevoir des paiements à distance par Internet sécurisés 3DSecure par Carte.
1.3 **Authentification du porteur par la Banque Émettrice de la Carte**
Cette solution technique repose sur un système d'authentification du Titulaire de la Carte par la Banque Émettrice de la Carte.
En cas d'échec ou d'absence d'authentification, l'opération de paiement sera abandonnée et ne donnera donc pas lieu à demande d'autorisation.

1.4 **Demande d'autorisation**
Une autorisation doit être demandée à chaque opération de paiement sécurisé 3D Secure quels que soient le montant et le type de Carte.
La demande d'autorisation doit comporter le cryptogramme visuel et les éléments relatifs à l'authentification du Titulaire de la Carte.
La présence du cryptogramme visuel dans la demande d'autorisation est obligatoire pour tout paiement par Internet sécurisé 3D Secure. Il doit donc être systématiquement transmis lors d'une demande d'autorisation à la Banque Emettrice de la Carte.

1.5 **Délai de transmission des opérations de paiement**
La réglementation interbancaire, dans le cadre des opérations couvertes par le présent contrat, fixe un délai maximum de 6 jours au-delà duquel l'Accepteur "CB" s'expose à recevoir un impayé pour remise tardive.

ARTICLE 2 : DESACTIVATION DE LA PROCEDURE DE SECURISATION 3DS

Comme indiqué dans le Préambule des Conditions Générales, l'Accepteur "CB" demande à l'Acquéreur "CB" de lui permettre de désactiver ponctuellement pour une opération de paiement par Carte la procédure de sécurisation du paiement à distance 3DS mise à sa disposition.
Techniquement, le service 3D Secure progressif est géré par l'intermédiaire d'un champ du formulaire de paiement utilisé par l'Accepteur "CB" et envoyé à la plate-forme de paiement de l'Acquéreur "CB"
Paramétrage à effectuer sur le formulaire de paiement par l'Accepteur "CB"
Le service 3D Secure progressif autorise l'accès et la gestion du champ "vads_threeds_mpi" de son formulaire de paiement.
Ce champ peut prendre les valeurs suivantes :

Valorisation vads_threeds_mpi	**Signification**
0	Authentification 3D Secure gérée par la plateforme de paiement **activée**
2	Authentification 3D Secure **désactivée** pour l'opération de paiement

Par défaut, la procédure 3DS de sécurisation sera toujours activée.
L'Accepteur "CB" renseignera la donnée à « 2 » s'il veut désactiver le protocole 3D Secure pour une opération de paiement donnée.
Une documentation technique est à la disposition de l'Accepteur "CB" auprès de l'Acquéreur "CB".

ARTICLE 3 : DATE DE VALEUR

La date de crédit au compte de l'Accepteur "CB" ne peut être postérieure à celle du jour ouvrable au cours duquel le montant de l'opération de paiement est crédité sur le compte de l'Acquéreur "CB".
La date de débit du compte de l'Accepteur "CB" ne peut être antérieure au jour où le montant de l'opération est débité de ce compte.

ARTICLE 4 - GARANTIE DU PAIEMENT

4.1. **Conditions**
Le strict respect de l'ensemble des conditions définies à l'article 1 des présentes Conditions Particulières et de celles de l'article 5 des Conditions Générales du présent Contrat conditionne la garantie de l'opération de paiement.

4.2 **Information sur l'existence de la garantie**
L'Acquéreur "CB" met à disposition de l'Accepteur "CB" un indicateur dans le Journal des opérations de paiement (journal de fonds) de sa solution technique qui lui permet de s'assurer que l'opération de paiement bénéficie de la garantie.

L'information communiquée à l'Accepteur "CB" se traduit par trois messages différents :

- **YES** : l'opération de paiement est garantie dans le cadre des conditions définies à l'article 1 ci-dessus et de celles de l'article 5 des Conditions Générales du présent Contrat.

- **NO** : l'opération de paiement n'est pas garantie,

- **UNKNOWN** : les informations relatives à l'opération de paiement en retour de la Banque Émettrice de la Carte ne permettent pas de déterminer si la garantie s'applique. Le règlement de l'opération de paiement ne se fera que sous bonne fin d'encaissement et ce, en l'absence de contestations.

ARTICLE 5 : DÉLAI DE COMMUNICATION DES JUSTIFICATIFS

Si l'Acquéreur "CB" en fait la demande, l'Accepteur "CB" s'engage à lui fournir tout justificatif des opérations de paiement dans un délai de 7 jours calendaires à compter de la demande de l'Acquéreur "CB".
Passé ce délai, le compte de l'Accepteur "CB" pourra être débité du montant de l'opération de paiement concernée en application de l'article 5.1 et 5.4.3 des Conditions Générales.

ARTICLE 6 : CONDITIONS TARIFAIRES

Les dates de valeur, les tarifs du contrat commerçant, la tarification de la convention de service Cyberplus Paiement et de ses options etc se trouvent sur la grille détaillée des premières pages des présentes. Les nouvelles conditions tarifaires entrent en vigueur au terme d'un délai de 30 jours à compter de leur notification à l'Accepteur CB. Passé ce délai, les modifications sont opposables à l'Accpteur s'il n'a pas résilié le présent contrat.

ARTICLE 7 : OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur "CB" s'engage à :

7.1 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.

7.2 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.

7.3 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 par son développeur le « capture date » à 3 jours AU MOINS afin de lui laisser le temps matériel de supprimer le paiement manuellement dans l'interface « Office » de Cyberplus Paiement (voir le Manuel) ou automatiquement par l'option « validation ». A DEFAUT : les sommes perçues indument doivent être systématiquement et immédiatement provisionnées sur un compte BPA dédié.

7.4 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. 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 7.3 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 œuvre 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.

7.5 Le non respect de l'une des dispositions de l'article 7 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 8 : CONTRAT SANS MOUVEMENTS

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 9 : INFORMATIQUE ET LIBERTE

9.1 - 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.

9.2 - 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.

Référentiel Sécuritaire 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 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 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 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 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 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 l'accepteur « CB ».
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.

Convention de Service Cyberplus Paiement
juin 2014

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

CONDITIONS GENERALES

1. DEFINITIONS

Toutes les définitions insérées dans les Conditions Générales du contrat d'acceptation en paiement à distance sécurisé, du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive, et du contrat d'acceptation en paiement à distance (ci-après « contrat d'acceptation en paiement à distance « classique » ») par cartes « CB » ou agréées « CB » sont applicables à la présente Convention.

Les définitions supplémentaires suivantes auront la signification qui suit :

Acheteur	désigne tout consommateur réalisant une opération d'achat à distance auprès du Client, Accepteur « CB »
Solution Cyberplus Paiement	désigne les offres commerciales du Service Cyberplus Paiement
Service Cyberplus Paiement	désigne l'ensemble des traitements et fonctionnalités liés à l'encaissement des paiements en vente à distance et intégrés dans la Solution Cyberplus Paiement
Formulaire d'Inscription Client	désigne le document d'enregistrement et de paramétrage des conditions du Service Cyberplus Paiement souscrites par le Client auprès de la Banque Populaire. Il fait partie des Conditions Particulières de la présente convention.

2. OBJET DE LA CONVENTION DE SERVICES

La Banque Populaire propose à ses clients commerçants ou entreprises, Accepteurs « CB » (ci-après le ou les « Client(s) »), réalisant des ventes à distance, une solution d'encaissement des ordres de paiement par carte donnés à distance à leur profit, ainsi qu'un ensemble de traitements et fonctionnalités associés, désignés sous le nom de « Service Cyberplus Paiement ».

