

## CONDITIONS GÉNÉRALES DE VENTE

VERSION APPLICABLE À PARTIR DU 1<sup>er</sup> mars 2024

### PRÉAMBULE

Ces conditions générales de vente sont conclues entre :

La personne, titulaire d'un compte de paiement ouvert dans les livres de Payplug et utilisant une ou plusieurs Solutions mises à sa disposition par Payplug, ci-après dénommée le « Client » ; et

**Payplug Enterprise SAS**, une Société par Actions Simplifiée de droit français dont le siège social est situé au 110 avenue de France, 75013 Paris, immatriculée au Registre du Commerce et des Sociétés (RCS) de Paris sous le numéro de 443 222 682 au RCS de Paris et un Établissement de paiement agréé le 03 janvier 2011 par l'Autorité de Contrôle de Prudential et de Résolution (« ACPR ») sous le numéro 16378. La société Payplug est propriétaire et gérante du site internet [www.Payplug.fr](http://www.Payplug.fr) ou, ci-après dénommée « Payplug ».

Le Client et Payplug seront ci-après dénommés les « Parties ».

Les présentes conditions générales de vente (les « CGV ») et ses annexes constituent le contrat entre les Parties, et régissant l'utilisation par le Client du service de paiement mis à sa disposition par Payplug et auquel le Client accède via une interface de gestion fournie par Payplug.

Les présentes CGV constituent l'offre de contrat-cadre de service de paiement entre Payplug et le Client. Le Client peut à tout moment les consulter, les reproduire, les stocker sur son ordinateur ou sur un autre support, se les envoyer par courrier électronique ou les imprimer sur papier de manière à les conserver ; il peut également obtenir gratuitement l'envoi d'un exemplaire par courrier postal à son adresse sur demande expresse auprès de Payplug, ainsi que les informations et conditions prévues à l'article 6 de l'arrêté du 29/07/2009 (informations fournies préalablement à l'exécution d'une opération de paiement isolée).

**Les présentes Conditions Générales de Vente s'appliquent à toutes les offres Payplug, sauf en cas d'accord spécifique convenu entre les Parties.**

## ARTICLE 1 – DEFINITIONS

Les termes utilisés dans les présentes CGV auront, lorsqu'ils sont utilisés avec la première lettre en majuscule et indépendamment du fait qu'ils soient utilisés au singulier ou au pluriel, le sens défini ci-après :

- « **Acheteur** » : désigne toute personne qui souhaite réaliser l'achat d'un bien ou le paiement d'un service par un Moyen de paiement dont il est titulaire et accepté par Payplug auprès du Client.
- « **Acquéreur "CB"** » : désigne toute entité (établissement de crédit ou de paiement, banque ...) membre du GIE CB, et qui contractuellement lié avec Payplug pour les besoins du présent Contrat.
- « **Avoir** » ou « **Solde** » : désigne le montant total disponible sur le Compte Client, à un instant T. Ce montant est la somme des crédits portés au Compte Client, desquels sont soustraits les débits du Compte Client.
- « **Carte** » : désigne tout moyen de paiement sous forme d'une carte et permettant la réalisation d'opérations de paiement au sens de l'article L133-3 du code monétaire et financier et dont le fonctionnement est défini par les règles du Réseau de Cartes auquel il est associé.
- « **Client** » : désigne toute personne physique majeure ou personne morale agissant pour les besoins de son activité professionnelle et ayant renseigné correctement les informations des Conditions Particulières et accepté les présentes CGV pour pouvoir ouvrir un Compte Client et un Compte Payplug, conformément aux instructions d'identification énumérées dans l'Article 10 des présentes CGV. Le Client a souhaité domicilier ses remises à l'encaissement auprès de Payplug.
- « **Commande** » : désigne toute transaction effectuée par un Acheteur auprès du Client et portant sur des Produits que ce dernier propose.
- « **Commission d'Interchange** » : désigne les commissions fixées par Visa, MasterCard et Cartes Bancaires. En acceptant les CGV, le Client accepte que les Frais de Transaction qui lui sont facturés par Payplug ne soient pas une représentation exacte des Commissions d'Interchange payées par Payplug à ses partenaires bancaires. Pour plus d'informations sur les Commissions d'Interchange, consultez les sites MasterCard, Visa, et Cartes Bancaires, ainsi que notre récapitulatif simplifié accessible via l'adresse <http://support.Payplug.com/>.
- « **Commission d'intervention** » : désigne les sommes perçues par Payplug pour l'intervention en raison d'une opération entraînant une irrégularité de fonctionnement du compte et nécessitant un traitement particulier (présentation d'un ordre de paiement irrégulier, coordonnées bancaires inexactes, absence ou insuffisance de provision, contestation de paiement...)
- « **Compte Client** » : désigne le compte de paiement ouvert au nom du Client auprès de Payplug. Le Compte Client n'offre pas la possibilité d'ouvrir un compte joint.
- « **Compte Bancaire** » : désigne le compte en banque du Client, renseigné par le Client au moment de son inscription, validé par Payplug, et utilisé pour recevoir les fonds lors d'un Virement.
- « **Compte Payplug** » : désigne le compte Internet ouvert par le Client sur le Site, ainsi que l'ensemble des informations qu'il a renseignées et qui constituent les Conditions Particulières, et auquel est associé son Identifiant.
- « **Conditions Générales de Vente** » ou « **CGV** » : désigne les présentes conditions générales de vente.
- « **Conditions Particulières** » : désigne le formulaire en ligne à remplir par le Client lors de son inscription au Site et contenant les informations nécessaires à la conclusion des présentes portant notamment sur son nom, prénom, date de naissance, adresse email valide, mot de passe et informations concernant le Client ainsi que les conditions tarifaires applicables au Client.
- « **Contrat** » : désigne ensemble les CGV, les Conditions Particulières et les Annexes si elles sont applicables.
- « **Donnée Sensible** » désigne toute Donnée à Caractère Personnel du Porteur, et notamment toute donnée bancaire, toute information ou donnée relative à un Ordre de Paiement ou une Opération de Paiement, et en particulier celles relatives à la Carte et au compte auquel elle est rattachée, dont le traitement, la transmission et le stockage doivent faire l'objet de mesures de protection en application des contraintes du système d'acceptation des Réseaux, de la norme PCI-DSS et de la Réglementation sur les Données Personnelles.
- « **Facilitateur de paiement** » : désigne toute entité ayant le statut de prestataire de services de

paiement au sens du code monétaire et financier, et qui organise et contrôle l'acceptation d'opérations de paiement pour tout Accepteur en paiement tel qu'un commerçant, ou toute personne au titre de son activité professionnel, dûment autorisée à recevoir du paiement et pour le compte duquel il reçoit les encaissements

- « **Frais de Transaction** » : désigne la commission prélevée par Payplug sur les Opérations de paiement effectuées par le Client, en rémunération des services rendus par Payplug et ceux de ses partenaires. Les Frais de Transaction sont visibles sur le Site. Ces Frais de Transaction peuvent faire l'objet d'une facturation minimum mensuelle. Les Frais de Transaction sont prévus aux Conditions Particulières.
- « **Identifiant** » : désigne les données nécessaires à l'identification du Client par Payplug se composant d'une adresse email valide et d'un mot de passe.
- « **Jour Ouvré** » : désigne un jour où les banques commerciales sont ouvertes à Paris (autre qu'un samedi, un dimanche ou un jour férié).
- « **Moyens de paiement acceptés par Payplug** » : désigne l'ensemble des moyens de paiement permettant la réalisation d'opérations de paiement au sens des articles L133-3 et L 341-1 du code monétaire et financier telle que la Carte ou toute autre dispositif de paiement acceptées par les Solutions. La liste des Moyens de paiement acceptés par Payplug est présente sur le Site.
- « **Passerelliste** » : désigne le prestataire de service qui pour le compte de son client est en charge d'assurer une liaison constante avec les établissements bancaires à l'occasion de l'exécution des opérations de paiement par cartes de paiement sur les Terminaux de paiement notamment pour s'assurer des demandes d'autorisations et de la sécurisation des transits de flux financiers.
- « **Portail** » : désigne l'interface de gestion à distance du Compte Payplug c'est-à-dire le compte Internet ouvert par le Client pour utiliser une des Solutions.
- « **Produit** » : désigne une information, un bien ou un service proposé à la vente par le Client.
- « **Propriétés** » : a le sens qui lui est donné à l'Article 15.
- « **Réglementation sur les Données Personnelles** » : désigne l'ensemble des dispositions applicables aux Données à Caractère Personnel, telles que (i) celles provenant de la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, incluant également toute évolution de ce texte, (ii) celles provenant du Règlement Européen 2016/679 du 27 avril 2016 en matière de respect et de protection des Données à Caractère Personnel à compter de son entrée en vigueur, et (iii) tout avis, recommandation, décision ou instruction émis par la Commission Nationale Informatique et Libertés ou toute autre autorité de contrôle qui s'y substituerait à la conclusion ou pendant l'exécution du Contrat.
- « **Remboursement** » : désigne l'opération par laquelle un Client procède à un remboursement en faveur d'un de ses Acheteurs. A la demande du Client, le montant du remboursement sera débité des Avoirs disponibles sur son Compte Client pour être crédité sur la Carte de son Acheteur ou les Moyens de paiement acceptés par Payplug utilisés lors de l'achat.
- « **Réseau de Cartes** » ou "Système de cartes de paiement" : désigne un système de paiement tel que défini à l'article 2 du Règlement n° 2015/751 du 29 avril 2015 (ci-après "le Règlement ") définissant les règles d'utilisation du ou des moyens de paiement qu'il émet, tel que la Carte. Ces règles sont disponibles sur les sites de chacun des réseaux.
- « **Responsable de traitement** » désigne la personne qui au sein d'une l'entité met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du Règlement RGPD et de protéger les droits des personnes concernées.
- « **Site** » : désigne indifféremment le site [www.Payplug.fr](http://www.Payplug.fr) et le site [www.Payplug.com](http://www.Payplug.com).
- « **Solution de Paiement en Ligne** » : désigne la solution de paiement fournie par Payplug et s'appuyant sur le Site, le Compte Client et l'ensemble des services fournis par Payplug, telle qu'elle est décrite à l'Annexe 1 des CGV.
- « **Solution de Paiement en magasin** » : désigne la solution de paiement via laquelle Payplug fournit au Client des produits et des services monétiques pour permettre au Client d'effectuer des encaissements à l'aide d'un Terminal de Paiement Électronique tel que décrit aux Annexes 2, 3 et/ou 4 des CGV.
- « **Solutions** » : désigne indifféremment la Solution de Paiement en Ligne et/ou la Solutions de Paiement en magasin.

- « **Sous-traitant** » désigne la personne physique ou morale (entreprise ou organisme public) qui traite des données personnelles conformément au Règlement RGPD pour le compte d'une autre personne (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation.
- « **Opération de paiement** » : désigne toute opération de paiement au sens de l'article L. 133-3 du Code monétaire et financier, consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre l'Acheteur et le Client, initiée par l'Acheteur ou, pour son compte, par le Client. Cette opération de paiement est (i) générée dans le cadre de l'activité du Client, (ii) reçue par Payplug sur la Solution dans le cadre du Contrat, et (iii) exécutée après autorisation de l'Acheteur.
- « **Terminal de Paiement Électronique** » ou « **TPE** » désigne un matériel utilisé dans le cadre de la Solution de Paiement en magasin.
- « **Virement** » : désigne une Opération de paiement au titre de laquelle Payplug exécute une opération de transfert de fonds, sur ordre du Client, depuis son Compte Client vers son Compte Bancaire.

## **ARTICLE 2 – ENTRÉE EN VIGUEUR DU CONTRAT – ACCEPTATION ET DOCUMENTS CONTRACTUELS APPLICABLES**

**2.1** Le Contrat entre en vigueur lors de l'ouverture d'un Compte Payplug.

**2.2** En cochant dans le formulaire d'inscription Payplug la mention « *J'accepte les Conditions Générales de Vente* », le Client reconnaît expressément qu'il :

- a attentivement lu et qu'il a compris les CGV en vigueur le jour de son acceptation,
- les accepte dans leur intégralité.

Cette acceptation vaut « signature numérique » du Contrat, conformément à l'article L. 314-13 II du Code monétaire et financier.

L'acceptation des CGV par le Client comme indiqué ci-dessus et la version en vigueur des CGV ainsi acceptées par le Client sont conservées et archivées par Payplug dans ses systèmes informatiques de façon inaltérable, sûre et fiable. Le Compte Client ne pourra être utilisé qu'après son activation conformément à l'article 12 des présentes CGV.

**2.2.1** Pour pouvoir bénéficier de la Solution de Paiement en Ligne, le Client reconnaît expressément qu'il a attentivement lu et compris les Conditions Générales de la Solution de Paiement en Ligne (Annexe 1) en vigueur le jour de son acceptation, et qu'il les accepte dans leur intégralité.

**2.2.2** Pour pouvoir bénéficier de la Solution de Paiement en magasin, le Client reconnaît expressément qu'il a attentivement lu et accepté :

- le Contrat d'Adhésion (Annexe 2 et ses sous-annexes),

Le cas échéant :

- le Contrat de Location de TPE (Annexe 3) dans le cas où le Client loue le TPE,
- le Contrat de Vente de TPE (Annexe 4) dans le cas où le Client fait l'acquisition du TPE auprès de Payplug ;
- les conditions générales d'utilisation (Annexe 5) dans le cas où le Client utilise le service Tap to Pay par Payplug (uniquement applicable en France).

Dans tous les cas, le Client reconnaît et accepte l'Annexe 6 sur la protection des données (art 28 RGPD) et s'engage la conformité du SAQ-A pré complété en Annexe 7.

**2.3** Le Contrat comporte les annexes suivantes :

Annexe 1 : Conditions Générales au Contrat de la Solution de Paiement en ligne Payplug

Annexe 2 : Contrat d'adhésion au système de paiement de proximité par cartes "CB" Ou cartes soumises aux règles "CB"

Annexe 3 : Conditions générales au contrat de location de TPE

Annexe 4 : Conditions générales au contrat de vente de TPE

Annexe 5 : Conditions générales d'utilisation du service « Tap to Pay sur Iphone »

Annexe 6 : Protection des données clauses sous-traitant (art.28 RGPD)

Annexe 7 : SAQ-A

## **ARTICLE 3 – MODIFICATION DU CONTRAT PAR PAYPLUG**

Payplug est en droit de modifier le Contrat à tout moment. En cas de modification importante, les nouvelles stipulations entreront en vigueur un (1) mois après leur publication et une notification concomitante sera adressée par email au Client sur l'adresse email que le Client aura indiquée à Payplug lors de son inscription.

Le Client disposera d'un délai d'un (1) mois à compter de la notification pour mettre fin au Contrat, sans pénalité, conformément au paragraphe IV de l'article L. 314-13 du Code monétaire et financier. En l'absence de dénonciation par le Client, dans ce délai, ce dernier sera réputé avoir accepté le Contrat tel que modifié conformément au paragraphe III de l'article L. 314-13 du Code monétaire et financier, à moins d'avoir notifié à Payplug, par lettre recommandée avec accusé de réception à l'adresse mentionnée au Préambule des présentes, son refus de celles-ci avant la date proposée pour l'entrée en vigueur des modifications.

## **ARTICLE 4 – COMPTE PAYPLUG ET CONNEXION**

### **4.1 Conditions préalables à l'inscription**

Pour pouvoir utiliser les Solutions, le Client doit (a) s'il agit en son nom et pour son compte (i) avoir plus de 18 ans, (ii) avoir la pleine capacité légale pour conclure le Contrat et (b) s'il agit en tant que représentant légal d'une personne morale et être expressément habilité à conclure le Contrat.

Le Client peut s'inscrire en ligne, et ainsi créer son Compte Payplug, via le Site en renseignant les informations demandées, en créant un Identifiant, et en acceptant le Contrat.

Le Client pourra aussi réaliser son inscription via son contact direct Payplug s'il est concerné et fournir tous les éléments demandés.

Le Client est tenu de fournir des informations exactes, complètes et sincères au moment de la création de son Compte Payplug. Si les informations fournies par le Client venaient à changer, celui-ci s'engage à en informer Payplug sans délai en mettant à jour les informations sur son Compte Payplug. Si les informations se révèlent fausses ou incomplètes, Payplug se réserve le droit, à sa seule discrétion, de fermer le Compte Payplug, de résilier l'accès aux Solutions au Client et de fermer le Compte Client.

### **4.2 Gestion des informations Payplug**

Les informations fournies par le Client au moment de son inscription constituent les Conditions Particulières.

Pour pouvoir procéder à un Virement des sommes figurant sur le Compte Client et encaissées en utilisant les Solutions, le Client sera invité à enregistrer un relevé d'identité bancaire (RIB) relatif à son Compte Bancaire. Le Compte Bancaire

enregistré doit appartenir au Client, être tenu en euro et doit être domicilié dans un des pays de l'Espace Économique Européen. Payplug se réserve le droit de refuser l'enregistrement d'un Compte Bancaire, notamment si celui-ci a déjà été enregistré en lien avec un autre Compte Payplug ou Compte Client.

### **4.3 Informations complémentaires**

Payplug se réserve le droit de demander au Client des informations et documents justificatifs supplémentaires, afin notamment d'autoriser le Client à dépasser certains seuils d'Opérations de Paiement définis par Payplug.

Payplug se réserve le droit de bloquer le Compte Client et le Compte Payplug d'un Client en attendant d'avoir reçu l'ensemble des documents et informations jugés nécessaires par Payplug et dans une forme qui soit satisfaisante

pour Payplug.

Payplug se réserve le droit de bloquer les Opérations de paiement du Client si Payplug estime avoir besoin de documents ou d'informations complémentaires sur le Client et tant que ces documents ou informations complémentaires n'auront pas été reçus par Payplug.

Le Client accepte et reconnaît qu'il est responsable du respect du caractère confidentiel de son Identifiant. Payplug ne saurait être tenu responsable de la perte de l'adresse email et/ou mot de passe, associés à ce Compte Payplug. En cas de suspicion d'une utilisation du Compte Payplug par un tiers, le Client est tenu d'en informer immédiatement Payplug à l'adresse [support@payplug.com](mailto:support@payplug.com).

## **ARTICLE 5 – OPÉRATIONS DE VIREMENTS**

Lorsqu'une Opération de paiement est réalisée avec succès, les fonds qui sont transférés à cette occasion sont reçus par le Client sur le Compte Client ouvert dans les livres de Payplug.

Sous réserve des stipulations ci-dessous, le Client obtient les fonds inscrits sur son Compte Client par le Virement réalisé vers son Compte Bancaire, dans les délais de traitement bancaires habituels propres à chaque établissement bancaire. Le Virement est exécuté par Payplug, après réception de l'ordre de paiement du Client, qui peut automatiser cette demande, depuis son Compte Payplug.

Par ailleurs, Payplug se réserve le droit de retenir aussi longtemps que nécessaire les fonds reçus et dus à un Client, dans les cas suivants :

- si Payplug a quelque soupçon que ce soit sur le Client ou sur une Opération de paiement,
- si le Client est impliqué dans un contentieux justifiant de retenir les fonds,
- si Payplug estime que le risque de Contestation de Paiement (tel que définit ci-après) est élevé en raison de l'activité du Client,
- si la loi, une décision de justice ou l'application de toute décision d'une autorité réglementaire ou gouvernementale l'exige.

Dans tous les cas, la nécessité de retenir les fonds sera justifiée par Payplug dans les limites prévues par la loi applicable.

En cas de soupçon, Payplug pourra être ponctuellement amené à s'enquérir auprès des Acheteurs de la bonne exécution de leur Commande. Payplug n'assume aucune responsabilité de quelque nature que ce soit pour les fonds qui seraient, du fait d'informations

incorrectes fournies par le Client, versés sur un compte bancaire autre que le sien.

Le Client ne percevra aucun intérêt ni aucun autre revenu sur le Solde de son Compte Client.

## **ARTICLE 6 – REMBOURSEMENT**

Les Remboursements doivent être attribuables à une Opération de paiement passée et réalisée dans les 180 jours précédents l'opération de Remboursement. Ils sont réalisés par un nouveau crédit opéré sur le Moyen de paiement utilisé par l'Acheteur pour l'Opération de paiement correspondante. Le montant du Remboursement ne peut en aucun cas dépasser le montant de l'Opération de paiement correspondante. Les remboursements se feront depuis le Compte Payplug, via le Portail ou tout autre moyen mis à disposition par Payplug ou ses partenaires.

Ces Remboursements ne feront pas l'objet de frais spécifiques dans la limite d'un montant total de Remboursements inférieur à 5% du volume généré sur les 30 jours précédents l'opération de Remboursement. Au-delà de cette limite, des frais liés à ces Remboursements pourront être ajoutés à l'initiative de Payplug et s'élèveront alors à hauteur des Frais de Transaction habituels.

## **ARTICLE 7 – CONTESTATIONS DE PAIEMENT**

Tout montant attribuable à une Opération de paiement peut être débité du Compte du Client, ou, si le montant a



déjà été viré sur son Compte Bancaire, réclamé au Client (ces actions constituant individuellement une « Contestation de Paiement » et ensemble les « Contestations de Paiement ») si l'Opération de paiement :

- est contestée de quelque manière que ce soit, notamment dans le cas où les biens ou services payés au Client
- n'auraient pas été fournis,
- est annulée par le Réseau de Cartes, une banque, l'Acheteur ou l'émetteur de la Carte.
- est considérée illégale, suspecte ou en violation des règles d'une banque ou d'un réseau concerné par cette Opération de paiement.

Pour toute Opération de paiement dont Payplug considère qu'elle pourrait donner lieu à une Contestation de Paiement, Payplug a le droit de retenir un montant égal à celui de la Contestation de Paiement sur le Compte Client en attendant de savoir si la Contestation de Paiement est réelle ou non. En lien avec la Contestation de Paiement, Payplug peut aussi débiter du Compte Client ou réclamer au Client un montant égal aux frais, pénalités ou amendes liés à la Contestation de Paiement et payés par Payplug ainsi que les frais de gestion destinés à couvrir les dépenses engagées par Payplug pour traiter cette Contestation de Paiement.

Si le Solde du Client est insuffisant pour payer la (les) Contestation(s) de Paiement, le Client doit immédiatement rembourser Payplug du montant de la (des) Contestation(s) de Paiement et des frais et dépenses engagés par Payplug concernant cette (ces) Contestation(s) de Paiement.

Si Payplug considère que les Contestations de Paiement sur le Compte Client sont trop fréquentes, Payplug se réserve le droit, à sa seule discrétion, de procéder à des vérifications ou d'imposer des conditions spécifiques à ce Compte Client, qui peuvent inclure, notamment :

- des Frais de Transaction additionnels, des frais de gestion de dossier, l'exigence d'une réserve suffisante sur le Compte Client pour couvrir les potentielles Contestations de Paiement Et frais associés futurs,
- une limitation sur le droit au Virement depuis ce Compte Client,
- une authentification des Acheteurs (3D Secure) systématique, et/ou
- la résiliation du Contrat et donc la fermeture du Compte Payplug et du Compte Client associé.

Le Client s'engage à assister Payplug, sur demande de ce dernier, dans la vérification des Opérations de paiement, notamment dans les démarches liées à la contestation des Contestations de Paiement.

## **ARTICLE 8 – FRAIS DIVERS ET CONDITIONS DE RÈGLEMENT**

Outre les Frais de Transaction, Payplug se réserve le droit de facturer les sommes suivantes au Client :

- Des frais liés à un forfait mensuel dans des conditions proposées par Payplug au Client et acceptées par ce dernier, notamment pour bénéficier de certaines offres ou fonctionnalités ;
- Des Commissions d'Intervention en cas de Contestation de Paiement : en cas d'interventions répétées de Payplug entre le Client et l'(les) Acheteur(s), notamment pour des litiges commerciaux ;

De manière générale, le Client remboursera Payplug tous les coûts, pertes ou dépenses qui pourraient résulter de l'utilisation des Solutions et dont le Client serait responsable, incluant, sans que cette liste soit limitative, toute réclamation liée au défaut d'un Produit fourni par le Client et acheté en utilisant les Solutions.

Payplug met à disposition du Client une facture mensuelle qui regroupe l'ensemble des frais facturés au Client. Cette facture est disponible dans le Compte Payplug du Client. Si le Client souhaite recevoir un relevé détaillé des Commissions d'Interchange payés par Payplug à ses partenaires pour chacune de ses Opérations de paiement, il peut l'obtenir en en faisant la demande auprès de Payplug.

De manière générale, les sommes dues à Payplug par le Client seront prélevées directement sur son Solde au moment de leur facturation. En cas de non-disponibilité des fonds nécessaires sur le Compte Client, Payplug pourra exiger le règlement immédiat de la facture et utiliser tout moyen à sa disposition, telle qu'une autorisation de prélèvement donnée par le Client pour récupérer les sommes dues. En cas de défaut de paiement, il sera alors appliqué des pénalités de retard de 0,5% par mois de retard ainsi qu'une indemnité forfaitaire pour frais de

recouvrement de 40 euros.

## **ARTICLE 9 - PREUVES**

Le Client, lorsqu'il utilise les Solutions, produit des traces électroniques. Ces traces électroniques vaudront comme mode de preuve, jusqu'à preuve contraire, notamment :

- de l'imputabilité de la demande d'Opération de paiement au Client,
- du consentement du Client à l'Opération de paiement, et
- de la date et du montant de l'Opération de paiement.

Les Parties reconnaissent que les traces électroniques sont admissibles et valables en tant que mode de preuve devant les tribunaux compétents. En tout état de cause, les Parties renoncent expressément à invoquer entre elles la nullité ou la non-opposabilité des traces électroniques en arguant du fait qu'elles ont été enregistrées de manière électronique.

## **ARTICLE 10 - OBLIGATIONS DU CLIENT VIS-À-VIS DE PAYPLUG**

10.1 Le Client s'engage à respecter le Contrat, à faire un usage des Solutions conforme au Contrat et aux lois et règlements en vigueur ainsi que plus généralement à respecter les lois et règlements applicables. Le Client s'interdit d'utiliser les Solutions pour des opérations contraires à la loi et aux bonnes mœurs.

10.2 Le Client doit assurer le suivi de son Compte Payplug et de l'historique de ses Opérations de paiement, et rembourser les Opérations de paiement indûment reçues, ou l'excédent lorsque le montant de l'Opération de paiement est incorrect. Tout manquement à ces obligations donne lieu à un cas de Contestation de Paiement tel que défini à l'Article 7 ci-dessus.

10.3 Le Client s'engage, lorsqu'il héberge lui-même la page de paiement, à ce que l'environnement, les infrastructures, les réseaux et ressources utilisés pour les sites soient conformes aux directives de sécurité émises par le GIE CB et/ou la norme PCI DSS. Toute perte financière supportée par Payplug imputable à un défaut de conformité du Client à la réglementation GIE CB ou PCI DSS sera répercutée sur le Client sans préjudice d'une action en responsabilité contractuelle menée parallèlement devant la juridiction compétente.

10.3 Le Client qui utilise les fonctionnalités de Payplug impliquant la conservation du numéro de carte de l'Acheteur s'engage à respecter les législations et réglementations applicables à ce type de fonctionnalité. Payplug ne saurait être tenu responsable des infractions aux législations et aux réglementations constatées dans le cadre des ventes réalisées grâce aux Solutions.

10.4 Le Client accepte d'afficher le matériel publicitaire de Payplug à la vue de ses Acheteurs et clients. Il pourra s'agir, sans que cette liste soit limitative, du logo Payplug, des logos des Réseaux de Cartes ou de tout logo que Payplug souhaiterait voir afficher pour répondre à une exigence de la banque, d'un Réseau de Cartes, des lois et règlements ou, plus généralement, de tout matériel publicitaire raisonnablement demandé par Payplug.

10.5 En utilisant les Solutions, le Client pourra recevoir des informations sur les Acheteurs, notamment numéros de téléphone et/ou adresses email et informations sur leur Cartes. Le Client doit garder toutes informations relatives à un quelconque Acheteur comme confidentielles et les utiliser uniquement dans le cadre de la Solution utilisée. Le Client ne doit ni dévoiler ces informations, ni les mettre à disposition de tiers ou les utiliser à des fins commerciales à moins d'avoir reçu le consentement écrit de l'Acheteur ou pour satisfaire à toute communication qui serait strictement nécessaire en vue de satisfaire au Contrat, aux exigences légales ou réglementaires ou bien à une décision de justice. Le Client doit se soumettre à toutes les réglementations en vigueur sur la protection de données personnelles.

10.6 Le Client accepte, en utilisant les Solutions, toutes les conditions et risques propres à l'utilisation de téléphones mobiles et d'Internet, notamment, sans que cette liste soit limitative, les possibles délais de transmission, coûts de connexion, dysfonctionnements techniques et risques de piratage. Le Client reconnaît être conscient et parfaitement informé des éventuels virus et autres programmes malfaisants pouvant circuler sur Internet, et il lui appartient de prendre toutes les mesures pour s'en protéger. Payplug ne pourra être tenu pour



responsable, de quelque manière que ce soit, de tout problème, défaut, dysfonctionnement d'une des Solutions imputable à une cause propre à l'utilisation des téléphones mobiles et d'Internet.

10.7 Le Client s'assure de la conformité des éléments requis attestant sa conformité aux exigences des Réseaux en matière de protection des Données Cartes (notamment les obligations liées au PCI-DSS) qu'il transmet à Payplug à tout moment.

Et notamment le Client :

- déclare exacte les informations indiquées dans le SAQ-A à la connaissance de Payplug et reproduit en Annexe 7,
- s'engage, le cas échéant, à communiquer dans les meilleurs délais, un SAQ rectifié et conforme à PAYPLUG ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) si le SAQ initial (Annexe 7) ne correspond pas ou plus à sa situation pour quelque motif que ce soit ;
- autorise Payplug à éditer un SAQ en son nom, à tout moment, sur la base du SAQ reproduit Annexe 7 ou le cas échéant le SAQ spécifique, notamment en cas de demande des Réseaux ;
- s'engage à transmettre à Payplug la mise à jour de son PCI-DSS chaque année .
- reconnaît la validation de l'ensemble des informations ainsi communiquées au titre du présent article.

## ARTICLE 11 – CLAUSE PÉNALE

Si le Client utilise les Solutions pour une activité différente de celle déclarée lors de son inscription et que cette activité est non-conforme aux CGV, Payplug se réserve le droit de fermer le Compte Payplug et le Compte Client et de réclamer au Client une pénalité égale à 5.000,00 €. En outre, Payplug pourra réclamer au Client le remboursement de tous les coûts que Payplug aura subi ou engagé du fait de l'activité du Client, sans préjudice de tout droit à dommages et intérêts complémentaires.

## ARTICLE 12 – ACTIVATION DU COMPTE

### 12.1 Documents d'identification

Pour commencer à encaisser des paiements, le Client doit demander l'activation de son Compte Client en téléchargeant les documents justificatifs listés sur le Site directement depuis son Compte Payplug. La liste des documents justificatifs à fournir en fonction du statut du Client peut être retrouvée sur le Site via l'adresse <http://support.Payplug.fr/>. En outre, il est expressément prévu que Payplug se réserve le droit de demander tout autre document ou information complémentaire si Payplug le juge nécessaire, notamment, pour lui permettre d'effectuer les vérifications utiles au respect de ses obligations légales y compris en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

A réception des documents mentionnés ci-dessus, sous réserve qu'ils soient jugés satisfaisants par Payplug, Payplug pourra activer le Compte Client.

Une fois le Compte Client activé, Payplug se réserve la possibilité d'imposer des limites par Opération de paiement et/ou par période pour le Client, sans avoir à le justifier.

### 12.2 Archivage des documents d'identification

Payplug conservera sur support électronique d'archivage, pendant cinq (5) ans après avoir mis fin aux relations avec les Clients, une copie du/des document(s) probant(s) ayant servi à leur identification.

## ARTICLE 13 – COMMUNICATION

En utilisant les Solutions, le Client accepte que les communications avec Payplug se fassent en majorité par des moyens électroniques. Payplug contactera le Client par email ou fournira des informations au Client en postant des annonces sur le Site. Le Client accepte ce moyen de communication et reconnaît, dans la mesure où ceci ne déroge pas à la loi, que ces communications électroniques ont la même valeur que des communications sur un support papier. Les courriers électroniques, les accusés de réception, ainsi que les messages affichés sur le Site

sont admissibles devant les tribunaux et font preuve des données et des faits qu'ils contiennent. Payplug considérera que toute communication électronique a été reçue par le Client dans les 24 heures suivant son annonce sur le Site ou l'envoi d'un email, sauf si Payplug a été notifié que l'email n'a pas été reçu par le Client.

Le Client comprend et accepte que Payplug puisse le contacter et lui demander des informations dans le cadre d'opérations de maintenance, de réparation ou d'amélioration des Solutions. De manière générale, le Client accepte que Payplug puisse le contacter par courrier ou par téléphone en cas de besoin. Dans la mesure où cela serait strictement nécessaire pour la maintenance ou la réparation de l'une des Solutions, le Client s'engage à ce que Payplug puisse librement avoir accès à ses locaux afin d'effectuer toute vérification nécessaire.

Pour permettre ces communications, le Client s'engage à toujours avoir au moins une adresse email, une adresse postale et un numéro de téléphone valides renseignés sur son Compte Payplug. Payplug n'assumera aucune responsabilité si une coordonnée renseignée n'est pas valide ou si celle-ci a changé sans que Payplug en soit informé.

