Conditions d'acceptation des paiements en vente à distance

eZyness

CONDITIONS GENERALES D'ADHESION A LA SOLUTION D'ACCEPTATION

Article 1 - Définitions

Accepteur
Acteur qui accepte la carte. Dans le cas présent, il s'agit de l'Agent (ci-après, le « Marchand »).

Acquéreur
Etablissement financier qui reçoit des informations financières concernant une transaction de la part de l'Accepteur et qui enregistre ces informations dans le système d'échanges. Dans le cas présent, il s'agit d'eZyness.

Bénéficiaire
Personne physique ou morale qui exploite une Boutique, il est bénéficiaire des fonds encaissés par le Marchand pour son compte via la Page de Paiement qu'il a intégré à sa Boutique. Dans le cas présent il s'agit du Titulaire.

Boutique
Boutique virtuelle créée, réalisée et présentée sur Internet, sous la responsabilité du Bénéficiaire, dans le but de commercialiser une offre de produits, services ou informations. La Boutique intègre la Page de Paiement fournie par le Marchand dans le cadre de son Offre d'acceptation des paiements en vente à distance.

Client
Tout titulaire de la carte transmettant son numéro de carte bancaire à des fins de paiement, via la Page de Paiement, soit en utilisant le réseau Internet pour se connecter à la Boutique. Dans le cas présent, il s'agit de l'Acheteur.

Donnée à caractère personnel / Données personnelles
Toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres.

Interface
Interface informatique permettant au Marchand de réaliser les opérations décrites à l'article 3.3 des présentes conditions générales.

Marchand
Personne physique ou morale qui édite et contrôle la Page de paiement de la Boutique. Le Marchand qui utilise la Solution d'acceptation est enregistré auprès d'eZyness. Le Marchand utilise la solution pour accepter les paiements des Clients pour le compte des Bénéficiaires. Dans le cas présent, il s'agit de l'Agent.

Page de Paiement
Page de paiement intégrant la Solution d'acceptation monétique en vente à distance, mise à disposition du Marchand par eZyness. La Page de paiement est mise à disposition des Bénéficiaires qui souscrivent à une option vente à distance dans le cadre d'une Offre du Marchand. Le Marchand accompagne le Bénéficiaire dans l'intégration de la Page de Paiement à sa Boutique. Les fonctionnalités et conditions d'utilisation de la Page de Paiement par le Bénéficiaire sont définies dans les CGV Agent ;

PCI-DSS
Payment Card Industry – Data Security Standard
Programme de sécurisation des données mis en œuvre par les réseaux internationaux (Visa, Mastercard, American Express). La Solution d'acceptation est certifiée conforme à PCI-DSS.

Solution d'acceptation
Solution technique qui permet au Marchand d'accepter des paiements.

3D Secure
Protocole permettant l'authentification d'un porteur de carte par l'émetteur de cette carte qui vise à s'assurer, lors de chaque paiement en ligne, que la carte est utilisée par son véritable titulaire.

Article 2 - Objet

Les présentes conditions générales ont pour objet de définir les conditions dans lesquelles eZyness propose au Marchand un service de paiement sécurisé, ci-après dénommé la Solution d'acceptation, afin de lui permettre de commercialiser des produits, services ou informations par internet et d'en obtenir le paiement par carte.

Article 3 - Description de la Solution d'acceptation

La Solution d'acceptation est une offre de paiement sécurisé par carte de paiement en vente à distance. La sécurité du paiement repose sur l'authentification du Marchand, sur la confidentialité et l'intégrité des données du Client et du Marchand.

3.1 Transactions de paiement en ligne

Lors d'une demande de paiement par carte, une demande d'autorisation est effectuée en ligne par eZyness pour chaque transaction.
Quel que soit le type de paiement, une réponse systématique est retournée vers le Client et vers le serveur « Marchand », quelle que soit l'issue de la transaction (acceptée ou refusée).

3.2 Contrôles d'acceptation des cartes

Les contrôles d'acceptation des cartes sont effectués à partir des Données personnelles (numéro de carte, date de validité et cryptogramme visuel) fournies. Dans le cas d'une transaction sur internet, ces données personnelles sont validées par le Client dans le formulaire de saisie des coordonnées bancaires.
Si ces contrôles sont positifs, la transaction se poursuit et le processus de déclenchement de demande d'autorisation est activé.
Dans le cas où ces contrôles s'avéreraient négatifs, le Client ou le Marchand est invité à recommencer jusqu'à abandon de la transaction après 3 tentatives fausses ou erronées.

Authentification 3D Secure :
Si la carte du Client est enregistrée dans le programme 3D Secure, un contrôle complémentaire d'acceptation est activé permettant au Marchand de déclencher une authentification du Client par l'émetteur de la carte.