Les présentes Conditions Générales ont pour objet de définir les modalités techniques et juridiques selon lesquelles la Banque Populaire permet au Client de bénéficier de la Solution Cyberplus Paiement.

L'adhésion à la Solution Cyberplus Paiement est effectuée par la signature du Formulaire d'Inscription Client. Par cette signature, le Client accepte les présentes Conditions Générales, souscrit à l'une des trois offres Cyberplus Paiement et, le cas échéant, aux services additionnels mentionnés dans son Formulaire d'Inscription Client, et s'engage à respecter les instructions du Kit documentaire visé à l'article 6 ci-après. Le Formulaire d'Inscription Client et les présentes Conditions Générales constituent la présente convention, ci-après dénommée la « Convention ».

Elle annule et remplace toute autre convention qui aurait pu être signée entre les Parties, relative à la Solution Cyberplus Paiement.

3. PRESENTATION DE LA SOLUTION CYBERPLUS PAIEMENT

La Solution Cyberplus Paiement se décline en trois offres commerciales correspondant chacune à un canal de vente à distance :

- L'offre **Cyberplus Paiement ACCESS** s'adresse aux Clients qui pratiquent une activité de vente à distance dite « classique » (téléphone, télécopie, ou courrier). Ils disposent d'un OUTIL DE GESTION DE CAISSE doté d'un accès sécurisé à partir duquel ils pourront saisir les données de carte bancaire de leurs Acheteurs. Ces données sont enregistrées et stockées sur le Serveur sécurisé de la Solution Cyberplus Paiement.
- L'offre **Cyberplus Paiement NET** permet aux Clients qui pratiquent une activité de vente à distance dite « en ligne » (toute interface PC fixe ou portable, Smartphone ou tablette disposant d'une connexion internet permettant d'afficher la page de paiement de la Solution Cyberplus Paiement), de proposer un formulaire de paiement en ligne à leurs Acheteurs internautes à partir de leur boutique en ligne pour enregistrer les données de leur carte bancaire.
- L'offre **Cyberplus Paiement MIX** est destinée aux Clients pratiquant à la fois une activité de vente à distance « classique » et/ou une activité de vente « en ligne » et qui recherchent une solution de paiement s'intégrant dans le processus de commande au sein de leur système d'information.

3.1 La Solution Cyberplus Paiement ACCESS

CYBERPLUS PAIEMENT ACCESS

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance « classique ».

La Solution Access comprend :

- **L'acceptation des moyens de paiement suivants :**
  - cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
  - cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
  - e-carte bleue,

- **L'OUTIL DE GESTION DE CAISSE**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de saisir, valider, consulter, annuler, modifier, rembourser et dupliquer une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.

- **Les canaux de vente**
  - vente à distance « classique »
    - téléphone,
    - télécopie,
    - catalogue papier,
    - courrier,
    - email.

- **Les typologies de paiement (1)** :
  - paiement à l'acte,
  - paiement en « n » fois,
  - paiement différé,

- **La sécurité de la Solution Cyberplus Paiement Access:**
  - certification PCI-DSS,

- accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
- renouvellement des mots de passe tous les trois (3) mois,
- envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire).

Les services additionnels

Ces services sont optionnels et comprennent :

- *Mail avec lien pour paiement*
- *Suivi Client*
- *Contrôle Risques*
- *Gestion Bancaire Simplifiée (sous forme visuelle uniquement)*
- *Gestion Utilisateur*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

(1) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

3.2 La Solution Cyberplus Paiement NET

CYBERPLUS PAIEMENT NET

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé ou d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

La Solution Cyberplus Paiement NET comprend :

❖ **Le formulaire de paiement**
- affichage des cours de change en devises (contre-valeur),
- affichage des pages de paiement en multi-langues (8 langues) (1),
- affichage dynamique pour les mobiles et les tablettes,
- restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
- personnalisation du logo du Client,
- prise en charge du protocole 3DS, le cas échéant selon les critères d'application dudit protocole choisis par le Client, et sous sa responsabilité, dans le cadre d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

❖ **L'acceptation des moyens de paiement suivants :**
- cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
- cartes privatives (2) : American Express, Cofinoga, Cetelem, JCB,
- e-carte bleue,

❖ **L' OUTIL DE GESTION DE CAISSE**
- consultation des opérations de paiement,
- suivi du fichier des remises bancaires,
- possibilité de valider, consulter, annuler, modifier, rembourser une opération de paiement,
- capacité d'exporter les transactions sous format XLS, XML ou CSV.

❖ **Les canaux de vente**
- vente en ligne **(site internet)**

- boutique en ligne depuis une connexion Internet (poste fixe, mobile et tablette connectés à Internet).

❖ **Les typologies de paiement (2)**
- paiement à l'acte,
- paiement en « n » fois,
- paiement différé,

❖ **La sécurité de la Solution Cyberplus Paiement :**
- certification PCI-DSS,
- accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
- renouvellement des mots de passe tous les trois (3) mois,
- envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
- génération d'un certificat d'authentification de chaque site ou boutique du Client
  - génération du certificat en temps réel
- garantie des paiements dans les conditions du protocole 3DS
  - restitution en temps réel vers le site ou boutique du Client de l'existence ou non de la garantie,
  - affichage en temps réel de l'existence ou non de la garantie à partir de l'outil gestion de caisse,
  - restitution en différé de l'existence ou non de la garantie dans les journaux de transactions.

(1) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français
(2) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

Les services additionnels

Ces services sont optionnels et comprennent :

- *Mail avec lien pour paiement*
- *Gestion personnalisation avancée*
- *Suivi Client,*
- *Contrôle Risques,*
- *Gestion Bancaire Simplifiée (sous forme visuelle et fichiers),*
- *Gestion Compte Client*
- *Gestion Utilisateur*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

3.3 La Solution Cyberplus Paiement MIX

CYBERPLUS PAIEMENT MIX

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé et/ou de la signature d'un contrat d'acceptation en paiement à distance « classique » ou d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

La Solution Cyberplus Paiement MIX comprend :

1] Pour la vente à distance en ligne

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement en ligne** :

- **soit le formulaire de paiement Cyberplus Paiement MIX**
  - utilisation du formulaire de paiement en HTTP POST,
  - affichage des cours de change en devises (contre-valeur),
  - affichage des pages de paiement en multi-langues (8 langues) (1),
  - affichage dynamique pour les mobiles et les tablettes,
  - restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3DS, le cas échéant selon les critères d'application dudit protocole choisis par le Client, et sous sa responsabilité, dans le cadre d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.
- **soit le formulaire de paiement de son site marchand (URL du Client)**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation
  - mise à disposition des outils permettant l'utilisation du protocole 3DS.

(1) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français

2] Pour la vente à distance classique

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement à distance « classique »** :

- **soit à partir de son système d'information**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation
- **soit avec l'OUTIL GESTION DE CAISSE**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de saisir, valider, consulter, annuler, modifier, rembourser et dupliquer une transaction,
  - capacité d'exporter les opérations de paiement sous format XLS, XML ou CSV.

3] Les canaux de vente

- vente à distance « classique »
  - téléphone,
  - fax,
  - catalogue papier,

- courrier,
- email,
- Logiciel métier interne (logiciel de commande),
- SVI (serveur vocal interactif),
- Call center (plate-forme téléphonique),
- Centre de saisie (plate-forme de saisie).