Le Client doit lire attentivement toutes les correspondances qu'il échange avec Payplug et avertir Payplug le plus rapidement possible s'il remarque que ces correspondances contiennent une information qui lui semble inexacte.

Le Client devra consulter régulièrement ses messages électroniques. Ceux-ci peuvent contenir des liens vers d'autres informations sur le Site. Lorsque la législation impose de fournir une information sur un support durable, Payplug enverra un email ou une notification renvoyant vers le Site, qui pourra être imprimée ou conservée sous tout autre format permettant au Client de consulter cette information à une date ultérieure. Le Client est tenu de conserver l'ensemble des communications envoyées ou mises à sa disposition par Payplug.

Dans le cas où le Client souhaiterait faire part à Payplug d'une réclamation (contestation ou requête...) relative à :

- un dysfonctionnement d'une des fonctionnalités d'une des Solutions,
- une erreur dans l'exécution d'une Opération de paiement ou dans son inexécution liée à l'une des Solutions,
- une erreur dans le prélèvement de toutes sommes par Payplug,

celui-ci devra le notifier à Payplug dans un délai de trente (30) jours à compter du jour où le Client en a eu connaissance ou est présumé en avoir eu connaissance (notamment compte tenu des habitudes de consultation de son Compte Payplug et de la date et heure de son dernier accès à son Compte Payplug) ou dans tout autre délai plus long prévu par des dispositions particulières ou par la loi.

Cette notification s'effectue par l'envoi d'un courrier électronique à l'adresse email suivante : [support@payplug.com](mailto:support@payplug.com) ou par téléphone au 01 85 08 38 28.

## **ARTICLE 14 – COORDONNÉES**

Le Client a transmis à Payplug les coordonnées de son interlocuteur principal et de son Service Client.

Ces coordonnées doivent permettre à Payplug de renvoyer les Acheteurs qui la contacteront relativement à un Achat vers le Client, lequel demeure leur seul cocontractant des Acheteurs.

## **ARTICLE 15 – RELATIONS AVEC LES TIERS**

Le Client confirme et accepte que Payplug n'est que le fournisseur des Solutions et qu'il est donc tiers extérieur à la relation commerciale existant entre le Client et son Acheteur et n'assume aucune sorte de responsabilité par rapport, notamment, à la qualité et à la nature des Produits vendus par le Client, leur prix, les rabais et les conditions de garantie y afférentes. En acceptant les CGV, le Client s'engage à se présenter comme une entité distincte de Payplug, et ne pourra en aucun cas se présenter ou agir en qualité de mandataire de Payplug conformément aux dispositions de l'article 1984 du Code civil.

Payplug ne garantit pas l'identité des Acheteurs, il ne garantit pas non plus la bonne exécution des Commandes par les Acheteurs. En cas de litige concernant le paiement ou l'exécution d'une Commande, l'Acheteur doit

s'adresser directement au Client afin d'essayer de résoudre son litige avec lui. Hormis les cas d'annulation de paiement autorisés pour les paiements récurrents ou par la loi, un règlement ou une décision judiciaire ou administrative, Payplug n'est pas en droit d'annuler une Opération de paiement pour des motifs de litige commercial ou autre opposant un Acheteur et le Client.

Payplug ne garantit et n'assume aucune responsabilité, de quelque nature ou forme que ce soit, pour tout acte ou omission de tiers qui utilisent les Solutions ou pour tout acte ou omission de tiers qui font de la publicité sur le Site.

Pour être en mesure de fournir les Solutions, Payplug signera des accords avec d'autres institutions de paiement et/ou banques. Ces dernières peuvent exiger que le Client signe un contrat avec elles, auquel cas Payplug fournira soit le contrat approprié soit les conditions générales d'utilisation que le Client devra compléter, et en acceptant dûment les termes ou le signer, selon le cas, avec le tiers concerné afin que Payplug puisse mettre la Solution concernée à sa disposition. Cela peut arriver lors de la procédure d'inscription ou à n'importe quel autre moment. Si le Client ne remplit pas, n'accepte pas ou ne signe pas, selon le cas, le contrat additionnel ou les conditions générales d'utilisation avec le tiers concerné, Payplug se réserve le droit, à sa seule discrétion, de suspendre ou de clôturer le Compte Payplug et le Compte Client par résiliation de Contrat.

En acceptant ces CGV, le Client confirme son acceptation des règles des Réseaux de Cartes.

Pour fournir les Solutions, Payplug peut également directement contracter avec des institutions de paiement et banque A ce titre, le Client déclare donner mandat à Payplug pour conclure avec ces tiers, tous contrats.

Le Client s'engage à ce que Payplug reste le seul interlocuteur de ces institutions de paiement et banque sur tous les sujets concernant l'application des contrats concernés.

Dans le cadre du contrat de partenariat entre Payplug et BPCE, Payplug est susceptible de notifier BPCE lorsqu'un client qui a été apporté par BPCE change de RIB. Cette notification n'inclut pas les données du changement de RIB par le client.

## **ARTICLE 16 – PROPRIÉTÉ INTELLECTUELLE**

Le Site, les logos, textes, offres, graphismes et tout logiciel mis à disposition du Client par Payplug, dans leur version actuelle ou future (ci-après les « Propriétés ») appartiennent exclusivement à Payplug et sont protégés au titre des droits de propriété intellectuelle de cette dernière.

Payplug concède au Client, à titre non exclusif, le droit d'utiliser les Propriétés dans la limite nécessaire à l'utilisation des Solutions. Le Client s'interdit de copier, modifier, intégrer les Propriétés sur quelque support que ce soit, d'effectuer une rétro-ingénierie quelconque ou d'user de toute autre méthode pour tenter d'accéder aux codes source des Propriétés. Plus généralement, le Client s'interdit de porter atteinte d'une quelconque manière que ce soit aux droits de propriété intellectuelle de Payplug sur les Propriétés dans leur version présente ou future.

Le Client s'interdit de vendre, céder, donner en licence, sous-licencier, donner en garantie, ou, plus généralement, transmettre à un tiers les Propriétés de toute autre manière.

Les commentaires ou suggestions du Client pour améliorer les Solutions seront gratuits et Payplug pourra les utiliser sans contrepartie.

Pendant toute la durée du Contrat, le Client autorise expressément Payplug à citer le Client comme référence client dans ses supports commerciaux et, pour cette seule finalité, à reproduire ses marques verbales, semi-figuratives ou figuratives.

## **ARTICLE 17 – FERMETURE DU COMPTE PAR PAYPLUG**

Payplug peut, à sa seule discrétion, prononcer le blocage ou la fermeture du Compte Client à condition que cette décision soit motivée (si la loi n'y fait pas obstacle) et d'en informer le Client au préalable.

Payplug peut, à sa seule discrétion, prononcer le blocage ou la fermeture du Compte Client en cas de résiliation du Contrat de Location de TPE par l'une ou l'autre des parties conformément aux stipulations de l'article 13 de

l'annexe 3.

Payplug se réserve, à sa seule discrétion, le droit de prononcer le blocage ou la fermeture du Compte Client sans l'en informer au préalable, dans l'un quelconque des cas suivants :

- le Client a dérogé aux présentes CGV ou à tout autre condition applicable à l'utilisation d'une des Solutions, incluant notamment les règles des Réseaux de Cartes ;
- le Client viole, ou Payplug a des raisons légitimes de croire que le Client viole, une loi ou un règlement applicable à l'utilisation d'une des Solutions ;
- Payplug a des raisons légitimes de croire que le Client est impliqué dans des activités frauduleuses, le blanchiment de capitaux, le financement du terrorisme ou une autre activité criminelle ;
- le Client engendre pour Payplug un risque de crédit ou de fraude trop élevé ;
- Payplug a des raisons légitimes de croire que le Compte Payplug du Client a été piraté ou que l'utilisation du Compte Payplug est susceptible de poser un problème de sécurité ; ou
- Payplug n'est pas en mesure d'informer le Client, notamment dans le cas où les coordonnées renseignées sur le Compte Payplug du Client sont inexactes, périmées ou incomplètes.

Si le Compte Client est fermé pour quelque raison que ce soit et le Compte Payplug clôturé en conséquence, le Client accepte d'ores et déjà :

- de continuer à respecter les CGV,
- d'arrêter immédiatement d'utiliser la Solution,
- que les Frais de Transaction et toute autre somme due par le Client à Payplug au moment de la fermeture du Compte Client restent dus,
- que Payplug a le droit, sous réserve des obligations de conservations imposées par la réglementation en vigueur et sauf disposition contraire de la loi ou décision de justice, de supprimer toutes les informations et données relatives au Client sur ses serveurs,
- que Payplug n'est redevable en rien au Client ou à tout autre tiers pour la fermeture de l'accès à la Solution ou pour la suppression des données du Compte Payplug, et ce quels que soient les éventuels dommages occasionnés par la fermeture de ce Compte Payplug.

La réactivation du Compte Payplug et du Compte Client se fera à la discrétion de Payplug.

Le Client dont le compte a été clôturé par Payplug n'est pas autorisé, sauf accord exprès de Payplug, à ouvrir un autre Compte Payplug. Tout Compte Payplug ouvert en violation de cette disposition pourra être immédiatement clôturé par Payplug, sans préavis.

L'Avoir disponible sur le Compte Client objet de la clôture donnera droit à un Virement au profit du Client sous réserve des opérations en cours et des éventuels impayés, rejets bancaires, Contestations de Paiement ou oppositions à venir.

Payplug se réserve le droit de demander en justice réparation du préjudice qu'il aura subi du fait de la violation des CGV.

## **ARTICLE 18 – DÉCÈS DU CLIENT**

En cas de décès du Client titulaire du Compte Payplug, le Client s'engage à faire le nécessaire pour que Payplug puisse être avisé par écrit le plus rapidement possible par les ayants droits ou leur mandataire et dont il informe des présentes. Si cet avis est donné verbalement, il doit être confirmé par écrit. Dès réception de cet écrit, Payplug veillera à ce qu'aucune opération ne soit effectuée sur les Avoirs éventuels et procédera à la clôture du Compte Payplug, ce qui aura pour conséquence la clôture du Compte Client.

Si les Avoirs présents sur le compte au nom du défunt sont supérieurs aux frais permettant de supporter les coûts de Virement, ils pourront par dérogation à l'Article 5 des présentes CGV, faire l'objet d'un Virement en faveur des ayants-droits uniquement en cas de production par ces ayants-droits ou leur mandataire des pièces probantes, selon la législation applicable, établissant la dévolution de la succession ainsi que de toute autre pièce que Payplug jugerait nécessaire.

A défaut de Virement pour quelle que raison que ce soit, y compris l'absence de production de document probant à Payplug, les stipulations des articles 21.2 et/ou 21.4 des présentes CGV s'appliqueront aux Avoirs.

## ARTICLE 19 - INDEMNISATION

Le Client s'engage à indemniser Payplug de l'intégralité de tous dommages, pénalités, coûts, frais et dépens (y compris les frais d'avocat engagés par Payplug dans ce cadre) liés à :

- une violation par le Client des CGV ou de toute loi, réglementation ou contrat applicables à l'utilisation de l'une des Solutions,
- une mauvaise utilisation des Solutions,
- toute Opération de paiement reçue par erreur par le Client, et
- toute utilisation du Compte Payplug du Client par un tiers utilisant ses Identifiant et mot de passe du fait d'une négligence imputable au Client.

## ARTICLE 20 – RESPONSABILITE

### 20.1 Responsabilité de Payplug

Chaque Client déclare être informé des contraintes et des limites des réseaux Internet et ne pourra en aucun cas rechercher la responsabilité de Payplug au titre de dysfonctionnements dans l'accès à leurs services, aux Solutions ou au Site, des vitesses d'ouverture et de consultation des pages des services, de l'inaccessibilité temporaire des services, de l'utilisation frauduleuse par des Clients ou des tiers des services, dans le cas où des liens hypertextes présents sur le Site renvoient sur d'autres sites internet dont le contenu contrevient aux législations en vigueur ou dont la visite par un Client ou un tiers lui causerait un quelconque préjudice.

Il est de la responsabilité de chaque Client de protéger son matériel informatique, son site internet ou autre matériel notamment contre toute forme d'intrusion et/ou de contamination par des virus, la responsabilité de Payplug ne pouvant être recherchée en cas de dysfonctionnement ou de détérioration du matériel ou du site internet d'un Client.

Chaque Client prend sous sa seule responsabilité l'ensemble des mesures de nature à assurer l'intégrité et la sauvegarde de l'ensemble de ses données, fichiers, documents et renonce à rechercher la responsabilité de Payplug en cas de dommages survenus à ceux-ci dans le cadre de l'utilisation de leurs services, des Solutions, de ou du Site.

La responsabilité de Payplug ne saurait davantage être engagée :

- dans le cas où un fournisseur stratégique de la chaîne de paiement ou de monétique serait défaillant, par exemple, et de manière non limitative, les réseaux d'acceptation de paiement du GIE Cartes Bancaires, les serveurs des systèmes d'acceptation Visa et Mastercard, les serveurs et systèmes de paiement bancaires 3D Secure, les systèmes de virement SEPA des banques partenaires, les systèmes interbancaires de virement STEP2 ou CORE, les systèmes de monétique et de traitement des flux
- dans le cas où les hébergeurs internet des systèmes de paiement seraient victimes de fraudes massives, d'attaques demandant une coupure du service pour enrayer une attaque massive et organisée,
- dans le cas d'une panne globale des systèmes de communication par Internet dans un pays ou une partie d'un pays, rendant indirectement impossible les paiements à distance
- dans le cas d'un phishing (génération de eCarte Bancaire via un vol de code d'accès à un compte bancaire en ligne, avec ou sans utilisation de faux documents) ou d'une opération de Carding (vol de carte bancaire, usurpation de codes 3D Secure) résultant d'une escroquerie en bande organisée
- dans le cas d'une coupure de service unilatérale à la demande d'une banque partenaire, ou du GIE Cartes Bancaires, ou de Visa, ou de Mastercard
- dans le cas d'une limitation des usages et des seuils d'utilisation de moyens de paiement qui seraient imposés à un pays dans son entièreté ou à une citoyenneté
- dans le cas d'une coupure unilatérale suivie ou non d'un gel d'avoir, du fait de Payplug ou d'une

demande des autorités de tutelle ou de police ou de gendarmerie, pour cause de risque de blanchiment, de fraude fiscale, de financement du terrorisme

- dans le cas d'une réquisition judiciaire ordonnant la fermeture immédiate d'un service ou d'un site
- dans le cas d'un filtrage de protection momentané ou permanent par pays ou type de Carte (carte Business, eCarte Bleue, carte prépayée...)
- dans le cas d'une fausse activité déclarée par le Client
- en cas de manquement à une quelconque obligation résultant d'un cas fortuit ou d'un événement de force majeure, y compris, mais sans y être limités, catastrophes, incendies, inondations, grève totale ou partielle, interne ou externe, défaillance ou pannes internes ou externes, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des télécommunications, faute ou négligence d'un tiers, et d'une manière générale tout événement irrésistible et imprévisible ne permettant pas le bon fonctionnement des services, de l'une des Solutions, ou du Site et indépendant de la volonté de Payplug. Il est précisé qu'en cas de force majeure perdurant au-delà d'une durée de trente (30) jours, chaque Partie pourra mettre un terme aux relations contractuelles régies par les présentes, sans qu'aucune indemnité ne soit due par aucune des Parties de ce fait.
- en cas de manquement du Client à une quelconque obligation résultant de l'application de dispositions légales, réglementaires ou administratives ;
- dans le cas où les informations ou les données personnelles communiquées par un Client sont fausses, erronées ou incomplètes ;
- en cas de non-respect, en tout ou partie, des présentes CGV par le Client ;
- dans le cas où certains services ou fonctionnalités ne seraient pas accessibles du Site en raison d'une

désactivation par un Client des cookies via l'interface du logiciel de navigation ;

- dans le cas où les fonctionnalités de l'une des Solutions, ou du Site s'avéreraient incompatibles avec certains équipements et/ou fonctionnalités du matériel informatique d'un Client ou d'un Acheteur ;
- au titre de tous dommages ou préjudices indirects ou immatériels tels que préjudice financier, perte de chance, perte de profit, perte de contrat, perte de commande, perte de clientèle, perte d'exploitation, préjudice ou trouble commercial, préjudice d'image, préjudice découlant de l'action d'un tiers, qui pourraient résulter de l'inexécution ou de l'exécution défectueuse des services prévus aux présentes CGV par Payplug.

Au surplus, il est rappelé que le rôle de Payplug aux termes des présentes se limite à mettre à la disposition des Clients les services, les Solutions, et le Site, sans intervenir d'aucune sorte dans les relations entre un Client et un Acheteur, ni prendre l'engagement de conclure pour le compte du Client ou de l'Acheteur un contrat à quelque titre que ce soit.

En conséquence, Payplug n'est pas responsable de la conclusion et/ou de la bonne exécution d'un contrat conclu entre un Client et un Acheteur, de la nature du transfert d'argent intervenu (paiement d'une dette, d'un produit, donation, prêt, paiement indu, etc.), ou de la validité ou l'exactitude du paiement intervenu et déclinent toute responsabilité quant aux conséquences directes et indirectes résultant de la relation entre un Client et un Acheteur.

Par ailleurs, la responsabilité de Payplug ne saurait être engagée à l'égard de la licéité, l'exactitude, la qualité ou la sincérité des offres et contenus mis en ligne par un Client sur son site internet et le respect par les Clients de leurs obligations légales et réglementaires.

## **20.2 Limitation de responsabilité de Payplug**

En tant que prestataire de services de paiement, Payplug est responsable à l'égard de l'Acheteur et/ou du Client, selon les cas, en cas d'opération de paiement non autorisée ou d'opération de paiement mal exécutée dans les conditions prévues aux articles L.133-18 et suivants du Code monétaire et financier. Toutefois, par dérogation aux dispositions de l'article L.133-24 du Code monétaire et financier, toute opération de paiement non autorisée ou mal exécutée devra être signalée à Payplug dans un délai de trente (30) jours à compter du jour où le Client en a eu connaissance ou est présumé en avoir eu connaissance, sous peine de forclusion de son action.

Dans tous les autres cas, la responsabilité de Payplug au titre des présentes ne pourra excéder à l'égard du Client, un montant égal aux frais de toute nature perçus par Payplug auprès de ce Client au titre des présentes au cours



des six (6) mois précédant la date de réalisation du fait dommageable, dans la limite d'un plafond global de huit mille (8.000) Euros. et ne peut être engagée qu'au titre d'un préjudice direct, personnel et certain.

Conformément aux dispositions de l'article 2254 du Code Civil, toute action judiciaire d'un Client à l'égard de Payplug au titre des présentes est atteinte par la prescription à l'expiration d'une durée d'un (1) an suivant la date à laquelle le Client a eu connaissance ou est présumé avoir eu connaissance du fait dommageable.

## **ARTICLE 21 – OBLIGATIONS DE PAYPLUG**

Conformément à l'article L. 133-22 du Code monétaire et financier, Payplug est responsable, sous réserve des articles L. 133-5 et L. 133-21 du Code monétaire et financier, de la bonne exécution de l'opération de paiement à l'égard de l'Acheteur jusqu'à réception des fonds par le Client, bénéficiaire du paiement. Lorsque Payplug est responsable d'une opération de paiement mal exécutée, Payplug restitue sans tarder son montant à l'Acheteur et rétablit le compte débité dans la situation qui aurait prévalu si l'opération de paiement mal exécutée n'avait pas eu lieu.

### **21.1 DISPONIBILITÉ DES SERVICES**

Payplug s'efforce d'assurer l'accès et le bon fonctionnement à ses services vingt-quatre heures sur vingt-quatre, sept jours sur sept. Toutefois, Payplug ne peut exclure que l'accès à ses services et leur fonctionnement soient interrompus notamment en cas de force majeure, de dysfonctionnements des équipements ou du réseau internet des Acheteurs et Clients, de défaillance des opérateurs de télécommunication, d'interruption de fourniture d'électricité, d'utilisation anormale, illicite ou frauduleuse de leurs services par un Acheteur, un Client ou un tiers, de décision des autorités compétentes, ou pour tout autre motif.

Payplug se réserve le droit d'apporter à ses services, et notamment à la Solution de Paiement en Ligne, ou au Site toutes les modifications et améliorations de son choix liées à l'évolution technique ou au bon fonctionnement des services.

Payplug se réserve le droit, sans préavis ni indemnité, de suspendre temporairement l'accès à ses services afin d'assurer des opérations de maintenance liées à l'évolution technologique ou nécessaires à la continuité des services (notamment correction d'erreurs, introduction de nouvelles fonctionnalités, exécution d'opérations, etc.) ou en cas de non-respect par un Client des présentes CGV.

Toutefois, les interruptions générales et temporaires du service seront, dans la mesure du possible, notifiées dans un délai raisonnable avant qu'elles n'interviennent, sauf lorsque ces interruptions ont un caractère d'urgence.

Dès la reprise normale des services, Payplug mettra en œuvre les efforts raisonnables pour traiter les opérations en

attente dans les meilleurs délais.

### **21.2 Conservation des Avoirs**

Payplug conservera les fonds versés par le Client, déduction faite des Frais de Transaction prélevés mensuellement Payplug et des frais et taxes éventuellement applicables, sur un compte bancaire ouvert avec affectation spéciale auprès de la banque de Payplug.

### **21.3 Archivage des enregistrements**

Payplug conservera sur support électronique d'archivage, dans les délais indiqués dans « Politique de confidentialité » accessible sur le Site, les enregistrements et documents des opérations effectuées de façon à pouvoir les reconstituer précisément, en particulier les opérations visées par la réglementation de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

### **21.4 Compte non-utilisé**

En cas de non-utilisation par le Client de son Compte Client pendant une durée d'un an, et après une relance par email à la dernière adresse électronique connue du Client restée sans réponse, Payplug se réserve le droit de

fermer le Compte Client et de verser les sommes correspondantes sur le Compte Bancaire. Si Payplug ne dispose pas d'un Compte Bancaire valide, ces sommes seront conservées pendant la durée de la prescription acquisitive et versées à l'État après 30 années révolues, sans préjudice du droit de Payplug de mettre fin aux présentes CGV.

## ARTICLE 22 - REPORTING

Le Client peut à tout moment obtenir, en ligne sur le Portail, un état détaillé des opérations de paiement qu'il réalise. Payplug conserve disponible pour le Client l'historique des Opérations de paiement pendant une durée au moins égale à trois (3) mois.

Le Client aura accès à l'historique des Opérations de paiement s sur le Portail, qui indiquera notamment pour chaque opération :

- une référence permettant d'identifier l'Opération de paiement concernée ;le cas échéant, les informations relatives à l'Acheteur ;
- le montant de l'Opération de paiement concernée ainsi que, le cas échéant, l'objet de l'Opération de paiement réalisée (nom de

l'article par exemple) ;

- le montant détaillé des frais applicables le cas échéant.

Le Client pourra également avoir accès à d'autres informations concernant les Opérations de paiement (telles que le numéro de carte tronqué, le type de carte utilisé, le pays de la carte, le nombre de tentatives nécessaires pour faire le paiement, le type de plateforme et le navigateur utilisés par l'Acheteur). Ces informations lui sont communiquées à des fins de lutte contre la fraude.

## ARTICLE 23 –TRAITEMENT DES DONNEES A CARACTERE PERSONNEL (POLITIQUE DE LA VIE PRIVÉE)

Payplug est amené à traiter des données personnelles du Client.

23.1 Lors que Payplug traite ces données en tant que Responsable de traitement, leurs finalités, destinataires et les conditions dans lesquelles le Client peut exercer ses droits sur ces données sont présentés dans la « Politique de confidentialité » accessible sur le Site (<https://www.payplug.com/fr/politique-de-confidentialite/>). Le Client s'engage à informer toutes les personnes dont il communique les données personnelles à Payplug de cette politique de confidentialité.

23.2 Toute Donnée à Caractère Personnel demeure la pleine et entière propriété du Client, et Payplug s'engage à se conformer à la Réglementation sur les Données Personnelles, et à assumer l'ensemble des responsabilités découlant de cette dernière. À ce titre, le Client (i) est informé que Payplug a effectué les démarches nécessaires pour que les Données à Caractère Personnel traitées soient « privacy by design » tel que prévu par la Réglementation sur les Données Personnelles, et (ii) s'engage en qualité de responsable du traitement à être en conformité avec la Réglementation sur les Données Personnelles dans le cadre du traitement des Données à Caractère Personnel et le cas échéant des Données Sensibles qu'il est amené à collecter, traiter et stocker dans le cadre de son Activité, de sorte à ce que la responsabilité de Payplug ne soit ni recherchée, ni engagée, notamment en raison du fait que Payplug intervient en qualité de sous-traitant du Client au sens de ladite Réglementation sur les Données Personnelles. A ce titre, les Parties conviennent que les obligations que Payplug devra respecter en qualité de Sous-traitant sont décrites à l'Annexe 6 attachée au Contrat.

Dans les limites prévues par les Prescriptions Légales, Payplug s'engage à (i) ne réaliser aucune copie des Données à Caractère Personnel auxquelles elle aurait accès dans le cadre de la fourniture du Service au Client sans l'accord préalable et écrit du Client, à l'exception de celles strictement nécessaires à la fourniture du Service ; (ii) détruire, à première demande du Client et au plus tard à l'expiration du Contrat, les Données à Caractère Personnel autres que celles enregistrées lors des Opérations de Paiement, et (iii) utiliser des moyens permettant de garantir qu'elles ont été définitivement effacées des supports sur lesquels elles auraient pu être stockées, en particulier en ce qui concerne les fichiers informatiques pour des besoins de sauvegarde et d'exploitation.

Les Données à Caractère Personnel incluant les Données Sensibles recueillies par Payplug dans le cadre du

Service sont destinées à l'usage de Payplug pour le compte du Client dans le cadre de l'exécution du Contrat, et Payplug s'en interdit toute autre exploitation. Payplug s'interdit de commercialiser, louer, transférer, céder et/ou mettre à disposition lesdites Données Sensibles à des tiers à quelques fins que ce soit à titre onéreux ou gratuit, sauf clause contraire prévue par les Prescriptions Légales (exemple : réquisition judiciaire).

Toute communication ou cession à des tiers des Données à Caractère Personnel des Porteurs (à l'exclusion de toutes données bancaires ou relatives aux Cartes) recueillies par Payplug dans le cadre du Service ne pourra avoir lieu qu'en conformité avec les Prescriptions Légales et avec l'accord préalable du Client. En outre, le cas échéant le Client pourra donner autorisation à Payplug de transférer les Données à Caractère Personnel à un tiers préalablement expressément nommé et ce, aux fins de la bonne exécution du présent contrat. Cette autorisation interviendra par voie de déclaration écrite.

Payplug garantit que l'hébergement et le stockage des Données Sensibles, que ce soit en base active et archive, aura lieu sur le territoire de l'Union Européenne et que la fourniture du Service technique de paiement au Client n'implique aucun transfert de Données Sensibles en dehors du territoire de l'Union Européenne, sauf réquisition des Autorités de Tutelle en conformité avec l'article 48 du RGPD et/ou exigences techniques requises par les Systèmes de Paiement en conformité avec le Chapitre V du RGPD. Les conditions de transfert hors de l'Espace économique européen des Données à caractère personnel traitées par Payplug en tant que sous-traitant en application de l'article 17.2.1 sont précisées à l'Annexe 6 du Contrat.

23.3 Les Parties reconnaissent que l'exécution du Contrat implique le Traitement, par chacune des Parties, en qualité de Responsable du Traitement distinct et indépendant, de Données à Caractère Personnel concernant les représentants, employés et contractants de l'autre Partie à des fins de gestion de la relation commerciale et contractuelle, chaque Partie s'engageant à traiter ces données conformément à la Réglementation relative à la Protection des Données. A ce titre, le Client dispose, conformément aux dispositions la Réglementation sur les Données Personnelles, d'un droit d'accès aux données qui le concernent, ainsi que d'un droit de modification, de rectification et de suppression de celles-ci.

23.4 Ce droit peut être exercé :

- (i) tant que le Contrat est en vigueur ; ou
- (ii) après l'expiration du Contrat, au moyen d'un courrier postal ou électronique aux coordonnées figurant sur le site Internet de Payplug.

## **ARTICLE 24 – SECRET PROFESSIONNEL**

Payplug est soumise au secret professionnel de l'article L 522-19 du Code Monétaire et Financier. Néanmoins, par la signature des présentes Conditions Générales de Vente, le Client accepte expressément que Payplug communique certaines informations administratives et financières relatives à la tenue et à la gestion du Compte Client à des entités du Groupe BPCE auquel Payplug appartient. Cette communication est faite dans le cadre du suivi de la relation d'apports d'affaires qui existe entre Payplug et les entités précitées et seulement si cette communication est rendue nécessaire pour l'exécution des obligations entre Payplug et ces entités. Les personnes destinataires des informations confidentielles sont elles-mêmes soumises au secret professionnel et doivent, à ce titre, les conserver confidentielles.

## **ARTICLE 25 – GENERALITES**

Au cas où des formalités administratives seraient nécessaires au titre de l'exécution des présentes CGV, Payplug et le Client se prêteront mutuelle assistance pour la régularisation de ces formalités.

Le fait pour l'une des Parties de ne pas se prévaloir d'un manquement par l'autre Partie à l'une quelconque des obligations visées dans les présentes ne saurait être interprété pour l'avenir comme une renonciation à l'obligation en cause. En cas de difficultés d'interprétation entre l'un quelconque des titres et l'une quelconque des clauses des CGV, il ne sera pas tenu compte des titres.

## **ARTICLE 26 – DROIT APPLICABLE**

Le Contrat est régi et interprété conformément au droit français.

La langue d'interprétation est la langue française en cas de contestation sur la signification d'un terme ou d'une stipulation du Contrat.

Tout différend relatif à la validité, l'interprétation ou l'exécution du Contrat relèvera de la compétence exclusive des tribunaux français compétents.

## **ARTICLE 27 – DIVISIBILITÉ**

Si un tribunal juge qu'une ou plusieurs des stipulations des présentes CGV est nulle, invalide ou inopposable, l'absence d'effet de l'une quelconque des stipulations des CGV n'affectera pas le reste des CGV qui devront être exécutées comme si cette stipulation n'avait jamais existé et la ou les stipulations concernées seront remplacées dans toute la mesure du possible dans les conditions de l'Article 3 par de nouvelles stipulations valables et opposables.

## **ARTICLE 28 – TRANSFERT**

Payplug pourra librement transférer ses droits et obligations dans le cadre du Contrat à un tiers de son choix. L'accord du Client à un tel transfert est considéré acquis en vertu des présentes CGV.

Le Client ne pourra en aucun cas transférer tout ou partie des droits et obligations résultant du Contrat à un tiers sans avoir préalablement reçu l'accord écrit de Payplug et fait les mises à jour correspondantes dans les informations de son Compte Payplug.

## **ARTICLE 29 – RECLAMATIONS**

Toute réclamation à propos de Payplug ou à l'une des Solutions devra être adressée par lettre recommandée avec accusé de réception dans un délai maximum de 6 mois à compter de la date d'opération contestée correspondant à l'Opération de paiement réalisée, sous peine de forclusion en indiquant « Réclamation » dans l'objet du courrier et à l'adresse suivante :

Payplug Enterprise

Service Réclamation

110 avenue de France

75013 PARIS

Les réclamations seront traitées dans les meilleurs délais et au plus tard dans les quinze (15) jours ouvrables suivant la réception de la réclamation.

Dans des situations exceptionnelles, si aucune réponse ne peut être donnée dans les quinze (15) jours ouvrables pour des raisons échappant à Payplug, ce-dernier envoie une réponse d'attente motivant clairement le délai complémentaire nécessaire pour répondre à la réclamation. En tout état de cause, le Client reçoit une réponse définitive au plus tard trente-cinq (35) jours ouvrables suivant la réception de la réclamation.

## ANNEXE 1 : Conditions Générales au Contrat de la Solution de Paiement en ligne Payplug

### ARTICLE 1 – DEFINITIONS

Sauf stipulation contraire prévue dans la présente annexe, l'ensemble des termes comportant une majuscule conservent la signification qui leur a été donnée aux Conditions Générales de Vente.

Les autres termes utilisés dans le présent Contrat de la Solution de Paiement en ligne Payplug auront, lorsqu'ils sont utilisés avec la première lettre en majuscule et indépendamment du fait qu'ils soient utilisés au singulier ou au pluriel, le sens défini ci-après :

- « Confirmation d'Achat » : désigne le canal d'avertissement de confirmation de l'*Opération de paiement*, envoyé automatiquement à l'Acheteur par Payplug. Cette confirmation reprend les éléments relatifs à l'achat : compte du Client, montant payé, date et heure.
- « Confirmation de Paiement » ou « Notification de Paiement » : désigne le courrier électronique, le SMS ou bien le message affiché sur le Portail de confirmation du paiement, envoyé automatiquement au Client par Payplug. Ce message rappelle au Client les éléments essentiels de l'Opération de paiement avec son numéro de référence.

### ARTICLE 2 - OBJET DU CONTRAT

#### 2.1 Présentation de la Solution de Paiement en Ligne

Le présent contrat (ci-après désigné le « Contrat de la Solution de Paiement en ligne ») a pour objet de définir les conditions dans lesquelles Payplug fournit un service permettant à un Client d'accepter des paiements. Payplug fournit en particulier une interface de programmation permettant au Client d'intégrer un système de paiement par Carte ou autres Moyens de Paiement acceptés par Payplug sur son propre site internet. En se connectant sur le Portail, le Client peut notamment créer un lien vers une page de paiement sécurisée, qu'il peut intégrer à son propre site internet ou partager sous forme d'URL, gérer les informations de son Compte Payplug, et toute action qui pourrait être proposée par Payplug sur le Compte Payplug du Client.