3.3 Opérations de création et de gestion de caisse

Le Marchand dispose également de la possibilité de créer et de gérer ses transactions directement sur l'Interface de la Solution d'acceptation :

3.3.1. Consultation des opérations

Cette fonction permet au Marchand de consulter les paiements effectués sur les Boutiques via la Page de paiement. Il peut ainsi :

- consulter une transaction à partir du numéro de la transaction, de la carte, ou de la date de la transaction
- consulter une liste de transactions à partir d'un ensemble de critères (numéro de transaction, date, statut, etc.).

La page de résultat lui permet de consulter l'ensemble des informations rattachées à une transaction précise.

3.3.2. Annulation totale ou partielle (avant remise en paiement)

Cette fonction permet de modifier le montant à envoyer en paiement, en l'annulant totalement ou partiellement. Elle est utile, par exemple, lorsqu'un Client a commandé plusieurs produits, au Marchand pour annuler partiellement la transaction du montant d'un produit indisponible afin de débiter le client uniquement du montant des produits réellement livrés. L'annulation d'une transaction doit être effectuée avant sa remise en paiement. Si la transaction a déjà été remise en banque, l'annulation est impossible. Il est également impossible d'annuler un montant supérieur au montant d'origine de la transaction.

3.3.3. Validation

La fonction de validation permet de déclencher la remise en paiement d'une transaction. Elle permet ainsi au Marchand de faire du paiement différé en débitant le Client à l'expédition des produits achetés.
En choisissant le mode validation, il est nécessaire de valider chacune des transactions pour les envoyer en paiement. Si un Marchand ne valide pas une transaction donnée avant que son délai de capture choisi ne prenne fin, cette transaction expirera. Il sera alors impossible de l'envoyer en paiement.

3.3.4. Remboursement total ou partiel (avant remise en paiement)

Le remboursement permet de créditer un Client qui a précédemment été débité (produit non parvenu, indisponible, détérioré, retour etc.). Le compte du Client sera crédité du montant remboursé et le compte du Marchand est débité de ce même montant. Le remboursement est remisé en paiement le jour même de l'opération. Le Marchand peut rembourser un client dans les 13 mois qui suivent sa commande. Il peut faire autant de remboursements partiels qu'il souhaite tant qu'il ne dépasse pas ce délai de treize mois et que le solde est supérieur à zéro.
Une opération de remboursement ne peut pas être annulée ou validée. Le montant cumulé des remboursements ne doit pas dépasser le montant de la transaction initiale.

3.3.5. Capture partielle

L'opération de capture partielle permet au Marchand de valider la transaction initiale plusieurs fois, par exemple dans le cas d'envois multiples. La capture partielle est une duplication limitée au montant restant à remiser en paiement. L'autorisation initiale est utilisée. Une nouvelle est créée seulement si l'initiale a expiré.
L'opération de capture partielle consiste à dupliquer la transaction initiale une ou plusieurs fois, toutefois dans la limite de son montant.
Exemple :
Un client a acheté un DVD à 30 EUR, un jeu à 50 EUR et un livre à 20 EUR.
Le Marchand fait une autorisation de paiement par carte pour un montant de 100 EUR.
Le Marchand a le DVD en stock. Il valide les 30 EUR au moment de l'envoi du DVD ; ces 30 EUR sont envoyés pour règlement (après la validation de la transaction initiale)
Le Marchand reçoit ensuite le jeu à envoyer au client. Il doit valider les 50 EUR, correspondant au prix du jeu. Il capture partiellement la transaction initiale avec un montant de 50 EUR. Un nouveau paiement de 50 EUR est émis et réglé.
Le Marchand reçoit le livre et doit valider les 20 EUR à l'envoi de ce dernier. Il recycle à nouveau la transaction initiale avec un montant de 20 EUR. Un nouveau paiement de 20 EUR est émis et réglé
La limite de l'opération du recyclage a été atteinte car le montant initial de 100 EUR a été réglé.

Les règles applicables aux transactions de paiement par cartes sont celles définies dans le Contrat d'Acceptation en paiement à distance sécurisé par cartes de paiement (internet).

Article 4 - Prestations d'eZyness

4.1 Mise en œuvre de la Solution d'acceptation

Après la signature du Contrat de Mandat d'Agent et de la mise en place de la Solution d'acceptation, sur demande du Marchand, eZyness lui adresse par courrier électronique son mot de passe et son identifiant d'accès.

Le Marchand procède à l'installation et à la réalisation des tests de conformité de la Solution d'acceptation sous sa seule responsabilité et conformément aux instructions fournies par eZyness.
En cas de besoin, le Marchand pourra recourir au service de support technique tel que décrit à l'Annexe 11 « Engagements de niveaux de services ».