- vente en ligne **(site internet)**
  - Boutique en ligne depuis une connexion Internet (poste fixe, mobile et tablette connectés à Internet).

4] L'acceptation des moyens de paiement suivants :

- cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
- cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
- e-carte bleue

5] Les typologies de paiement (1)

- paiement à l'acte,
- paiement en « n » fois,
- paiement différé,

6] La sécurité

- certification PCI-DSS,
- accès à l'outil de gestion de caisse par identifiant et mot de passe,
- renouvellement des mots de passe tous les trois (3) mois,
- envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
- gestion de certificat pour l'authentification de chaque canal,
  - génération du certificat en temps réel,
- garantie des paiements dans les conditions du protocole 3DS,
  - restitution en temps réel dans la réponse automatique,
  - affichage en temps réel à partir de l'outil gestion de caisse,
  - restitution en différé dans les journaux de transactions.

(1) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire.

Les services additionnels

Ces services sont optionnels et comprennent :

- *Mail avec lien pour paiement*
- *Gestion personnalisation avancée*
- *Suivi Client*
- *Contrôle Risques*
- *Gestion Bancaire Simplifiée (sous forme visuelle et fichiers)*
- *Gestion Compte Client*
- *Gestion Utilisateur*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

4. CONDITIONS DES FONCTIONS DE LA SOLUTION CYBERPLUS PAIEMENT

4.1 PAIEMENT DIFFERE

Le Client a la possibilité de choisir le délai de rétention des paiements effectués via le Service Cyberplus Paiement avant remise en banque.

Le Client définit librement ce délai dans l'OUTIL DE GESTION DE CAISSE. Par défaut, le délai de remise en banque est paramétré au jour de l'opération de paiement.

4.2 VALIDATION MANUELLE DES PAIEMENTS

Par défaut, l'envoi en remise des paiements dont la sécurisation est assurée par le Service Cyberplus Paiement est automatique.

Le Client a la possibilité de confirmer cet envoi en remise de façon manuelle.

Le Client signifie librement son choix (validation automatique ou manuelle) dans l'OUTIL DE GESTION DE CAISSE.

Dans le cas où le Client sélectionne « validation manuelle », chaque demande de paiement sécurisé en ligne effectuée par ses Acheteurs doit être validée à l'aide de la fonction « valider » présente dans l'OUTIL DE GESTION DE CAISSE.

La Banque Populaire ne pourra donc être tenue responsable par le Client ou par tout tiers de la non réalisation d'un règlement consécutif à un défaut de validation en mode manuel ainsi que des conséquences qui pourraient en découler.

4.3 PAIEMENT EN PLUSIEURS FOIS

Le Client a la possibilité de faire bénéficier ses Acheteurs d'un service de paiement en plusieurs fois par carte "CB" ou agréée "CB" (ex : VISA ou MasterCard).

Le Client doit communiquer le détail des échéances à son Acheteur préalablement à la validation de la commande.

Par ailleurs, la carte de son Acheteur doit être compatible avec cette option (date d'expiration suffisamment lointaine).

Le paiement par e-Carte Bleue n'est pas autorisé dans le cadre de ce service.

Si le Client a souscrit au service additionnel « Suivi Client », l'e-mail de confirmation de paiement est adressé à l'Acheteur lors de la première échéance et il comporte un échéancier de paiement précisant les dates et montants des prochaines échéances.

La Banque Populaire fournit le service de sécurisation exclusivement pour le premier paiement. Elle ne pourra être tenue pour responsable par le Client ou son Acheteur du fait que la banque dudit Acheteur refuse d'honorer les demandes de paiements en plusieurs fois.

4.4 AFFICHAGE MULTI-DEVISES

Ce service permet au Client de proposer à ses propres clients un paiement dans une devise autre que l'euro.

Le Client est informé que les paiements par carte dont la sécurisation est assurée par le Service Cyberplus Paiement s'effectuent selon les modalités prévues dans les accords conclus entre la Banque Populaire et les réseaux internationaux (ex : Visa, MasterCard …).

Aux termes de ces accords, la compensation des paiements réalisés sur le site internet du Client dans une devise étrangère acceptée par lui se fera en euros en application du taux de change en vigueur à la date de traitement de l'opération de paiement et appliqué par le réseau international dont la marque figure sur la carte utilisée pour le paiement,

Le produit de ce paiement sera imputé sur un compte dont la devise de tenue de compte est l'euro.

Le Client reconnaît qu'il est seul responsable, pour les différentes devises applicables, de l'indication du taux de conversion des paiements effectuées en devises étrangères qu'il a paramétré sur son site internet, la Banque Populaire n'étant responsable ni de la conversion, ni du taux de change appliqué.

5.1 PERSONNALISATION AVANCEE

Le service de Personnalisation avancée permet au Client de modifier en toute autonomie les aspects graphiques et textuels du formulaire de paiement par défaut ou standard, selon sa propre charte visuelle à partir de l'OUTIL GESTION DE CAISSE de Cyberplus Paiement. Cette interface permet la création ou l'importation de plusieurs formulaires de paiement par boutique permettant au Client de les gérer dynamiquement selon ses temps forts commerciaux (ex : page dédiée pour Noël). Le service permet la prévisualisation des formulaires à la fois en mode web et mobile et une mise en ligne en temps réel depuis l'OUTIL GESTION DE CAISSE.

L'utilisation de ce service par le Client s'effectue sous réserve du respect par ce dernier des stipulations figurant à l'article 11 des présentes.

Le Client assume également la pleine et entière responsabilité de la personnalisation de son formulaire de paiement et s'engage à prendre à sa charge toutes les conséquences que pourraient avoir, à l'égard de la Banque Populaire, une utilisation de ce service non conforme à la loi.

5.2 MAIL AVEC LIEN POUR PAIEMENT

Le service Mail avec lien pour paiement permet au Client de transmettre à ses Acheteurs, sous sa seule responsabilité, des courriers électroniques ponctuels intégrant dans le corps des messages un lien URL pointant vers le formulaire de paiement Cyberplus Paiement.

Le Client peut opter pour ce service, afin de transmettre des messages électroniques afférents à un produit, un service, une cotisation, un règlement de facture ou une proposition contractuelle, quelle qu'en soit la nature, et de permettre à ses Acheteurs, destinataires de ce courrier électronique, de procéder éventuellement à un paiement par carte.

Le Client est seul responsable du respect des lois et règlements applicables aux ventes et prestations réalisées à distance, ainsi que celles applicables au commerce électronique. Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et, le cas échéant, se soumettre aux dispositions relatives aux dons et règlement de cotisations qui lui sont applicables .

5.2.1 Gestion du contenu de l'e-mail et envoi aux Acheteurs

Insertion d'un lien URL vers le formulaire de paiement Cyberplus Paiement

Via l'OUTIL GESTION DE CAISSE, le Client peut paramétrer sous sa seule responsabilité les caractéristiques de l'ordre de paiement associé au lien URL inséré dans l'e-mail (durée, montant et devise) et modifier le texte par défaut proposé par le service Mail avec lien pour paiement. Une fois ces étapes de paramétrages terminées, le Client peut procéder à l'envoi depuis le Service Cyberplus Paiement des e-mails de façon unitaire dans la limite de 100 adresses saisies depuis l'OUTIL GESTION DE CAISSE.