#### 2.2 Présentation des services de paiement en Ligne proposés par Payplug

Payplug, établissement de paiement offre au Client les services de paiement suivants :

- Acquisition des ordres de paiement lui permettant :
  - o d'encaisser, via la Solution de Paiement en Ligne, les montants correspondant aux Opérations de paiement réalisées par les Acheteurs en contrepartie des Produits proposés par le Client ; et
  - o de procéder à des Remboursements, tels que définis à l'Article 6 des CGV ;
- Virement de fonds associés au Compte Client permettant au Client d'ordonner le transfert de tout ou partie de son Solde vers son Compte Bancaire tel que défini à l'Article 5 des CGV.
  
- Des Moyens de Paiement complémentaires

### ARTICLE 3 – DÉCLARATION DU CLIENT

Le Client déclare expressément avoir la capacité et/ou avoir reçu les autorisations requises pour utiliser le service de paiement en Ligne proposé par Payplug et garantit Payplug contre toute responsabilité pouvant résulter pour lui de l'utilisation du service de paiement par une personne n'ayant pas ces capacités et/ou autorisations requises.

## ARTICLE 4 – DURÉE DU CONTRAT

Le Contrat de la Solution de Paiement en ligne est conclu pour une durée indéterminée.

Le Client dispose d'un délai de quatorze (14) jours calendaires pour renoncer sans pénalité au Contrat de la Solution de Paiement en ligne. Ce délai court à compter du jour où le Contrat de la Solution de Paiement en ligne est conclu c'est-à-dire le jour où le Compte Payplug est ouvert. Pendant ce délai de renonciation, l'exécution du Contrat de la Solution de Paiement en ligne ne pourra commencer qu'à la demande expresse du Client. Ce droit de renonciation peut être exercé par le Client sans pénalité et sans indication de motif.

Le Client est tenu de notifier sa décision de renonciation à Payplug par lettre recommandée avec accusé de réception à l'adresse mentionnée à l'Article 16 des présentes CGV.

Aucune indemnité ne peut être réclamée au Client du fait de cette renonciation.

Si le Client n'exerce pas son droit de renonciation, le Contrat de la Solution de Paiement en ligne sera maintenu conformément aux stipulations des présentes CGV.

Le Client reconnaît expressément et accepte que toute instruction de paiement adressée à Payplug avant l'écoulement du délai de renonciation, constitue une demande expresse du Client d'exécuter le Contrat de la Solution de Paiement en ligne. Le Client ne sera donc pas en droit d'annuler une instruction de paiement qu'il aurait donnée et confirmée pendant le délai de renonciation.

## ARTICLE 5 – OBLIGATIONS D'ORDRE GENERAL DU CLIENT

### 5.1 Obligation relative à son activité marchande

Le Client s'engage à respecter l'ensemble des dispositions légales ou réglementaires qui lui sont applicables et plus particulièrement dans le cadre de la vente à distance ou de la protection du consommateur.

Le Client s'engage à respecter les conditions générales de ventes qu'il a communiquées à l'Acheteur et à fournir à ce dernier le ou les Produits achetés via la Solution de Paiement en Ligne conformément aux informations communiquées lors de la Commande.

Le Client est seul responsable des Produits qu'il diffuse gratuitement ou qu'il commercialise et ce même s'il a recours à la Solution de Paiement en Ligne pour procéder au paiement.

### 5.2 Obligation d'information

Le Client s'engage à fournir à l'Acheteur une information claire, détaillée et facilement accessible relative à toute Commande ou offre de transaction en ligne. A titre d'exemple, le Client devra, selon le cas, informer l'Acheteur sur son identité ou sa dénomination sociale, son siège social et son adresse postale et email, le montant des frais de livraison s'il y en a, les modalités de paiement du prix et de la livraison, la durée de validité de l'offre de vente et de son prix, l'existence du droit de rétractation et ses modalités.

Le Client s'engage à mettre ses conditions générales de vente et ses mentions légales à la disposition de l'Acheteur de façon à ce que celui-ci puisse les reproduire et les conserver facilement.

Le Client autorise Payplug à accéder gratuitement, à des fins de contrôles, vérifications et tests, aux contenus des documents et services de nature électronique pour le paiement desquels il utilise la Solution de Paiement en Ligne.

### 5.3 Obligations relatives aux contenus du site internet

– Respect des droits d'autrui

Le Client s'engage à respecter les droits d'autrui et notamment :

- les droits de la personnalité (tels que droit à l'image, droit au respect de la vie privée),
- les droits de propriété intellectuelle, à savoir notamment, le droit des marques, le droit d'auteur (portant notamment sur les logiciels, les sons, les images, les photographies, les textes, les images animées,



les films), les droits voisins (artistes interprètes, producteurs de phonogrammes et de vidéogrammes), et les droits sui generis des producteurs de bases de données,

- d'une manière générale, les droits des personnes et des biens.

### 5.3.2

#### - **Contenus interdits**

Le Client n'a pas le droit d'utiliser la Solution de Paiement en Ligne pour des Produits :

- contraires à l'ordre public et aux bonnes mœurs,
- à caractère pornographique
- lié à l'activité de voyance, le vaudou, l'hypnose, etc...
- à caractère injurieux, diffamatoire, raciste, xénophobe, homophobe, révisionniste ou portant atteinte à l'honneur ou la réputation d'autrui,
- incitant à la discrimination, à la haine d'une personne ou d'un groupe de personnes en raison de leur origine, de leur orientation sexuelle, de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée,
- menaçant une personne ou un groupe de personnes,
- tout contenu dégradant ou portant atteinte à la personne humaine ou à son intégrité,
- incitant à commettre un délit, un crime ou un acte de terrorisme ou faisant l'apologie des crimes de guerre ou des crimes contre l'humanité,
- incitant au suicide,
- permettant à des tiers de se procurer directement ou indirectement des logiciels piratés, des numéros de série de logiciels, des logiciels permettant les actes de piratage et d'intrusion dans les systèmes informatiques et de télécommunication, des virus et autres bombes logiques et d'une manière générale tout outil logiciel ou autre, dont le Client ne disposerait pas des droits de diffusion,
- permettant de porter atteinte aux droits d'autrui et à la sécurité des personnes et des biens,
- en violation du caractère privé des correspondances,
- confidentiels en vertu d'une mesure législative ou d'un acte juridique (et notamment, des informations internes, privilégiées, constitutives d'un délit d'initié ou relevant du secret professionnel)
- liée à une activité interdite par les Réseaux de Carte ou par un partenaire de Payplug

### 5.3.3

#### **Protection des mineurs**

Le Client s'engage à prendre toutes les mesures appropriées eu égard à l'état de l'art pour bloquer l'accès des mineurs aux Opérations de paiement portant sur des Produits interdits aux mineurs ou pouvant nuire à leur moralité et à leur développement, tels que notamment les contenus de nature érotique ou pornographique ou comportant des scènes de violence.

A ce titre, le Client s'engage :

- à configurer les pages de paiement en sélectionnant la classe d'âge minimale des catégories de Produits qu'il propose, afin d'empêcher l'accès des mineurs aux éléments susvisés,
- à prévenir de manière explicite - sous forme de message d'avertissement - que les contenus ou les services proposés peuvent porter atteinte à la sensibilité du public et sont réservés à un public majeur.

A défaut, Payplug sera en droit de modifier les configurations des pages de paiement proposées par le Client afin d'en interdire l'accès à des mineurs. Payplug est également en droit, en cas de non-respect, de suspendre immédiatement le Compte Payplug du Client.

## **ARTICLE 6 – MOYENS DE PAIEMENT ACCEPTÉS**

La Solution de Paiement en Ligne permet au Client d'accepter des paiements réalisés grâce à des Cartes appartenant aux Réseaux de Cartes acceptés ou tout autres Moyens de Paiement acceptés par Payplug tels que définis au préambule des CGV. La liste des Réseaux de Cartes acceptés est indiquée sur le Site et peut-être modifiée par Payplug à tout moment sans notification préalable. Tout arrêt d'un Moyen de Paiement sera notifié par notification simple.

En application du règlement européen 2015/751 entré en vigueur le 9 juin 2016, le Client peut choisir le réseau de carte qu'il souhaite utiliser lorsque les cartes sont co-brandées (par exemple CB et VISA). D'après ce même règlement c'est finalement à l'Acheteur de choisir le réseau au moment du paiement. Sur la page de paiement mise à disposition par Payplug, l'Acheteur peut choisir le Réseau de Cartes par lequel il souhaite que son paiement soit traité. En l'absence de choix par l'Acheteur, le réseau choisi par défaut peut être consulté ici <http://support.payplug.fr> quel est le réseau choisi par défaut.

## ARTICLE 7 – OPÉRATION DE PAIEMENT ET REMBOURSEMENT

### 7.1 Opération de paiement

Payplug permet au Client d'encaisser des Opérations de paiement notamment via des liens de paiement dynamiques qu'il peut intégrer à son site ou générer à la volée.

Payplug peut être amené à proposer au Client la possibilité d'enregistrer un Carte pour réaliser des Opérations de paiement ultérieurement. Les fonctionnalités associées font l'objet d'une description dans notre [FAQ](#) disponible sur le Site à l'adresse : <http://support.payplug.com/>.

Une authentification de l'Acheteur selon les modalités dites de « 3D Secure » peut être déclenchée à l'initiative de Payplug si le montant, les conditions de l'Opération de paiement ou les informations disponibles le justifient. Payplug peut, pour chaque Opération de paiement, décider d'utiliser ou non une authentification. Le Client ne peut en aucun cas contester ou exiger un changement des règles d'authentification appliquées par Payplug. Toutefois, si le Client le demande et si Payplug accepte, il pourra être conjointement décidé d'appliquer systématiquement des règles d'authentification pour toutes les Opérations de paiement reçues par le Client.

Si le Client et l'Acheteur sont tous deux physiquement présents au moment de l'Opération de paiement, alors il appartient au Client, sous sa seule responsabilité, de vérifier que :

- le nom indiqué sur la Carte est bien celui de l'Acheteur ;
- l'Acheteur indique dans la page internet reçue un numéro de carte et une date d'expiration identiques à ceux indiqués sur sa Carte ; et
- l'Acheteur valide l'Opération de paiement.

Payplug se réserve le droit de refuser une Opération de paiement pour tout motif qu'il jugera légitime. Dans ce cas, Payplug en informera au plus vite le Client et précisera, si possible, le motif de refus.

Pour chaque Opération de paiement réalisée, le Client autorise Payplug à prélever sur son Compte Client à la fin du mois en cours le montant des Frais de Transaction.

Une fois l'Opération de paiement réalisée, le Client reçoit une Confirmation de Paiement sur le Site ou par email. Les Confirmations d'Achat sont envoyées par Payplug à l'Acheteur uniquement sous forme électronique par email ou par SMS. Elles contiennent les informations relatives à l'Opération de paiement, telles que le montant et le nom du Client.

Une fois qu'une Opération de paiement est réalisée, Payplug met à jour l'historique des Opérations de paiement accessible sur le Compte Payplug du Client, notamment via le Portail.

Le Client peut consulter son Solde à tout moment en se connectant à son Compte Payplug via le Portail. Payplug se réserve le droit d'imputer des frais de recherche de document au Client pour la fourniture d'informations supplémentaires qui ne seraient pas renseignées dans l'historique des Opérations de paiement (par exemple : données géographiques, informations sur les erreurs de paiement, nombre de tentatives de paiement, etc.). Payplug s'assurera que l'historique des Opérations de paiement pourra être consulté en ligne pendant une durée au moins égale à 3 mois par le titulaire du Compte Payplug ouvert correspondant.

Le Client s'engage à vérifier régulièrement l'exactitude des Opérations de paiement renseignées sur son Compte Payplug et à signaler toute anomalie à Payplug, et en tout état de cause dans les délais et selon les conditions prévues par les présentes CGV. Dans ce cadre, le Client est responsable en cas d'erreur de saisie de données relatives à l'Opération de paiement qu'il a voulu réaliser (n° de téléphone ou adresse email de l'Acheteur, montant,

quantité, etc.).

En cas de fermeture du Compte Payplug pour quelque raison que ce soit, et sauf dans les cas où la loi l'exige, Payplug n'est pas tenu de fournir des informations concernant les Opérations de paiement réalisées.

## **ARTICLE 8 – PROBLÈME TECHNIQUE**

En cas de problème technique au cours d'une Opération de paiement, d'un Remboursement, ou dans le suivi des Opérations de paiement, le Client se référera à la FAQ disponible sur le Site. Si le Client ne trouve pas la réponse à son problème sur le Site, il contactera Payplug à l'adresse suivante : [support@payplug.com](mailto:support@payplug.com) ou au numéro de téléphone suivant : 01 85 08 38 28. Payplug fera ses meilleurs efforts pour accompagner le Client dans la résolution des problèmes techniques qu'il pourrait rencontrer en utilisant la Solution de Paiement en Ligne.

Toutefois la responsabilité de Payplug ne pourra pas être engagée dans les cas mentionnés à l'Article 20 des CGV ci-dessus, notamment si une Opération de paiement échoue du fait d'un problème technique non imputable à Payplug (notamment, de manière non limitative, tout problème imputable aux banques, aux Réseaux de Cartes ou encore lié à l'utilisation de téléphones mobiles ou d'Internet).

## **ARTICLE 9 – RÉSILIATION DU CLIENT DE LA SOLUTION DE PAIEMENT EN LIGNE**

### **9.1 Si le Client a souscrit à la Solution de Paiement en Ligne mais pas à la Solution de Paiement en magasin**

Le Contrat de la Solution de Paiement en ligne étant à durée indéterminée, le Client peut à tout moment et moyennant le respect d'un préavis de trente (30) jours calendaires, procéder à sa résiliation. Cette résiliation emporte alors résiliation de l'ensemble du Contrat. Le Client doit, pour ce faire, adresser sa notification au service client Payplug, par lettre recommandée avec accusé de réception, à l'adresse postale suivante : Siège Payplug 110 avenue de France, 75013 Paris ou par un autre moyen mis à disposition du Client par Payplug pour effectuer sa résiliation. Dans ce cas, tous les fonds figurant sur le Compte Client et dus à la date de fermeture lui seront retournés par Virement dans les conditions définies à l'article 16 des CGV et le Compte Payplug et le Compte Client seront clôturés.

### **9.2 Si le Client a souscrit à la Solution de Paiement en Ligne et à la Solution de Paiement en magasin**

Le Client peut à tout moment et moyennant le respect d'un préavis de trente (30) jours calendaires, procéder à la résiliation de la Solution de Paiement en Ligne. Cette résiliation emporte alors résiliation uniquement sur la Solution de Paiement en Ligne. Le Client doit, pour ce faire, adresser sa notification au service client Payplug, par lettre recommandée avec accusé de réception, à l'adresse postale suivante : Payplug Entreprise 110 avenue de France, 75013 Paris ou par un autre moyen mis à disposition du Client par Payplug pour effectuer sa résiliation.

## **ANNEXE 2 : CONTRAT D'ADHÉSION AU SYSTÈME DE PAIEMENT DE PROXIMITÉ ou A Distance PAR CARTES "CB" OU CARTES SOUMISES AUX RÈGLES "CB"**

Le Client demande à Payplug, de pouvoir bénéficier de l'encaissement de ses ordres et/ou opérations de paiement via le Système de paiement du Groupement des Cartes Bancaires "CB" lui-même (Groupement d'Intérêt Economique régi par les articles L. 251-1 et suivants du Code de commerce, ci-après désigné le « GIE CB »). Dans ce contexte, les parties sont convenues ce qui suit :

L'adhésion du Client au Système de Paiement de proximité par Cartes "CB" ou cartes soumises aux règles « CB » (ci-après le « Système "CB" »), selon les règles établies par le GIE CB dans le cadre du contrat d'adhésion (ci-après le « Contrat d'Adhésion »), et formée des documents suivants :

- le présent Contrat d'Adhésion accepté en ligne par le Client ;
- Pour les Cartes CB les Conditions Générales au Contrat de la Solution de Paiement en ligne Payplug (ANNEXE 1) sous réserve de l'application prioritaires des règles du GIE CB spécifiques.
- les Conditions Particulières convenues avec Payplug en sous-annexe 1 ;
- les conditions générales d'adhésion au Système de Paiement de proximité par cartes "CB" ou cartes soumises aux règles « CB » (ci- après les « Conditions Générales "CB" »), en sous-annexe 2 ;
- le « Référentiel Sécuritaire », en sous-annexe 3 ;
- l'addendum au Contrat d'Adhésion indiquant les conditions d'utilisation des équipements électroniques utilisant la technologie sans contact, en sous-annexe 4.

En acceptant en ligne le présent Contrat, le Client déclare (i) qu'il en a pris connaissance et (ii) les accepte sans réserve.

## **SOUS-ANNEXE 1 - CONDITIONS PARTICULIÈRES DU CONTRAT D'ADHÉSION AU SYSTÈME DE PAIEMENT DE PROXIMITÉ**

PAR CARTES "CB" OU SOUMISES AUX RÈGLES "CB"

Les présentes Conditions Particulières sont convenues entre Payplug et le Client dans le cadre du Contrat d'Adhésion au Système de paiement par cartes « CB » (Ci-après "Système CB") ; et font parties intégrantes du Contrat.

Sauf stipulation contraire prévue aux présentes Conditions Particulières et/ou au Contrat d'Adhésion, l'ensemble des termes comportant une majuscule conservent la signification qui leur a été donnée aux Conditions Générales de Vente sous réserve des définitions complémentaires apportés au Contrat d'Adhésion au système de paiement de proximité par cartes « CB ». Par cartes CB ci-après "Cartes CB" ou cartes soumises aux règles CB (sans la marque "CB") ci-après " Cartes soumises aux règles « CB »" on entend les Cartes soumises aux règles du Groupement des Cartes bancaires CB.

### **ARTICLE 1 – INFORMATIONS PRÉALABLES – DOCUMENTS REQUIS**

La demande d'adhésion au Système "CB" ne pourra être analysée que lorsque le Client aura remis à Payplug l'ensemble des documents demandés dans le cadre de la connaissance Clients et mentionnés dans le Portail Payplug tel que défini dans les conditions prévues à l'article 12 des Conditions Générales de Vente.

### **ARTICLE 2 – ACTIVITE & POINTS DE VENTE DU CLIENT**

Le Client atteste de la véracité des éléments suivants qui ont été déclarés dans le Portail Payplug dans le cadre du Contrat :

- Type d'activité
- Produits et/ou services vendus
- Enseigne
- Adresse
- Code postal
- Ville
- Téléphone

Les informations ci-dessus seront fournies à Payplug pour l'ensemble des Boutiques du Client.

### **ARTICLE 3 – CONDITIONS LIEES A LA GARANTIE**

#### **3.1 La liste d'opposition sera soit :**

- Fournie par Payplug
- Intégrée au TPE
- Traitée par un recours systématique à une demande d'autorisation

#### **3.2 Délai de communication des justificatifs**

Les justificatifs de paiement devront être communiqués à Payplug dans un délai de huit (8) jours calendaires à compter de la demande.

Si le Client ne communique pas le justificatif, ou le communique au-delà du délai ci-dessus, il s'expose à une Contestation.

#### **3.3 Autorisation**

Le montant du seuil de demande d'autorisation par Carte, par jour et par Boutique (au jour de la signature du Contrat d'Adhésion) est déterminé au cas par cas par le Client et dans les limites autorisées par les lois et

règlements en vigueur (y compris tout dispositif défini au sein du Système « CB »).

Ce montant peut être modifié par Payplug, conformément aux dispositions de l'article 8 de la sous-annexe 2 « Conditions générales du Contrat d'Adhésion au système de paiement de proximité par cartes "CB" ou cartes soumises aux règles "CB" »

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

#### **3.4 Délai de Remise**

Le délai maximum de réception des enregistrements par l'Acquéreur "CB" au-delà duquel ils ne seront réglés que sous réserve de bonne fin d'encaissement (délai de remise) est de sept (7) jours calendaires à compter de la date de l'opération de paiement.

### **ARTICLE 4 – CONDITIONS D'UTILISATION RELATIVES A L'EQUIPEMENT ELECTRONIQUE**

L'Équipement Électronique –tel que défini en Sous-Annexe 2- utilisé dans le cadre du Contrat d'Adhésion est loué ou acheté par le Client à Payplug ou par un tiers.

Le GIE CB s'est engagé à informer tous les constructeurs connus et référencés par lui, des mises à jour de logiciels jugées indispensables.

Le Client assure sous sa seule responsabilité l'installation, le fonctionnement, le remplacement, la maintenance et la mise à niveau de l'Équipement Électronique.

#### **4**

#### **4.1 Dans le cadre de l'acceptation des Cartes, le Client doit pendant l'exécution du Contrat d'Adhésion :**

#### **Veiller à ce que sa police d'assurance couvre notamment :**

- les risques inhérents à la garde de cet Équipement Électronique dont Payplug ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de sa destruction ou de son altération ;
- les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu lui être confiés.

#### **4.2 Laisser libre accès au constructeur de l'Équipement Électronique, à Payplug ou à toute personne désignée par ce dernier pour les différents travaux ou paramétrages à effectuer sur l'Équipement Électronique.**

#### **4.3 Ne pas utiliser l'Équipement Électronique à des fins illicites ou non autorisées par le constructeur ou Payplug et n'y apporter aucune modification de logiciel, et notamment tout modification ayant un impact sur le Système "CB" sans accord préalable de Payplug et sans nouvelle procédure d'agrément dans le respect des dispositions prévues par les Conditions Générales "CB".**

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



## **ARTICLE 5 – FRAIS ET CONDITIONS DE RÈGLEMENT**

Les frais et conditions de règlement sont ceux indiqués dans le Portail Payplug.

## **ARTICLE 6 – REGLEMENT DES OPERATIONS**

Les sommes dues au Client au titre des opérations de paiement effectuées, déduction faite des remboursements, frais et éventuels impayés, sont cantonnées par Payplug conformément à ses obligations au titre de l'article L. 522-17 du CMF.

Il est précisé que les sommes dues au Client au titre des opérations de paiement ne lui sont versées que sous réserve (i) de la bonne fin de l'encaissement par Payplug des fonds provenant du compte de l'Acheteur, et (ii) de toute Contestation.

## **ARTICLE 7 – RELEVES D'OPERATIONS**

Le Client donne mandat à Payplug d'établir pour son compte les relevés d'opérations. Ceux-ci mentionnent, pour chaque opération de paiement, la date d'exécution du paiement, son montant et sa devise, ainsi que les Frais, ces éléments étant distingués conformément aux dispositions de l'article L. 133-11 alinéa 2 du CMF.

Ces relevés seront à disposition du Client dans le Portail Payplug.

## **ARTICLE 8 – RESPONSABILITES**

Le Client s'engage à garantir Payplug contre tous préjudices et dommages, coûts, frais ou honoraires de quelque nature que ce soit (y compris les honoraires d'avocats ou d'experts) que pourrait avoir à subir Payplug du fait d'un manquement du Client à ses obligations aux termes du Contrat d'Adhésion ou dans le cas d'une action judiciaire ou menace d'action judiciaire émanant d'un tiers (en particulier tout Porteur de Carte). Le cas échéant, le Client s'engage à indemniser Payplug à hauteur du préjudice subi par cette dernière.

Les Parties sont convenues de la nécessité de maintenir un principe de proportionnalité entre l'indemnisation qui peut être réclamée, les tarifs pratiqués par Payplug et le comportement répréhensible reproché à la Partie fautive.

La responsabilité de Payplug à l'égard du Client, dans le cadre du Contrat d'Adhésion, est limitée, sous réserve du respect des dispositions légales applicables, à l'indemnisation des seuls préjudices directs subis par le Client.

En tout état de cause, la responsabilité de Payplug ne pourra être engagée que dans l'hypothèse où elle aura été valablement établie par une juridiction compétente et ne pourra en aucun cas dépasser le montant des Frais perçus par Payplug dans le cadre du Contrat d'Adhésion au titre de sa rémunération pour le Service au cours des douze (12) mois précédant le fait générateur du litige.

Les Parties conviennent expressément que cette limitation de la responsabilité de Payplug dans le cadre du Contrat d'Adhésion et au titre du Service rendu :

- (i) est raisonnable et proportionnée aux risques assumés, d'une part, et aux bénéfices tirés de l'exécution du Contrat d'Adhésion, d'autre part, par chacune des Parties ;
- (ii) est la condition de la fourniture du Service selon les modalités financières susvisées.

## **ARTICLE 9 – DÉCLARATION DU CLIENT**

Préalablement à la signature du Contrat d'Adhésion, Payplug a fourni au Client une information complète relative aux services qu'elle propose.

Le Client déclare et garantit à Payplug que les informations le concernant sont exactes et complètes.

Le Client reconnaît que c'est notamment sur la base de ces informations préalables qu'ont été établies les présentes Conditions Particulières, et s'engage à notifier à Payplug toute modification de ces Informations Préalables qui surviendrait en cours d'exécution du Contrat d'Adhésion, en particulier dès lors qu'une telle



modification rend inexacte une mention figurant dans les présentes Conditions Particulières.

Le Client donne son accord pour recevoir sur son Portail l'ensemble des factures qui lui sont adressées.

## ARTICLE PRÉLIMINAIRE ET DÉFINITIONS

Pour l'application des présentes Conditions Générales "CB" relatives au Système de paiement de proximité par Cartes « CB » ou Cartes soumises aux règles « CB », les mots et expressions commençant par une lettre majuscule ont, nonobstant toute définition qui serait donnée dans les présentes ou dans les CGV, le sens qui leur est attribué ci-dessous, qu'ils soient employés au singulier ou au pluriel :

- 1) Par "Équipement Électronique", il faut entendre tout dispositif de paiement qui comporte un système permettant le contrôle du code confidentiel comme par exemple le terminal de paiement électronique (ci-après "TPE"). Actuellement, ce contrôle est opérationnel avec les Cartes portant la marque "CB" et certaines Cartes portant les marques Visa et MasterCard émises par un Emetteur membre CB mais soumises aux règles "CB". Toute extension de l'application de ce contrôle à d'autres Cartes sera notifiée par Payplug au Client, conformément aux dispositions de l'article 8 des Conditions Générales "CB". L'agrément de l'Équipement Électronique est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par le GIE CB, qui dispose de la liste des Équipements Électroniques agréés par le GIE CB et qui peut la communiquer au Client sur sa demande.
- 2) Par « Service », il faut entendre le service de paiement de proximité mis à la disposition du Client par Payplug.
- 3) Par « Boutique », il faut entendre le lieu d'utilisation du système de paiement de proximité du Client.

## ARTICLE 1 – DÉFINITION DU SYSTÈME "CB"

Le Système "CB" repose notamment sur l'utilisation de Cartes "CB" ou cartes soumises aux règles "CB" pour le paiement d'achats de biens ou de prestations de services auprès du Client en sa qualité d'Accepteur "CB" et adhérent au Système "CB", et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Lorsque Payplug représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte "CB" ou cartes soumises aux règles "CB" et de remise des opérations de paiements à Payplug, et non la mise en jeu de la garantie du paiement visée à l'article 5 des présentes.

## ARTICLE 2 – DISPOSITIONS RELATIVES AUX CARTES "CB" OU CARTES SOUMISES AUX RÈGLES "CB"

Sont utilisables dans le Système "CB" :

- (i) les Cartes sur lesquelles figure la marque "CB" ;
- (ii) les Cartes émises par tout Système de paiement et soumises aux règles "CB", c'est-à-dire :
  - les Cartes portant uniquement la marque Visa ou MasterCard mais acceptée dans le Système "CB" par le GIE CB ;
  - les Cartes émises dans le cadre de réseaux étrangers ou internationaux homologuées par le GIE CB et dont le Client peut obtenir les signes de reconnaissance auprès de Payplug ;
  - toutes autres Cartes dont l'acceptation par le GIE CB viendrait à être notifiée au Client par Payplug.

A toutes fins utiles, il est précisé que l'ensemble de ces cartes est désigné ci-après par le terme générique "Carte".

### ARTICLE 3 – OBLIGATIONS DU CLIENT

Le Client reconnaît que Payplug doit lui faire appliquer l'ensemble du dispositif applicable au Système CB, dans le cadre de l'encaissement des ordres et/ou opérations de paiement du Client.

A ce titre, le Client s'engage à :

- pour les TPE : afficher visiblement chaque marque, catégorie de cartes ou application de paiement qu'il accepte notamment en apposant à l'extérieur et à l'intérieur de son établissement des panonceaux, vitrophanies et enseignes qui lui sont fournis par Payplug ou IE système de cartes de paiement ;
- afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que les Acheteurs en soient préalablement informés. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes ;
- s'identifier clairement par le numéro SIRET et le code activité (NAF/APE) que l'INSEE lui a attribués. Si le Client n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par Payplug lui permettant l'accès au Système "CB" ;
- afin que l'Acheteur n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec Payplug la conformité des informations transmises pour identifier sa Boutique, ces informations devant indiquer une dénomination commerciale connue des Acheteurs et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, vente à distance, etc.) ;
- accepter les Cartes portant les marques des systèmes de cartes de paiement dont les règles de fonctionnement sont définies à l'article 2 des présentes et qui sont effectués en contrepartie d'actes de vente ou de fournitures de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ;
- transmettre les enregistrements des opérations de paiement, dans un délai maximum de six (6) mois à compter de la date de l'opération de paiement. Au-delà de ce délai, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Système "CB" ;
- faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des clients et concernant des biens et services dont l'achat a été réglé par Carte au titre du présent Contrat d'Adhésion ;
- utiliser obligatoirement l'Équipement Électronique tel que défini par l'Article Préliminaire ci-dessus et agréé par les systèmes de cartes de paiement concernés ;
- ne pas modifier les paramètres de son fonctionnement et ne pas y installer de nouvelles applications, notamment en acceptant l'intervention de tiers, sans avoir au préalable obtenu l'autorisation écrite de l'Acquéreur "CB" et/ou Payplug ;
- prendre toutes les mesures propres à assurer la garde de son Équipement Électronique et être vigilant quant à l'utilisation qui en est faite ;
- 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 Sécuritaire et acceptent que les audits soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article ;
- Lorsque le système de cartes de paiement le prévoit : permettre à l'Acquéreur "CB" – par l'intermédiaire de Payplug - de faire procéder aux frais du Client dans ses locaux ou ceux de ses prestataires ou sous-traitants, à la vérification par un tiers indépendant du respect tant des Conditions Générales "CB" que des exigences sécuritaires du Contrat d'Adhésion. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du Contrat d'Adhésion et/ou pendant sa durée ;
- Le Client autorise la communication du rapport à Payplug et l'Acquéreur "CB", aux systèmes de cartes de paiement concernés dont les marques sont apposées sur les Cartes acceptées par de le Client ;
- A la demande de l'Acquéreur « CB » et/ou celle de Payplug selon les volumes d'opérations cartes

acceptées du Client, ce dernier doit respecter les exigences du Référentiel Sécuritaire qui lui seront communiquées par l'Acquéreur « CB » et/ou Payplug à première demande.

#### ARTICLE 4 – OBLIGATIONS DE PAYPLUG

Le Client déclare avoir été préalablement informé que tout ou partie des obligations listées ci-dessous est susceptible de nécessiter un certain temps de traitement compte tenu des différents intermédiaires impliqués dans l'encaissement des ordres et/ou opérations de paiement du Client.

A ce titre, Payplug s'engage à :

- Fournir au Client, sur demande de celui-ci, les informations le concernant directement, relatives au fonctionnement du système de cartes de paiement et à son évolution, les catégories de cartes, les marques et les applications de paiement dont il assure l'acceptation ainsi que les Commissions d'Interchange et les commissions de services applicables à chacune des cartes et marques acceptées par lui ;
- Respecter le choix de la marque et de la catégorie de la Carte et de l'application de paiement au sens de l'article 2 de cette sous-annexe 2 utilisé pour donner l'ordre de paiement effectué au point de vente conformément au choix du Client ou de l'Acheteur ;
- Mettre à la disposition du Client, selon les Conditions Particulières, les informations relatives à la sécurité des opérations de paiement ;
- Indiquer au Client la liste et les caractéristiques des Cartes pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN) ;
- Créditer le Compte Client des sommes qui lui sont dues, en application du Contrat ;
- Ne pas débiter, au-delà du délai maximum de quinze (15) mois à partir de la date du crédit initial porté au Compte Client les opérations de paiement non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte ;
- Communiquer, à la demande du Client, les éléments essentiels des procédures administratives annexes, notamment :
  - o Gestion et renvoi des Cartes capturées par le Client ;
  - o Gestion et restitution des Cartes oubliées par leurs titulaires
- Selon les modalités convenues avec le Client, communiquer à sa demande, les informations suivantes :
  - o référence lui permettant d'identifier l'opération de paiement,
  - o le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité, et
  - o le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquitté par le Client ainsi que la Commission d'Interchange.

Le Client peut demander à ce que ces informations soient regroupées par marque, application de paiement, catégorie de carte et par taux de Commission d'Interchange application à l'opération.