4.2 Maintenance

Le Marchand bénéficie d'un service de maintenance de l'Interface pour toute la durée des présentes conditions générales.
Cette maintenance s'analyse comme une maintenance curative, qui comprend la correction des anomalies quant au fonctionnement de la Solution d'acceptation.
Par anomalie, il convient d'entendre un fonctionnement non conforme aux spécifications telles que décrites dans la Documentation remise au Marchand.
eZyness s'engage à faire bénéficier le Marchand de toutes les évolutions fonctionnelles et techniques liées au développement par eZyness de la Solution d'acceptation.

4.3 Disponibilité de la Solution d'acceptation

Le Marchand pourra utiliser la Solution d'acceptation 24 heures sur 24 et 7 jours sur 7.
Toutefois, eZyness se réserve le droit, après en avoir avisé le Marchand 5 jours ouvrés à l'avance, de rendre inaccessible la Solution d'acceptation pendant 4 heures consécutives, afin de réaliser des travaux de maintenance technique.
Dans toute la mesure du possible, ces travaux seront réalisés aux heures de moindre utilisation de la Solution d'acceptation.

4.4 La sécurisation de la Solution d'acceptation

eZyness met en œuvre les moyens nécessaires pour sécuriser par chiffrement et déchiffrement les données échangées en réalisant les opérations suivantes :

- Identification et authentification de la Page de Paiement du Marchand demandant la réalisation d'un paiement.
- Identification du Marchand demandant la réalisation d'un paiement.
- Affichage de pages sécurisées en mode SSL (Secure Socket Layer) pour la saisie par le Client de ses données personnelles de paiement et pour l'accès par le Marchand au service de création et gestion des transactions.
- Contrôle de l'intégrité et de la confidentialité des données transmises, en veillant à l'absence de toute interception et altération de ces données par un tiers.
- Traçabilité et horodatage des transactions.
- Stockage durable et inaltérable des historiques de transactions.

Le Marchand peut accéder directement à l'Interface de la Solution d'acceptation pour la réalisation des opérations décrites à l'article 3.3. L'utilisation de cette fonction par le Marchand est assurée après une procédure d'identification par un système d'identifiant et de code confidentiel qui constituent son moyen d'authentification.

Toute opération résultant de ce moyen d'authentification est considérée comme émanant directement du Marchand.
Il est précisé que les technologies utilisées et les procédures mises en place pour assurer la sécurisation des paiements sont conformes à la législation française relative aux opérations bancaires et sont agréées PCI-DSS (Payement Card Industry Data Security Standard).

Article 5 - Utilisation des logos et des marques

eZyness ainsi que ses prestataires sont autorisés par le Marchand à utiliser, reproduire et représenter sur tous supports, notamment en ligne, les logos, dessins ou marques qu'il utilise à l'égard de sa Clientèle, pour l'exécution de la Solution d'acceptation ou pour promouvoir celle-ci , et ce pendant la durée des présentes conditions générales et dans le monde entier.

Article 6 - Responsabilité

6.1 Responsabilité d'eZyness

eZyness ne garantit pas un fonctionnement sans anomalie, ni un fonctionnement ininterrompu de la Solution d'acceptation, eZyness n'étant tenue qu'à une obligation de moyen. Par exemple, eZyness n'est pas responsable de l'Interface de la Solution d'acceptation qui est implantée dans un environnement informatique placé sous la responsabilité du Marchand.

eZyness est responsable de l'exploitation de la Solution d'acceptation et assume la gestion des moyens de télécommunications utilisés dans le cadre de la mise à disposition de cette Solution. Cependant, eZyness n'engage pas sa responsabilité sur les services offerts par les réseaux de télécommunication tels qu'Internet et/ou réseaux d'autorisation bancaire. La responsabilité d'eZyness se limite à un fonctionnement de la Solution d'acceptation conforme à la Documentation remise au Marchand.

eZyness sera libérée de ses obligations et pourra résilier les présentes Conditions Générales dans les conditions prévues à l'article 10, en cas de manquement par le Marchand à ses obligations, et notamment pour les raisons suivantes :

1. Incompatibilité entre tout ou partie du système informatique du Marchand et la Solution d'acceptation.
2. Modification de l'Interface par le Marchand ou par un tiers.

La responsabilité d'eZyness ne pourra pas être mise en jeu en cas de défaillance de la Solution d'acceptation résultant de faits indépendants de sa volonté et notamment en cas de force majeure tel que défini à l'article 13 des présentes conditions générales ou en cas de défaillance due à l'installation du Marchand ou du réseau Internet.

6.2 Responsabilité du Marchand

Le Marchand reconnaît avoir reçu d'eZyness les informations suffisantes pour apprécier le fonctionnement et l'adéquation de la Solution d'acceptation à ses besoins.

Le Marchand est responsable de l'ensemble de son système informatique : exploitation, sécurité, sauvegarde des données, protection de son certificat, procédures de secours. Il ne saurait tenir eZyness responsable des conséquences d'une utilisation non conforme de la Solution d'acceptation.