La Banque Populaire s'engage à insérer dans le courrier électronique rédigé par le Client, un lien URL pointant vers le formulaire de paiement Cyberplus Paiement, afin de permettre à tout Acheteur destinataire d'un message de donner éventuellement un ordre de paiement.

5.2.2 Génération de liens URLs par le service Cyberplus Paiement et gestion des envois d'e-mails par le Client

Via l'utilisation de Web services, le Client peut demander la génération de liens URL. A cette fin, le Client adresse les caractéristiques de l'ordre de paiement au service Cyberplus Paiement qui lui restitue un lien URL correspondant (durée, montant et devise). Une fois le lien récupéré, le Client peut procéder à la gestion du contenu de l'e-mail et à son envoi depuis ses propres outils à partir de son système d'information ou celui d'un tiers.

La Banque Populaire s'engage à produire le lien URL comportant les caractéristiques de l' ordre de paiement pointant sur le formulaire de paiement Cyberplus Paiement, mais ne pourra être tenue responsable du contenu de l'e-mail.

5.2.3 Licéité du contenu du message

Le Client est seul responsable des informations contenues dans ses messages adressés à ses Acheteurs.

En tant que diffuseur et non éditeur des messages, la Banque Populaire n'assurera aucun contrôle sur la licéité du contenu des messages du Client.

Le Client s'engage à ce que les messages émis respectent la réglementation en vigueur (respect des bonnes mœurs, de l'ordre public, interdiction de toute forme de manifestation raciste…).

Le Client s'engage également à respecter les droits de la personnalité et le droit de la propriété intellectuelle d'autrui. Il déclare notamment posséder les droits de reproduction et de représentation de l'image des personnes et des œuvres intellectuelles, textes, éléments graphiques, artistiques, sonores présents dans les messages.

Par ailleurs, le Client s'engage aussi à respecter la législation propre au commerce, à la vente à distance, à la consommation et à la protection des données nominatives et à ne pas se recommander de la Banque Populaire auprès de ses Acheteurs.

5.2.4 Licéité de l'émission du message

Le Client est seul responsable des adresses électroniques utilisées dans le cadre du service Mail avec lien pour paiement.

À cet égard, il s'assure notamment que la personne à laquelle il adresse ce message, l'a expressément et préalablement autorisé à recevoir des courriers électroniques de cette nature et qu'elle a été dûment informée de ses droits.

Le Client s'engage à respecter l'ensemble de la réglementation relative à la prospection par courrier électronique et au Code des postes et télécommunications et plus particulièrement les dispositions de l'article L34-5 dudit code.

La Banque Populaire ne saurait être tenue pour responsable de toutes communications ou de tout envoi d'un courrier électronique sans le consentement préalable et exprès du destinataire, des conséquences résultant d'un problème ou défaut d'acheminement des messages adressés par le Client à ses propres Acheteurs, dont la liste des adresses électroniques a été communiquée à la Banque Populaire dans le cadre du service Paiement par e-mail.

La Banque Populaire garantit au Client qu'aucun usage commercial ne sera fait par celle-ci des données et notamment des adresses électroniques transmises par le Client à la Banque Populaire dans le cadre du service Mail avec lien pour paiement.

5.2.5 Responsabilités

Le Client s'engage à informer la Banque Populaire, par lettre recommandée avec accusé de réception de toutes plaintes, actions en justice, réclamations exercée par tout tiers, directement ou indirectement, liées à la diffusion des messages liés au service Mail avec lien pour paiement.

Le Client s'engage à assurer à ses frais la défense de la Banque Populaire dans le cas où cette dernière ferait objet d'une action en revendication relative aux données contenues dans les messages, et à prendre à sa charge l'indemnité due en réparation du préjudice éventuellement subi.

5.3 CONTROLE RISQUES

Ce service est constitué d'un ensemble de contrôles permettant au Client d'affiner sa gestion client en fonction de ses propres critères de risque. Le résultat des contrôles est restitué en temps réel dans l'OUTIL GESTION DE CAISSE par le biais d'un indicateur. Il existe également la possibilité de disposer de ces informations dans le journal des transactions. Il est possible de choisir, pour chaque contrôle, un mode de fonctionnement différent (filtre ou scoring).

La Banque Populaire ne saurait être tenue pour responsable des choix du Client concernant ses critères de risque. En souscrivant ce service additionnel, le Client reconnaît avoir reçu de la Banque Populaire la documentation relative au service et avoir été informé de la possibilité de recourir à l'Assistance Clients visée à l'article 10. Le Client reconnaît disposer des compétences nécessaires à son paramétrage et son utilisation.

5.4 GESTION COMPTE CLIENT

Le service Gestion Compte Client offre la possibilité au Client de proposer un moyen de payer plus rapide et plus convivial à ses Acheteurs. Une fois le compte client créé de façon sécurisée sur la plate-forme de paiement, l'Acheteur n'a plus besoin de saisir les données de sa carte bancaire à chaque paiement.

L'Acheteur et le Client sont notifiés de la création du compte client et de l'identifiant qui lui est rattaché.

La conservation sécurisée des identifiants de ses Acheteurs est sous la responsabilité exclusive du Client

5.5 GESTION BANCAIRE SIMPLIFIEE

Ce service comprend le rapprochement bancaire et le rapprochement des impayés

Le service de rapprochement bancaire permet de faire le lien entre les commandes enregistrées sur les différents canaux de vente avec les règlements indiqués sur le relevé d'opérations cartes du Client. Ce service rapproche quotidiennement et automatiquement les commandes validées sur le site internet du Client ou tout autre canal de vente avec son relevé d'opérations cartes. Le résultat de ce rapprochement se matérialise par la restitution d'un indicateur disponible depuis l'OUTIL DE GESTION DE CAISSE et/ou sous forme de fichier.

Le rapprochement des impayés permet d'informer le Client, sous la forme d'un indicateur de type OUI ou NON, de la réception d'un impayé sur un paiement par carte. Ce service est disponible sous forme visuelle à partir de l'OUTIL GESTION DE CAISSE et/ou sous forme de fichier à l'identique de ce qui existe pour le rapprochement bancaire.

5.6 GESTION UTILISATEUR

La gestion utilisateur permet à un Client de gérer, sous sa seule responsabilité, en toute autonomie les accès et les habilitations à l'OUTIL GESTION DE CAISSE pour chacun de ses collaborateurs. Il est disponible directement à partir de l'OUTIL DE GESTION DE CAISSE et repose sur la désignation d'un administrateur à partir du Formulaire d'Inscription Client.

5.7 SUIVI CLIENT

Le service Suivi Client permet d'apporter d'avantage de personnalisation du service de paiement vis-à-vis des Acheteurs. Pour chaque paiement validé, un e-mail de confirmation personnalisé au logo de la Banque Populaire est adressé en temps réel au client pour l'informer du détail du paiement lié à sa commande. En cas de paiement en « n fois », un échéancier est présenté dans l'e-mail pour informer le client des dates et des montants des prochains paiements.

6. DOCUMENTATION DU SERVICE CYBERPLUS PAIEMENT

Dès réception du Formulaire d'Inscription Client composant les Conditions Particulières, la Banque Populaire adresse au Client un Kit documentaire intégrant les modalités techniques de mise en œuvre du Service Cyberplus Paiement. Les modalités de recettes et de passage en production sont décrites dans ce Kit documentaire.
Ce Kit est spécifique à la Solution Cyberplus Paiement souscrite par le Client auprès de la Banque Populaire.