#### ARTICLE 5 – GARANTIE DU PAIEMENT

- 5.1 Les opérations de paiement sont garanties, sous réserve du respect de l'ensemble des mesures de sécurité définies par le Contrat ainsi que les conditions spécifiques à chacun des systèmes de carte de paiement.
- 5.2 Toutes les mesures de sécurité sont indépendantes les unes des autres, étant précisé que (i) lesdites mesures de sécurité listées aux présentes ne s'appliqueront qu'à Payplug, et (ii) l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel.
- 5.3 En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous

## ARTICLE 6 – MESURES DE SÉCURITÉ

Nonobstant les mesures de sécurisation prévues au Contrat, les mesures de sécurité ci-dessous s'appliquent comme suit :

6.1 Le Client doit informer immédiatement Payplug et/ou l'Acquéreur "CB" en cas de fonctionnement anormal de l'Équipement Électronique, et de toutes autres anomalies (absence de reçu, impossibilité de réparer rapidement, etc.).

### 6.2 Lors du paiement

6.2.1 Dans le cadre de toute opération de paiement réalisée sur un Équipement Électronique de type TPE, le Client s'engage à :

6.2.1.1 vérifier l'acceptabilité de la Carte, c'est-à-dire :

- la présence de la marque "CB" sur la Carte ou l'application de paiement du système de carte de paiement concerné par l'application ;
- la présence de l'hologramme sauf pour les Cartes ne le prévoyant pas tel que celles portant la marque "V Pay" ;
- la présence de la puce sur les Cartes et catégorie de cartes lorsqu'elle y est prévue par le système de carte de paiement ;
- que le type de Carte est défini dans les Conditions Particulières, ou figure à l'article 2 ci-dessus ;
- la période de validité (fin de validité et éventuellement début).

6.2.1.2 utiliser l'Équipement Électronique, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées ;

L'Équipement Électronique doit notamment :

- après la lecture de la puce des Cartes, lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  - vérifier :
    - le code émetteur de la Carte (BIN) ;
    - le code service ;
    - la date de fin de validité de la Carte.
- lorsque la puce n'est pas présente, sur une carte soumise aux règles "CB", ou qu'elle ne fonctionne pas, après lecture de la piste ISO 2, vérifier :
  - le code émetteur de la Carte (BIN) ;
  - Le code service ;
  - La date de fin de validité de la Carte.

- 6.2.1.3 contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition, diffusée par Payplug, pour la Boutique concerné et selon les Conditions Particulières ;
- 6.2.1.4 lorsque la puce le demande à l'Équipement Électronique, faire composer par l'Acheteur, dans les meilleures conditions de confidentialité, son code confidentiel ou ses données de sécurité personnalisées ou mettre en œuvre la méthode d'authentification prévue et adaptée à la technologie applicable. La preuve de la frappe du code confidentiel ou de la vérification des données de sécurité personnalisées est apportée par le certificat qui doit figurer sur le ticket émis par le TPE (ci-après "Ticket TPE") ;

Lorsque le code confidentiel ou les données de sécurité personnalisées n'est pas (ou ne sont pas) vérifié(es), l'opération de paiement n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation ;

- 6.2.1.5 obtenir une autorisation d'un montant identique à l'opération de paiement :
- lorsque le montant de l'opération de paiement en cause, ou le montant cumulé des opérations de paiement réglées au moyen de la même Carte, dans la même journée et pour la même Boutique, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières, et ceci quelle que soit la méthode d'acquisition des informations ;
  - lorsque l'équipement Électronique ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières.

A défaut, l'opération de paiement ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.

Lorsque la puce n'est pas présente sur la Carte agréée "CB" ou lorsqu'elle ne fonctionne pas, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

Une opération de paiement pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.

Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations de paiement faites postérieurement le même jour et avec la même Carte, dans la même Boutique.

- 6.2.1.6 faire signer le Ticket TPE :
- lorsque le montant de l'opération de paiement est supérieur à mille cinq cents (1 500) euros ;
  - en règle générale, dans tous les cas où l'équipement Électronique le demande.



- 6.2.1.7 lorsque la signature est requise et que la Carte comporte un panneau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur ledit panneau ;

Pour une Carte sur laquelle ne figure pas le panneau de signature, vérifier la conformité de la signature utilisée avec celle qui figure sur la pièce d'identité présentée par l'Acheteur.

- 6.2.1.8 remettre à l'Acheteur l'exemplaire du Ticket TPE qui lui est destiné.

### **6.3 Après le paiement**

Le Client s'engage à :

- 6.3.1** transmettre à l'Acquéreur "CB" et/ou Payplug dans les délais et selon les modalités prévues dans les Conditions Particulières du Contrat d'Adhésion CB, les enregistrements électroniques des opérations de paiement, et s'assurer que les montants correspondant à ces opérations de paiement ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières. Toute opération de paiement ayant fait l'objet d'une autorisation transmise par l'Acquéreur "CB" et/ou Payplug doit obligatoirement être remise à ce dernier ;
- 6.3.2** archiver et conserver, à titre de justificatif, pendant quinze (15) mois à compter de la date de l'opération de paiement :
- un exemplaire du Ticket TPE comportant, lorsqu'elle est requise, la signature de l'Acheteur ;
  - l'enregistrement magnétique représentatif de l'opération de paiement ou le journal de fond lui-même.
- 6.3.3** communiquer, à la demande de l'Acquéreur "CB" et/ou Payplug et dans les délais prévus dans les

Conditions Particulières, tout justificatif des opérations de paiement ;

- 6.3.4** ne stocker, sous quelque forme que ce soit, aucune des données cartes ci-après :

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

- 6.3.5** prendre toutes les précautions utiles pour que soient assurées la confidentialité et l'intégrité des données à caractère personnel de l'Acheteur, qu'il est amené à recueillir à l'occasion de son activité, notamment lors de la réalisation d'une opération de paiement par Carte ainsi que du contrôle de l'accès à celles-ci, et ce, conformément aux prescriptions de la réglementation sur les données personnelles.

## **ARTICLE 7 – MODALITES ANNEXES DE FONCTIONNEMENT**

### **7.1 Réclamation**

Toute réclamation doit être formulée selon la procédure décrite à l'article 29 des CGV.

## 7.2 Convention de preuve

Les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur "CB" et/ou Payplug. En cas de conflit, les enregistrements électroniques produits par l'Acquéreur "CB" et/ou Payplug ou par le système de cartes de paiement prévaudront sur ceux produits par le Client signataire du Contrat d'Adhésion, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur "CB" et/ou Payplug ou par le système de cartes de paiement.

## 7.3 Retrait à son Titulaire d'une Carte faisant l'objet d'un blocage ou en opposition pour les TPE

**En cas de retrait d'une Carte à un Acheteur faisant l'objet d'un blocage ou en opposition, ledit retrait ayant notamment eu lieu sur instruction du serveur d'autorisation en raison de la présence de la Carte sur la liste des Cartes faisant l'objet d'un blocage ou en opposition et/ou contrefaites, le Client utilise la procédure de gestion et de renvoi des Cartes capturées.**

Pour toute capture de Carte faisant l'objet d'un blocage ou en opposition et/ou contrefaite et sur instruction de l'Équipement Électronique, une prime sera versée au Client ou à toute personne exerçant une activité au sein de son établissement et qu'il aura indiquée.

## 7.4 Oubli d'une Carte par l'Acheteur

**En cas d'oubli de sa Carte par l'Acheteur, le Client peut la lui restituer dans un délai maximum de deux (2) jours ouvrés après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord demandé selon la procédure communiquée par l'Acquéreur "CB" et/ou Payplug. Au-delà de ce délai, le Client utilise la procédure de gestion et de restitution des Cartes oubliées.**

## 7.5 Remboursement

**Si l'équipement Électronique le permet, le remboursement partiel ou total de l'achat d'un bien ou d'un service réglé par Carte, doit être effectué, au profit de l'Acheteur utilisé, sous réserve de l'accord de celui-ci. Le Client doit alors utiliser la procédure dite de "transaction crédit" et dans le délai prévu dans les règles du système de cartes de paiement qui s'appliquent à l'opération de paiement concernée ou dans les Conditions Particulières, effectuer la remise correspondante à l'Acquéreur "CB" et/ou Payplug à qui il avait remis l'opération initiale. Le montant de la "transaction crédit" ne doit pas dépasser le montant de l'opération de paiement initiale.**

Par défaut le Remboursement se fera depuis le Portail Payplug comme désigné par l'article 6 des Conditions Générales de Vente.

## 7.6 Carte non signée pour les TPE

En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, le Client doit demander à l'Acheteur de justifier de son identité et d'apposer sa signature sur le panonceau de signature, prévu à cet effet au verso de la Carte, ainsi que vérifier la conformité de cette signature avec celle figurant sur la pièce d'identité présentée par l'Acheteur. Si l'Acheteur refuse de la signer, le Client doit refuser le paiement par Carte.

## ARTICLE 8 – MODIFICATIONS

**8.1** Le Client reconnaît et accepte que l'Acquéreur "CB" et/ou Payplug peut modifier à tout moment les

Conditions Générales ainsi que les Conditions Particulières.

- 8.2** L'Acquéreur "CB" et/ou Payplug peut notamment apporter les modifications suivantes :
- des modifications techniques, telles que l'acceptation de nouvelles cartes, des modifications de logiciel, le changement de certains paramètres, etc.
  - des modifications sécuritaires, telles que la modification du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes ou la suspension de l'adhésion au Système de carte de paiement.
- 8.3** Les nouvelles conditions d'adhésion au Système "CB" entrent en principe en vigueur au terme d'un délai minimum de deux (2) mois, à compter de la notification au Client des modifications effectuées par l'Acquéreur "CB" et/ou Payplug.
- 8.4** Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque l'Acquéreur "CB" et/ou Payplug ou le Système de carte de paiement constate, dans la Boutique, une utilisation anormale de Cartes perdues, volées ou contrefaites.
- 8.5** Passés les délais visés au présent article, les modifications notifiées au Client lui sont opposables, s'il n'a pas résilié le Contrat d'Adhésion.
- 8.6** Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du Contrat d'Adhésion, voire la suspension par le Système de carte de paiement de l'adhésion du Client au Système de carte de paiement, dans les conditions prévues à l'article 10 des présentes.

## **ARTICLE 9 – DUREE ET RESILIATION DU CONTRAT D'ADHESION**

- 9.1 Le Contrat d'adhésion est conclu pour une durée indéterminée.

Chaque Partie peut mettre fin au Contrat d'Adhésion à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux Parties au titre du Contrat). Le Client garde alors la faculté de continuer à adhérer au Système "CB" avec tout Acquéreur "CB" de son choix.

- 9.2 Toute cessation d'activité du Client, toute cession ou mutation de son fonds de commerce, entraîne la résiliation immédiate et de plein droit du Contrat d'Adhésion.
- 9.3 Le Client sera tenu de restituer à l'Acquéreur "CB" et/ou Payplug, les dispositifs techniques et sécuritaires et les documents en sa possession, dont l'Acquéreur "CB" et/ou Payplug est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'adhésion, le Client s'engage à retirer immédiatement de son établissement tout signe d'acceptation des Cartes.

## **ARTICLE 10 – SUSPENSION DE L'ADHESION ET RADIATION DU SYSTEME "CB"**

- 10.1 Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations de paiement en cours, à une suspension de l'adhésion du Client au Système "CB". Elle est précédée, le cas échéant, d'un avertissement adressé au Client, voire d'une réduction de son

seuil de demande d'autorisation. Cette suspension est motivée et notifiée par l'envoi d'une lettre recommandée avec accusé de réception. Son effet est immédiat.

Elle peut être décidée en raison, notamment :

- d'une utilisation anormale de Cartes perdues, volées ou contrefaites ;
- d'une utilisation d'Équipement Électronique non agréé ;
- d'un risque de dysfonctionnement important du Système "CB".

10.2 Le Client s'engage alors à restituer à l'Acquéreur "CB" et/ou Payplug l'Équipement Electronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur "CB" et/ou Payplug est propriétaire et à retirer immédiatement de son établissement tout signe d'acceptation des Cartes.

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

10.4 A l'expiration de ce délai, le Client peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet de son Contrat d'Adhésion auprès de l'Acquéreur "CB" et/ou Payplug, ou souscrire un nouveau contrat d'adhésion avec un Acquéreur "CB" de son choix.

10.5 En cas de comportement frauduleux de la part du Client responsable de la Boutique, celui-ci peut être immédiatement radié, ou sa suspension convertie en radiation.

## **ARTICLE 11 – NON - RENONCIATION**

Le fait pour l'une des Parties de ne pas exiger l'exécution d'une disposition du Contrat d'Adhésion ne peut en aucun cas être considéré comme constituant de leur part une renonciation, quelle qu'elle soit, à l'exécution de celui-ci.

### **SOUS-ANNEXE 3 : RÉFÉRENTIEL SÉCURITAIRE**

Les exigences constituant le Référentiel Sécuritaire présentées ci-après doivent impérativement être mises en œuvre par le Client pendant toute la durée du Contrat d'Adhésion.

#### **EXIGENCE 1 (E1) – GÉRER LA SÉCURITÉ DU SYSTÈME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE**

Pour assurer la sécurité des données des opérations de paiement et notamment, des données des Acheteurs, une organisation, des procédures et des responsabilités doivent être établies.

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

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

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

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

#### **EXIGENCE 2 (E2) – GERER L'ACTIVITE HUMAINE ET INTERNE**

Les obligations et les responsabilités du personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.

Les obligations et les responsabilités du personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers. Le personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.

Le personnel doit être régulièrement sensibilisé aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers le réseau Internet) et notamment, à l'introduction de virus.

Il convient que le personnel reçoive une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

#### **EXIGENCE 3 (E3) – GERER LES ACCES AUX LOCAUX ET AUX INFORMATIONS**

Tout dispositif (équipement réseau, serveur, ...) qui stocke ou qui traite des données relatives à une opération de paiement et, notamment, des données de Acheteurs, doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.

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

Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.

La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

#### **EXIGENCE 4 (E4) – ASSURER LA PROTECTION LOGIQUE DU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation doivent être établies et leur respect doit être contrôlé.

Seul le serveur supportant l'application commerciale doit être accessible par les internautes.

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

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

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

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

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

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

#### **EXIGENCE 5 (E5) – CONTRÔLER L'ACCÈS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

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

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

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

#### **EXIGENCE 6 (E6) – GÉRER LES ACCÈS AUTORISÉS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

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

Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification.

L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les

droits accordés à ceux-ci doivent être restreints aux opérations de paiement qui leur sont autorisées.

L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.

Les changements de situation (changement de poste, départ, ...) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.

La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.

Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.

Les tentatives d'accès doivent être limitées en nombre. Les mots de passe doivent être changés régulièrement.

Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

### **EXIGENCE 7 (E7) – SURVEILLER LES ACCÈS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

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

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

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

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

Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées.

Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

### **EXIGENCE 8 (E8) – CONTRÔLER L'INTRODUCTION DE LOGICIELS PERNICIEUX**

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.

L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et d'acceptation.

La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

### **EXIGENCE 9 (E9) – APPLIQUER LES CORRECTIFS DE SÉCURITÉ (PATCHES DE SÉCURITÉ) SUR LES LOGICIELS D'EXPLOITATION**

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.

Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.



#### **EXIGENCE 10 (E10) – GERER LES CHANGEMENTS DE VERSION DES LOGICIELS D'EXPLOITATION**

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée.

Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

#### **EXIGENCE 11 (E11) – MAINTENIR L'INTÉGRITÉ DES LOGICIELS APPLICATIFS RELATIFS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.

Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

La demande de modification doit être approuvée par le responsable fonctionnel du système.

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

#### **EXIGENCE 12 (E12) – ASSURER LA TRAÇABILITÉ DES OPÉRATIONS TECHNIQUES (ADMINISTRATION ET MAINTENANCE)**

Les opérations techniques effectuées doivent être enregistrées de manière chronologique dans un cahier de bord pour permettre la reconstruction, la revue et l'analyse en temps voulu des séquences de traitement et des autres activités liées à ces opérations.

#### **EXIGENCE 13 (E13) – MAINTENIR L'INTÉGRITÉ DES INFORMATIONS RELATIVES AU SYSTÈME COMMERCIAL ET D'ACCEPTATION**

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurées lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

#### **EXIGENCE 14 (E14) – PROTÉGER LA CONFIDENTIALITÉ DES DONNÉES BANCAIRES**

Les données d'un titulaire de Carte ne peuvent être utilisées que pour exécuter un ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un titulaire de Carte ne doit en aucun cas être stocké.

Les données bancaires à caractère personnel relatives à une opération de paiement et, notamment, les données d'un titulaire de Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant du Client et les éléments secrets servant à chiffrer.



Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

### **EXIGENCE 15 (E15) – PROTÉGER LA CONFIDENTIALITÉ DES IDENTIFIANTS ET AUTHENTIFIANTS DES UTILISATEURS ET DES ADMINISTRATEURS**

La confidentialité des identifiants et 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.

### **NORME PCI DSS**

La norme PCI DSS au respect de laquelle le Client est tenu (pour ce qui le concerne) doit pouvoir être consultée par le Client et est disponible à l'adresse suivante :

<https://www.pcisecuritystandards.org>

## **SOUS-ANNEXE 4 – ADDENDUM AU CONTRAT D'ADHÉSION –**

### **CONDITIONS APPLICABLES AUX ÉQUIPEMENTS ÉLECTRONIQUES**

#### **UTILISANT LA TECHNOLOGIE SANS CONTACT**

Lorsque le Client utilise un Équipement Électronique disposant de la technologie dite "sans contact" les conditions de fonctionnement sont régies par le présent avenant et par les conditions du Contrat d'Adhésion, sous réserve des modifications prévues ci-après.

Il est expressément convenu entre le Client et Payplug que :

#### **ARTICLE 1**

Cet Équipement Électronique disposant de la technologie "sans contact" permet le règlement rapide d'achats de biens ou de prestations de services par des Acheteurs avec une lecture à distance de la Carte et sans frappe du code confidentiel

#### **ARTICLE 2**

En toutes circonstances, le Client doit se conformer aux directives qui apparaissent sur cet Équipement Électronique.

#### **ARTICLE 3**

Le montant unitaire maximum de chaque opération de paiement en mode "sans contact" est limité à 30 euros (ou le cas échéant tout autre montant décidé ultérieurement par le GIE CB). Au-delà de ce montant unitaire maximum, les conditions de l'opération de paiement telles que prévues dans les Conditions Générales "CB" modifiées par le présent avenant, restent inchangées.

#### **ARTICLE 4**

Pour les Cartes, lorsque la puce le demande à l'Équipement Électronique, faire composer par l'Acheteur, dans les meilleures conditions de confidentialité, son code confidentiel. La preuve de la frappe du code confidentiel est apportée par le certificat qui doit figurer sur le Ticket.

En cas d'opération en mode "sans contact" permise par l'Équipement Électronique, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, sous réserve du respect de l'ensemble des autres mesures



de sécurité à la charge du Client.

#### **ARTICLE 5**

L'ensemble des autres dispositions du Contrat d'Adhésion reste applicable.

## **ANNEXE 3 : CONDITIONS GÉNÉRALES AU CONTRAT DE LOCATION DE TPE**

### **ARTICLE 1 – OBJET DU CONTRAT**

Le présent contrat (ci-après désignée le « Contrat de Location de TPE ») a pour objet de définir les conditions dans lesquelles Payplug (ci-après désignée « le Loueur ») fournit au locataire (ci-après « le Client »), qui l'accepte, les produits et services monétiques suivants (ci-après désignés « les prestations ») :

- un Terminal de Paiement Électronique (TPE) acceptant les cartes Contact et Sans Contact de technologie RTC, GPRS ou IP (ci-après « TPE » ou « équipement ») composé du terminal et de tous les câbles et accessoires (pinpad, ...) associés, la technologie Sans Contact étant incluse dans le terminal ou dans l'un des accessoires associés (pinpad ou cible dédiée à la lecture Sans Contact), et/ou un Editeur Lecteur de Chèques,
- des logiciels associés au TPE et les licences d'utilisation de ces logiciels,
- la formation à l'utilisation du TPE à la demande du Client via les supports fournis par Payplug,
- une assistance technique et téléphonique (ci-après « ATT »),
- la maintenance du TPE suivant l'offre souscrite par le Client sur le Portail Payplug,
- pour les TPE IP : un câble de connexion entre l'équipement et le modem-routeur du Fournisseur d'Accès à Internet (ci-après « FAI »), un abonnement à un service Monétique IP souscrit auprès d'un Passerelliste sélectionné par le Loueur,
- pour les TPE GPRS : une carte SIM, installée dans l'équipement et nécessaire au fonctionnement de celui-ci, un abonnement GPRS monétique souscrit auprès d'un opérateur de télécommunications, un réseau de transport de flux électronique souscrit auprès d'un opérateur de transport de données,
- pour les TPE IP, GPRS ou RTC, la livraison de l'équipement au Client par transporteur.

Sauf stipulation contraire prévue aux présentes Conditions Générales au Contrat de Location de TPE, l'ensemble des termes comportant une majuscule conservent la signification qui leur a été donnée aux Conditions Générales de Vente et au Contrat d'Adhésion au système de paiement de proximité par carte « CB » ou « CB cartes soumises aux règles ».

La fourniture de ces prestations au Client a vocation de permettre à ce dernier d'effectuer les encaissements de ses clients dans les conditions définies ci-après.

### **ARTICLE 2 – PREREQUIS A LA FOURNITURE DES PRESTATIONS AU CLIENT**

Pour pouvoir bénéficier des prestations et signer le présent Contrat de Location de TPE, le Client doit obligatoirement avoir souscrit au préalable un Contrat d'Adhésion au système de paiement de proximité par cartes « CB » ou cartes soumis aux règles « CB » (« Contrat d'Adhésion ») et doit exercer son activité commerciale dans un pays autorisé par Payplug.

Pour les TPE IP, le Client doit disposer d'un accès haut-débit à Internet opérationnel.

## ARTICLE 3 – DESCRIPTION DES PRESTATIONS

### 3.1 Livraison, installation et formation

Le Loueur contacte le Client afin de valider les informations techniques nécessaires. Le transporteur sélectionné par le Loueur livre l'équipement à l'adresse signifiée par le Client à Payplug.

À réception de l'Équipement, et en présence du transporteur, le Client est tenu d'effectuer les vérifications d'usage afin de constater que l'équipement est en bon état et ne présente pas de détériorations particulières avant de signer le bon de livraison qui lui sera présenté par le transporteur. En cas de défauts constatés, le Client devra émettre des réserves en les mentionnant sur ledit bon de livraison et en refusant de réceptionner l'équipement.

Le Client assure lui-même et sous sa seule responsabilité le branchement de l'équipement sur ses réseaux électriques et/ou réseau téléphonique commuté ou ADSL. Concernant le TPE IP Mobile Wifi, le Client devra appairer lui-même son TPE avec son routeur Wifi (par exemple box Internet ou smartphone) en entrant le mot de passe du routeur Wifi dans les paramètres de son équipement.

La formation du Client à l'utilisation de l'équipement est assurée par le Loueur via les supports fournis par Payplug. Suivant l'offre souscrite sur le Portail Payplug, le Client peut contacter l'Assistance Technique Téléphonique (ATT) pendant les horaires indiqués sur le Portail Payplug ou sur la page du support (FAQ), en vue de sa formation à l'utilisation de l'équipement. Le Client accepte de procéder aux manipulations demandées par le Loueur dans le cadre de la formation par téléphone relative à l'utilisation de l'équipement.

Si l'installation du TPE est infructueuse, le Loueur proposera une installation sur site (en option), qui lui sera facturée. Dans ce cas, le Client s'engage à ce que lui-même ou l'un de ses représentants dûment habilités soit présent dans les locaux à la date et à l'heure convenues pour l'installation. L'installation sera effectuée uniquement à l'adresse du point de vente indiqué par le Client. L'installation du TPE sera réalisée par un technicien mandaté par le Loueur à cet effet. Le Client s'engage à lui donner accès aux locaux du point de vente, à répondre à ses demandes et à se conformer à ses recommandations.

À l'issue de l'opération d'installation et de formation sur site, le technicien demandera au Client ou à son représentant, mandaté à cet effet, de signer un PV d'intervention. Si le Client constate une non-conformité du fonctionnement du TPE, il peut le mentionner sur le PV d'intervention. Dans cette hypothèse, le Loueur devra dans les meilleurs délais et dès notification de ces réserves, corriger les points de non-conformité évoqués. En l'absence de réserves, le TPE est réputé fonctionner de façon conforme.

### 3.2 Assistance Technique et Téléphonique (ATT) - maintenance corrective – intervention sur site

En cas d'anomalie dans le fonctionnement de son TPE, le Client appelle l'ATT du Loueur, au numéro et aux horaires disponibles (sauf jours fériés) sur le Portail Payplug ou sur la page du support au numéro et aux horaires indiqués sur la lettre et le sticker accompagnant le TPE.

Le coût éventuel de la communication est, au jour de la signature du Contrat de Location de TPE, signalé sur le Portail Payplug ou sur la page du support, auxquels s'ajoutent les coûts de communication/service facturés par l'opérateur téléphonique du Client depuis un poste mobile ou fixe.



L'ATT diagnostique, par téléphone suivant les indications données par le Client, la nature de l'incident et tente, lorsque cela est possible, de le régler par téléphone. Pour ce faire, le Client accepte de réaliser lui-même les différentes manipulations demandées par l'ATT par téléphone et destinées à diagnostiquer la panne et à assurer la remise en service rapide de l'équipement.

Certaines opérations de maintenance du TPE peuvent nécessiter des investigations techniques plus approfondies. Dans un tel cas, l'ATT du Loueur met fin à la communication téléphonique, réalise de son côté ces investigations et recontacte le Client afin de l'informer de la procédure à suivre pour rétablir le bon fonctionnement du TPE.

Certaines opérations de maintenance du TPE peuvent nécessiter de le connecter au réseau téléphonique commuté (ligne analogique), pour les TPE GPRS et IP, si le modèle de ce dernier le permet, ou à Internet pour les TPE IP. Dans le cas d'une telle demande de l'ATT du Loueur, le Client fait son affaire de réaliser lui-même une telle connexion afin de permettre la réalisation de l'opération à la date et à l'heure prévues par le Loueur. Le coût des télécommunications effectuées sur le réseau téléphonique commuté est à la charge du Client.

Si le Client n'est pas en mesure de répondre à une demande du Loueur concernant la connexion au réseau téléphonique commuté ou à Internet, la remise à niveau technique de l'équipement peut nécessiter de réaliser un échange, tel que décrit ci-dessous. L'échange donnera lieu, dans ce cas, à facturation séparée des prestations, après présentation d'un devis au Client expressément accepté de ce dernier.

Seul le Loueur peut décider d'un échange ou pas du TPE.

Dans le cas où la remise en service s'avère impossible par téléphone, pour des raisons non imputables au Client, l'ATT peut décider de déclencher l'échange du TPE défectueux par un TPE comparable (technologie, logiciels,...), aux conditions de remplacement et de livraison suivant l'offre souscrite sur le Portail Payplug.

Le Client doit débrancher l'équipement défectueux, le remettre dans son carton d'origine, le placer dans un lieu sûr et le tenir en bon état à la disposition du livreur qui viendra lui apporter le TPE de remplacement. Il est rappelé au Client que l'échange standard concerne le terminal, les câbles et accessoires (pinpad, la base, ...) associés, sauf, le câble de connexion avec le modem-routeur du FAI, pour les TPE IP. L'échange du TPE GPRS implique également l'échange de la carte SIM contenue dans l'équipement, qui n'a pas à être manipulée par le Client lors de cette opération.

Au jour de la livraison, le transporteur désigné par le Loueur fait signer au Client un récépissé de livraison. Si le Client constate, à la livraison, une non-conformité du TPE livré, il peut refuser la livraison. Dans cette hypothèse, le Loueur livrera au Client un nouvel équipement conforme, et fera ses meilleurs efforts afin que la livraison ait lieu dans les meilleurs délais et dès notification de ce refus de livraison par le transporteur.

Dans le cas où le Client a souscrit à l'option de maintenance sur site dans son offre sur le Portail Payplug, un technicien mandaté par le Loueur débranchera le TPE et procédera à l'installation du nouvel équipement. Lors de cette intervention, il est possible que le TPE puisse être remis en service par le technicien, et que l'échange du matériel ne soit plus nécessaire.





Le Client s'engage à ce que lui-même ou l'un de ses représentants dûment habilités soit présent pour réceptionner l'équipement de remplacement, ou accueillir le technicien, à la date et à l'heure convenues avec l'ATT par téléphone.

À l'issue de l'opération de remplacement du TPE, le technicien demandera au Client ou à son représentant, mandaté à cet effet, de signer un PV d'intervention. Si le Client constate une non-conformité du fonctionnement du TPE, il peut le mentionner sur le PV d'intervention. Dans cette hypothèse, le Loueur devra dans les meilleurs délais et dès notification de ces réserves, corriger les points de non-conformité évoqués. En l'absence de réserves, le TPE est réputé fonctionner de façon conforme.

### **3.3 Maintenance évolutive des logiciels associés aux TPE**

La maintenance évolutive des TPE consiste en la fourniture au Client des mises à jour des versions logicielles, qu'elles soient demandées par le constructeur du TPE, ou requises par la réglementation applicable. Si la taille mémoire disponible sur le TPE est insuffisante pour effectuer la maintenance évolutive ou si celle-ci n'est pas possible techniquement, le Client devra résilier le présent Contrat de Location de TPE afin de souscrire à un nouveau contrat de location dont le matériel respecte la réglementation en vigueur.

Dans ce cas, aucuns frais associés à la rupture anticipée du présent Contrat de Location de TPE ainsi qu'aux frais de dossier du nouveau contrat de location ne seront facturés au Client.

Les tarifs du nouvel équipement sont ceux en vigueur à la date de la résiliation.

### **3.4 Télécommunications**

#### **3.4.1 Pour les TPE IP**

Les coûts des opérations de traitement et de transport/routage réalisées par l'opérateur du Service Monétique IP sont inclus dans le service proposé par le Loueur au Client.

Le service Monétique IP ne couvre pas l'ensemble des télécommunications nécessaires au bon fonctionnement des échanges entre le TPE IP et les serveurs bancaires ou privés : le Client doit disposer d'un accès haut-débit à Internet pour transporter les données entre le TPE IP et le point d'accès au Service Monétique IP, pour effectuer les téléchargements nécessaires à la maintenance évolutive (Cf. §3.3) et, au besoin, transporter les données nécessaires aux échanges entre les logiciels privés exploités par le Loueur et les serveurs adéquats

Le Client pourra contracter auprès du Fournisseur d'Accès Internet (FAI) de son choix pour disposer d'un accès Wifi et/ou haut-débit à Internet. Le choix du FAI est du seul ressort du Client. Celui-ci peut changer à sa convenance de FAI, à condition d'en informer le Loueur. Aucun service spécifique du type « option monétique » ou « passerelle monétique » n'est à souscrire auprès du FAI du Client : seul est nécessaire le service de base soit, l'accès à un routeur Wifi et/ou à Internet haut-débit. La tarification de ce service d'accès haut-débit à Internet est du ressort du FAI et à la charge du Client.

Description du mode secours RTC :



En cas d'indisponibilité des services offerts par le FAI du Client, c'est-à-dire en cas de non-fonctionnement de la connexion haut-débit à Internet, le TPE IP tentera d'effectuer ses télécommunications sur le réseau téléphonique commuté (ligne analogique), si le Client dispose d'une telle connexion opérationnelle, c'est-à-dire en l'absence de dégroupage total de la ligne téléphonique du Client, si le TPE IP est correctement raccordé à la ligne analogique et si le réseau téléphonique commuté (ligne analogique) est disponible lorsque le TPE IP tente d'effectuer sa connexion.

Le coût des télécommunications effectuées en mode « secours », c'est à dire des télécommunications effectuées sur le réseau téléphonique commuté (ligne analogique) pour pallier l'indisponibilité des services procurés par le FAI du Client, est à la charge du Client.

Description du mode secours GPRS (Back up GPRS) :

Si le Client a souscrit à l'option Back-Up GPRS, (en cas d'indisponibilité de la connexion haut-débit à Internet), le TPE IP basculera automatiquement sur le réseau mobile (GPRS) afin d'assurer la continuité du service.

Le Loueur contactera le Client lors de chaque déclenchement de ce mode de secours afin d'en connaître les raisons.

Le réseau mobile (GPRS) devant uniquement être utilisé en cas de défaillance de la connexion au réseau haut-débit Internet, le Loueur se réserve le droit de résilier de plein droit le Contrat de Location de TPE, en respectant un délai de préavis de 5 jours calendaires, s'il constate que l'utilisation du réseau mobile par le Client est contraire aux stipulations ci-dessus.

#### 3.4.2 Pour les TPE GPRS

Le Loueur remet au Client, à titre de prêt à usage, une carte SIM permettant l'utilisation :

- d'un abonnement GPRS souscrit auprès d'un opérateur de télécommunications,
- d'un réseau de transport de flux électronique souscrit auprès d'un opérateur de transport de données.

Les coûts des télécommunications réalisées par l'intermédiaire de l'opérateur mobile au titre de l'usage de l'abonnement

GPRS monétique sont inclus dans le service proposé par le Loueur au Client.

Le choix de l'opérateur de télécommunications et de l'opérateur de transport de données est du seul ressort du Loueur.

Le Loueur se réserve le droit de changer d'opérateur à sa convenance. Période de test

Considérant l'incertitude existant a priori sur la fourniture d'un service GPRS adapté aux besoins spécifiques du Client, le Loueur assure au Client une période dite « de test », de quinze (15) jours à dater de la livraison de l'équipement, afin d'évaluer la bonne réussite des opérations quotidiennes réalisées avec l'équipement.