Le Marchand est seul responsable de l'usage et de la conservation du mot de passe et du code confidentiel lui permettant d'accéder à l'Interface de la Solution d'acceptation, et des conséquences d'une divulgation volontaire ou non faite à un tiers. En cas de perte ou de vol de ce moyen d'authentification, il incombe au Marchand de le signaler sans délai et par tout moyen à eZyness. Le Marchand est responsable des créations des transactions, des opérations et consultations antérieures à ce signalement.

De façon générale, le Marchand s'engage à respecter les dispositions d'ordre public du droit français, notamment dans la mise en œuvre de son site Web ainsi que dans le contenu et la commercialisation de son offre.
Le Marchand s'engage à utiliser la Solution d'acceptation uniquement dans le but d'organiser (créer, gérer, annuler) le recouvrement de la vente de biens et de services au Client. La revente, la mise à disposition et l'utilisation par un

tiers de la Solution d'acception est interdite.
Le Marchand s'engage notamment à ne pas porter atteinte aux droits des tiers et s'interdit de proposer sur son site des produits, des prestations, des données ou informations contraires aux bonnes mœurs, à la dignité humaine, à la protection des mineurs ou, plus généralement, à l'ordre public.
Il garantit une présentation de son offre loyale et conforme aux dispositions du droit français de la consommation en ce qui concerne plus particulièrement celles relatives aux offres faites à distance (obligation d'information sur l'entreprise, sur le contenu de l'offre et sur les prix, respect de la faculté de retour, etc.).
Lorsque le service fourni par le Marchand à ses Clients constitue en tout ou partie un service de communication audiovisuelle, le Marchand fait son affaire de la déclaration préalable requise par les textes.
Il s'engage à respecter les règles de déontologie qui pourraient être édictées à l'attention des professionnels d'Internet et de la vente à distance.
Le Marchand sera également seul responsable de l'exécution de la livraison et des conséquences notamment financières qui pourraient résulter du non-respect des délais. Le Marchand est responsable des suites à donner dans le cas où un Client exercerait la faculté de retour du produit livré pour échange ou remboursement prévu par l'article L.221-18 du code de la consommation. Il se chargera ainsi de l'échange ou du remboursement de la somme directement auprès du Client et de l'annulation des factures correspondantes.

Le Marchand assume seul la responsabilité pleine et entière de son service, du contenu des commandes et de leurs suites notamment fiscales. Il fait sien tous litiges afférents et, notamment, ceux mettant en cause l'utilisation de la Page de paiement et des Données sur son site Web ou le contenu de son offre et de ses engagements contractuels.
Il garantit eZyness contre toute réclamation ou action de quelque nature qu'elle soit, émanant des Clients.

6.3 Les obligations visées à l'article 6.2 étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

Article 7 - Preuve des transactions financières

Les parties conviennent expressément que les données enregistrées par eZyness sur l'Interface de la Solution d'acceptation constituent la preuve des transactions financières passées entre le Marchand et les Clients.

Article 8 - Droit d'usage & Propriété intellectuelle

Dans le cadre des présentes conditions générales, eZyness concède au Marchand l'usage de la Solution d'acceptation pour l'exploitation en France de sa Page de paiement, dans le cadre et pour la durée des présentes conditions générales, à l'exclusion de toute autre utilisation. Le Marchand s'engage notamment à ne pas modifier, traduire, arranger, ni adapter la Solution d'acceptation de quelque façon que ce soit. Les présentes conditions générales n'emportent cession d'aucun droit de reproduction ni de représentation. eZyness se réserve le droit de modifier ou de remplacer à tout moment la Solution d'acceptation. Le Marchand s'engage à intégrer ces modifications dans un délai de 30 jours à compter de sa réception, à restituer l'ancien sur demande à eZyness et à détruire la copie de sauvegarde.
A défaut, eZyness pourra demander la résiliation des présentes conditions générales dans les conditions définies à l'article 10.
De façon commune aux présentes Conditions Générales de de la Solution d'acceptation, le droit d'usage de la Solution fournie par eZyness ne peut en aucun cas être cédé à un tiers que ce soit à titre gratuit ou onéreux. Le Marchand s'interdit toute reproduction pour communication à des tiers, même à titre gratuit, ainsi que toute constitution ou reconstitution de bases de données obtenues dans le cadre de l'utilisation de la Solution.
Le Marchand déclare détenir les droits de propriété intellectuelle nécessaires à l'utilisation des logos, marques, dessins et créations sur son site web, Page de paiement ou catalogue qu'il diffuse, et garantit eZyness contre tout recours ou action émanant de tiers.

Article 9 – Modification des conditions générales

9.1 Modification des conditions générales et des clauses

eZyness peut modifier les présentes conditions générales sous réserve d'en informer le Marchand au moins un mois avant l'entrée en vigueur des nouvelles conditions contractuelles. Le Marchand pourra, en cas de désaccord, résilier les présentes conditions générales selon les modalités fixées à l'article 10 « Résiliation de la Solution d'acceptation ».