6.1 SOLUTION CYBERPLUS PAIEMENT ACCESS

Le Kit documentaire ACCESS est composé des éléments suivants :

Un guide de démarrage,

- Un manuel utilisateur de l'outil de « gestion de caisse »,

- Un descriptif des journaux de reporting.

6.2 SOLUTIONS CYBERPLUS PAIEMENT NET ET MIX

Les Kits documentaires NET et MIX sont composés des éléments suivants :

- Un guide de démarrage,
- Un guide d'implémentation de la page de paiement pour les paiements en ligne,
- Un kit d'images pour le formulaire de paiement en ligne,
- Un guide des cartes de test,
- Un guide d'implémentation standard des web services,
- Un manuel utilisateur de l'outil « gestion de caisse »,
- Un descriptif des journaux de reporting,
- Un guide pratique commerçant :
  - Prise en main rapide de l'outil « gestion de caisse »,
  - Cinématique des transactions,
  - Garantie de paiement 3DSecure,
  - Suivi Client-Accepteur «CB» (service additionnel),
  - Gestion Bancaire Simplifiée en mode visuel (service additionnel),
  - Contrôle Risques (service additionnel).
- Un Procès verbal de recette,

Un service de Support Technique et d'Assistance Clients tels que décrits aux articles 7.3.3 et 10 ci-dessous est à la disposition du Client.

Le Client s'engage à respecter les présentes Conditions Générales ainsi que les spécifications d'utilisation du Service Cyberplus Paiement telles que décrites dans la Documentation.

Le Client reconnaît disposer de la compétence nécessaire pour procéder aux vérifications et tests nécessaires tant lors de l'installation qu'au cours de l'utilisation du Service Cyberplus Paiement.

Pendant l'exécution du contrat, le Client reste gardien et seul responsable de ses matériels, logiciels, fichiers, programmes, informations ou bases de données.

Le Client est seul responsable de la gestion et du stockage du certificat de production de sa boutique en ligne. En cas de défaillance sécuritaire, la Banque Populaire ne peut être tenue pour responsable.

Le Client reconnaît que la Banque Populaire a satisfait à ses obligations de conseil et d'information concernant les caractéristiques essentielles et les modalités de fonctionnement de la Solution Cyberplus Paiement et/ou des services additionnels, eu égard aux besoins qu'il a exprimés.

7. OBLIGATIONS DU CLIENT RELATIVES AU SERVICE CYBERPLUS PAIEMENT

7.1 MISE EN GARDE ET CONDITIONS D'ADHESION

Il appartient au Client de s'assurer notamment de l'adéquation de la Solution Cyberplus Paiement à ses propres besoins et de la possibilité, ainsi que de l'opportunité pour lui d'utiliser ce service.

Le Client est tenu de vérifier que son environnement informatique, en ce compris ses serveurs, systèmes d'exploitation, logiciels et ordinateurs ou ceux d'un tiers s'il a recourt à la sous-traitance, est en parfait état de fonctionnement afin de permettre à ses propres clients d'utiliser le Service Cyberplus Paiement.

Le Client reconnaît, par ailleurs, avoir été informé des risques inhérents à l'utilisation des réseaux internet et particulièrement, en termes de :

- Défaut de sécurité et de confidentialité dans la transmission, dans la réception des instructions et/ou des informations sur les demandes de paiement sécurisé ;
- Performance dans la transmission des messages, d'informations sur la demande de paiement sécurisé et d'exécution d'instructions ;
- Mise à jour différée de l'ensemble des informations sur les demandes de paiement sécurisé effectuées.

Le Client est informé que pour bénéficier du Service Cyberplus Paiement, il doit :

- être titulaire d'un compte bancaire ouvert auprès d'une Banque Populaire,
- avoir souscrit un contrat d'acceptation en paiement à distance par cartes bancaires CB ou agréées CB en cours de validité avec Banque Populaire,
- le cas échéant, avoir souscrit auprès du réseau privatif concerné le contrat d'acceptation en paiement par carte nécessaire pour permettre à ses clients de payer avec une telle carte (ex : American Express …). La Banque Populaire décline toute responsabilité en cas de défaut de fourniture par le réseau privatif des identifiant et mot de passe correspondant au contrat souscrit, et en cas d'anomalie ou dysfonctionnement dans le traitement des ordres de paiement reçus dans le cadre dudit réseau privatif.

7.2 SECURITE

Le Client s'engage à mettre en œuvre et à faire mettre en œuvre les dispositifs (matériel, procédures...) permettant d'assurer la confidentialité et la sécurité des documents de spécifications techniques, les fichiers, les données, les éléments sécuritaires remis par la Banque Populaire dans le cadre de la présente Convention.

7.2.1 Confidentialité des identifiants du Client

La Banque Populaire propose au Client un accès sécurisé à l'OUTIL DE GESTION DE CAISSE.

Le Client s'engage à respecter et à faire respecter l'ensemble des obligations de sécurité, qui sont mises à sa charge, et notamment à conserver sous son contrôle exclusif et dans le respect des obligations de confidentialité à sa charge, les identifiant et mot de passe. Il s'engage également à modifier régulièrement son mot de passe.

Le Client est entièrement responsable de l'usage et de la conservation de son identifiant et de son mot de passe, ainsi que des conséquences d'une divulgation, même involontaire, à quiconque ou d'une usurpation. Toute utilisation des codes d'accès et mots de passe du Client sera réputée effectuée par ce dernier. L'identification et l'authentification du Client au moyen de l'utilisation de l'identifiant et mot de passe valent imputabilité des opérations effectuées au Client.

En cas de perte ou d'oubli, le Client peut demander l'attribution d'un nouvel identifiant et d'un nouveau mot de passe

7.2.2 Protection des fichiers et documents

Le Client se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à la Banque Populaire en constituant un double de ceux-ci. Le Client se déclare à cet égard pleinement informé de ce que les supports informatisés présentent une fragilité et une fiabilité nécessitant, d'une part de vérifier la qualité et l'exhaustivité de ses sauvegardes, d'autre part de réaliser des sauvegardes multiples.

Le Client est informé qu'il fait son affaire de la conservation et de l'archivage des documents concernant sa clientèle et/ou son activité pendant la durée légale et/ou règlementaire fixée par les textes.

7.3 MOYENS TECHNIQUES D'ACCES AU SERVICE CYBERPUS PAIEMENT

7.3.1 Environnement informatique du Client

Le Client doit s'assurer que son site internet et son environnement informatique, en ce compris ses serveurs, systèmes d'exploitation, logiciels et ordinateurs, permettent l'installation et l'utilisation du Service Cyberplus Paiement.

En cas d'hébergement de son site internet par un tiers, le Client doit s'assurer auprès de son hébergeur de la compatibilité de son environnement informatique avec le serveur Cyberplus Paiement.

Le Client s'engage à activer les fonctionnalités nécessaires à l'utilisation du Service Cyberplus Paiement, dans les meilleurs délais ou à les désactiver en cas de suspension, quelles qu'en soient les causes.

Dans le cadre de l'évolution du Service Cyberplus Paiement, le Client est informé que la Banque Populaire se réserve le droit de modifier, à tout moment, les spécifications techniques et caractéristiques du Service Cyberplus Paiement. Dans cette hypothèse, le Client sera préalablement informé par la Banque Populaire des modifications techniques substantielles.

7.3.2 Installation sur l'environnement informatique du Client

Le Service Cyberplus Paiement ne peut être utilisé que sur l'environnement informatique du seul site internet du Client précisé lors de la souscription dans son Formulaire d'Inscription Client.