Pendant cette période de test, le Client bénéficie de la possibilité de résilier ce Contrat de Location de TPE : le Loueur s'engage, dans ce cas, à rembourser au Client l'ensemble des sommes versées au titre de la souscription de TPE GPRS. Les seuls frais à la charge du Client sont ceux de la restitution de l'équipement au Loueur,

restitution devant être effective dans les cinq (5) jours suivant la résiliation sous peine de ne plus bénéficier des avantages cités et de voir la résiliation considérée comme une résiliation anticipée de contrat, telle que prévue à l'article 11.2 du Contrat de Location de TPE. Couverture de l'abonnement monétique GPRS

Le fonctionnement de l'abonnement monétique GPRS n'est possible que dans la zone géographique de couverture propre à l'opérateur de télécommunications. L'abonnement GPRS fonctionne sur les pays autorisés par Payplug.

Le bon fonctionnement des logiciels associés au TPE GPRS et, tout particulièrement du logiciel de paiement Carte Bancaire est lié à la possibilité d'établir une communication GPRS sur les lieux et au moment où le Client en éprouve la nécessité. Ce bon fonctionnement dépend donc de la disponibilité géographique et fonctionnelle des équipements de l'opérateur de télécommunications.

Cette disponibilité est tributaire de nombreux critères tels que la distance géographique du plus proche équipement de l'opérateur, la configuration physique du lieu où se trouve le Client, le relief aux alentours, les perturbations et parasitages en radiofréquences de la zone, la proximité éventuelle de systèmes de brouillage des télécommunications mobiles et le nombre de tentatives simultanées d'accès aux équipements de l'opérateur de télécommunications. Ces conditions étant indépendantes de la volonté des parties, le Loueur ne peut en aucun cas et en aucune façon garantir au Client la bonne exécution de toutes les opérations réalisées avec l'équipement.

#### 3.4.3 Pour les TPE RTC

Le coût des télécommunications effectuées sur le réseau téléphonique commuté (ligne analogique) est à la charge du Client.

### **ARTICLE 4 – OBLIGATIONS DU LOUEUR**

Le Loueur s'engage à assurer ou faire assurer par les sous-traitants de son choix, agissant pour son compte et sous sa responsabilité, les prestations énoncées au sein de l'article 3 des présentes.

### **ARTICLE 5 – OBLIGATIONS DU CLIENT**

Le Client accepte sans réserve et sans restriction l'ensemble des clauses du présent Contrat de Location de TPE et s'engage plus particulièrement à respecter les obligations mises à sa charge à l'article 3 des présentes.

#### **5.1 Utilisation de l'équipement**

Le Client s'engage à utiliser l'équipement dans des conditions normales et conformes à la destination prévue. Le Client s'engage à utiliser l'équipement conformément aux spécifications techniques telles que définies dans le guide d'utilisation remis lors de la livraison de l'équipement : caractéristiques du réseau d'alimentation, du support de transmission, température... Le Client ne peut en aucun cas apporter de modification à l'équipement pour les TPE IP au câblage entre l'équipement et le modem-routeur de son FAI et aux logiciels associés. En aucun cas, l'équipement mis à disposition ne subira, sans accord du Loueur, d'intervention ou de modification en vue de le rendre compatible avec d'autres matériels et logiciels utilisés chez le Client.

Le Client garantit en général le Loueur contre toute conséquence qui résulterait d'une action ou d'une réclamation exercée à l'encontre du Loueur qui serait la conséquence d'une utilisation du TPE non conforme aux spécifications techniques telles que définies dans le guide d'utilisation.

La garantie porte notamment sur tous dommages et intérêts et/ou amendes pénales auxquels serait condamné le Loueur et s'étend aux frais de justice éventuels, y compris les frais irrépétibles et les frais d'avocats.

## **5.2 Modification de la situation du Client**

Le Client s'engage à informer le Loueur de toute modification de sa situation pouvant avoir un effet sur le présent Contrat de Location de TPE et en particulier : changement de raison sociale, changement d'adresse professionnelle...

Si les modifications de la situation du Client nécessitent une intervention du Loueur pour adapter la configuration du TPE, cette intervention sera facturée au Client (Cf. article 6).

## **5.3 Moyens de télécommunications**

### **5.3.1 TPE IP - Utilisation du réseau ADSL**

La prestation d'installation ne comprend ni mise en conformité ni adaptation des installations électrique, téléphonique et réseau du point de vente du Client. Le Client s'engage à installer à proximité immédiate de l'emplacement d'exploitation du TPE IP, une prise d'alimentation électrique, le modem-routeur permettant d'accéder au réseau de son FAI et une prise de connexion au réseau téléphonique commuté. À défaut, le Client prendra à sa charge les travaux nécessaires qu'il fera exécuter par le prestataire de son choix. Les travaux doivent être exécutés préalablement à l'installation du TPE IP.

De plus, Le Client s'engage :

- à tenir informé le Loueur de tout changement relatif au FAI,
- à tenir informé le Loueur de toute modification effectuée sur son réseau IP, - sauf accord écrit préalable du Loueur, à ne pas procéder lui-même ou à ne pas faire procéder par un tiers non expressément habilité par le Loueur, tout type de travaux sur l'équipement du Contrat de Location de TPE.

Si le Client souhaite faire évoluer la configuration de son réseau IP et que cela nécessite par la suite une intervention du Loueur pour adapter la configuration du TPE IP ou si le Client modifie la configuration de son réseau IP et que cela provoque un dysfonctionnement du TPE IP nécessitant une intervention du Loueur pour corriger le dysfonctionnement, ces interventions seront facturées au Client (Cf. article 6).

Il est rappelé au Client que le maintien en bonne condition opérationnelle de la connexion Wifi et/ou Internet haut-débit à laquelle est raccordé le TPE IP ou le TPE IP Mobile Wifi est intégralement de son ressort. Il appartient au Client de vérifier régulièrement ce bon fonctionnement. À défaut, si le mode secours de son TPE IP fonctionne correctement et qu'il effectue par ce moyen de nombreuses transactions, le montant des échanges effectués sur le réseau téléphonique commuté, facturé par l'opérateur correspondant, peut devenir conséquent et restera intégralement à la charge du Client.

### **5.3.2 TPE GPRS - Utilisation de la carte SIM.**

Le Client, en sa qualité de gardien de la carte SIM, est seul responsable de l'utilisation conforme de celle-ci à son usage, tel qu'il est prévu au sein du présent Contrat de Location de TPE, et de la conservation de celle-ci.

La carte SIM est configurée pour interdire la réception d'appel, les services voix, l'itinérance avec certains des opérateurs mobiles étrangers, les SMS et le GSM Data.

Dans le cas où la carte SIM disposerait d'un pin code (code secret) permettant d'en protéger l'utilisation, le Client

ne devra en aucun cas le modifier.

En outre, la carte SIM ne peut être utilisée par le Client que sur le TPE GPRS mis à sa disposition dans le cadre de l'exécution du Contrat de Location de TPE.

### 5.3.3 Utilisation du service monétique IP et GPRS

Le Client ne peut utiliser le service Monétique IP ou abonnement GPRS Monétique mis à sa disposition par le Loueur, dans le cadre du présent Contrat de Location de TPE, que pour permettre le bon fonctionnement des logiciels associés au TPE IP ou GPRS. Le Client ne peut en aucun cas céder, louer, prêter ou utiliser, pour son compte ou pour le compte de tiers, ce service Monétique IP ou GPRS pour permettre le fonctionnement :

- d'autres appareils que le TPE IP / GPRS fourni par le Loueur,
- d'autres logiciels que ceux installés par le Loueur sur le TPE IP ou GPRS, - du logiciel Cartes Bancaires installé sur le TPE IP ou GPRS dans un cadre contractuel différent de celui négocié avec le Loueur au sein des présentes.

Dans les situations énumérées ci-dessus :

- le Loueur ne s'engage en aucun cas au bon fonctionnement de l'équipement et du service Monétique IP ou abonnement GPRS Monétique,
- le Loueur se réserve le droit de mettre en œuvre tout moyen technique de son choix lui permettant

d'empêcher le bon fonctionnement du service Monétique IP ou abonnement GPRS Monétique.

Le Loueur se réserve enfin le droit de résilier le présent contrat de location pour faute du Client, et d'appliquer les éventuelles pénalités telles que définies à l'article 11.

### 5.4 Paiement

Le Client s'engage à payer le prix des prestations tel que fixé à l'article 11.

## ARTICLE 6 – PRESTATIONS NON COMPRIS DANS LE CONTRAT

Les interventions du Loueur ou de toute personne habilitée par ce dernier, requises du fait du non-respect par le Client des dispositions de l'article 5 donneront lieu à facturation en sus des prestations. De même, toute autre prestation demandée par le Client mais n'entrant pas dans le périmètre des prestations, telles qu'énumérées à l'article 3 des présentes, notamment la fourniture de batterie de rechange ou de cordons supplémentaires, donnera lieu à facturation en sus des prestations.

Pour les TPE GPRS uniquement : le montant des communications GPRS effectuées à l'aide du TPE GPRS en contravention des dispositions de l'article 5.3.2 donneront lieu à facturation séparée, en supplément des prestations. Dans une telle hypothèse, le Loueur se réserve le droit de mettre en œuvre tout moyen technique de son choix lui permettant d'empêcher le fonctionnement de l'abonnement GPRS monétique.

Pour le TPE IP Mobile Wifi : la fourniture d'un routeur Wifi (exemple : box Internet ou Smartphone) est à la seule charge du Client.

## ARTICLE 7 – GARANTIE

### 7.1 Garantie sur l'équipement

Durant toute la durée du Contrat de Location de TPE, tout équipement défectueux sera, au choix du Loueur, remplacé ou réparé suivant l'offre souscrite dans le portail Payplug par le Loueur.

Toutefois, sont exclus de la garantie, toute réparation ou tout remplacement de l'équipement ayant pour origine :

- le non-respect des spécifications fournies par le Loueur concernant le fonctionnement des équipements, les prescriptions d'installation et/ou d'utilisation, telles qu'explicitées aux articles 3 et 5 des présentes, - les pannes ou dysfonctionnements dus à une cause extérieure à l'équipement (foudre, incendie, choc, chutes, dégâts des eaux et liquides divers...), - les pannes ou dysfonctionnements dus à une utilisation anormale de l'équipement,
- l'intervention d'un tiers sur l'équipement, non expressément habilité par le Loueur,
- les opérations de remise à niveau technique des équipements, autres que celles jugées nécessaires par le Loueur,
- les pannes ou dysfonctionnements dus à des modifications apportées à l'équipement sans accord préalable du Loueur,
- les pannes ou dysfonctionnements dus à un défaut d'entretien courant.

Dans les cas énumérés ci-dessus, l'équipement sera, au choix du Loueur, remplacé et/ou réparé et facturé au Client en sus des prestations.

La durée de la garantie des batteries des équipements mobiles est limitée dans le temps à six (6) mois. Ces batteries ne se réparent pas, mais peuvent être remplacées par des batteries neuves : pendant toute la durée du Contrat de Location de TPE, le Client peut contacter le Loueur pour commander des batteries neuves qui seront facturées au Client.

### 7.2 Garantie sur les logiciels associés à l'équipement

Le Loueur déclare détenir directement ou via ses partenaires les droits nécessaires à la concession au Client, de droits d'utilisation non exclusifs des logiciels associés. Le Loueur garantit le Client contre tout risque d'éviction, sur les pays autorisés par Payplug, dès lors qu'il utilise lui-même les équipements conformément à leur destination, et qu'il n'a pas tenté de les modifier ou de les faire modifier par un tiers. Si le Client venait à être inquiété de ce chef, il en aviserait immédiatement le Loueur qui devrait prendre immédiatement les mesures propres à faire cesser tout trouble dans la jouissance et prendrait seul à ses frais toute mesure de défense nécessaire.

## ARTICLE 8 – PROPRIETE

### 8.1 Propriété de l'équipement

Le Client ne dispose d'aucun droit de propriété sur l'équipement loué, le redressement ou la liquidation judiciaire du Client ne pouvant modifier la présente clause. Il ne peut le vendre, le céder, le prêter, le sous-louer, le nantir, le donner en gage, directement ou indirectement... sans autorisation expresse préalable et écrite du Loueur. Il ne peut en aucun cas l'utiliser à d'autres usages que ceux prévus par le Loueur au sein du présent Contrat de Location de TPE dans l'article 5.1.

Pour les TPE GPRS uniquement : la carte SIM remise au Client par le Loueur reste la propriété insaisissable, inaliénable et incessible de l'opérateur de télécommunications choisi par le Loueur pour la fourniture des prestations. Le Client s'interdit en conséquence de concéder sur la carte SIM un quelconque droit et s'engage à la restituer à l'issue du présent Contrat de Location de TPE.

## 8.2 Propriété intellectuelle

Le Loueur concède au Client, pendant toute la durée du présent Contrat de Location de TPE, une licence d'utilisation des logiciels associés au TPE. Les logiciels associés au TPE sont ceux nécessaires à son fonctionnement (partie système) et ceux listés dans les conditions particulières du présent Contrat de Location de TPE. Cette licence comprend les droits :

- d'utiliser les logiciels associés au TPE pour le fonctionnement du TPE, dans le strict cadre contractuel défini aux présentes. Le Client n'est pas autorisé à sous-licencier les logiciels associés ou à les utiliser à d'autres fins que celles prévues dans le cadre du présent Contrat de Location de TPE, ni à les utiliser pour la formation de tiers.
- d'utiliser la documentation fournie avec les logiciels associés aux fins indiquées ci-dessus.

Le Client n'acquiert aucun droit de propriété sur les logiciels associés au TPE ni sur la documentation fournie. Le Client s'engage à ne pas effectuer ou permettre le désassemblage, la décompilation ou l'ingénierie à rebours des logiciels associés au TPE. Le Client s'engage à n'effectuer aucune copie des logiciels.

## ARTICLE 9 – RESPONSABILITE ET ASSURANCE

### 9.1 Exclusion de responsabilité du Loueur

Le Loueur décline toute responsabilité en cas de mauvais fonctionnement de l'équipement causé par une utilisation non conforme de celui-ci par le Client.

Il est rappelé au Client que les obligations du Loueur portent sur la mise à disposition d'un moyen d'encaissement, non sur les conséquences de son absence.

Dans tous les cas, il est rappelé que le Loueur n'est tenu qu'à une obligation générale de moyens.

En aucun cas la responsabilité du Loueur ne pourra être recherchée, quel que soit le type d'action intentée, pour un dommage indirect, qu'il soit matériel ou immatériel, et notamment pour tout manque à gagner, trouble commercial, perte de données, de clientèle, d'exploitation, de chances, de bénéfice ou actions intentées par un tiers contre le Client ainsi que leurs conséquences, lié au présent Contrat de Location de TPE ou à son exécution.

Seuls sont indemnisables, dans le cadre du présent Contrat de Location de TPE, les dommages matériels et financiers directs.

Le Loueur ne pourra être tenu responsable que des dommages et intérêts directs résultant d'une faute prouvée. Dans ce cas, le montant maximum de sa responsabilité ne pourra excéder le montant annuel de la prestation due au titre du présent Contrat de Location de TPE.

Si le Client subissait un risque financier occasionné par l'absence d'un moyen d'encaissement opérationnel, il lui incomberait de prendre toutes les mesures nécessaires afin de se prémunir face à cette situation, notamment en disposant de multiples équipements usant de moyens de télécommunications réellement indépendants. Il appartient au Client de se faire aider de spécialistes des télécommunications si nécessaire.

Pour les TPE IP uniquement :

Le TPE IP est doté d'un mode secours, pour le bon fonctionnement duquel il est nécessaire de connecter l'équipement à une ligne téléphonique analogique (réseau téléphonique commuté) en sus de la connexion assurée par le câble avec le modem-routeur du FAI. Le Loueur ne pourra en aucun cas être tenu pour responsable et ce pour quelque cause que ce soit en cas de connexion du mode secours de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune surfacturation du prix des communications par les opérateurs.

Il est rappelé au Client que le mode de secours, l'usage par le TPE IP des télécommunications par le réseau



téléphonique commuté en lieu et place d'Internet, est destiné à améliorer la disponibilité globale du service d'encaissement et non pas à apporter une garantie de connexion au serveur bancaire. Selon la configuration des télécommunications du Client, un même et unique événement peut rendre indisponible les deux modes de télécommunications, IP et analogique. C'est notamment le cas avec un TPE IP connecté en ADSL et en analogique sur une même ligne téléphonique en dégroupage partiel, car les échanges Internet et téléphoniques (en mode secours) utilisent alors le même support physique, à savoir le câble de cuivre de la ligne téléphonique : une rupture de ce support rendrait inopérant simultanément les deux modes de télécommunications.

La responsabilité du Loueur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client et tels qu'explicités à l'article 7.1 du Contrat de Location de TPE.

De même, la responsabilité du Loueur ne peut pas être engagée :

- en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des indisponibilités pour les équipements radio,
- en cas de difficultés liées à l'indisponibilité du service fourni par le FAI du Client,
- en cas d'intervention technique effectuée par une personne non habilitée par le Loueur,
- en cas de mauvaise utilisation par le Client du service Monétique IP, ou d'utilisation non conforme à sa destination telle que prévue aux présentes conditions générales,
- en cas de Force Majeure telle que définie dans l'article 12 du Contrat de Location de TPE.

Pour le TPE IP Mobile Wifi, la responsabilité du Loueur ne peut pas être engagée :

- en cas de rupture de connexion entre le TPE et le routeur Wifi,
- en cas de rupture de réseau entre le routeur Wifi et le réseau acheminant les données vers les serveurs bancaires ou privés pour le TPE IP Mobile Wifi.

Pour les TPE GPRS uniquement :

En ce qui concerne les modèles de TPE GPRS disposant également d'une connexion RTC, le Loueur ne pourra en aucun cas être tenu pour responsable pour quelque cause que ce soit en cas de connexion de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune facturation du prix des communications par les opérateurs.

Le Loueur décline toute responsabilité en cas de mauvais fonctionnement de l'équipement et de l'abonnement GPRS monétique, causé par une utilisation non conforme de ceux-ci par le Client. La responsabilité du Loueur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client et tels qu'explicités à l'article 7.1 du Contrat de Location de TPE.

De même, la responsabilité du Loueur ne peut pas être engagée :

- en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des indisponibilités pour les équipements radio, - en cas de difficultés liées aux lieux et aux conditions de réception (absence de couverture GPRS, voir articles 3.4.2 et 5.3.3 du Contrat de Location de TPE),
- en cas d'intervention technique effectuée par une personne non habilitée par le Loueur,
- en cas de mauvaise utilisation par le Client du service GPRS Monétique, notamment de la carte SIM, ou d'utilisation non conforme à sa destination telle que prévue aux présentes conditions générales,
- en cas de Force Majeure telle que définie dans l'article 12 du Contrat de Location de TPE.

Pour les TPE RTC uniquement :

Le Loueur ne pourra en aucun cas être tenu pour responsable pour quelque cause que ce soit en cas de connexion de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune surfacturation du prix des communications par les opérateurs.

La responsabilité du Loueur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client et tels qu'explicités à l'article 7.1 du Contrat de Location de TPE.

De même, la responsabilité du Loueur ne peut pas être engagée :

en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des indisponibilités pour les équipements radio, - en cas d'intervention technique effectuée par une personne non habilitée par le Loueur,

- en cas de Force Majeure telle que définie dans l'article 12 du Contrat de Location de TPE.

## **9.2 Responsabilité du Client**

Le Client est responsable des risques de perte et de détérioration totale ou partielle du TPE, du câble de connexion avec le modem-routeur du FAI pour le TPE IP, de la carte SIM pour le TPE GPRS et des logiciels associés. Pendant toute la durée du présent Contrat de Location de TPE, le Client veillera à la conservation de l'équipement dont il assumera la garde à ses risques et périls. En conséquence, il est et demeure responsable de tous les dommages causés par cet équipement, comme de tous les risques de détérioration et de perte, de destruction totale ou partielle de l'équipement, quelle que soit la cause du dommage (incendie, vol, etc..).

## **9.3 Assurance**

Le Client s'engage à souscrire dès la signature du présent Contrat de Location de TPE, toute assurance nécessaire à la couverture du risque lié à ses obligations de garde et de conservation de l'équipement loué, à payer les primes de manière régulière, à maintenir ladite assurance pendant toute la durée du Contrat de Location de TPE et à présenter tous les justificatifs sur simple demande du Loueur.

## **ARTICLE 10 – DUREE DU CONTRAT - RENOUELEMENT ET FIN DE CONTRAT**

Le présent Contrat de Location de TPE est conclu pour une durée de vingt-quatre (24) mois, qui court à compter de la date de livraison de l'équipement. Il est renouvelable par tacite reconduction, par périodes successives d'un (1) an, sauf dénonciation par l'une ou l'autre des parties réalisées en respectant la procédure suivante :

- Trois (3) mois avant la date d'échéance contractuelle, le Client doit envoyer une lettre recommandée avec demande d'avis de réception à l'adresse suivante : Payplug - 110 avenue de France, 75013 Paris.
- Trois (3) mois avant la date d'échéance contractuelle, le Loueur doit envoyer une lettre avec demande d'avis

de réception à l'adresse indiqué par le Client sur son espace Payplug.

- La restitution devra être réalisée par la remise de l'équipement, les câbles et accessoires, le câble de connexion au modem-routeur du FAI pour le TPE IP, la carte SIM pour le TPE GPRS ainsi que les logiciels associés et la documentation qui lui a été fournie, par le Client au Loueur dans un délai de quinze (15) jours ouvrés à compter de la date de fin du Contrat de Location de TPE, entre les mains du Loueur, les frais de transport sécurisé, ainsi que la preuve d'envoi, étant à la charge du Client. Le bordereau de clôture du Contrat de Location de TPE dûment complété et signé par les deux parties devra être joint au colis par le Client.

Si la résiliation intervient à la suite d'un changement de matériel, se référer à l'article 11.3.

À défaut de restitution ou en cas de non-respect des modalités de celle-ci par le Client, les conditions prévues à l'article 11 seront appliquées. Il est rappelé en sus que la non-restitution du matériel constitue le délit pénal d'abus de confiance, le Loueur conservant la faculté d'exercer toute voie de droit.

Le Client garantit le Loueur contre toute conséquence qui résulterait d'une action ou d'une réclamation exercée à l'encontre du Loueur en raison de l'utilisation des équipements et logiciels associés après le terme du Contrat de Location de TPE. La garantie porte notamment sur tous dommages et intérêts et/ou amendes pénales auxquels serait condamné le Loueur et s'étend aux frais de justice éventuels, y compris les frais irrépétibles et les frais d'avocats.

## **ARTICLE 11 – TARIFS ET REVISION - PENALITES – CHANGEMENT DE MATÉRIEL - MODALITES DE REGLEMENT**

### **11.1 Tarifs révisions tarifaires**

Les tarifs appliqués sont ceux figurant sur le Portail Payplug. Le loyer est établi par le Loueur.

### **11.2 Pénalités**

11.2.1 Si l'équipement se trouve hors d'usage ou non couvert par la Garantie (voir article 7) à la suite d'un échange standard, le Loueur pourra facturer au Client une indemnité calculée au prorata de la durée du Contrat de Location de TPE déjà écoulee depuis sa livraison du TPE ou de son renouvellement :

Pour tous les modèles de TPE :

- 350 € HT durant la 1ère année de location
- 250 € HT durant la 2ème année de location
- 90 € HT durant la 3ème année de location
- 30 € HT durant la 4ème année de location et au-delà, le cas échéant.

11.2.2 Si l'équipement n'est pas restitué ou restitué dans un état incomplet ou dégradé par le Client à la fin du Contrat de Location de TPE, telle qu'explicitée à l'article 10, le Loueur ou toute autre entité qui serait mandatée par celui-ci pourra facturer au Client une indemnité calculée au prorata de la durée du Contrat de Location de TPE déjà écoulé depuis la livraison du TPE ou de son renouvellement :

Pour tous les modèles de TPE :

- 350 € HT durant la 1ère année de location
- 250 € HT durant la 2ème année de location
- 90 € HT durant la 3ème année de location
- 30 € HT durant la 4ème année de location et au-delà, le cas échéant.

Le paiement de cette indemnité ne vaudra pas transfert de propriété de l'équipement, le Client devant dans tous les cas restituer celui-ci dans les conditions prévues à l'article 10. En conséquence de la fin du Contrat de Location de TPE, le Client ne bénéficie plus du droit d'usage des licences logicielles, ni de la documentation associée, ni du service Monétique IP pour les TPE IP, ni du service Monétique GPRS pour les TPE GPRS. De même, le Client ne bénéficie plus des services de maintenance et d'Assistance Technique Téléphonique.

11.2.3 En cas de résiliation anticipée du Contrat de Location de TPE par le Client ou en cas de non-respect du préavis prévu à l'article 10, le Client est tenu de verser au Loueur une indemnité Hors Taxes calculée au prorata de la durée écoulee depuis la livraison du TPE. Voir tarifs ci-dessous :

|                                      | Location de 48 mois | Location de 24 mois |     | Location 12 mois |     |
|--------------------------------------|---------------------|---------------------|-----|------------------|-----|
|                                      | IP / GPRS           | IP / GPRS           | RTC | IP / GPRS        | RTC |
| 1 <sup>ère</sup> année               | 690                 | 480                 | 280 | 200              | 110 |
| 2 <sup>ème</sup> année               | 580                 | 210                 | 90  |                  |     |
| 3 <sup>ème</sup> année               | 270                 |                     |     |                  |     |
| 4 <sup>ème</sup> année               | 120                 |                     |     |                  |     |
| Au-delà de la 4 <sup>ème</sup> année |                     |                     |     |                  |     |

En cas de résiliation du Contrat de Location de TPE avant l'échéance par l'une ou l'autre des parties, le Client est tenu de retourner au Loueur l'équipement, les accessoires et câbles, le câble de connexion au modem-routeur du FAI pour les TPE IP, la carte SIM pour les TPE GPRS, les logiciels associés et la documentation qui lui a été fournie, suivant la procédure décrite à l'article 10. Le montant des prestations (ci-après désigné le « loyer ») sera prélevé jusqu'à réception de l'équipement par le Loueur, et en tout état de cause, au plus tard jusqu'à l'échéance du Contrat de Location de TPE.

Il est entendu entre les parties que les pénalités mentionnées ci-dessus peuvent se cumuler le cas échéant.

### 11.3 Changement de matériel

Si le Client souhaite changer de matériel au cours de l'exécution de son Contrat de Location de TPE, le Client, après avoir obtenu l'accord du Loueur, devra résilier le présent Contrat de Location de TPE et souscrire à un nouveau contrat de location. Dans ce cas, le Client se verra exonéré des indemnités de rupture anticipée prévues à l'article 11.2.3 ci-dessus.

Le Client s'engage alors à restituer son ancien matériel au Loueur dans un délai de quinze (15) jours ouvrés à compter de la date de résiliation du Contrat de Location de TPE, l'équipement, les câbles et accessoires, le câble de connexion au modem-routeur du FAI pour le TPE IP, la carte SIM pour le TPE GPRS ainsi que les logiciels associés et la documentation qui lui a été fournie. Les frais de transport sont pris en charge par le Loueur via un bon de retour pré-affranchi. Si l'installation du nouveau matériel est réalisée par un technicien sur site, ce dernier se chargera de la reprise de l'ancien équipement. Le bordereau de clôture du Contrat de Location de TPE dûment complété et signé par les deux parties devra être joint au colis par le Client.

Cette prestation est facturée au Client dans les conditions suivant l'offre souscrite sur le Portail Payplug.

#### **11.4 Modalités de paiement des loyers et frais de dossier**

Le paiement des loyers est opéré par prélèvements mensuels (terme à échoir) sur le compte Payplug selon les CGV en vigueur, à partir du mois qui suit celui de la livraison de l'équipement. Le mois au cours duquel l'équipement a été livré fait l'objet de facturation prorata temporis ; le mois au cours duquel l'équipement est restitué au Loueur est facturé en intégralité.

Les frais de dossier, les frais d'installation et les frais relatifs aux options logicielles associées ou consommables (cordons, batterie, carte de domiciliation, etc...), demandées lors de la signature du Contrat de Location de TPE sont prélevés en une seule fois au début du mois suivant la date de livraison.

Les frais relatifs aux options logicielles ou à un déplacement technicien pour une installation sur site, demandés en cours de réalisation du Contrat de Location de TPE (logiciels associés, déplacement sur site, consommables, non demandés initialement par le Client) seront prélevés en sus du loyer sur la base des tarifs en vigueur.

En cas d'impossibilité de procéder aux prélèvements (fermeture du compte par exemple), le Client devra payer par chèque ou tout autre moyen mis à disposition par Payplug en une seule fois la totalité des loyers restant à couvrir jusqu'à l'échéance du Contrat de Location de TPE. À défaut de paiement par le Client, à la suite d'une relance valant mise en demeure de payer, envoyée par courrier recommandé avec demande d'avis de réception restée sans effet pendant quinze (15) jours, le Loueur se réserve le droit d'engager toute action destinée à recouvrer les sommes. Dans le cas où le Loueur intenterait toute action en justice contre le Client pour défaut de paiement, le Loueur se réserve le droit de suspendre le service Monétique IP du Client sans préavis particulier.

#### **ARTICLE 12 – FORCE MAJEURE**

Les cas de force majeure suspendent les obligations du présent Contrat de Location de TPE. S'ils ont une durée d'existence supérieure à deux (2) mois, le présent Contrat de Location de TPE pourra être résilié par l'une ou l'autre des parties, sans que cette résiliation puisse donner droit à l'allocation de dommages et intérêts. De façon expresse, sont considérés comme cas de force majeure, outre ceux habituellement retenus par la jurisprudence des Cours et Tribunaux français : guerre, grève générale, émeute, catastrophe naturelle, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit.

Dans le cas de la survenance d'un événement relevant de ces cas, les Parties ont une obligation réciproque d'information afin de définir, de concert, des solutions de remplacement. La partie défaillante fera ses meilleurs efforts pour limiter et/ou éviter les effets du cas de force majeure, et trouver toute solution adaptée afin de reprendre l'exécution de ses obligations dans les meilleurs délais.

#### **ARTICLE 13 – RESILIATION**

En cas de résiliation du Contrat de Location de TPE, le Client est tenu de restituer au Loueur l'équipement, les câbles et accessoires, le câble de connexion avec le modem-routeur du FAI pour les TPE IP, la carte SIM pour les TPE GPRS, les logiciels associés et la documentation qui lui a été fournie, selon la procédure décrite à l'article 10. Le Contrat de Location de TPE pourra être résilié immédiatement de plein droit et sans autre formalité que celle énoncée ci-dessous, sauf application des dispositions de l'article 12, dans les cas suivants :

- à l'initiative de l'une ou l'autre partie, en cas de non-respect de ses obligations par l'une ou l'autre des parties.
- à l'initiative du Loueur, en cas de décès du Client, cessation d'activité, cession du fonds de commerce.

En cas de résiliation du Contrat de Location de TPE du fait du manquement du Client à l'une de ses obligations au Contrat de Location de TPE, les pénalités prévues à l'article 11 s'appliqueront, sans que ces pénalités puissent être qualifiées de libératoires. Par ailleurs, les autres dispositions de l'article 11, relatives à la restitution des équipements, câbles et accessoires, câble de connexion au modem-routeur du FAI pour les TPE IP, carte SIM pour les TPE GPRS, logiciels et documentation associés ainsi que les stipulations de l'article 10 s'appliqueront. En cas de résiliation du Contrat de Location de TPE pour manquement de l'une des parties à ses obligations, la partie invoquant le manquement de l'autre partie peut demander devant les tribunaux compétents réparation de son dommage, étant entendu qu'elle ne saurait

prétendre à une totale indemnisation supérieure au montant des sommes versées, au titre du présent Contrat de Location de TPE, dans l'année contractuelle de la survenance du dommage.

#### **ARTICLE 14 – CESSATION DU CONTRAT**

Le Loueur peut à tout moment vendre ou transférer le présent Contrat de Location de TPE à toute personne physique ou morale de son choix sans que cela ouvre au Client un droit à résiliation anticipée.

Le Client ne peut céder ou transférer les droits et/ou les obligations, résultant pour lui du présent Contrat de Location de TPE sans le consentement écrit et préalable du Loueur.

## ANNEXE 4 : CONDITIONS GÉNÉRALES AU CONTRAT DE VENTE DE TPE

### ARTICLE 1 – OBJET DU CONTRAT

Le présent contrat (ci-après désignée le « Contrat de Vente de TPE ») a pour objet de définir les conditions dans lesquelles Payplug (ci-après désignée « le Vendeur ») fournit au Client (ci-après « le Client »), qui l'accepte, les produits et services monétiques suivants (ci-après désignés « les prestations ») :

- un Terminal de Paiement Électronique (TPE) acceptant les cartes Contact et Sans Contact de technologie RTC, GPRS ou IP (ci-après « TPE » ou « équipement ») composé du terminal et de tous les câbles et accessoires (pinpad, ...) éventuellement associés, la technologie Sans Contact étant incluse dans le terminal ou dans l'un des accessoires associés (pinpad ou cible dédiée à la lecture Sans Contact), et/ou un Editeur Lecteur de Chèques,
- des logiciels associés au TPE et les licences d'utilisation de ces logiciels,
- la formation à l'utilisation du TPE à la demande du Client et via les supports fournis par Payplug à cet effet,
- une assistance technique et téléphonique (ci-après « ATT »),
- la maintenance du TPE, suivant l'offre souscrite dans le Portail Payplug,
- pour les TPE IP :

un câble de connexion entre l'équipement et le modem-routeur du Fournisseur d'Accès à Internet (ci-après «FAI»),  
un abonnement à un service Monétique IP souscrit auprès d'un Passerelliste sélectionné par le Vendeur,

- pour les TPE GPRS :

une carte SIM, installée dans l'équipement et nécessaire au fonctionnement de celui-ci, un abonnement GPRS monétique souscrit auprès d'un opérateur de télécommunications,

un réseau de transport de flux électronique souscrit auprès d'un opérateur de transport de données,

- pour les TPE IP, GPRS ou RTC, la livraison de l'équipement au Client par transporteur.