9.2 Modification technique de la Solution d'acceptation

Si les conditions d'exploitation de la Solution d'acceptation l'exigent, eZyness pourra modifier les caractéristiques techniques de ses prestations, sous réserve d'une information suffisante du Marchand. A cette occasion, eZyness pourra demander au Marchand des informations complémentaires à celles données au moment de la conclusion du Contrat de Mandat d'Agent.
Dans ce cas, le Marchand pourra résilier les présentes conditions générales moyennant un préavis de 1 mois adressé par lettre recommandée avec accusé de réception. La résiliation n'ouvre droit à aucune indemnité. La fermeture de la Solution d'acceptation interviendra le dernier jour du mois de réception de la lettre de résiliation par eZyness sauf si le Marchand

demande la fermeture anticipée de la Solution d'acceptation.

Article 10 –Résiliation de la Solution d'acceptation

A tout moment, chaque Partie dispose de la faculté de résilier les présentes conditions générales. A cet effet, la Partie souhaitant résilier les présentes conditions générales devra notifier son intention à l'autre Partie par lettre recommandée avec avis de réception. La résiliation de la Solution d'acceptation sera effective un mois après la réception de cette lettre recommandée, sous réserve du dénouement des opérations en cours.
La résiliation des présentes conditions générales n'entraine pas nécessairement la résiliation du Contrat de Mandat d'Agent.

Article 11 - Suspension

Pour des raisons de sécurité et/ou de risque de fraude, eZyness pourra suspendre l'accès à la Solution d'acceptation. Dans ce cas, elle en informera dans les meilleurs délais et par tous moyens le Marchand.

Article 12 - Protection des données à caractère personnel des Clients

12.1. Données à caractère personnel des Clients

12.1.1 Traitements de données à caractère personnel par eZyness

Dès lors que la prestation implique un traitement de Données à caractère personnel du Client, il est convenu qu'eZyness aura la qualité de sous-traitant intervenant dans le cadre de la mise en œuvre du traitement pour le compte du Marchand.
Dans ce contexte, eZyness assure qu'il dispose des compétences techniques et organisationnelles nécessaires afin de réaliser les prestations qui lui sont confiées par le Marchand dans le respect des obligations fixées dans le présent article et exclusivement pour l'objet prévu aux présentes Conditions Générales.
eZyness est autorisée à procéder à un traitement de Données à caractère personnel répondant aux caractéristiques mentionnées en annexe 8.2 « Caractéristiques des traitements de Données à caractère personnel ».
En conséquence, eZyness s'engage à :

- ne procéder au traitement de Données à caractère personnel que sur instruction écrite du Marchand et informer ce dernier si une instruction lui paraît contraire à la règlementation sur la protection des données ;
- ne conserver les Données à caractère personnel traitées, sous une forme permettant l'identification des personnes, que le temps nécessaire à l'exécution des prestations ;
- assister le Marchand, sous réserve d'en être informé, afin de répondre à toute demande d'exercice de droits par les personnes concernées et/ou toute demande d'information des autorités de contrôle et de protection des données ;
- informer le Marchand de toute demande qui lui serait adressée directement et plus généralement de tout événement affectant significativement le traitement des Données à caractère personnel.

eZyness peut sous-traiter l'exécution de tout ou partie des prestations à un tiers, ce que reconnait et accepte le Marchand au travers des présentes conditions générales. eZyness s'engage à communiquer au Marchand qui en ferait la demande, la liste de ses sous-traitants et leur rôle respectif.

Les sous-traitants restent en toute circonstance placés sous l'autorité d'eZyness, qui demeure l'unique responsable de l'exécution de la totalité des prestations et plus spécifiquement du respect du niveau de qualité, de sécurité et de confidentialité. eZyness se porte fort du respect des obligations contractuelles concernées par ses sous-traitants.
Le cas échéant, eZyness fera son affaire de la bonne tenue de son registre des traitements de données à caractère personnel en veillant à y inscrire le(s) traitement(s) qu'il met en œuvre pour le compte du Marchand.

12.1.2 Sécurité et confidentialité des données à caractère personnel

eZyness prendra toute mesure nécessaire pour préserver l'intégrité, la disponibilité et la confidentialité des Données à caractère personnel.
eZyness s'engage notamment à mettre en place les mesures techniques et organisationnelles permettant d'assurer un niveau de sécurité et de confidentialité approprié au regard des risques identifiés par le Marchand et communiqués à eZyness.
eZyness s'engage en particulier à :

- mettre en œuvre les mesures nécessaires afin de protéger les Données à caractère personnel contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé ;
- ne rendre accessibles et consultables les Données à caractère personnel traitées qu'aux seuls personnels dûment habilités en raison de leurs fonctions et qualité, dans la stricte limite de ce qui leur est nécessaire à l'accomplissement de leurs fonctions ;
- notifier au Marchand, sous 48 heures à partir du moment où il en a connaissance, toute violation de Données à caractère personnel.