Préalablement à tout changement d'activité et/ou d'URL concernant son site internet, le Client sollicitera l'accord de la Banque Populaire. En outre le Client s'assurera de la compatibilité de son nouvel environnement informatique et/ou de son nouveau site internet avec le Service Cyberplus Paiement.

Toute modification ou adaptation de l'environnement informatique et/ou du site internet, nécessaire à l'utilisation du Service Cyberplus Paiement, reste à la charge du Client et s'effectue sous sa seule responsabilité.

En tout état de cause, la Banque Populaire ne saurait supporter aucune conséquence liée à l'impossibilité totale ou partielle d'utiliser le Service Cyberplus Paiement, à la suite d'une modification de l'environnement informatique du Client ou d'une incompatibilité de systèmes informatiques.

Le Service Cyberplus Paiement s'appuie sur deux guides d'implémentation :

- Guide d'implémentation du formulaire de paiement,
- Guide d'implémentation standard Web service (uniquement pour l'offre commerciale Cyberplus paiement MIX).

Concernant les droits de propriété intellectuelle et la confidentialité, le Client s'engage à respecter scrupuleusement les dispositions des articles 12 et 13 de la présente Convention. Il s'engage également à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement du Service Cyberplus Paiement.

7.3.3 Support Technique à l'intégration du Service Cyberplus Paiement

Le Client pourra, dès signature du Formulaire d'Inscription Client, solliciter le Support Technique pour obtenir une aide à l'intégration des éléments nécessaires au Service Cyberplus Paiement :

Le Support Technique est assuré par la société partenaire LYRA NETWORK du lundi au vendredi **de 9h00 à 18h00.**
Tél. : 0811 363 364 (numéro Azur – coût d'un appel local depuis un poste fixe).
E-mail : supportvad@lyra-network.com.

Le Client peut bénéficier de ce service à compter de la date de signature du Formulaire d'Inscription Client, en cas de problèmes ou de questions lors de l'interfaçage de son site internet au serveur Cyberplus Paiement.

7.3.4 Présentation du SITE INTERNET et /ou des messages

Sauf en cas d'option pour la personnalisation de sa page de paiement, le Client s'engage à faire figurer sur la page d'accueil de son site internet, ainsi que sur les messages qu'il adresse à partir de son site internet l'ensemble des informations relatives au Service Cyberplus Paiement.

A cet égard, le Client s'engage à y faire figurer :

- les Signes Distinctifs mis à sa disposition par la Banque Populaire pour l'utilisation du Service Cyberplus Paiement et, le cas échéant des Services Additionnels,
- les logos utilisés pour l'authentification 3-D Secure, tels que notamment Verified by Visa, Mastercard Secure code.

Le Client s'engage à communiquer à la Banque Populaire l'URL de son site internet via le Formulaire d'Inscription Client et à valider l'activation de la connexion au Service Cyberplus Paiement de la Banque Populaire et, le cas échéant, aux Services Additionnels.

Les parties s'engagent à coopérer pour la mise en place de tout hyperlien. Le Client dispose, après installation d'un hyperlien, d'un délai de quinze (15) jours pour adresser toute observation à la Banque Populaire. A défaut, le Client est réputé avoir validé le ou les hyperliens réalisés.

Le Client s'engage à vérifier la permanence et le maintien de la connexion au Service et reste seul responsable de la capacité de son serveur à traiter le trafic électronique, en termes d'accès simultané et de temps de réponse, qui sera généré à partir de la connexion au Service

8. DISPONIBILITE DU SERVICE CYBERPLUS PAIEMENT

Le Service Cyberplus Paiement est accessible tous les jours (7 jours/7), 24 heures sur 24, sous réserve des indisponibilités occasionnelles énoncées ci-dessous.

Le Service Cyberplus Paiement peut être momentanément inaccessible afin de réaliser des opérations d'actualisation, de sauvegarde ou de maintenance. Dans ces hypothèses, la Banque Populaire s'efforcera d'en informer le Client par courrier électronique avant toute intervention.

D'une manière générale, le Client reconnaît que la disponibilité du Service Cyberplus Paiement ne saurait s'entendre de manière absolue, et qu'un certain nombre de défaillances, de retards ou de défauts de performance peuvent intervenir indépendamment de la volonté de la Banque Populaire, compte tenu de la structure du réseau internet ou GSM et des spécificités liées au Service Cyberplus Paiement.

9. MODIFICATION ET EVOLUTION DU SERVICE CYBERPLUS PAIEMENT

Il est expressément convenu entre les parties que la Banque Populaire se réserve le droit de modifier à tout moment, pour des raisons notamment techniques et/ou de sécurité, les conditions du Service Cyberplus Paiement.

Il est entendu entre les parties que toute nouvelle condition du Service Cyberplus Paiement entrera en vigueur à la date précisée par la Banque Populaire dans le courrier de notification adressé au Client par tous moyens. Seront joints à ce courrier les éléments d'information nécessaires pour l'exécution des mises à niveau.

Le Client disposera du délai stipulé dans le courrier de notification pour accepter ou résilier le Service Cyberplus Paiement dont les conditions auront été modifiées.

Si le Client n'effectue pas les dites mises à niveau dans les délais impartis, la responsabilité de la Banque Populaire ne saurait être recherchée en cas de dysfonctionnement du Service Cyberplus Paiement

10. ASSISTANCE CLIENTS LORS DE L'EXPLOITATION DU SERVICE CYBERPLUS PAIEMENT

Le Client pourra faire appel à l'Assistance Clients en cas de problèmes survenus lors de l'exploitation du Service Cyberplus Paiement.

L'Assistance Clients est assurée par l'équipe Cyberplus Paiement du lundi au vendredi de **9h00 à 18h00.**
Tél. : 0811.363.364 (numéro Azur – coût d'un appel local depuis un poste fixe)
E-mail : cyberplus.paiement@paiements.natixis.fr

L'Assistance Clients Cyberplus Paiement concerne toutes les demandes liées à la gestion courante des services (paramétrage du site/boutique et suivi des opérations de paiement) et au fonctionnement ou utilisation des outils de la Solution Cyberplus Paiement.

Le Client pourra contacter l'Assistance Clients par messagerie électronique ou par téléphone ou pendant les heures d'ouverture du service, telles que ci-avant précisées.

Avant chaque appel téléphonique, il appartient au Client :

- de se reporter à la Documentation visée à l'article 6 des présentes Conditions Générales et de décrire de façon précise et exhaustive, les symptômes du problème rencontré aux fins d'en faciliter le diagnostic ;
- d'adresser à la Banque Populaire la totalité des éléments demandés ;
- de rendre disponible le cas échéant son mandataire désigné sous le terme « d'Interlocuteur technique » dans le Formulaire d'Inscription Client, dont le Client garantit la compétence technique.

Le Client autorise la Banque Populaire à effectuer toutes les opérations de contrôle permettant de vérifier l'utilisation du Service Cyberplus Paiement conformément à la Documentation.

A partir des informations communiquées par le Client, la Banque Populaire procède au diagnostic et indique au Client, par téléphone ou par courrier électronique, la procédure à suivre pour pallier les problèmes rencontrés par ce dernier.