Sauf stipulation contraire prévue aux présentes Conditions Générales au Contrat de Vente de TPE, l'ensemble des termes comportant une majuscule conservent la signification qui leur a été donnée aux Conditions Générales de Vente et au Contrat d'Adhésion au système de paiement de proximité par carte « CB » ou « CB cartes soumises aux règles ».

La fourniture de ces prestations au Client a vocation de permettre à ce dernier d'effectuer les encaissements de ses clients dans les conditions définies ci-après.

### ARTICLE 2 – PREREQUIS A LA FOURNITURE DES PRESTATIONS AU CLIENT

Pour pouvoir bénéficier des prestations et signer le présent Contrat de Vente de TPE, le Client doit obligatoirement avoir souscrit au préalable un Contrat d'Adhésion au système de paiement de proximité par cartes « CB » ou cartes soumises aux règles « CB » (« Contrat d'Adhésion ») et doit exercer son activité commerciale dans les pays autorisés par Payplug.



Pour les TPE IP, le Client doit disposer d'un accès haut-débit à Internet opérationnel.

## **ARTICLE 3 – DESCRIPTION DES PRESTATIONS**

### **3.1 Livraison, installation et formation**

Le Client renseigne les informations techniques nécessaires lors de la souscription de son offre sur le Portail Payplug. Le transporteur sélectionné par le Vendeur livre l'équipement à l'adresse signifiée par le Client à Payplug.

À réception de l'Équipement, et en présence du transporteur, le Client est tenu d'effectuer les vérifications d'usage afin de constater que l'équipement est en bon état et ne présente pas de détériorations particulières avant de signer le bon de livraison qui lui sera présenté par le transporteur. En cas de défauts constatés, le Client devra émettre des réserves en les mentionnant sur ledit bon de livraison et en refusant de réceptionner l'équipement.

Le Client assure lui-même et sous sa seule responsabilité le branchement de l'équipement sur ses réseaux électriques et/ou réseau téléphonique commuté ou ADSL. Concernant le TPE IP Mobile Wifi, le Client devra appairer lui-même son TPE avec son routeur Wifi (par exemple box Internet ou smartphone) en entrant le mot de passe du routeur Wifi dans les paramètres de son équipement.

Les modalités de formations, d'installation et de support sont précisés sur le portail Payplug et suivant l'offre souscrite par le client.

### **3.2 Assistance Technique et Téléphonique (ATT) - maintenance corrective – intervention sur site**

Suivant l'offre souscrite sur le Portail Payplug, le Client dispose d'une Assistance Technique et Téléphonique, au numéro et aux horaires indiqués sur le Portail Payplug ou sur la page du support, ou numéro et aux horaires indiqués sur la lettre et le sticker accompagnant le TPE.

Le coût de la communication est, au jour de la signature du Contrat de Vente de TPE, indiqué sur le portail Payplug, auxquels s'ajoutent les coûts de communication/service facturés par l'opérateur téléphonique du Client depuis un poste mobile ou fixe.

L'ATT diagnostique, par téléphone suivant les indications données par le Client, la nature de l'incident et tente, lorsque cela est possible, de le régler par téléphone. Pour ce faire, le Client accepte de réaliser lui-même les différentes manipulations demandées par l'ATT par téléphone et destinées à diagnostiquer la panne et à assurer la remise en service rapide de l'équipement.

Certaines opérations de maintenance du TPE peuvent nécessiter des investigations techniques plus approfondies. Dans un tel cas, l'ATT du Vendeur met fin à la communication téléphonique, réalise de son côté ces investigations et recontacte le Client afin de l'informer de la procédure à suivre pour rétablir le bon fonctionnement du TPE.

Certaines opérations de maintenance du TPE peuvent nécessiter de le connecter au réseau téléphonique commuté (ligne analogique), pour les TPE GPRS et IP, si le modèle de ce dernier le permet, ou à Internet pour les TPE IP. Dans le cas d'une telle demande de l'ATT du Vendeur, le Client fait son affaire de réaliser lui-même une telle connexion afin de permettre la réalisation de l'opération à la date et à l'heure prévues par le Vendeur. Le coût des télécommunications effectuées sur le réseau téléphonique commuté est à la charge du Client.

Si le Client n'est pas en mesure de répondre à une demande du Vendeur concernant la connexion au réseau téléphonique commuté ou à Internet, la remise à niveau technique de l'équipement peut nécessiter de réaliser un échange, tel que décrit ci-dessous. L'échange pourra donner lieu, selon les conditions de l'offre souscrite dans le portail Payplug, à facturation séparée des prestations, après présentation d'un devis au Client expressément accepté de ce dernier.

Seul le Vendeur peut décider d'un échange ou pas du TPE et dans les conditions de l'offre souscrite par le Client dans le portail Payplug.

Dans le cas où la remise en service s'avère impossible par téléphone, pour des raisons non imputables au Client, l'ATT peut décider de déclencher l'échange du TPE défectueux par un TPE similaire (technologie, logiciels...) aux conditions de remplacement et de livraison suivant l'offre souscrite sur le Portail Payplug.

Le Client doit débrancher l'équipement défectueux, le remettre dans son carton d'origine, le placer dans un lieu sûr et le tenir en bon état à la disposition du livreur qui viendra lui apporter le TPE de remplacement. Il est rappelé au Client que l'échange standard concerne le terminal, les câbles et accessoires (pinpad, la base, ...) associés, sauf, le câble de connexion avec le modem-routeur du FAI, pour les TPE IP. L'échange du TPE GPRS implique également l'échange de la carte SIM contenue dans l'équipement, qui n'a pas à être manipulée par le Client lors de cette opération.

Au jour de la livraison, le transporteur désigné par le Vendeur fait signer au Client un récépissé de livraison. Si le Client constate, à la livraison une non-conformité du TPE livré, il peut refuser la livraison. Dans cette hypothèse, le Vendeur livrera au Client un nouvel équipement conforme, et fera ses meilleurs efforts afin que la livraison ait lieu dans les meilleurs délais et dès notification de ce refus de livraison par le transporteur.

Dans le cas où le Client a souscrit à l'option de maintenance sur site suivant l'offre souscrite dans le Portail Payplug, un technicien mandaté par le Vendeur débranchera le TPE et procédera à l'installation du nouvel équipement. Lors de cette intervention, il est possible que le TPE puisse être remis en service par le technicien, et que l'échange du matériel ne soit plus nécessaire.

Le Client s'engage à ce que lui-même ou l'un de ses représentants dûment habilités soit présent pour réceptionner l'équipement de remplacement, ou accueillir le technicien, à la date et à l'heure convenues avec l'ATT par téléphone.

À l'issue de l'opération de remplacement du TPE, le technicien demandera au Client ou à son représentant, mandaté à cet effet, de signer un PV d'intervention. Si le Client constate une non-conformité du fonctionnement du TPE, il peut le mentionner sur le PV d'intervention. Dans cette hypothèse, le Vendeur devra dans les meilleurs délais et dès notification de ces réserves, corriger les points de non-conformité évoqués. En l'absence de réserves, le TPE est réputé fonctionner de façon conforme.

### **3.3 Maintenance évolutive des logiciels associés aux TPE**

La maintenance évolutive des TPE consiste en la fourniture au Client des mises à jour des versions logicielles, qu'elles soient demandées par le constructeur du TPE, ou requises par la réglementation applicable. Si la taille mémoire disponible sur le TPE est insuffisante pour effectuer la maintenance évolutive ou si celle-ci n'est pas possible techniquement, le Client devra résilier le présent Contrat de Vente de TPE afin de souscrire à un nouveau



contrat de Vente dont le matériel respecte la réglementation en vigueur.

Dans ce cas, aucuns frais associés à la rupture anticipée du présent Contrat de Vente de TPE ainsi qu'aux frais de dossier du nouveau contrat de Vente ne seront facturés au Client.

Les tarifs du nouvel équipement sont ceux en vigueur à la date de la résiliation.

### **3.4 Télécommunications**

#### **3.4.1 Pour les TPE IP**

Les coûts des opérations de traitement et de transport/routage réalisées par l'opérateur du Service Monétique IP sont inclus dans le service proposé par le Vendeur au Client.

Le service Monétique IP ne couvre pas l'ensemble des télécommunications nécessaires au bon fonctionnement des échanges entre le TPE IP et les serveurs bancaires ou privés : le Client doit disposer d'un accès haut-débit à Internet pour transporter les données entre le TPE IP et le point d'accès au Service Monétique IP, pour effectuer les téléchargements nécessaires à la maintenance évolutive et, au besoin, transporter les données nécessaires aux échanges entre les logiciels privés exploités par le Vendeur et les serveurs adéquats

Le Client pourra contracter auprès du Fournisseur d'Accès Internet (FAI) de son choix pour disposer d'un accès Wifi et/ou haut-débit à Internet. Le choix du FAI est du seul ressort du Client. Celui-ci peut changer à sa convenance de FAI, à condition d'en informer le Vendeur. Aucun service spécifique du type « option monétique » ou « passerelle monétique » n'est à souscrire auprès du FAI du Client : seul est nécessaire le service de base soit l'accès à un routeur Wifi et/ou à Internet haut-débit. La tarification de ce service d'accès haut-débit à Internet est du ressort du FAI et à la charge du Client.

Description du mode secours RTC :

En cas d'indisponibilité des services offerts par le FAI du Client, c'est-à-dire en cas de non-fonctionnement de la connexion haut-débit à Internet, le TPE IP tentera d'effectuer ses télécommunications sur le réseau téléphonique commuté (ligne analogique), si le Client dispose d'une telle connexion opérationnelle, c'est-à-dire en l'absence de dégroupage total de la ligne téléphonique du Client, si le TPE IP est correctement raccordé à la ligne analogique et si le réseau téléphonique commuté (ligne analogique) est disponible lorsque le TPE IP tente d'effectuer sa connexion.

Le coût des télécommunications effectuées en mode « secours », c'est-à-dire des télécommunications effectuées sur le réseau téléphonique commuté (ligne analogique) pour pallier l'indisponibilité des services procurés par le FAI du Client, est à la charge du Client.

Description du mode secours GPRS (Back up GPRS) :

Si le Client a souscrit à l'option Back-Up GPRS, (en cas d'indisponibilité de la connexion haut-débit à Internet), le TPE IP basculera automatiquement sur le réseau mobile (GPRS) afin d'assurer la continuité du service.

#### **3.4.2 Pour les TPE GPRS**

Le Vendeur remet au Client, à titre de prêt à usage, une carte SIM permettant l'utilisation :



- d'un abonnement GPRS souscrit auprès d'un opérateur de télécommunications,
- d'un réseau de transport de flux électronique souscrit auprès d'un opérateur de transport de données.

Les coûts des télécommunications réalisées par l'intermédiaire de l'opérateur mobile au titre de l'usage de l'abonnement GPRS monétique sont inclus dans le service proposé par le Vendeur au Client.

Le choix de l'opérateur de télécommunications et de l'opérateur de transport de données est du seul ressort du Vendeur. Le Vendeur se réserve le droit de changer d'opérateur à sa convenance.

#### Période de test

Considérant l'incertitude existant a priori sur la fourniture d'un service GPRS adapté aux besoins spécifiques du Client, le Vendeur assure au Client une période dite « de test », de quinze (15) jours à dater de la livraison de l'équipement, afin d'évaluer la bonne réussite des opérations quotidiennes réalisées avec l'équipement.

Pendant cette période de test, le Vendeur s'engage, dans ce cas, à rembourser au Client l'ensemble des sommes versées au titre de la souscription de TPE GPRS. Les seuls frais à la charge du Client sont ceux de la restitution de l'équipement au Vendeur, restitution devant être effective dans les cinq (5) jours suivant la résiliation sous peine de ne plus bénéficier des avantages cités.

#### Couverture de l'abonnement monétique GPRS

Le fonctionnement de l'abonnement monétique GPRS n'est possible que dans la zone géographique de couverture propre à l'opérateur de télécommunications. L'abonnement GPRS fonctionne sur les pays autorisés par Payplug.

Le bon fonctionnement des logiciels associés au TPE GPRS et, tout particulièrement du logiciel de paiement Carte Bancaire est lié à la possibilité d'établir une communication GPRS sur les lieux et au moment où le Client en éprouve la nécessité. Ce bon fonctionnement dépend donc de la disponibilité géographique et fonctionnelle des équipements de l'opérateur de télécommunications.

Cette disponibilité est tributaire de nombreux critères tels que la distance géographique du plus proche équipement de l'opérateur, la configuration physique du lieu où se trouve le Client, le relief aux alentours, les perturbations et parasitages en radiofréquences de la zone, la proximité éventuelle de systèmes de brouillage des télécommunications mobiles et le nombre de tentatives simultanées d'accès aux équipements de l'opérateur de télécommunications. Ces conditions étant indépendantes de la volonté des parties, le Vendeur ne peut en aucun cas et en aucune façon garantir au Client la bonne exécution de toutes les opérations réalisées avec l'équipement.

#### 3.4.3 Pour les TPE RTC

Le coût des télécommunications effectuées sur le réseau téléphonique commuté (ligne analogique) est à la charge du Client.

## ARTICLE 4 – OBLIGATIONS DU CLIENT

Le Client accepte sans réserve et sans restriction l'ensemble des clauses du présent Contrat de Vente de TPE et s'engage plus particulièrement à respecter les obligations mises à sa charge à l'article 3 des présentes.

### 4.1 Utilisation de l'équipement

Le Client s'engage à utiliser l'équipement dans des conditions normales et conformes à la destination prévue. Le Client s'engage à utiliser l'équipement conformément aux spécifications techniques telles que définies dans le guide d'utilisation remis lors de la livraison de l'équipement : caractéristiques du réseau d'alimentation, du support de transmission, température... Le Client ne peut en aucun cas apporter de modification à l'équipement pour les TPE IP au câblage entre l'équipement et le modem-routeur de son FAI et aux logiciels associés. En aucun cas, l'équipement mis à disposition ne subira, sans accord du Vendeur, d'intervention ou de modification en vue de le rendre compatible avec d'autres matériels et logiciels utilisés chez le Client.

Le Client garantit en général le Vendeur contre toute conséquence qui résulterait d'une action ou d'une réclamation exercée à l'encontre du Vendeur qui serait la conséquence d'une utilisation du TPE non conforme aux spécifications techniques telles que définies dans le guide d'utilisation.

La garantie porte notamment sur tous dommages et intérêts et/ou amendes pénales auxquels serait condamné le Vendeur et s'étend aux frais de justice éventuels, y compris les frais irrépétibles et les frais d'avocats.

### 4.2 Moyens de télécommunications

#### 4.2.1 TPE IP - Utilisation du réseau ADSL

La prestation d'installation ne comprend ni mise en conformité ni adaptation des installations électrique, téléphonique et réseau du point de vente du Client. Le Client s'engage à installer à proximité immédiate de l'emplacement d'exploitation du TPE IP, une prise d'alimentation électrique, le modem-routeur permettant d'accéder au réseau de son FAI et une prise de connexion au réseau téléphonique commuté. À défaut, le Client prendra à sa charge les travaux nécessaires qu'il fera exécuter par le prestataire de son choix. Les travaux doivent être exécutés préalablement à l'installation du TPE IP.

Si le Client souhaite faire évoluer la configuration de son réseau IP et que cela nécessite par la suite une intervention du Vendeur pour adapter la configuration du TPE IP ou si le Client modifie la configuration de son réseau IP et que cela provoque un dysfonctionnement du TPE IP nécessitant une intervention du Vendeur pour corriger le dysfonctionnement, ces interventions seront facturées au Client.

Il est rappelé au Client que le maintien en bonne condition opérationnelle de la connexion Wifi et/ou Internet haut-débit à laquelle est rattaché le TPE IP ou le TPE IP Mobile Wifi est intégralement de son ressort. Il appartient au Client de vérifier régulièrement ce bon fonctionnement. À défaut, si le mode secours de son TPE IP fonctionne correctement et qu'il effectue par ce moyen de nombreuses transactions, le montant des échanges effectués sur le réseau téléphonique commuté, facturé par l'opérateur correspondant, peut devenir conséquent et restera intégralement à la charge du Client.

#### 4.2.2 TPE GPRS - Utilisation de la carte SIM

Le Client, en sa qualité de gardien de la carte SIM, est seul responsable de l'utilisation conforme de celle-ci à son usage, tel qu'il est prévu au sein du présent Contrat de Vente de TPE, et de la conservation de celle-ci.

La carte SIM est configurée pour interdire la réception d'appel, les services voix, l'itinérance avec certains des opérateurs mobiles étrangers, les SMS et le GSM Data.

Dans le cas où la carte SIM disposerait d'un pin code permettant d'en protéger l'utilisation, le Client ne devra en

aucun cas le modifier.

En outre, la carte SIM ne peut être utilisée par le Client que sur le TPE GPRS mis à sa disposition dans le cadre de l'exécution du Contrat de Vente de TPE.

#### 4.2.3 Utilisation du service monétique IP et GPRS

Le Client ne peut utiliser le service Monétique IP ou abonnement GPRS Monétique mis à sa disposition par le Vendeur, dans le cadre du présent Contrat de Vente de TPE, que pour permettre le bon fonctionnement des logiciels associés au TPE IP ou GPRS. Le Client ne peut en aucun cas céder, louer, prêter ou utiliser, pour son compte ou pour le compte de tiers, ce service Monétique IP ou GPRS pour permettre le fonctionnement :

- d'autres appareils que le TPE IP / GPRS fourni par le Vendeur,
- d'autres logiciels que ceux installés par le Vendeur sur le TPE IP ou GPRS,
- du logiciel Cartes Bancaires installé sur le TPE IP ou GPRS dans un cadre contractuel différent de celui négocié avec le Vendeur au sein des présentes.

Dans les situations énumérées ci-dessus :

- le Vendeur ne s'engage en aucun cas au bon fonctionnement de l'équipement et du service Monétique IP ou abonnement GPRS Monétique,
- le vendeur se réserve le droit de mettre en œuvre tout moyen technique de son choix lui permettant

d'empêcher le bon fonctionnement du service Monétique IP ou abonnement GPRS Monétique.

### **ARTICLE 5 – PRESTATIONS NON COMPRIS DANS LE CONTRAT**

Les interventions du Vendeur ou de toute personne habilitée par ce dernier, requises du fait du non-respect par le Client des dispositions de l'article 4 donneront lieu à facturation en sus des prestations. De même, toute autre prestation demandée par le Client mais n'entrant pas dans le périmètre des prestations, telles qu'elles sont énumérées à l'article 3 des présentes, notamment la fourniture de batterie de rechange ou de cordons supplémentaires, donnera lieu à facturation en sus des prestations.

Pour le TPE IP Mobile Wifi : la fourniture d'un routeur Wifi (exemple : box Internet ou Smartphone) est à la seule charge du Client.

### **ARTICLE 6 – GARANTIE SUR LES LOGICIELS ASSOCIÉS À L'ÉQUIPEMENT**

Le Vendeur déclare détenir directement ou via ses partenaires les droits nécessaires à la concession au Client, de droits d'utilisation non exclusifs des logiciels associés. Le Vendeur garantit le Client contre tout risque d'éviction, dans les pays autorisés par Payplug, dès lors qu'il utilise lui-même les équipements conformément à leur destination, et qu'il n'a pas tenté de les modifier ou de les faire modifier par un tiers. Si le Client venait à être inquiété de ce chef, il en aviserait immédiatement le Vendeur qui devrait prendre immédiatement les mesures propres à faire cesser tout trouble dans la jouissance et prendrait seul à ses frais toute mesure de défense nécessaire.

### **ARTICLE 7 – PROPRIETE INTELLECTUELLE**

Le Vendeur concède au Client, pendant toute la durée du Contrat d'Adhésion, une licence d'utilisation des logiciels



associés au TPE. Les logiciels associés au TPE sont ceux nécessaires à son fonctionnement (partie système). Cette licence comprend les droits :

- d'utiliser les logiciels associés au TPE pour le fonctionnement du TPE, dans le strict cadre contractuel défini aux présentes. Le Client n'est pas autorisé à sous-licencier les logiciels associés ou à les utiliser à d'autres fins que celles prévues dans le cadre du présent Contrat de Vente de TPE, ni à les utiliser pour la formation de tiers.
- d'utiliser la documentation fournie avec les logiciels associés aux fins indiquées ci-dessus.

Le Client n'acquiert aucun droit de propriété sur les logiciels associés au TPE ni sur la documentation fournie. Le Client s'engage à ne pas effectuer ou permettre le désassemblage, la décompilation ou l'ingénierie à rebours des logiciels associés au TPE. Le Client s'engage à n'effectuer aucune copie des logiciels.

## **ARTICLE 8 – EXCLUSION DE RESPONSABILITÉ DU VENDEUR**

Le Vendeur décline toute responsabilité en cas de mauvais fonctionnement de l'équipement causé par une utilisation non conforme de celui-ci par le Client.

Il est rappelé au Client que les obligations du Vendeur portent sur la mise à disposition d'un moyen d'encaissement, non sur les conséquences de son absence.

Dans tous les cas, il est rappelé que le Vendeur n'est tenu qu'à une obligation générale de moyens.

En aucun cas la responsabilité du Vendeur ne pourra être recherchée, quel que soit le type d'action intentée, pour un dommage indirect, qu'il soit matériel ou immatériel, et notamment pour tout manque à gagner, trouble commercial, perte de données, de clientèle, d'exploitation, de chances, de bénéfice ou actions intentées par un tiers contre le Client ainsi que leurs conséquences, lié au présent Contrat de Vente de TPE ou à son exécution.

Seuls sont indemnisables, dans le cadre du présent Contrat de Vente de TPE, les dommages matériels et financiers directs.

Le Vendeur ne pourra être tenu responsable que des dommages et intérêts directs résultant d'une faute prouvée. Dans ce cas, le montant maximum de sa responsabilité ne pourra excéder le montant annuel de la prestation due au titre du présent Contrat de Vente de TPE.

Si le Client subissait un risque financier occasionné par l'absence d'un moyen d'encaissement opérationnel, il lui incomberait de prendre toutes les mesures nécessaires afin de se prémunir face à cette situation, notamment en disposant de multiples équipements usant de moyens de télécommunications réellement indépendants. Il appartient au Client de se faire aider de spécialistes des télécommunications si nécessaire.

Pour les TPE IP uniquement :

Le TPE IP est doté d'un mode secours, pour le bon fonctionnement duquel il est nécessaire de connecter l'équipement à une ligne téléphonique analogique (réseau téléphonique commuté) en sus de la connexion assurée par le câble avec le modem-routeur du FAI. Le Vendeur ne pourra en aucun cas être tenu pour responsable et ce pour quelque cause que ce soit en cas de connexion du mode secours de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune surfacturation du prix des communications par les opérateurs.

Il est rappelé au Client que le mode de secours, l'usage par le TPE IP des télécommunications par le réseau téléphonique commuté en lieu et place d'Internet, est destiné à améliorer la disponibilité globale du service d'encaissement et non pas à apporter une garantie de connexion au serveur bancaire. Selon la configuration des télécommunications du Client, un même et unique événement peut rendre indisponible les deux modes de télécommunications, IP et analogique. C'est notamment le cas avec un TPE IP connecté en ADSL et en analogique sur une même ligne téléphonique en dégroupage partiel, car les échanges Internet et téléphoniques



(en mode secours) utilisent alors le même support physique, à savoir le câble de cuivre de la ligne téléphonique : une rupture de ce support rendrait inopérant simultanément les deux modes de télécommunications.

La responsabilité du Vendeur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client.

De même, la responsabilité du Vendeur ne peut pas être engagée :

- en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des indisponibilités pour les équipements radio,
- en cas de difficultés liées à l'indisponibilité du service fourni par le FAI du Client,
- en cas d'intervention technique effectuée par une personne non habilitée par le Vendeur,
- en cas de mauvaise utilisation par le Client du service Monétique IP, ou d'utilisation non conforme à sa destination telle que prévue aux présentes conditions générales.

Pour le TPE IP Mobile Wifi, la responsabilité du Vendeur ne peut pas être engagée :

- en cas de rupture de connexion entre le TPE et le routeur Wifi,
- en cas de rupture de réseau entre le routeur Wifi et le réseau acheminant les données vers les serveurs bancaires ou privés pour le TPE IP Mobile Wifi.

Pour les TPE GPRS uniquement :

En ce qui concerne les modèles de TPE GPRS disposant également d'une connexion RTC, le Vendeur ne pourra en aucun cas être tenu pour responsable pour quelque cause que ce soit en cas de connexion de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune facturation du prix des communications par les opérateurs.

Le Vendeur décline toute responsabilité en cas de mauvais fonctionnement de l'équipement et de l'abonnement GPRS monétique, causé par une utilisation non conforme de ceux-ci par le Client. La responsabilité du Vendeur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client.

De même, la responsabilité du Vendeur ne peut pas être engagée :

- en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des indisponibilités pour les équipements radio, - en cas de difficultés liées aux lieux et aux conditions de réception (absence de couverture GPRS).
- en cas d'intervention technique effectuée par une personne non habilitée par le Vendeur,
- en cas de mauvaise utilisation par le Client du service GPRS Monétique, notamment de la carte SIM, ou d'utilisation non conforme à sa destination telle que prévue aux présentes conditions générales.

Pour les TPE RTC uniquement :

Le Vendeur ne pourra en aucun cas être tenu pour responsable pour quelque cause que ce soit en cas de connexion de l'équipement à une ligne téléphonique autre qu'analogique (réseau téléphonique commuté). Il décline notamment toute responsabilité en raison d'éventuelles fraudes à la carte bancaire, et ne supportera aucune surfacturation du prix des communications par les opérateurs.

La responsabilité du Vendeur ne saurait également être recherchée en cas de dysfonctionnements ou de pannes de l'équipement imputables au Client.

De même, la responsabilité du Vendeur ne peut pas être engagée :

- en cas d'aléas de propagation d'ondes électromagnétiques qui peuvent entraîner des perturbations ou des





indisponibilités pour les équipements radio,  
- en cas d'intervention technique effectuée par une personne non habilitée par le Vendeur,

## **ARTICLE 9 – MODALITES DE PAIEMENT ET FRAIS DE DOSSIER**

Le paiement est opéré par tout moyen mis à disposition du client par Payplug pour le TPE, le paiement étant nécessaire avant la livraison de l'équipement.

Le paiement des frais de dossier, les frais d'installation et les frais relatifs aux options logicielles associées ou consommables (cordons, batterie, carte de domiciliation, etc...), demandées lors de la signature du Contrat de vente de TPE est opéré par tout moyen mis à disposition du client par Payplug.

Les frais de transaction et l'abonnement éventuel liés à l'utilisation du TPE sont prélevés sur le solde du compte Payplug du marchand suivant les CGV en vigueur.

Les frais relatifs aux options logicielles ou à un déplacement technicien pour une installation sur site, demandés en cours de réalisation du Contrat de vente de TPE (logiciels associés, déplacement sur site, consommables, non demandés initialement par le Client) seront prélevés en sus du paiement sur la base des tarifs en vigueur.

En cas d'impossibilité de procéder aux prélèvements (fermeture du compte par exemple), à la suite d'une relance valant mise en demeure de payer, envoyée par courrier recommandé avec demande d'avis de réception restée sans effet pendant quinze (15) jours, le Vendeur se réserve le droit d'engager toute action destinée à recouvrer les sommes. Dans le cas où le Vendeur tenterait toute action en justice contre le Client pour défaut de paiement, le Vendeur se réserve le droit de suspendre le service Monétique IP du Client sans préavis particulier.

## ANNEXE 5 : Conditions générales d'utilisation du service « Tap to Pay sur Iphone »

Les présentes conditions générales d'utilisation (ci-après les « **CGU** ») ont pour objet de déterminer les modalités d'utilisation du service « Tap to Pay sur Iphone » (ci-après le « **Service** ») via l'application mobile « Tap to Pay avec Payplug » (ci-après « l'**Application** ») proposée par PAYPLUG ENTERPRISE SAS (RCS PARIS 443 222 682) (ci-après « **Payplug** » ou « l'**Éditeur** ») par une personne titulaire d'un compte de paiement ouvert dans les livres de Payplug (ci-après le « **Client** »).

Le Client reconnaît avoir pris connaissance des présentes CGU et s'engage à les respecter sans aucune réserve ni restriction.

### 1. Objet du Service

Le Service permet aux Clients de proposer à ses clients (ci-après les « **Utilisateurs** ») de procéder au paiement des biens et/ou des services, au moyen d'un paiement sans contact sur le téléphone mobile du Client conformément aux règles définies à cet effet par Apple et dédiées aux mobiles IOS. .

Le téléchargement de l'Application est gratuit.

### 2. Conditions préalables à l'utilisation du Service

Le Client adhère au Contrat de services.

Afin de pouvoir bénéficier du Service, le Client doit s'assurer d'avoir téléchargé l'Application depuis un espace dédié aux applications Apple tel que « *App Store* » et avoir satisfait aux conditions générales de Tap to Pay sur Iphone pour commerçants (<https://register.apple.com/tou/tap-to-pay-on-iphone/latest/fr>) (ci-après les « **Conditions d'Apple** »).

Pour des raisons techniques, l'Application peut être incompatible avec certaines gammes de téléphones mobiles. En raison de l'évolution constante de la gamme d'appareils mobiles sur le marché, l'Éditeur n'est pas en mesure de fournir une liste actualisée de l'ensemble des téléphones mobiles compatibles avec l'Application.

Le Client doit s'identifier grâce à la saisie d'un identifiant et d'un mot de passe confidentiel qui remplissent les conditions de sécurité minimale indiquées dans l'Application et qui lui est envoyé par Payplug lors de la souscription.

Cet accès nominatif est obtenu à la suite de la conclusion du Contrat de service. L'Application ne peut être utilisée que sur un seul appareil mobile de manière simultanée.

### 3. Accès au Service

Tous les frais supportés par le Client pour accéder au Service (matériel informatique, logiciels, connexion Internet et mobile, etc.) sont à sa charge exclusive.

Pour des raisons de maintenance mais également en cas de force majeure, difficultés informatiques, difficultés liées aux réseaux de télécommunications ou autres difficultés techniques, l'Éditeur pourra interrompre l'accès au Service et ne saurait être tenu responsable de l'impossibilité d'accéder à l'Application.

Le Client s'engage à installer les mises à jour proposées par l'Éditeur. Il en sera informé lors de l'utilisation de l'Application.

### 4. Politique de gestion des données

#### 4.1. Données non personnelles

Le Client accepte que l'Éditeur puisse collecter et utiliser des données non personnelles quantitatives dérivées de l'utilisation des Services dans le seul cadre de son activité professionnelle, à des fins d'analyse sectorielle, comparative, d'analyses de données et marketing à destination de sa clientèle. Toutes les données ainsi collectées et utilisées par l'Éditeur le seront sous forme agrégée et anonymisée exclusivement, ne permettant en aucune façon d'identifier le Client ses clients ou ses Utilisateurs, ses données client ou toutes tierces parties

utilisant les Services, et seront conservées dans ces mêmes conditions.

Les données collectées concernent notamment l'interaction du Client et des Utilisateurs avec l'Application, telles que les rubriques et les pages visitées par session ainsi que le nombre de clics et de défilements. Par ailleurs, l'Éditeur traite des informations sur la version du système d'exploitation utilisée, l'identification de l'appareil mobile, la langue du système et le pays sélectionné ainsi que sur la version de l'Application utilisée.

#### **4.2. Données d'identification**

L'installation de l'Application et l'utilisation des fonctionnalités requièrent une transmission de données régulière depuis le téléphone mobile du Client. L'étendue et la fréquence de la transmission de données dépendent du type et du degré d'utilisation du Service.

Afin de se connecter à l'Application, le Client doit communiquer à l'Éditeur ses données à caractère personnel obligatoires, telles que leurs nom, prénom, coordonnées et adresse électronique. À défaut, le Service ne sera pas accessible.

Lorsque le Client se connecte, ses identifiants de connexion sont collectés et utilisés. Afin d'éviter que le Client n'ait à se reconnecter à chaque utilisation de l'Application, ses identifiants de connexion sont stockés de manière chiffrée dans l'Application jusqu'à ce qu'à ce que le Client se déconnecte.

Les données personnelles recueillies dans le cadre des Services proposés par l'Application sont traitées pour gérer les fonctionnalités du Service, selon des protocoles sécurisés.

Les données personnelles collectées sont conservées le temps nécessaire à leur traitement. La durée affichée couvre la durée de conservation en base active et en archive intermédiaire.

En cas d'inactivité de l'Application pendant une durée de 13 mois consécutive, les données personnelles seront effacées, et le Client n'aura plus accès au Service.