Dans ce contexte eZyness communiquera au Marchand tous les éléments dont il dispose concernant les conditions entourant cette violation de Données à caractère personnel et notamment la nature et l'étendue des Données à caractère personnel impactées, le nombre de personnes concernées, les conséquences probables et les conditions techniques dans lesquelles la violation a eu lieu.

12.1.3 Communication à des tiers

Les Données à caractère personnel traitées en exécution es présentes Conditions Générales ne pourront faire l'objet d'aucune divulgation à des tiers en dehors des cas prévus dans le contrat ou de ceux prévus par une disposition légale et/ou réglementaire.
eZyness informera le Marchand de toute demande d'accès ou de communication émanant d'un tiers se prévalant d'une autorisation découlant de l'application de dispositions légales ou réglementaires.

12.1.4 Localisation géographique des données à caractère personnel

Dans l'hypothèse où eZyness réaliserait tout ou partie du traitement de Données à caractère personnel en dehors du territoire d'un pays membre de l'Union européenne, de l'Espace Economique Européen (EEE) ou d'un pays reconnu comme adéquat par l'Union Européenne – y compris l'hébergement – il s'engage à encadrer le transfert des Données à caractère personnel par des garanties appropriées, notamment des clauses types adoptées par la Commission Européenne.
Dans le cas où eZyness aurait recours à la sous-traitance de tout ou partie du traitement de Données à caractère personnel, il s'assure qu'aucune information à caractère personnel n'est transférée hors de l'Union Européenne, de l'EEE ou d'un pays reconnu comme adéquat par ses propres sous-traitants ou partenaires sans un encadrement par des garanties appropriées. Ces garanties seront préalablement portées à la connaissance du Marchand.

12.1.5 Restitution et destruction des données à caractère personnel

Au terme du contrat et sauf obligation légale de conservation, eZyness s'engage à restituer ou à détruire, selon les instructions et dans les délais indiqués par le Marchand, l'ensemble des Données à caractère personnel traitées, sauf obligation légale de conservation qui sera portée à la connaissance du Marchand. Dans le cas d'une destruction des Données à caractère personnel, celle-ci pourra, à la demande du Marchand, être attestée par un procès-verbal de destruction.

12.1.6 Audit

eZyness s'engage à faire réaliser des audits réguliers sur les services qu'elle rend au titre des présentes Conditions Générales et à communiquer sur demande, au maximum une fois par an, les résultats de ces audits au Marchand.

12.2. Données à caractère personnel du Marchand

Les données à caractère personnel des représentants du Marchand font l'objet de traitements dont le responsable est eZyness, conformément à la réglementation relative à la protection des données à caractère personnel.

Elles sont traitées pour la souscription à la Solution d'acceptation et pour l'exécution des ordres de paiement transmis et leur sécurisation, et en vertu de l'exécution du Contrat et du respect d'obligations légales ou règlementaires, telles que la lutte contre le blanchiment des capitaux et de financement du terrorisme. Les données des représentants du Marchand seront conservées pendant la durée de la relation contractuelle.

L'ensemble de ces données pourra être conservé au-delà des durées précisées, dans le respect des délais de prescription légaux applicables.

Les données à caractère personnel collectées sont obligatoires pour la souscription à la Solution d'acceptation et aux Services d'eZyness. A défaut, les demandes de souscription ne pourront pas être traitées et le Marchand s'expose à un refus ou à la résiliation des services concernés.

Les données collectées sont destinées à eZyness pour les traitements et finalités cités ci-avant. Elles pourront également être communiquées à toute autorité administrative ou judiciaire habilitée ou plus généralement à tout tiers autorisé, pour satisfaire à ses obligations légales ou réglementaires.

Les représentants du Marchand disposent d'un droit d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement. Ils peuvent faire une demande de portabilité pour les données qu'ils ont fournies et qui sont nécessaires au contrat ou au traitement desquelles ils ont consenti. Ils peuvent à tout moment retirer leur consentement lorsque celui-ci a été préalablement donné. Ils peuvent aussi donner des instructions relatives à la conservation, à l'effacement et à la communication de ses données après leur décès. Ils peuvent exercer ces droits en s'adressant au responsable de traitement, eZyness, selon les modalités prévues à l'article 25 « Notification » du Contrat.

eZyness peut prendre des décisions automatisées, y compris par profilage, concernant le Marchand. Ces décisions sont prises après interrogation des fichiers réglementaires (FICOBA, FICP, FCC, ...), après analyse du profil de risque du Marchand et des pièces justificatives fournies. Selon les cas ces décisions peuvent se traduire par le refus d'accès à un produit ou un service.