11. RESPECT DE LA LEGISLATION EN VIGUEUR

Le Client s'engage à respecter la législation et les réglementations en vigueur, en particulier, à ne pas diffuser des informations contraires aux bonnes mœurs, à l'ordre public, aux droits et à la réputation de tiers, à la dignité humaine

Le Client reconnaît à ce titre qu'il a l'entière et pleine responsabilité de la licéité des contenus qu'il diffuse dans le cadre de l'utilisation de la Solution Cyberplus Paiement et du Service Cyberplus Paiement. Par conséquent, il garantit notamment que les contenus :
- ne portent pas atteinte à la vie privée de tiers
- ne pas portent pas atteinte aux droits de propriété intellectuelle de tiers
- n'incitent pas à la réalisation de crimes et délits
- ne font aucune discrimination
- ne provoquent pas la haine ou la violence en raison de la race, de l'ethnie ou de la nation,
- ne transmettent pas de fausses nouvelles,
- ne sont pas diffamatoires, injurieux, offensants et/ou outrageants
- ne pas portent pas atteinte au droit à l'image des personnes.
- ne portent pas atteinte à l'image ni ne dénigrent les produits ou services offerts par des tiers
- ne contiennent pas d'informations fausses de nature à causer un préjudice à des tiers en influençant leur comportement
- ne sont pas obscènes, vulgaires, pornographiques ou indécents,
- ne constituent pas ou n'encouragent pas des comportements susceptibles de constituer un délit,

La Banque Populaire ne pourra être tenue responsable de toute infraction à la législation et réglementations précitées.
Le Client garantit la Banque Populaire qu'il détient l'ensemble des droits d'auteur sur les contenus qu'il diffuse dans le cadre de l'utilisation du Service Cyberplus Paiement et de la Solution Cyberplus Paiement.
Le client garantit la Banque Populaire contre tous recours et/ou actions que pourraient former à un titre quelconque, les tiers sur tout ou partie des contenus diffusés par le Client.

Le Client s'engage, sous les mêmes conditions, à adhérer aux bons usages de la profession de la vente à distance et à les mettre en œuvre, à respecter les règles du commerce concernant la vente en général et de la vente à distance en particulier, ainsi que la législation notamment sur les devises, les taxes, les publications.

Dans le cas de vente en ligne à partir d'un site marchand, le Client déclare et garantit que ledit site, ainsi que les liens rattachés, ne présentent pas de caractère illicite, immoral ou illégal et qu'ils ne portent pas atteinte aux droits des tiers, notamment aux droits de la personnalité et aux droits de la propriété intellectuelle.

De même le Client garantit que les produits et services qu'il délivre via son site internet sont conformes à l'activité qu'il a initialement déclarée à la Banque Populaire lors de son adhésion au Service Cyberplus Paiement. A cet égard, le Client s'engage à informer sans délai la Banque Populaire de tout changement d'activité.

Le Client s'engage à ne pas mettre en œuvre une activité de galerie marchande virtuelle multi-sites ou de prestation de paiement centralisée sans l'accord écrit de la Banque Populaire.

Le Client garantit qu'il ne conservera, ni ne stockera, de manière informatique ou manuelle, les références bancaires des Acheteurs (numéro de la carte bancaire, numéro de compte bancaire,…) auxquelles il aurait eu accès, dans le cadre de l'utilisation du Service Cyberplus Paiement.

Toutefois, si le Client conserve les numéros de cartes bancaires des Acheteurs dans un fichier ayant pour finalité de lutter contre la fraude au paiement, celui-ci garantit la Banque Populaire qu'il a déclaré au préalable ce fichier ainsi que sa durée de conservation auprès de la CNIL et qu'il a informé clairement les Acheteurs de l'existence et de la finalité d'un tel traitement afin que ces derniers puissent s'y opposer et ce, conformément aux dispositions de la Loi Informatique et Libertés.

Le Client déclare détenir le droit d'usage et de diffusion des éléments (textes, éléments graphiques ...) qu'il utilise, et ne pas porter atteinte à un quelconque droit de propriété intellectuelle ou droit de la personnalité.

12. DROIT DE PROPRIETE INTELLECTUELLE

La Banque Populaire conserve, en tant que titulaire des droits, la propriété intellectuelle des documents techniques et plus généralement de tous les éléments remis au Client, ainsi que toutes les prérogatives s'y rattachant. Le Client n'acquiert par le Contrat Cyberplus Paiement aucun droit de propriété intellectuelle mais un simple droit d'utilisation personnel, non transférable et non exclusif pour la durée des présentes.

Le Client s'engage à ne pas modifier ou faire modifier les documents techniques ou les éléments remis, à ne pas les utiliser pour un autre usage que celui prévu par le Contrat Cyberplus Paiement, à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement.

Il s'oblige aussi à ne pas dupliquer ou faire dupliquer la documentation technique ou les éléments reçus pour une autre raison que celle des tests d'évaluation et dans ce cas, à détruire les copies dupliquées et à retourner l'ensemble de la documentation Cyberplus Paiement dès la fin des tests.

La Banque Populaire demeure propriétaire des procédés, moyens, méthodes et savoir-faire qu'elle met en œuvre pour exécuter ses prestations.

13. CONFIDENTIALITE – SECRET BANCAIRE

13.1 Le Client s'engage à garder le secret le plus absolu notamment sur les méthodes utilisées par la Banque Populaire et dont il pourrait avoir connaissance dans le cadre de l'exécution de la présente Convention Cyberplus Paiement. A ce titre, il s'engage notamment à ne transférer ou mettre à la disposition ou à la connaissance d'aucun tiers autre qu'un sous-traitant et dans la stricte limite nécessaire à la transmission des ordres de paiement vers le Service Cyberplus Paiement, et sous aucun prétexte, la Documentation technique visée à l'article 6 ci-avant, manuels utilisateurs, matériels ou droits dont il pourrait bénéficier ou avoir l'usage.

En cas de sous-traitance, le Client s'engage à imposer à ses sous-traitants le respect de la confidentialité des méthodes et Documentation technique précitées de la Banque Populaire relative à la présente Convention.

Il s'oblige en outre à informer sans délai la Banque Populaire de toute potentialité de divulgation du secret.

13.2 Les documents ou renseignements fournis par le Client, ainsi que les états, études et documents provenant de leur traitement sont couverts par le secret bancaire. En particulier, aucune communication n'en pourra être effectuée à des tiers, sauf dispositions légales l'y autorisant ou autorisation expresse du Client. La Banque Populaire s'oblige à respecter de façon absolue cette obligation au secret et à la faire respecter de la meilleure façon par son personnel, ses sous-traitants, ou prestataires de services. Pour l'application de cette disposition, il est précisé que conformément aux dispositions de l'article L.511-33,6° du Code monétaire et financier, des informations confidentielles pourront être communiquées à toute personne devant intervenir ou accéder aux fichiers et en particulier les conseils ou sous-traitants de la Banque Populaire.

13.3 L'obligation de confidentialité continuera à lier les parties et leurs ayants droit, pendant toute la durée de la Convention de service et pendant cinq (5) ans après sa résiliation ou son expiration. Le présent article survivra à la résiliation ou à l'expiration de la Convention pour quelque cause que ce soit.

14. CONDITIONS FINANCIERES - FACTURATION ET REGLEMENT

14.1 Les conditions financières du Service Cyberplus Paiement sont indiquées dans le Formulaire d'Inscription Commerçant spécifique à chaque Solution Cyberplus Paiement.

Sauf dispositions contraires, figurant dans le Formulaire d'Inscription Commerçant spécifique à la Solution Cyberplus Paiement, les factures de la Banque Populaire sont payables sans escompte dès réception.