Le Client est informé qu'il dispose d'un droit d'accès, d'opposition, de rectification et de suppression portant sur les données personnelles le concernant. Pour toute information ou exercice de vos droits Informatique et Libertés sur les traitements de données personnelles gérés par l'Éditeur, il peut exercer ses droits sur toutes les données à caractère personnel que l'Éditeur traite, y compris celles qu'il traite en responsabilité conjointe avec nos clients, en le contactant par courrier électronique ([privacy@payplug.com](mailto:privacy@payplug.com)) ou par courrier postal en indiquant, nom, prénom, coordonnées de contact et en fournissant une copie de sa pièce d'identité (Payplug - Délégué à la Protection Des Données - 110, avenue de France 75013 Paris).

Les personnes concernées ont le droit d'introduire une réclamation auprès d'une autorité de contrôle en charge de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. En France, l'autorité de contrôle est : Commission Nationale de l'Informatique et des Libertés (CNIL), 3 place de Fontenoy TSA 80715 - 75334 PARIS Cedex

#### **5. Obligations du Client**

Le Client s'engage durant toute la durée d'utilisation du Service à :

- fournir des informations sincères et exactes concernant son état civil et ses coordonnées, notamment son adresse électronique ;
- garder son mot de passe confidentiel et à le modifier en cas de soupçon d'utilisation abusive ou frauduleuse ;
- utiliser le Service conformément au droit applicable, au Contrat de services, aux Conditions d'Apple et aux présentes CGU ;
- utiliser le Service uniquement pour son activité en France.

L'usurpation d'identité est passible de sanctions pénales.

L'accès à l'Application est réservé au Client et toute personne physique sur laquelle il a une autorité (par exemple, ses salariés...); à ce titre le Client s'interdit de communiquer ses accès, son identifiant et son mot de passe à un

tiers. Toute utilisation du Service sera présumée avoir été effectuée par le Client.

Le Client est tenu d'avertir sans délai l'Éditeur de toute utilisation non autorisée du Service et de modifier ses identifiants de connexion et son mot de passe s'il a des raisons de croire que son compte est utilisé frauduleusement par des tiers.

Ces dispositions s'appliquent également à tous les accès fournis à des personnes physiques préalablement autorisés par le Client.

## **6. Propriété intellectuelle**

Les marques, logos, signes distinctifs ainsi que tous les contenus de l'Application (textes, images, son...) font l'objet d'une protection par le Code de la propriété intellectuelle et plus particulièrement par le droit d'auteur.

L'ensemble des contenus (textes, sons, marques, logos, photographies, etc.), figurant sur les pages de l'Application sont la propriété exclusive de l'Éditeur. Toute reproduction, représentation, diffusion ou extraction non autorisée, en tout ou partie, du contenu de l'Application constituerait une contrefaçon des droits de propriété intellectuelle de l'Éditeur susceptible d'engager la responsabilité civile et pénale du contrefacteur.

Le Client doit solliciter l'autorisation préalable de l'Éditeur pour toute reproduction, publication, copie des différents contenus.

## **7. Responsabilité**

L'Éditeur s'efforce d'assurer l'exactitude et la mise à jour des informations à caractère général diffusées sur l'Application, dont il se réserve le droit de modifier et de corriger le contenu à tout moment et sans préavis. En conséquence, l'Éditeur ne garantit en aucune façon la complétude, la précision, l'exactitude, l'exhaustivité ou l'adéquation des informations mises à disposition sur l'Application, y compris l'ensemble des liens hypertextes ou toute autre liaison informatique utilisée, directement ou indirectement, à partir de l'Application.

En tout état de cause, l'Éditeur ne pourra en aucun cas être tenu responsable :

- de tout dommage direct ou indirect, notamment en ce qui concerne les pertes de profits, le manque à gagner, les pertes de clientèle ;
- d'un dysfonctionnement, d'une indisponibilité d'accès, d'une mauvaise utilisation, d'une mauvaise configuration du téléphone portable du Client, ou encore de l'emploi d'un appareil peu usité ou obsolète par le Client ;
- en raison d'une indisponibilité technique de la connexion, qu'elle soit due notamment à un cas de force majeure, à une maintenance, à une mise à jour, à une modification, à une intervention de l'hébergeur, à une grève interne ou externe, à une panne de réseau, à une coupure d'alimentation électrique, ou encore à une mauvaise configuration ou utilisation du périphérique du Client.

Il est strictement interdit de mettre en place un lien hypertexte en direction de l'Application sans l'autorisation écrite et préalable de l'Éditeur.

Le Client s'assure de garder son identifiant et son mot de passe secret. Toute divulgation du mot de passe, quelle que soit sa forme, est interdite. Il assume les risques liés à l'utilisation de son identifiant et de son mot de passe. L'Éditeur décline toute responsabilité à cet égard.

Il appartient au Client de prendre toutes les mesures appropriées de façon à protéger ses propres données et/ou logiciels stockés sur son équipement mobile contre toute atteinte.

L'Éditeur ne peut être tenu pour responsable d'éventuels virus qui pourraient infecter le smartphone ou tout matériel mobile du Client, à la suite d'une utilisation, à l'accès, ou au téléchargement provenant de l'Application.

Tout manquement par le Client aux présentes Conditions Générales d'Utilisation, toute utilisation abusive ou frauduleuse du Service entraînera de plein droit la suspension à effet immédiat du Service.



#### **8. Droit applicable**

Les CGU sont soumises au droit français.

Tout litige est du ressort du tribunal compétent de l'Éditeur.

## ANNEXE 6 : PROTECTION DES DONNÉES CLAUSES SOUS-TRAITANT (ART.28 RGPD)

### I. OBJET

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable du traitement les opérations de traitement de données à caractère personnel définies ci-après. Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la législation et la réglementation en vigueur applicables au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après « le règlement européen sur la protection des données » ou « RGPD »).

Les Parties conviennent que les présentes clauses et leurs annexes font partie intégrante du (ou des) contrat(s) (incluant tout avenant) qui les lie(nt) (ci-après ensemble désignés le « Contrat »).

A toutes fins utiles, les parties conviennent que les termes suivants, comportant ou non une majuscule, conservent le sens qui leur a été attribué à l'article 4 du RGPD : « sous-traitant », « données à caractère personnel », « responsable du traitement », « traitement », « traiter », « personne concernée », « autorité de contrôle ».

Pour l'exécution de la présente annexe (ci-après "Annexe"), les parties conviennent que **Payplug** aura la qualité de sous-traitant et que le Client aura la qualité de responsable du traitement, étant précisé que le terme « Client » conserve la signification qui lui a été attribuée dans le Contrat.

### II. DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Pour l'exécution du Service, objet de la présente Annexe, le sous-traitant met à la disposition du responsable du traitement les informations nécessaires suivantes décrites à la Sous-annexe A :

- Nom et coordonnées de contact du sous-traitant
- Nom et coordonnées de contact du délégué ou du référent à la protection des données du sous-traitant. Pour l'exécution du Service objet de la présente Annexe, le responsable du traitement met à la disposition du sous-traitant les informations nécessaires suivantes décrites à la Sous-annexe B :
  - Nom et coordonnées de contact du responsable du traitement
  - Nom et coordonnées de contact du délégué ou du référent à la protection des données du responsable du traitement
- Le sous-traitant est autorisé à traiter pour le compte du responsable du traitement les données à caractère personnel nécessaires pour fournir le ou les Service(s) décrit(s) à la Sous-annexe C :
  - La nature des opérations réalisées sur les données ;
  - La ou les finalité(s) du traitement ;
  - Les données à caractère personnel traitées ;
  - Les catégories de personnes concernées ;
  - La durée du traitement.

### III. DUREE

La présente Annexe entre en application à compter de sa date de signature et est conclue pour une durée indéterminée et expirera de plein droit et avec effet immédiat à compter de la cessation du Contrat, et ce dans les limites des clauses ayant vocation à continuer de s'appliquer à compter de l'expiration de la présente Annexe conformément au RGPD et plus généralement aux dispositions légales et réglementaires en vigueur.

### IV. OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DU TRAITEMENT

Le sous-traitant s'engage à :

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance comme décrit dans la Sous-annexe C ;
2. Traiter les données conformément aux instructions documentées du responsable du traitement. Néanmoins, si le sous-traitant considère qu'une instruction constitue une violation du règlement européen

sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable du traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre de la présente Annexe ;
  4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu de la présente Annexe :
    - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
    - Reçoivent la formation nécessaire en matière de protection des données à caractère personnel
  5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.
- 6 Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après le « sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable du traitement de tout changement envisagé concernant l'ajout ou le remplacement de tout sous-traitant ultérieur. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance. Le responsable du traitement dispose d'un délai d'un mois à compter de la date de réception de cette information pour présenter ses objections.

Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations de la présente Annexe pour le compte et selon les instructions du responsable du traitement, et dans le respect des dispositions prévues par le RGPD. Il appartient au sous-traitant de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données à caractère personnel, le sous-traitant demeure pleinement responsable à l'égard du responsable du traitement de l'exécution de ses obligations par ledit sous-traitant ultérieur.

## 7 Droit d'information des personnes concernées

Il appartient au responsable du traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

## 8 Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable du traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au responsable de traitement aux coordonnées détaillées en annexe B.

## 9 Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel sans retard indu, après en avoir pris connaissance, par courrier électronique aux coordonnées détaillées en annexe B. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement, si

nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

En tout état de cause, le sous-traitant fera ses meilleurs efforts pour identifier la cause de toute violation de données à caractère personnel ayant pu entraîner une fuite des celles-ci et prendra le cas échéant toutes les mesures raisonnables et nécessaires afin d'y apporter les mesures de remédiation appropriées pour autant que celles-ci soient raisonnablement considérées comme sous son contrôle.

Les obligations listées dans le présent article ne sont pas applicables si les violations de données à caractère personnel sont causées par le responsable du traitement ou l'un de ses utilisateurs.

#### 10 Aide du sous-traitant dans le cadre du respect par le responsable du traitement de ses obligations

Le sous-traitant aide le responsable du traitement pour la réalisation d'analyses d'impact relative à la protection des données. Le sous-traitant aide le responsable du traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

#### 11 Mesures de sécurité

Le sous-traitant surveille de manière régulière et assure un maintien en conditions de sécurité technique et organisationnelle garantissant la confidentialité, l'intégrité et la sécurité des données à caractère personnel (incluant la protection contre les accès non autorisés ou contre la mise en œuvre de traitements contraires au RGPD, la protection contre les destructions accidentelles ou malveillantes, la protection contre les atteintes en confidentialité, disponibilité ou en intégrité, la diffusion ou l'accès non autorisée aux données à caractère personnel) tel que détaillé en annexe D.

#### 12 Sort des données à caractère personnel

Au terme de la prestation de services relatifs au traitement de ces données et dans la limite des dispositions légales et réglementaires applicables au sous-traitant, le sous-traitant s'engage à :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable du traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable du traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

#### 13 Le Délégué à la Protection des Données

Le sous-traitant a désigné un référent à la protection des données personnelles en accord avec l'Article 4(19) et l'Article 37(2) du RGPD comme détaillé en Sous-annexe A.

#### 14 Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement comprenant :



- le nom et les coordonnées du responsable du traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles détaillées dans la Sous-annexe D.

#### 15 Documentation - Audit

Le Responsable de traitement dispose à tout moment, moyennant un préavis de trente (30) jours ouvrables, d'un droit d'audit documentaire des prestations ou des services/ produits/ solutions sous réserve de la validation des Inspections générales de BPCE SA dont dépend Payplug. Ce droit d'audit est limité à une (1) fois au cours d'une période de 12 mois, sauf en cas d'incident de sécurité ou violation des données à caractère personnel. En outre le Responsable de traitement devra se présenter aux locaux de Payplug aux fins de consultations des éléments de conformité PCI-DSS couvrant le périmètre d'audit concerné. A cette occasion il devra prendre connaissance du ROC (Report On Compliance) le document de référence certifiant la conformité PCI-DSS de Payplug.

La conduite de l'audit par le Responsable de traitement devra respecter les obligations de confidentialité du présent Contrat. Le Sous-traitant s'engage par conséquent à fournir tous documents utiles afin de permettre un audit de tout ou partie des Prestations ou des services/ Produits/ Solutions, notamment des conditions d'exploitation de ses infrastructures, des moyens mis en place afin de sécuriser et de sauvegarder les Données - et tout particulièrement les Données à caractère personnel - et, plus généralement, du respect par le Sous-traitant des normes et standards applicables et à minima des éventuels référentiels techniques et de sécurité décrits au sein de la présente annexe et/ou adressés par tout moyen par le Responsable de traitement.

Tout audit pourra être réalisé par le Responsable de traitement ou par une société tierce mandatée par le Responsable de traitement, non concurrente du Sous-traitant de toute société du Groupe BPCE ; soumise au secret professionnel et aux obligations de confidentialité prévues à l'article 15 du Contrat et qui devra être préalablement approuvée par le Sous-traitant. Il est précisé qu'à cette occasion Payplug se réserve le droit de refuser l'auditeur ainsi désigné et que cela sera sans frais pour Payplug.

Plus spécifiquement, l'audit permettra :

- de s'assurer que le site physique du Sous-traitant ou de son sous-traitant ultérieur où sont hébergées les Données et tout particulièrement les Données personnelles est sécurisé,
- de vérifier que les Données du Responsable de traitement et tout particulièrement les Données personnelles et les répliques sont bien localisées sur le territoire de l'Union Européenne,
- s'agissant de l'organisation de la sécurité, d'avoir connaissance des éventuelles vulnérabilités liées aux différents processus d'exploitation du système et à la gestion de la sécurité.
- s'agissant de la configuration des composants du système d'information, de prendre connaissance des configurations techniques des composants utilisés par le système où transitent les Données du Responsable de traitement et les Données personnelles.
- s'agissant de la sécurité des sites d'hébergement, de prendre connaissance des mesures nécessaires de sécurisation du site d'hébergement sont mises en œuvre conformément aux exigences du Responsable de traitement.
- de prendre connaissance des moyens techniques et organisationnels mis en œuvre pour assurer la protection des Données personnelles.

Le Sous-traitant s'engage à collaborer de bonne foi avec le Responsable de traitement et/ou la société tierce diligentée afin de lui faciliter son audit en lui procurant toutes les informations nécessaires et en répondant à l'ensemble des demandes afférentes à cet audit.

Lorsqu'un audit ayant pour objet les prestations du sous-traitant ultérieur autorisé par le Responsable de traitement, le Sous-traitant s'engage à obtenir l'accord écrit de son Sous-traitant ultérieur pour les besoins de cet

audit.

Le Responsable de traitement communiquera le résultat de l'audit au Sous-traitant qui aura un délai de trente (30) jours ouvrables pour faire valoir ses observations par écrit. Si le résultat de l'audit révèle un écart avec les engagements contractuels du Sous-traitant, le Sous-traitant devra présenter, dans les trente (30) jours ouvrables, au Responsable de traitement un plan d'action approprié avec des mesures correctives et le mettre en œuvre dans les délais raisonnables et qui seront convenus entre le Responsable de traitement et le Sous-traitant.

Les frais de l'audit seront à la charge du Responsable de traitement.

## **V. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT**

Le responsable du traitement s'engage à :

- déterminer les finalités et les moyens du traitement qu'il délègue au sous-traitant ;
- fournir au sous-traitant les données visées au II des présentes clauses ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

## **VI. LIMITES DE RESPONSABILITÉ**

Le sous-traitant reconnaît que la présente Annexe est rédigée en application du RGPD et ce afin de satisfaire toutes les exigences prévues par le RGPD en matière de sous-traitance des données à caractère personnel. A ce titre, il reconnaît et accepte que toutes obligations lui incombant au titre des présentes, incluant les instructions écrites dictées ultérieurement par le responsable du traitement, ne doivent pas être de nature à engager la responsabilité du responsable du traitement pour un manquement au RGPD.

A ce titre et en cas de manquement du sous-traitant à l'une de ses obligations essentielles prévues aux présentes, le sous-traitant indemniserà le responsable du traitement si la responsabilité de ce dernier est engagée par une personne concernée, l'un de ses représentants et/ou une autorité de contrôle et que le responsable du traitement est définitivement reconnu comme étant responsable vis-à-vis de ces derniers par une décision de justice.

## **VII. DISPOSITIONS DIVERSES**

Pour éviter toute confusion, il est précisé que toute référence mentionnée dans la présente Annexe est applicable aux annexes. Le droit applicable au Contrat est également applicable à la présente Annexe.

Sauf dispositions contraires prévues par les lois et règlements en vigueur et/ou le RGPD, les dispositions du Contrat relatives à la compétence juridictionnelle sont également applicables à la présente Annexe.

## **VIII. LISTE DES SOUS-ANNEXES**

SOUS-ANNEXE A - COORDONNEES DE CONTACT DU SOUS-TRAITANT

SOUS-ANNEXE B - COORDONNEES DE CONTACT DU RESPONSABLE DU TRAITEMENT

SOUS-ANNEXE C- DESCRIPTION DU TRAITEMENT

SOUS-ANNEXE D - MESURES DE SECURITE DU SOUS-TRAITANT

## **SOUS-ANNEXE A – COORDONNEES DE CONTACT DU SOUS-TRAITANT**

Cette Sous-annexe détaille les coordonnées de contact du sous-traitant.

### **I. Nom et coordonnées de contact du sous-traitant**

**Payplug Enterprise Sas**, société par actions simplifiée, au capital de 32 425 914,10 euros, dont le siège social est situé 110 avenue de France 75013 Paris, enregistrée sous le numéro unique d'identification 443 222 682 au Registre du Commerce et des Sociétés de Paris.

### **II. Nom et coordonnées de contact du délégué ou référent à la protection des données personnelles**

Le sous-traitant a désigné un référent à la protection des données personnelles en accord avec l'Article 4(19) et l'Article 37(2) du RGPD.

La personne désignée peut être contactée aux coordonnées suivantes :

- Adresse : **Payplug Enterprise**, Données Personnelles, 110 avenue de France 75013 Paris
- Adresse électronique : [privacy@payplug.com](mailto:privacy@payplug.com)
- Téléphone : + 33 (0) 1 84 07 07 07

## **SOUS-ANNEXE B – COORDONNEES DE CONTACT DU RESPONSABLE DU TRAITEMENT**

Les coordonnées de contact du Responsable du traitement ont été déclarés lors de l'onboarding.

## **SOUS-ANNEXE C – DESCRIPTION DU TRAITEMENT**

Cette Sous-annexe détaille le traitement défini par le responsable du traitement et faisant l'objet de la sous-traitance comme exigé par l'Article 28(3) du RGPD.

### **I. Nature des opérations réalisées sur les données à caractère personnel**

Les opérations réalisées sur les données à caractère personnel conformément à l'article 4(2) du RGPD sont : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

### **II. Finalités du traitement**

Les finalités du traitement sont les suivantes :

- La réalisation par PAYPLUG ENTERPRISE SAS des Services de paiement au sens de l'article L.314-1 II du Code Monétaire et Financier pour les catégories « 3 a », «3 c » et « 5 », à savoir l'exécution de prélèvements (« SEPA Direct Debit »), de virements (« SEPA Credit Transfers ») et l'acquisition d'ordres de paiement via carte bancaire et autres moyens de paiement règlementés.
- Le cas échéant, la fourniture par PAYPLUG ENTERPRISE SAS de l'offre « Smart3-D Secure» au responsable de traitement, cette offre permettant d'optimiser la conversion du responsable de traitement

en réduisant les étapes de l'authentification forte (3DS) via l'envoi par PAYPLUG ENTERPRISE SAS de demandes d'exemptions auprès des banques émettrices des clients finaux du responsable de traitement.

- Le cas échéant, la conservation par PAYPLUG ENTERPRISE SAS des numéros de carte bancaire des clients finaux du responsable de traitement, afin de faciliter les transactions ultérieures de ces derniers.

### III. Données à caractère personnel traitées

Le responsable du traitement peut transmettre des données à caractère personnel à destination des services du sous-traitant dans la mesure où celles-ci sont déterminées et contrôlées exclusivement par le responsable du traitement et qui peuvent inclure, sans limitation, les catégories suivantes de données à caractère personnel :

#### Données Personnelles :

- Données de paiement : (Statut de la transaction, montant de la transaction, devise, date et heure de la transaction)
- Données de titulaire de carte PCI DSS : (PAN, CW, date d'expiration, nom et prénom)
- Données de facturation (Nom, prénom, adresse de facturation),
- Données d'expédition (Nom, prénom, adresse d'expédition),
- Données de contact (nom, prénom, adresse postale, adresse email, numéro de téléphone)
- Données de connexion (Adresse IP)
- Données de localisation (Code Postal, pays IP, pays Carte)

Données d'ordre financier (Historique des transactions des porteurs, volume des transactions, multiplicité des cartes, historique des incidents de paiements des porteurs, BIN) Données relatives aux empreintes d'opération de paiement : Donnée de paiement + données personnelles (adresse IP, empreinte de l'équipement du titulaire de carte) dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations en conformité avec le considérant 49 du RGPD.

#### Catégories de Données Personnelles :

- Etat civil, données d'identification, images : Oui (Empreinte d'opération de paiement)
- Vie personnelle : Oui (Empreinte d'opération de paiement)
- Vie professionnelle : Oui (Empreinte d'opération de paiement)
- Information d'ordre économique/financier : Oui (Empreinte d'opération de paiement)
- Données de connexion : Oui (Empreinte d'opération de paiement)
- Données de localisation : Oui (Empreinte d'opération de paiement)
- Données sensibles (Article 9 du RGPD) : Non

Période pendant laquelle les données à caractère personnel collectées sont conservées à défaut de toute autre période de conservation prévue par les lois et règlements applicables ou imposés par une autorité de contrôle :

5 ans à compter de la fin de la relation d'affaires avec le responsable de traitement (conformité aux exigences légales et réglementaires applicables au sous-traitant en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme).

### IV. Catégories de personnes concernées

Le responsable du traitement peut transmettre des données à caractère personnel à destination des services du sous-traitant dans la mesure où celles-ci sont déterminées et contrôlées exclusivement par le responsable du traitement et qui peuvent concerner, sans limitation, les catégories suivantes de personnes :

- clients finaux

### V. Durée du traitement

Sauf accord contraire des parties, le sous-traitant est autorisé à traiter les données à caractère personnel pendant toute la durée prévue à l'article III de l'Annexe 6.

## SOUS-ANNEXE D – MESURE DE SECURITE

Le sous-traitant surveille de manière régulière et assure un maintien en conditions de sécurité technique et organisationnel garantissant la confidentialité, l'intégrité et la sécurité des données à caractère personnel (incluant la protection contre les accès non autorisés ou contre la mise en œuvre de traitements contraires au RGPD, la protection contre les destructions accidentelles ou malveillantes, la protection contre les atteintes en confidentialité, disponibilité ou en intégrité, la diffusion ou l'accès non autorisée aux données à caractère personnel) conformément à l'article 32 du RGPD.

La gouvernance en matière de sécurité du sous-traitant doit être organisée afin de :

- prévenir tout accès et usage non autorisé aux systèmes d'information hébergeant les traitements de données à caractère personnel (contrôle d'accès) ;
- garantir que les personnes autorisées à opérer les systèmes d'information hébergeant les traitements de données à caractère personnel n'ont accès aux données personnelles qu'en respect du besoin d'en connaître et que les données à caractère personnel concernées ne peuvent être lues, copiées, altérées ou supprimées sans autorisation dans le cadre de leur traitement, usage ou après stockage (contrôle d'accès);
- garantir que les données à caractère personnel ne peuvent être lues, copiées, altérées ou supprimées sans autorisation pendant leur transport, numérique ou non, et qu'il est possible de vérifier et de tracer l'ensemble des intermédiaires concourant à la transmission des données à caractère personnel (contrôle de transmission) ;
- garantir qu'il est possible de vérifier et de tracer si et par qui des données à caractère personnel ont été intégrées, altérées ou supprimées des systèmes d'information hébergeant les traitements de données à caractère personnel (contrôle d'accès en entrée);
- garantir que le traitement des données à caractère personnel est strictement réalisé conformément aux instructions du donneur d'ordre (contrôle d'origine) ;
- garantir que les données à caractère personnel sont protégées contre toute destruction accidentelle ou malveillante (contrôle de disponibilité) ; et
- garantir que les données à caractère personnel collectées pour des finalités différentes puissent faire l'objet de traitements distincts (en permettant, en particulier, que les mesures déployées pour garantir une séparation logique des données en fonction des typologies de recueil du consentement et/ou de catégories de personnes concernées, conformément aux instructions du responsable du traitement).

## ANNEXE 7 : SAQ A

Ci-après le SAQ-A validé par le Client prévu à l'article 10.7 des CGV, sous réserve de toutes modifications du Client déclarées à Payplug :

### Partie 1b. Auditeur

Fournir les informations suivantes pour tous les auditeurs impliqués dans l'évaluation. S'il n'y avait aucun auditeur pour un type d'auditeur donné, saisir Non Applicable.

Auditeur(s) de Sécurité Interne du PCI SSC

Nom(s) du ou des ISA :

Auditeur de Sécurité Qualifié

Nom de l'entreprise :

Adresse postale de l'entreprise :

Site web de l'entreprise :

Nom de l'Auditeur Principal :

Numéro de téléphone de l'auditeur :

Adresse e-mail de l'auditeur :

Numéro de certificat de l'auditeur :

### Partie 2. Sommaire Exécutif

**Partie 2a. Canaux de Paiement de l'Entreprise du Commerçant (sélectionner toutes les options qui s'appliquent) :**

Indiquer tous les canaux de paiement utilisés par l'entreprise qui sont inclus dans cette évaluation.

- Commande par correspondance/par téléphone (MOTO)  
 E-Commerce  
 Avec carte

Y a-t-il des canaux de paiement non inclus dans cette évaluation ?

Oui  Non

Si oui, indiquer le ou les canaux qui ne sont pas inclus dans l'évaluation et expliquer brièvement pourquoi le canal a été exclu.

### Partie 2b. Description du Rôle avec les Cartes de Paiement

Pour chaque canal de paiement inclus dans cette évaluation et sélectionné dans la partie 2a ci-dessus, décrire la manière dont l'entreprise stocke, traite et/ou transmet les données de compte.

| Canal      | Comment l'Entreprise Stocke, Traite et/ou Transmet les Données de Compte                                     |
|------------|--|
| E-Commerce | Externalisation du traitement, stockage et transport des données de compte auprès du PSP Payplug Enterprise. |
|            |  |
|            |  |

### Partie 2c. Description de l'Environnement des Cartes de Paiement

Fournir une description de **haut niveau** de l'environnement couvert par cette évaluation.

Par exemple :

- Connexions vers et depuis l'environnement de données de titulaire de carte (CDE).
- Composants système critiques au sein du CDE, tels que les dispositifs POI, les bases de données, les serveurs Web, etc., et tout autre composant de paiement nécessaire, le cas échéant.
- Composants système susceptibles d'avoir une incidence sur la sécurité des données de compte.

L'environnement E-Commerce externalise le traitement, le stockage et le transport des données de cartes de paiement auprès du PSP Payplug Enterprise, certifié PCI DSS PSP de niveau 1. Aucune donnée carte n'est traitée ou conservée.

Indiquer si l'environnement inclut une segmentation pour réduire le périmètre de l'évaluation.

(Se reporter à la section « Segmentation » du standard PCI DSS afin d'obtenir des directives sur la segmentation.)

Oui  Non

## Partie 2. Sommaire Exécutif (suite)

### Partie 2d. Emplacements/Installations dans le Périmètre

Énumérer tous les types d'emplacements/d'installations physiques (par exemple, les points de vente, les bureaux de l'entreprise, les centres de données, les centres d'appels et les salles de courrier) dans le périmètre de l'évaluation du standard PCI DSS.

| Type d'Installation                  | Nombre total d'emplacements<br>(Combien d'emplacements de ce type sont dans le périmètre) | Emplacement(s) de l'installation<br>(ville, pays) |
|--------------------------------------|---|---|
| Par exemple : Centre de données      | 3   | Boston, MA, USA                                   |
| Siège de la société avec son adresse |   |   |
|                                      |   |   |

### Partie 2e. Produits et Solutions Validés par le PCI SSC

Le commerçant utilise-t-il un élément identifié sur une liste du PCI SSC de produits et de solutions validés\*?

Oui  Non

Fournir les informations suivantes concernant chaque élément utilisé par le commerçant à partir des listes du PCI SSC de produits et de solutions validés.

| Nom du Produit ou de la Solution validés par le PCI SSC | Version du Produit ou de la Solution | Standard du PCI SSC selon lequel le produit ou la solution ont été validés | Numéro de référence de la liste du PCI SSC | Date d'expiration de la liste (JJ-MM-AAAA) |
|---|--------------------------------------|--|--|--|
| N/A   |                                      |  |  | JJ-MM-AAAA                                 |
|   |                                      |  |  | JJ-MM-AAAA                                 |
|   |                                      |  |  | JJ-MM-AAAA                                 |
|   |                                      |  |  | JJ-MM-AAAA                                 |

## Partie 2. Sommaire Exécutif (suite)

### Partie 2f. Prestataires de Services Tiers

L'entité entretient-elle des relations avec un ou plusieurs prestataires de services tiers qui :

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• Stockent, traitent ou transmettent les données de compte au nom de l'entité (par exemple, les passerelles de paiement, les processeurs de paiement, les prestataires de services de paiement (PSP) et le stockage hors site).</li> </ul>  | <input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non |
| <ul style="list-style-type: none"> <li>• Gèrent les composants système inclus dans le périmètre de l'évaluation de PCI DSS de l'entité– par exemple, via les services de mesures de sécurité du réseau, les services anti-malware, la gestion des incidents et des événements liés à la sécurité (SIEM), les centres de contact et d'appel, les services d'hébergement Web et les Fournisseurs de cloud IaaS, PaaS, SaaS et FaaS.</li> </ul> | <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non |
| <ul style="list-style-type: none"> <li>• Pourraient avoir une incidence sur la sécurité du CDE de l'entité (par exemple, les prestataires fournissant une assistance via un accès à distance et/ou les développeurs de logiciels sur mesure)</li> </ul>  | <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non |

**Si oui :**

| Nom du prestataire de services : | Description du ou des services fournis : |
|----------------------------------|--|
| Payplug Enterprise               | Acquisition des ordres de paiement       |
|                                  |  |

## Partie 2. Sommaire Exécutif (suite)

### Partie 2g. Synthèse de l'Évaluation

(SAQ - Section 2 et Annexes associées)

Indiquer ci-dessous toutes les réponses qui ont été sélectionnées pour chaque exigence du standard PCI DSS.

| Exigence de PCI DSS* | Réponses aux Exigences  |                          |                                     |                          |
|----------------------|---|--------------------------|-------------------------------------|--------------------------|
|                      | Plusieurs réponses peuvent être sélectionnées pour une exigence donnée. Indique toutes les réponses qui s'appliquent. |                          |                                     |                          |
|                      | En Place  | En Place avec CCW        | Non Applicable                      | Pas en Place             |
| Exigence 2 :         | <input checked="" type="checkbox"/>   | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Exigence 3 :         | <input checked="" type="checkbox"/>   | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Exigence 6 :         | <input checked="" type="checkbox"/>   | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Exigence 8 :         | <input checked="" type="checkbox"/>   | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Exigence 9 :         | <input type="checkbox"/>  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Exigence 11 :        | <input type="checkbox"/>  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Exigence 12 :        | <input checked="" type="checkbox"/>   | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |



## Partie 2h. Éligibilité pour Remplir le SAQ A

Le commerçant certifie son éligibilité pour remplir ce Questionnaire d'Auto-Évaluation car, pour ce canal de paiement :

|                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Le commerçant n'accepte que les transactions sans carte (e-commerce ou commande par courrier/téléphone).  |
| <input checked="" type="checkbox"/> | Tout le traitement des données de compte est entièrement sous-traité à un prestataire de services tiers (TPSP)/processeur de paiement conforme au standard PCI DSS ;  |
| <input checked="" type="checkbox"/> | Le commerçant ne stocke, ne traite ni ne transmet par voie électronique aucune donnée de compte sur les systèmes ou dans les locaux du commerçant, mais s'appuie entièrement sur un ou plusieurs TSP pour gérer toutes ces fonctions.                               |
| <input checked="" type="checkbox"/> | Le commerçant a examiné le ou les formulaires d'Attestation de Conformité PCI DSS pour son ou ses TPSP et a confirmé que le ou les TPSP sont conformes au standard PCI DSS pour les services utilisés par le commerçant.  |
| <input checked="" type="checkbox"/> | Toutes les données de compte que le commerçant pourrait conserver sont sur papier (par exemple, des rapports ou des reçus imprimés), et ces documents ne sont pas reçus par voie électronique.  |
| <input checked="" type="checkbox"/> | <i>Par ailleurs, pour les canaux de commerce électronique :</i><br>Tous les éléments de la ou des pages/formulaires de paiement livrés au navigateur du client proviennent uniquement et directement d'un TPSP/processeur de paiement conforme au standard PCI DSS. |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*   |                                     |                          |                          |                          |
|---|--|--|-------------------------------------|--------------------------|--------------------------|--------------------------|
|   |  | (Cocher une réponse pour chaque exigence)  |                                     |                          |                          |                          |
|   |  | En Place   | En Place avec CCW                   | Non Applicable           | Pas en Place             |                          |
| <b>2.2</b> Les composants système sont configurés et gérés en toute sécurité.   |  |  |                                     |                          |                          |                          |
| <i>Remarque : Pour le SAQ A, l'exigence 2.2.2 s'applique aux comptes par défaut des fournisseurs de commerce électronique des commerçants sur les serveurs Web.</i> |  |  |                                     |                          |                          |                          |
| <b>2.2.2</b>  | <p>Les comptes par défaut du fournisseur sont gérés comme suit :</p> <ul style="list-style-type: none"> <li>Si le ou les comptes par défaut du fournisseur sont utilisés, le mot de passe par défaut est modifié conformément à l'exigence 8.3.6.</li> <li>Si le ou les comptes par défaut du fournisseur ne sont pas utilisés, le compte est supprimé ou désactivé.</li> </ul> <p>(suite)</p> | <ul style="list-style-type: none"> <li>Examiner les standards relatifs à la configuration du système.</li> <li>Examiner la documentation du fournisseur.</li> <li>Observer un administrateur système se connectant à l'aide des comptes par défaut du fournisseur.</li> <li>Examiner les fichiers de configuration.</li> </ul> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus | Réponse*                                  |                   |                |              |
|---|--------------|---|-------------------|----------------|--------------|
|   |              | (Cocher une réponse pour chaque exigence) |                   |                |              |
|   |              | En Place                                  | En Place avec CCW | Non Applicable | Pas en Place |
| <b>Notes d'Applicabilité</b>  |              |   |                   |                |              |
| <p>Cela s'applique à TOUS les comptes et mots de passe par défaut des fournisseurs, y compris, sans toutefois s'y limiter, ceux utilisés avec des valeurs par défaut par les systèmes d'exploitation, les logiciels qui fournissent des services de sécurité, les comptes d'application et système, les terminaux de point de vente (POS), les applications de paiement et le Protocole simplifié de gestion de réseau (SNMP).</p> <p>Cette exigence s'applique également lorsqu'un composant système n'est pas installé dans l'environnement d'une entité ; par exemple, des logiciels et des applications qui font partie du CDE et qui sont accessibles via un service d'abonnement cloud.</p> |              |   |                   |                |              |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*   |                                     |                          |                          |                          |
|--|---|--|-------------------------------------|--------------------------|--------------------------|--------------------------|
|  |   | (Cocher une réponse pour chaque exigence)  |                                     |                          |                          |                          |
|  |   | En Place   | En Place avec CCW                   | Non Applicable           | Pas en Place             |                          |
| <b>3.1</b> Les processus et mécanismes de protection des données de compte stockées sont définis et compris. |   |  |                                     |                          |                          |                          |
| <b>3.1.1</b>   | <p>Toutes les politiques de sécurité et procédures opérationnelles identifiées dans l'exigence 3 sont :</p> <ul style="list-style-type: none"> <li>Documentées.</li> <li>Tenues à jour.</li> <li>Utilisées.</li> <li>Connues de toutes les parties concernées.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner la documentation.</li> <li>Interroger le personnel.</li> </ul> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*<br>(Cocher une réponse pour chaque exigence) |                          |                          |                          |
|--|---|---|--------------------------|--------------------------|--------------------------|
|  |   | En Place  | En Place avec CCW        | Non Applicable           | Pas en Place             |
| <b>3.2 Le stockage des données de compte est réduit au minimum.</b>  |   |   |                          |                          |                          |
| <b>3.2.1</b><br>Le stockage des données de compte est réduit au minimum grâce à la mise en œuvre de politiques, procédures et processus de conservation et d'élimination des données qui incluent au moins les éléments suivants : <ul style="list-style-type: none"> <li>Couverture de tous les emplacements des données de compte stockées.</li> <li>Couverture de toutes les données d'authentification sensibles (SAD) stockées avant la fin de l'autorisation. <i>Cette note est une bonne pratique jusqu'à sa date d'entrée en vigueur ; se reporter aux Notes d'Applicabilité ci-dessous pour plus de détails.</i></li> <li>Limiter la quantité de stockage des données et la durée de conservation à ce qui est requis pour les exigences légales ou réglementaires et/ou commerciales.</li> <li>Des exigences de rétention spécifiques pour les données de compte stockées qui définissent la durée de la période de conservation et incluent une justification commerciale documentée.</li> <li>Des processus de suppression sécurisée ou rendre des données de compte irrécupérables lorsqu'elles ne sont plus nécessaires conformément à la politique de conservation.</li> </ul> Un processus pour vérifier, au moins une fois tous les trois mois, que les données de compte stockées dépassant la période de conservation définie ont été supprimées en toute sécurité ou rendues irrécupérables.<br><i>(suite)</i> | <ul style="list-style-type: none"> <li>Examiner les politiques, procédures et processus de rétention et de suppression des données.</li> <li>Interroger le personnel.</li> <li>Examiner les fichiers et les enregistrements système sur les composants système où les données de compte sont stockées.</li> <li>Observer les mécanismes utilisés pour rendre les données de compte irrécupérables.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus | Réponse*<br>(Cocher une réponse pour chaque exigence) |                   |                |              |  |  |  |  |
|--|--------------|---|-------------------|----------------|--------------|--|--|--|--|
|  |              | En Place  | En Place avec CCW | Non Applicable | Pas en Place |  |  |  |  |
| <b>Notes d'Applicabilité</b>   |              |   |                   |                |              |  |  |  |  |
| Lorsque les données de compte sont stockées par un TPSP (par exemple, dans un environnement cloud), les entités sont tenues de collaborer avec leurs prestataires de services afin de comprendre comment le TPSP satisfait à cette exigence pour l'entité. Les considérations incluent de s'assurer que toutes les instances géographiques d'un élément de données sont supprimées en toute sécurité.<br><i>La puce ci-dessus (concernant la couverture des SAD stockées avant l'achèvement de l'autorisation) est une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera requise dans le cadre de l'exigence 3.2.1 et doit être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i> |              |   |                   |                |              |  |  |  |  |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*<br>(Cocher une réponse pour chaque exigence) |                          |                          |                          |
|--|---|---|--------------------------|--------------------------|--------------------------|
|  |   | En Place  | En Place avec CCW        | Non Applicable           | Pas en Place             |
| <b>6.3 Les vulnérabilités de sécurité sont identifiées et corrigées.</b>   |   |   |                          |                          |                          |
| <b>6.3.1</b><br>Les vulnérabilités de sécurité sont identifiées et gérées de la manière suivante : <ul style="list-style-type: none"> <li>Les nouvelles vulnérabilités de sécurité sont identifiées à l'aide de sources reconnues par l'industrie pour les informations sur les vulnérabilités de sécurité, y compris les alertes des équipes internationales et nationales d'intervention en cas d'urgence informatique (CERT).</li> <li>Les vulnérabilités se voient attribuer un classement de risques basé sur les meilleures pratiques de l'industrie et la prise en compte de l'incidence potentielle.</li> <li>Les classements des risques identifient, au minimum, toutes les vulnérabilités considérées comme à haut risque ou critiques pour l'environnement.</li> <li><i>Point intentionnellement laissé vide pour ce SAQ.</i></li> </ul> | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Interroger le personnel responsable.</li> <li>Examiner la documentation.</li> <li>Observer les processus.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus  | Réponse*                                  |                          |                          |                          |
|---|---|---|--------------------------|--------------------------|--------------------------|
|   |   | (Cocher une réponse pour chaque exigence) |                          |                          |                          |
|   |   | En Place                                  | En Place avec CCW        | Non Applicable           | Pas en Place             |
| <b>6.3.3</b> Tous les composants système sont protégés contre les vulnérabilités connues en installant les correctifs/mises à jour de sécurité applicables comme suit : <ul style="list-style-type: none"> <li>Les correctifs/mises à jour critiques ou de haute sécurité sont installés dans le mois suivant leur publication.</li> <li>Point intentionnellement laissé vide pour ce SAQ.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Examiner les composants système et les logiciels connexes.</li> <li>Comparer la liste des correctifs de sécurité installés aux listes de correctifs récents des fournisseurs.</li> </ul> | <input checked="" type="checkbox"/>       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**6.4** Les applications Web destinées au public sont protégées contre les attaques.

**Remarque :** Pour le SAQ A, l'exigence 6.4.3 s'applique au(x) site(s) Web d'un commerçant qui inclut la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un cadre en ligne ou un iFrame).

|  |   |                          |                          |                                     |                          |
|--|---|--------------------------|--------------------------|-------------------------------------|--------------------------|
| <b>6.4.3</b> Tous les scripts de la page de paiement qui sont chargés et exécutés dans le navigateur du client sont gérés comme suit : <ul style="list-style-type: none"> <li>Une méthode est mise en œuvre pour confirmer que chaque script est autorisé.</li> <li>Une méthode est mise en œuvre pour assurer l'intégrité de chaque script.</li> <li>Un inventaire de tous les scripts est maintenu avec une justification écrite expliquant pourquoi chacun est nécessaire.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Interroger le personnel responsable.</li> <li>Examiner les registres d'inventaire.</li> <li>Examiner les configurations du système.</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
|  | <ul style="list-style-type: none"> <li>Examiner les registres d'inventaire.</li> </ul>  | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
|  | <ul style="list-style-type: none"> <li>Examiner les configurations du système.</li> </ul>   | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS | Tests Prévus | Réponse*                                  |                   |                |              |
|---------------------|--------------|---|-------------------|----------------|--------------|
|                     |              | (Cocher une réponse pour chaque exigence) |                   |                |              |
|                     |              | En Place                                  | En Place avec CCW | Non Applicable | Pas en Place |

**8.2** L'identification des utilisateurs et les comptes associés pour les utilisateurs et les administrateurs sont strictement gérés tout au long du cycle de vie d'un compte.

|   |  |                                     |                          |                          |                          |
|---|--|-------------------------------------|--------------------------|--------------------------|--------------------------|
| <b>8.2.1</b> Tous les utilisateurs reçoivent un identifiant unique avant que l'accès aux composants système ou aux données des titulaires de cartes ne soit autorisé. | <ul style="list-style-type: none"> <li>Interroger le personnel responsable.</li> <li>Examiner les journaux d'audit et autres preuves.</li> </ul> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--|-------------------------------------|--------------------------|--------------------------|--------------------------|

| Exigence de PCI DSS   | Tests Prévus  | Réponse*                                  |                          |                          |                          |
|---|---|---|--------------------------|--------------------------|--------------------------|
|   |   | (Cocher une réponse pour chaque exigence) |                          |                          |                          |
|   |   | En Place                                  | En Place avec CCW        | Non Applicable           | Pas en Place             |
| <b>8.2.2</b> Les comptes de groupe, partagés ou génériques, ou d'autres « credentials » partagés ne sont utilisés que si nécessaire sur une base exceptionnelle et sont gérés comme suit : <ul style="list-style-type: none"> <li>L'utilisation du compte est interdite à moins que cela ne soit nécessaire dans des circonstances exceptionnelles.</li> <li>L'utilisation est limitée au temps nécessaire à la circonstance exceptionnelle.</li> <li>La justification commerciale de l'utilisation est documentée.</li> <li>L'utilisation est explicitement approuvée par la direction.</li> <li>L'identité de l'utilisateur individuel est confirmée avant que l'accès à un compte ne soit accordé.</li> <li>Chaque action entreprise est attribuable à un seul utilisateur.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner les listes des comptes d'utilisateurs sur les composants système et la documentation applicable.</li> <li>Examiner les politiques et procédures d'authentification.</li> <li>Interroger les administrateurs système.</li> </ul> | <input checked="" type="checkbox"/>       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b><br>Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction (comme les identifiants utilisés par les caissiers sur les terminaux de point de vente).  |   |   |                          |                          |                          |
| <b>8.2.5</b> L'accès des utilisateurs dont le contrat a été résilié est immédiatement révoqué.  | <ul style="list-style-type: none"> <li>Examiner les sources d'informations pour les utilisateurs dont le contrat a été résilié.</li> <li>Examiner les listes d'accès des utilisateurs actuels.</li> <li>Interroger le personnel responsable.</li> </ul>                         | <input checked="" type="checkbox"/>       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*                                  |                          |                                     |                          |
|---|--|---|--------------------------|-------------------------------------|--------------------------|
|   |  | (Cocher une réponse pour chaque exigence) |                          |                                     |                          |
|   |  | En Place                                  | En Place avec CCW        | Non Applicable                      | Pas en Place             |
| <b>8.3 Une authentification robuste pour les utilisateurs et les administrateurs est établie et gérée.</b>  |  |   |                          |                                     |                          |
| <b>8.3.1</b> Tous les accès d'utilisateurs aux composants système pour les utilisateurs et les administrateurs sont authentifiés via au moins l'un des facteurs d'authentification suivants : <ul style="list-style-type: none"> <li>• Quelque chose que vous connaissez, comme un mot de passe ou une phrase secrète.</li> <li>• Un objet que vous possédez, tel qu'un dispositif à token ou une carte à puce.</li> <li>• Quelque chose que vous êtes, comme un élément biométrique.</li> </ul>  | <ul style="list-style-type: none"> <li>• Examiner la documentation décrivant le ou les facteurs d'authentification utilisés.</li> <li>• Pour chaque type de facteur d'authentification utilisé avec chaque type de composant système, observer le processus d'authentification.</li> </ul> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b><br>Cette exigence n'est pas destinée à s'appliquer aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction (comme les identifiants utilisés par les caissiers sur les terminaux de point de vente).<br>Cette exigence ne remplace pas les exigences d'authentification à plusieurs facteurs (MFA), mais s'applique aux systèmes dans le périmètre qui ne sont pas autrement soumis aux exigences de la MFA.<br>Un certificat numérique est une option valide pour « quelque chose que vous avez » s'il est unique pour un utilisateur particulier. |  |   |                          |                                     |                          |
| <b>8.3.5</b> Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils sont définis et réinitialisés pour chaque utilisateur comme suit : <ul style="list-style-type: none"> <li>• Réglés sur une valeur unique pour la première utilisation et lors de la réinitialisation.</li> <li>• Doivent être modifiés immédiatement après la première utilisation.</li> </ul>   | <ul style="list-style-type: none"> <li>• Examiner les procédures de définition et de réinitialisation des mots de passe/phrases secrètes.</li> <li>• Observer le personnel chargé de la sécurité.</li> </ul>   | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*                                  |                          |                                     |                          |
|--|---|---|--------------------------|-------------------------------------|--------------------------|
|  |   | (Cocher une réponse pour chaque exigence) |                          |                                     |                          |
|  |   | En Place                                  | En Place avec CCW        | Non Applicable                      | Pas en Place             |
| <b>8.3.6</b> Si des mots de passe/phrases secrètes sont utilisés comme facteurs d'authentification pour répondre à l'exigence 8.3.1, ils devront répondre au niveau de complexité minimum suivant : <ul style="list-style-type: none"> <li>• Une longueur minimale de 12 caractères (ou SI le système ne prend pas en charge 12 caractères, une longueur minimale de huit caractères).</li> <li>• Contenir à la fois des caractères numériques et alphabétiques.</li> </ul>  | <ul style="list-style-type: none"> <li>• Examiner les paramètres de la configuration du système.</li> </ul> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b><br>Cette exigence n'est pas destinée à s'appliquer : <ul style="list-style-type: none"> <li>• Aux comptes d'utilisateurs dans les terminaux de points de vente qui n'ont accès qu'à un seul numéro de carte à la fois afin de faciliter une seule transaction (comme les identifiants utilisés par les caissiers sur les terminaux de point de vente).</li> <li>• Aux comptes d'applications ou système, qui sont régis par les exigences de la section 8.6.</li> </ul> <i>Cette exigence reste une bonne pratique jusqu'au 31 mars 2025, après quoi elle sera obligatoire et devra être pleinement prise en compte lors d'une évaluation du standard PCI DSS.</i><br>Jusqu'au 31 mars 2025, les mots de passe doivent avoir une longueur minimale de sept caractères conformément à l'exigence 8.2.3 du standard PCI DSS v3.2.1. |   |   |                          |                                     |                          |
| <b>8.3.7</b> Les personnes ne sont pas autorisées à soumettre un nouveau mot de passe/phrase secrète qui soient les mêmes que ceux des quatre derniers mots de passe/phrase secrètes utilisés.   | <ul style="list-style-type: none"> <li>• Examiner les paramètres de la configuration du système.</li> </ul> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*                                  |                          |                          |                          |
|---|--|---|--------------------------|--------------------------|--------------------------|
|   |  | (Cocher une réponse pour chaque exigence) |                          |                          |                          |
|   |  | En Place                                  | En Place avec CCW        | Non Applicable           | Pas en Place             |
| <b>8.3.9</b> Si les mots de passe/phrases secrètes sont utilisés comme seul facteur d'authentification pour l'accès utilisateur (c'est-à-dire dans toute mise en œuvre d'authentification à un seul facteur), alors soit : <ul style="list-style-type: none"> <li>• Les mots de passe/phrases secrètes sont modifiés au moins une fois tous les 90 jours,</li> <li><b>OU</b></li> <li>• La posture de sécurité des comptes est analysée de manière dynamique et l'accès en temps réel aux ressources est automatiquement déterminé en conséquence.</li> </ul> | <ul style="list-style-type: none"> <li>• Inspecter les paramètres de la configuration du système.</li> </ul> | <input checked="" type="checkbox"/>       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*                                  |                          |                                     |                          |
|--|---|---|--------------------------|-------------------------------------|--------------------------|
|  |   | (Cocher une réponse pour chaque exigence) |                          |                                     |                          |
|  |   | En Place                                  | En Place Avec CCW        | Non Applicable                      | Pas en Place             |
| <b>9.4</b> Les supports contenant les données des titulaires de carte sont stockés, consultés, distribués et détruits de manière sécurisée.  |   |   |                          |                                     |                          |
| <b>Remarque :</b> Pour SAQ A, les exigences à la section 9.4 s'appliquent uniquement aux commerçants avec des documents papier (par exemple, des reçus ou des rapports imprimés) avec des données de compte, y compris des numéros de comptes primaires (PAN). |   |   |                          |                                     |                          |
| 9.4.1  | Tous les supports contenant des données de titulaire de carte sont physiquement sécurisés.  | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 9.4.1.1  | Les sauvegardes sur des supports hors ligne avec les données des titulaires de cartes sont stockées dans un emplacement sécurisé.   | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 9.4.2  | Tous les supports contenant des données de titulaires de cartes sont classés en fonction de la sensibilité des données.   | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 9.4.3  | Les supports avec les données des titulaires de cartes envoyées à l'extérieur de l'installation sont sécurisés comme suit :<br><ul style="list-style-type: none"> <li>Point intentionnellement laissé vide pour ce SAQ.</li> <li>Les supports sont envoyés par courrier sécurisé ou par un autre mode de livraison pouvant être suivi avec précision.</li> <li>Point intentionnellement laissé vide pour ce SAQ.</li> </ul> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus   | Réponse*                                  |                          |                                     |                          |
|--|--|---|--------------------------|-------------------------------------|--------------------------|
|  |  | (Cocher une réponse pour chaque exigence) |                          |                                     |                          |
|  |  | En Place                                  | En Place Avec CCW        | Non Applicable                      | Pas en Place             |
| 9.4.4  | La direction approuve tous les supports avec des données de titulaires de cartes qui sont déplacés hors de l'installation (y compris lorsque les supports sont distribués à des personnes individuelles).  | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b>   |  |   |                          |                                     |                          |
| Les personnes qui approuvent les mouvements des supports devraient avoir le niveau approprié d'autorité de gestion pour accorder cette approbation. Cependant, il n'est pas spécifiquement exigé que ces personnes aient l'indication « responsable » dans leur titre. |  |   |                          |                                     |                          |
| 9.4.6  | Les documents papier contenant les données des titulaires de cartes sont détruits lorsqu'ils ne sont plus nécessaires pour des raisons commerciales ou juridiques, comme suit :<br><ul style="list-style-type: none"> <li>Les documents sont déchiquetés, incinérés ou réduits en pâte afin que les données des titulaires de cartes ne puissent pas être reconstituées.</li> <li>Les documents sont stockés dans des conteneurs de stockage sécurisés avant destruction.</li> </ul> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*                                  |                          |                                     |                          |
|---|--|---|--------------------------|-------------------------------------|--------------------------|
|   |  | (Cocher une réponse pour chaque exigence) |                          |                                     |                          |
|   |  | En Place                                  | En Place Avec CCW        | Non Applicable                      | Pas en Place             |
| <b>11.3</b> Les vulnérabilités externes et internes sont régulièrement identifiées, priorisées et traitées. |  |   |                          |                                     |                          |
| 11.3.2  | Les analyses de vulnérabilités externes sont effectuées comme suit :<br><ul style="list-style-type: none"> <li>Au moins une fois tous les trois mois.</li> <li>Par un Fournisseur d'Analyse Agréé PCI SSC (ASV).</li> <li>Les vulnérabilités sont résolues et les exigences du <i>Guide du Programme</i> de l'ASV pour une analyse réussie sont respectées.</li> <li>Des réanalyses sont effectuées au besoin pour confirmer que les vulnérabilités sont résolues conformément aux exigences du <i>Guide du Programme</i> de l'ASV pour une analyse réussie.</li> </ul> <i>(suite)</i> | <input type="checkbox"/>                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |



| Exigence de PCI DSS   | Tests Prévus  | Réponse*   |                          |                          |                                     |                          |
|---|---|--|--------------------------|--------------------------|-------------------------------------|--------------------------|
|   |   | (Cocher une réponse pour chaque exigence)  |                          |                          |                                     |                          |
|   |   | En Place   | En Place Avec CCW        | Non Applicable           | Pas en Place                        |                          |
| <b>Notes d'Applicabilité</b><br>Pour la conformité initiale au standard PCI DSS, il n'est pas nécessaire que quatre analyses de réussite soient effectuées dans les 12 mois si l'auditeur vérifie : 1) le résultat de l'analyse le plus récent était une analyse réussie, 2) l'entité a documenté des politiques et des procédures exigeant une analyse au moins une fois tous les trois mois, et 3) les vulnérabilités notées dans les résultats de l'analyse ont été corrigées comme indiqué dans une ou plusieurs nouvelles analyses.<br>Cependant, pour les années suivantes après l'évaluation initiale du standard PCI DSS, des analyses réussies au moins tous les trois mois doivent avoir eu lieu.<br>Les outils d'analyse de l'ASV peuvent analyser une vaste gamme de types de réseaux et de topologies. Tous les détails concernant l'environnement cible (par exemple, les équilibres de charge, les fournisseurs tiers, les ISP, les configurations spécifiques, les protocoles utilisés, les interférences d'analyse) doivent être réglés entre l'ASV et le client de l'analyse.<br>Se reporter au Guide du Programme de l'ASV publié sur le site Web du PCI SSC afin de connaître les responsabilités du client de l'analyse, la préparation de l'analyse, etc. |   |  |                          |                          |                                     |                          |
| 11.3.2.1  | Les analyses externes des vulnérabilités sont effectuées après toute modification importante comme suit : <ul style="list-style-type: none"> <li>• Les vulnérabilités notées 4,0 ou plus par le CVSS sont résolues.</li> <li>• De nouvelles analyses sont effectuées au besoin.</li> <li>• Les analyses sont effectuées par du personnel qualifié et l'indépendance organisationnelle du testeur existe (il n'est pas nécessaire qu'il soit un QSA ou un ASV).</li> </ul> | <ul style="list-style-type: none"> <li>• Examiner les documents de contrôle des modifications.</li> <li>• Interroger le personnel.</li> <li>• Examiner les rapports d'analyse externe et, le cas échéant, des nouvelles analyses.</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*  |                          |                                     |                                     |                          |
|--|---|---|--------------------------|-------------------------------------|-------------------------------------|--------------------------|
|  |   | (Cocher une réponse pour chaque exigence)   |                          |                                     |                                     |                          |
|  |   | En Place  | En Place Avec CCW        | Non Applicable                      | Pas en Place                        |                          |
| <b>11.6</b> Les modifications non autorisées sur les pages de paiement sont détectées et traitées.   |   |   |                          |                                     |                                     |                          |
| <b>Remarque :</b> Pour le SAQ A, l'exigence 11.6.1 s'applique au site Web d'un commerçant qui inclut la page/le formulaire de paiement intégré d'un TPSP/processeur de paiement (par exemple, un cadre en ligne ou un iFrame). |   |   |                          |                                     |                                     |                          |
| 11.6.1   | Un mécanisme de détection des modifications et des altérations est déployé de la manière suivante : <ul style="list-style-type: none"> <li>• Alerter le personnel des modifications non autorisées (y compris les indicateurs de compromission, de changements, d'ajouts et de suppressions) des en-têtes HTTP et du contenu des pages de paiement reçus par le navigateur du consommateur.</li> <li>• Le mécanisme est configuré pour évaluer l'en-tête HTTP reçu et la page de paiement.</li> <li>• Les fonctions du mécanisme sont exécutées comme suit :               <ul style="list-style-type: none"> <li>– Au moins une fois tous les sept jours</li> </ul> <b>OU</b> <ul style="list-style-type: none"> <li>– Périodiquement, (à la fréquence définie dans l'analyse des risques ciblée de l'entité, qui est réalisée selon tous les éléments spécifiés dans l'exigence 12.3.1).</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Examiner les paramètres système et les paramètres de configuration du mécanisme.</li> <li>• Examiner les pages de paiement surveillées.</li> <li>• Examiner les résultats des activités de surveillance.</li> <li>• Examiner les paramètres de configuration du mécanisme.</li> <li>• Examiner les paramètres de configuration.</li> <li>• Interroger le personnel responsable.</li> <li>• Le cas échéant, examiner l'analyse des risques ciblée.</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
|  |   | <input type="checkbox"/>  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                          |
|  |   | <input type="checkbox"/>  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                          |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*  |                                     |                          |                          |                          |
|--|---|---|-------------------------------------|--------------------------|--------------------------|--------------------------|
|  |   | (Cocher une réponse pour chaque exigence)   |                                     |                          |                          |                          |
|  |   | En Place  | En Place Avec CCW                   | Non Applicable           | Pas en Place             |                          |
| <b>12.8</b> Le risque pour les fonds documentaires associés aux relations avec les prestataires de services tiers (TPSP) est géré. |   |   |                                     |                          |                          |                          |
| 12.8.1   | Une liste de tous les prestataires de services tiers (TPSP) avec lesquels les données de compte sont partagées ou qui pourraient affecter la sécurité des données de compte, est conservée, y compris une description pour chacun des services fournis. | <ul style="list-style-type: none"> <li>• Examiner les politiques et les procédures.</li> <li>• Examiner la liste des TPSP.</li> </ul> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS  | Tests Prévus  | Réponse*<br>(Cocher une réponse pour chaque exigence) |                          |                          |                          |
|--|---|---|--------------------------|--------------------------|--------------------------|
|  |   | En Place  | En Place Avec CCW        | Non Applicable           | Pas en Place             |
| <b>12.8.2</b> Les accords écrits avec les TPSP sont maintenus comme suit : <ul style="list-style-type: none"> <li>Des accords écrits sont maintenus avec tous les TPSP avec lesquels les données de compte sont partagées ou qui pourraient avoir une incidence sur la sécurité du CDE.</li> <li>Les accords écrits comprennent des reconnaissances des TPSP qu'ils sont responsables de la sécurité des données de compte que les TPSP possèdent ou autrement stockent, traitent ou transmettent au nom de l'entité, ou dans la mesure où ils pourraient avoir une incidence sur la sécurité du CDE de l'entité.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Examiner les accords écrits avec les TPSP.</li> </ul>                                | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b><br>La formulation exacte d'une reconnaissance dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas à inclure la formulation exacte fournie dans cette exigence.<br>La preuve qu'un TPSP respecte les exigences du standard PCI DSS (par exemple, une Attestation de Conformité au standard PCI DSS (AOC) ou une déclaration sur le site Web d'une entreprise) n'est pas la même chose qu'un accord écrit spécifié dans cette exigence.   |   |   |                          |                          |                          |
| <b>12.8.3</b> Un processus établi est mis en œuvre pour engager les TPSP, y compris une diligence raisonnable appropriée avant l'engagement.   | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Examiner les justificatifs.</li> <li>Interroger le personnel responsable.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*<br>(Cocher une réponse pour chaque exigence) |                          |                          |                          |
|---|--|---|--------------------------|--------------------------|--------------------------|
|   |  | En Place  | En Place Avec CCW        | Non Applicable           | Pas en Place             |
| <b>12.8.4</b> Un programme est mis en œuvre pour surveiller l'état de conformité au standard PCI DSS des TPSP au moins une fois tous les 12 mois.   | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Examiner la documentation.</li> <li>Interroger le personnel responsable.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>Notes d'Applicabilité</b><br>Lorsqu'une entité passe un accord avec un TPSP pour satisfaire aux exigences du standard PCI DSS au nom de l'entité (par exemple, via un service de pare-feu), l'entité doit collaborer avec le TPSP pour s'assurer que les exigences applicables du standard PCI DSS sont satisfaites. Si le TPSP ne satisfait pas aux exigences applicables du standard PCI DSS, ces exigences ne sont pas non plus « En Place » chez l'entité. |  |   |                          |                          |                          |
| <b>12.8.5</b> Des informations sont conservées sur les exigences du standard PCI DSS qui sont gérées par chaque TPSP, celles qui sont gérées par l'entité et celles qui sont partagées entre le TPSP et l'entité.   | <ul style="list-style-type: none"> <li>Examiner les politiques et les procédures.</li> <li>Examiner la documentation.</li> <li>Interroger le personnel responsable.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| Exigence de PCI DSS   | Tests Prévus   | Réponse*<br>(Cocher une réponse pour chaque exigence) |                          |                          |                          |
|---|--|---|--------------------------|--------------------------|--------------------------|
|   |  | En Place  | En Place Avec CCW        | Non Applicable           | Pas en Place             |
| <b>12.10</b> Les incidents de sécurité soupçonnés et confirmés qui pourraient avoir un impact sur le CDE sont traités immédiatement.  |  |   |                          |                          |                          |
| <b>12.10.1</b> Un plan de réponse aux incidents existe et est prêt à être activé en cas d'incident de sécurité soupçonné ou avéré. Le plan comprend, mais n'est pas limité à : <ul style="list-style-type: none"> <li>Les rôles, responsabilités et stratégies de communication et de contact en cas d'incident de sécurité soupçonné ou avéré, y compris la notification des marques de paiement et des acquéreurs, au minimum.</li> <li>Les procédures de réponse aux incidents avec des activités de confinement et d'atténuation spécifiques pour différents types d'incidents.</li> <li>Les procédures de reprise et de continuité de l'activité.</li> <li>Les processus de sauvegarde des données.</li> <li>L'analyse des exigences légales en matière de signalement des compromissions.</li> <li>La couverture et les réponses de tous les composants système critiques.</li> <li>La référence ou l'inclusion des procédures de réponse aux incidents des marques de paiement.</li> </ul> | <ul style="list-style-type: none"> <li>Examiner le plan de réponse aux incidents.</li> <li>Interroger le personnel.</li> <li>Examiner la documentation des incidents précédemment signalés.</li> </ul> | <input checked="" type="checkbox"/>                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

## Annexe C : Explication des Exigences Indiquées comme Non Applicables

Cette Annexe doit être remplie pour chaque exigence pour laquelle l'option Non Applicable a été sélectionnée.

| Exigence       | Raison pour laquelle l'Exigence est Non Applicable                                |
|----------------|---|
| Par exemple :  |   |
| Exigence 3.5.1 | Les données de compte ne sont jamais stockées par voie électronique               |
| 6.4.3          | Bonne pratique jusqu'au 31 mars 2025  |
| 8.3.1          | Externalisation du traitement, stockage, transport à un PSP                       |
| 8.3.5          | Externalisation du traitement, stockage, transport à un PSP                       |
| 8.3.6          | Bonne pratique jusqu'au 31 mars 2025  |
| 8.3.7          | Externalisation du traitement, stockage, transport à un PSP                       |
| 9.4            | Pas de document papier avec des données de compte                                 |
| 11.3           | Obligation introduite par le standard 4.0, standard 3.2.1 actif jusqu'à mars 2024 |
| 11.6.1         | Bonne pratique jusqu'au 31 mars 2025  |
|                |   |

### 4 Section 3 : Détails de la Validation et de l'Attestation

#### Partie 3. Validation du Standard PCI DSS

Cette AOC est basé sur les résultats notés dans le SAQ A-EP (Section 2), en date du (Date d'achèvement de l'auto-évaluation JJ-MM-AAAA). Sur la base des résultats documentés dans le SAQ A-EP indiqué ci-dessus, chaque signataire identifié dans l'une des parties 3b-3d, selon le cas, affirme le statut de conformité suivant pour le commerçant identifié dans la partie 2 de ce document.

Sélectionner une Option :

|                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <b>Conforme</b> : Toutes les sections du SAQ de PCI DSS sont complètes et toutes les exigences sont marquées comme étant soit 1) En Place, 2) En Place avec CCW, ou 3) Non Applicables, ce qui donne une note globale <b>CONFORME</b> ; ainsi (Nom de l'Entreprise du Commerçant) a démontré sa conformité à toutes les exigences du standard PCI DSS incluses dans ce SAQ. |
|-------------------------------------|---|

#### Partie 3a. Confirmation du Commerçant

Le ou les signataires confirment :

(Sélectionner toutes les options qui s'appliquent)

|                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Le Questionnaire d'Auto-Évaluation A-EP du standard PCI DSS, version 4.0 a été rempli conformément aux instructions qui y figurent.  |
| <input checked="" type="checkbox"/> | Toutes les informations contenues dans le SAQ susmentionné et dans cette attestation représentent fidèlement les résultats de l'évaluation du commerçant à tous les égards importants. |
| <input checked="" type="checkbox"/> | Les mesures de sécurité du standard PCI DSS seront maintenues à tout moment, selon l'environnement du commerçant.  |