Le Client peut s'adresser au Délégué à la Protection des Données de La Banque Postale - 115, rue de Sèvres - 75275 Paris Cedex 06.

En cas de difficulté en lien avec la gestion de ses données à caractère personnel, le Client a le droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Article 13 - Force majeure

eZyness ne pourra être tenue responsable de tout cas fortuit ou de force majeure, défini à l'article 1218 du code civil.

Article 14 - Réclamation

Toute réclamation doit être justifiée et formulée par écrit à l'Acquéreur, dans un délai maximum de 6 mois, à compter de la date de l'opération contestée sous peine de non acceptation de cette réclamation.

ANNEXE 8.2 – Caractéristiques du traitement de Données à caractère personnel

La présente Annexe a pour objet de détailler la nature et les conditions du traitement de Données à caractère personnel par eZyness.

1. Objet et finalité du Traitement

La fourniture des Prestations, notamment les activités suivantes, implique un traitement de Données à caractère personnel dont l'objet et la finalité sont les suivants :
Le Marchand collecte les données de paiement des Clients et les transmet à eZyness pour permettre le traitement des opérations de paiement.

2. Nature du Traitement

☒ Saisie de données
☒ Accès aux données en lecture
☐ Accès aux données en modification
☐ Accès aux données en suppression
☒ Hébergement/stockage de données
☒ Transmission de données
☐ Autres (préciser)

3. Durée du Traitement

☐ La durée du traitement correspond à la durée du Contrat
☒ Sur la base de la durée du Contrat, les parties conviennent que la durée du traitement est de correspond à la durée des présentes Conditions générales et au-delà, conformément aux délais de prescription légaux s'appliquant à eZyness

4. Catégories de Données à caractère personnel traitées

☐ Données d'identification (état civil, identité, adresse, …)
☐ Vie professionnelle (CV, parcours professionnel, formation, …)
☐ Vie personnelle (habitude de vie, situation familiale, …)
☒ Information d'ordre économique (revenus, situation financière, …)
☐ Données de localisation (déplacements, données GPS, GSM, …)
☐ Données de connexion (adresse IP, logs, …)
☐ Appréciation sur les difficultés des personnes (recours aux services d'une assistante sociale, difficultés financières, ...)
☐ Numéro de Sécurité Sociale (NIR)
☐ Données biométriques
☐ Infractions, condamnations, mesures de sûreté
☐ Données de santé
☐ Données génétiques
☒ Autres (préciser) Données de paiement

5. Catégories de Personnes concernées

☒ Clients
☐ Collaborateurs
☐ Autres (préciser)

ANNEXE 8-3 Conditions d'acceptation en paiement à distance sécurisé par carte de paiement

PARTIE 1 CONDITIONS COMMUNES A TOUS LES SCHEMAS

ARTICLE 1 – DEFINITIONS

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

2) Par "Marque", il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptible de désigner le Schéma.
Les Marques pouvant être acceptées et entrant dans le champ d'application du présent Contrat sont visées en partie 2.

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

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

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

6) Par " Schéma ", il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.
Les Schémas Visa / MasterCard / CB reposent sur l'utilisation de Cartes Visa / MasterCard / CB auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

7) Par « Carte », on entend une catégorie d'instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marque(s).
Lorsque la Carte est émise dans l'Espace Economique Européen (ci-après l'"EEE" qui comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :
- crédit ou carte de crédit,
- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

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

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

10) Par « Contrat » ou « Contrat d'acceptation en paiement à distance sécurisé par cartes de paiement », il faut entendre ensemble les Conditions communes à tous les Schémas (Partie 1) et les dispositions spécifiques à chaque Schéma (Partie 2).

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

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

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

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

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

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

2.4 Respecter les lois et règlements (y compris en matière fiscale), les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique, et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (ex : mobile et ordinateur). A cet effet l'Accepteur organise la traçabilité adéquate des informations liées au paiement à distance.

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

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

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

Les informations doivent indiquer une dénomination commerciale connue des titulaires de Carte.

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

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

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

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

2.12 Régler, selon les dispositions prévues à l'Annexe 9 Conditions financières, les commissions, frais et, d'une manière générale, toute somme due notamment au titre de l'acceptation des Cartes.

2.13 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 Accepteur et le Référentiel Sécuritaire PCI DSS et acceptent que les audits visés à l'article 2.15 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé à cet article.

2.14 A la demande de l'Acquéreur, selon les volumes d'opérations Cartes acceptées chez lui, à respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat ainsi que celles du Référentiel Sécuritaire PCI DSS dont il peut prendre connaissance à

l'adresse suivante : http//fr.pcisecuritystandards.org/minisite/en/.