14.2 Dans le cas où une facture ne serait pas réglée dans les trente (30) jours de son envoi par la Banque Populaire au Client, la Banque Populaire aura la faculté de suspendre l'exécution des prestations prévues par la présente Convention de service, jusqu'au règlement de la facture en souffrance, et sans que cette suspension puisse être considérée comme une inexécution des ses obligations contractuelles, ou comme une résiliation de Contrat Cyberplus Paiement du fait de la Banque Populaire, ou n'ouvre un quelconque droit à indemnisation pour le Client.

Tout mois commencé sera entièrement dû.

14.3 En outre, à compter du trente et unième jour, la somme due portera intérêt au taux de trois (3) fois le taux d'intérêt légal sans qu'une mise en demeure préalable soit nécessaire, même par simple lettre, l'intérêt étant dû et exigible par le seul fait de l'échéance du terme contractuel.

15. RESPONSABILITE DE LA BANQUE POPULAIRE

La Banque Populaire garantit ses prestations dans les conditions ci-dessous précisées :

15.1 Le Service est conforme aux spécifications de la documentation technique, à l'exclusion de toute adéquation à des besoins implicites envisagés par le Client. La Banque Populaire ne saurait toutefois être tenue pour responsable des dysfonctionnements du Service Cyberplus Paiement ayant pour origine l'intervention du Client ou de tiers, tels que notamment le fournisseur d'accès Internet (FAI) ou l'opérateur Télécom (par exemple, accès momentanément indisponible, lenteur ou retard dans l'affichage des pages HTML).

15.2 La Banque Populaire ne répond ni des dommages indirects tels que notamment manque à gagner, perte financière, perte de clientèle, perte de bénéfices ou d'économies escomptées, trouvant leur origine ou étant la conséquence de la Convention de service, ni des dommages causés à des personnes ou des biens distincts de l'objet de la présente convention de service.

15.3 Au cas où la responsabilité de la Banque Populaire serait retenue, et ce pour quelque raison que ce soit, les parties conviennent expressément que, quel que soit le préjudice subi, la Banque Populaire ne sera pas tenu de payer un montant supérieur aux redevances versées par le Client au titre des douze (12) derniers mois de facturation de la présente Convention de service.

15.4 La responsabilité de la Banque Populaire ne pourra également être engagée en cas d'usage impropre du Service Cyberplus Paiement, par l'Acheteur, le Client ou tout tiers non autorisé.

15.5 De même, la responsabilité de la Banque Populaire ne pourra être engagée en raison des conséquences susceptibles de découler d'un usage frauduleux ou abusif de l'identifiant et du mot de passe.

15.6 La Banque Populaire ne saurait être tenue pour responsable des difficultés liées à une mauvaise utilisation du Service Cyberplus paiement et de la Documentation visée à l'article 6 des présentes Conditions Générales.

15.7 La Banque Populaire ne saurait être tenue pour responsable des difficultés d'accès au site internet du Client ou au Service Cyberplus Paiement en raison de la saturation et de la complexité du réseau internet.

16. DIVERS

16.1 En cas de difficulté d'interprétation ou de contradiction entre les titres des articles et le texte de leur contenu, le contenu des articles primera sur leur titre.

16.2 Les dispositions de la présente Convention prévalent sur toute proposition ou accord antérieur, ainsi que sur toute autre communication antérieure entre les parties ayant trait au Service Cyberplus Paiement.

16.3 Si l'une quelconque des stipulations de la présente Convention est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle sera réputée non écrite, mais n'entraînera pas la nullité de la Convention.

16.4 Aucune des deux parties ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution ou des retards dans l'exécution de la présente Convention du fait de la survenance d'un cas de force majeure ou d'évènements tels que l'intervention des autorités civiles ou militaires, l'interruption totale ou partielle des réseaux de communications, le refus de licence d'importation, les incendies, les grèves, les conflits sociaux, les dysfonctionnements de matériels ou toute autre cause qui serait raisonnablement hors de son contrôle.

17. MODIFICATION DES CONDITIONS

La Banque Populaire peut modifier à tout moment la présente Convention, pour des raisons techniques ou relatives à la sécurité du Service Cyberplus Paiement. Elle en informera alors le Client par écrit.

A défaut d'accord sur les modifications, le Client a la possibilité de résilier la présente Convention sans indemnité de part ni d'autre et sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

Sauf exercice de la faculté de résiliation par le Client, les nouvelles conditions entreront en vigueur dans le délai d'un (1) mois à compter de l'envoi de la lettre ou d'un courriel d'information.

18. DUREE - SUSPENSION ET RESILIATION DU CONTRAT

18.1 Durée de la Convention

La présente Convention est conclue pour une durée indéterminée.

18.2 La suspension de la Convention

La Banque Populaire pourra suspendre l'exécution de la présente Convention sans que cette suspension soit constitutive d'une résiliation ou d'un manquement à l'une de ses propres obligations, dans les cas suivants :

- dans le cas où le Client ne remplirait pas les obligations mises à sa charge (fourniture de données, accès aux renseignements, etc...) nécessaires à la bonne exécution de la présente Convention, Cette suspension pourra ainsi intervenir en cas de retard de paiement tel que prévu à l'article 14.2 de la présente Convention
- dans le cas où le contrat d'acceptation en paiement à distance sécurisé, le contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou le contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signés par acte séparé feraient l'objet d'une suspension.

La suspension sera notifiée au Client par lettre recommandée avec accusé de réception indiquant les motifs de la suspension. L'exécution reprendra une fois que les motifs à l'origine de cette suspension auront disparus, compte tenu des modifications de prix et de délais encourues de ce fait.

18.3 La résiliation de la Convention pour manquement

En cas de manquement par l'une quelconque des parties, aux obligations dont elle a la charge au titre des présentes, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer de plein droit la résiliation de la présente Convention.

En pareil cas, la Banque Populaire, lorsqu'elle prononce la résiliation, aura droit au paiement des prestations exécutées et non facturées, et pourra demander en sus une indemnité de résiliation égale au triple de la facturation du mois précédent.

18.4 La résiliation de la Convention de plein droit

La Convention sera résiliée de plein droit en cas de résiliation du contrat d'acceptation en paiement à distance sécurisé, du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signé(s) par acte(s) séparé(s).

Par ailleurs, la résiliation de la Convention entraîne automatiquement la résiliation de tous les contrats d'acceptation conclus entre la Banque Populaire et le Client pour l'exécution de la présente Convention.

18.5 La résiliation de la Convention sans motif

Chacune des parties peut résilier à tout moment la présente convention. La résiliation deviendra effective au terme d'un délai de trois (3) mois à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception.

19. ENTREE EN VIGUEUR - ELECTION DE DOMICILE - DROIT APPLICABLE - REGLEMENT DES LITIGES

La présente Convention entre en vigueur dès signature par les parties et souscription, par acte(s) séparé(s), du contrat d'acceptation en paiement à distance sécurisé, ou du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB ».

La présente Convention est soumise au droit français.

Pour l'exécution de la présente Convention, il est fait élection de domicile, par la Banque Populaire et par le Client en leur siège social mentionné aux Conditions Particulières.

Pour le règlement de toute contestation ou de tout litige relatif à la présente Convention ou découlant de son exécution, il est fait expressément attribution de compétence au tribunal dans le ressort duquel est situé le siège social de la Banque Populaire.