2.15 Permettre à l'Acquéreur et/ou au(x) Schéma(s) concerné(s) de faire procéder aux frais de l'Accepteur dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.13 ci-dessus, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement sur Internet en fonction des risques de sécurité liés au Système d'Acceptation utilisé. Cette vérification, appelée "procédure d'audit", s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.
Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, l'Acquéreur peut procéder, le cas échéant à la demande du(des) Schéma(s) concerné(s), à une suspension de l'acceptation des Cartes portant la (les) Marques du(des) Schémas concerné(s) par l'Accepteur, voire à la résiliation du présent Contrat, dans les conditions prévues dans le Contrat de Mandat d'agent et à l'article 9 de la présente Partie 1. L'Accepteur autorise la communication du rapport à l'Acquéreur et au(x) Schéma(s) concerné(s).

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

2.17 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.

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

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

2.20 Dans le cas où l'Acquéreur serait condamné, par un Réseau national ou international Carte, à payer des pénalités qui résulteraient du non-respect par l'Accepteur de ses obligations en matière de sécurité et/ou de fraude, l'Acquéreur se réserve la possibilité de demander à l'Accepteur le remboursement de son préjudice correspondant à ces pénalités.

2.21 Les obligations visées à l'article 2 étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 3 - OBLIGATIONS DE L'ACQUEREUR

L'Acquéreur s'engage à :
3.1 Mettre à la disposition de l'Accepteur, toute information relative à la sécurité des opérations de paiement.

3.2 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie 2 du présent Contrat et son/leur évolution, la (les) Marque(s) et Catégorie(s) de carte dont il assure l'acceptation.

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

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

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

3.6 Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les dispositions prévues à l'Annexe 10 Prescriptions techniques de la Solution.

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

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

3.9 Fournir à l'Accepteur, sur demande de ce dernier, le détail des frais et commissions pour chacune des Catégories de carte et Marques qu'il accepte.

ARTICLE 4 : GARANTIE DU PAIEMENT

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 qu'en Partie 2 du présent Contrat.
Toutes les mesures de sécurité sont indépendantes les unes des autres.

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

Cas de la non-authentification forte du Porteur

Lorsque l'Accepteur émet le souhait que l'opération de paiement ne fasse pas l'objet d'une authentification forte et que l'Emetteur n'authentifie pas fortement le titulaire de la Carte, l'opération de paiement ne sera pas garantie.

ARTICLE 5 - MESURES DE SECURITE

5.1 Lors du paiement

L'Accepteur s'engage à :

5.1.1 Appliquer la procédure de sécurisation des ordres de paiement communiquée en Annexe 8-3.3.

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

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

5.2 Après le paiement
L'Accepteur s'engage à :

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

5.2.2 Archiver et conserver, à titre de justificatif, pendant la durée de (24) mois à partir de la date de l'opération :
- l'enregistrement électronique représentatif de chaque opération ou le journal de fond lui-même.
- le cas échéant, un exemplaire du Ticket.

5.2.3 Communiquer, à la demande de l'Acquéreur et dans le délai de 7 jours tout justificatif des opérations de paiement.

5.2.4 **L'Accepteur s'engage à :**
- ne pas stocker sous quelque forme que ce soit le cryptogramme visuel,
- prendre toutes les précautions utiles pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci.

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

5.2.6 Les obligations visées à l'article 5 étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 6 : MODALITES ANNEXES DE FONCTIONNEMENT

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

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

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

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

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

6.4 Les obligations visées aux articles 6.2 et 6.3 étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 7 : MODIFICATIONS

7.1 L'Acquéreur peut modifier à tout moment le présent Contrat.

L'Acquéreur peut notamment apporter :

- des modifications techniques telles que l'acceptabilité de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'état du Système d'Acceptation suite à un dysfonctionnement etc.
- des modifications sécuritaires telles que :

- la suppression de l'acceptabilité de certaines Cartes,
- la suspension de l'acceptabilité de Cartes portant certaines Marques.

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

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

7.4 Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur.

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

ARTICLE 8 : DUREE ET RESILIATION DU CONTRAT

8.1. Le présent Contrat est conclu pour la même durée que celle du Contrat de mandat d'agent. Les modalités de résiliation sont celles prévues dans le Contrat de mandat d'agent.

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

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

Dans le cas où, après résiliation du présent Contrat, il se révèlerait des impayés, ceux-ci seront à la charge de

l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

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

ARTICLE 9 - SUSPENSION DE L'ACCEPTATION

9.1 L'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur. La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

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

9.2 La suspension peut être décidée en raison notamment :
9.2.1 du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation d'un Schéma,
9.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
9.2.3 d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,
9.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
9.2.5 de retard volontaire ou non motivé de transmission des justificatifs,
9.2.6 d'un risque aggravé en raison des activités de l'Accepteur.

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

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

9.5 **L'Accepteur s'engage à informer le Bénéficiaire des dispositions prévues à l'article 9.**

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

10.1 En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés, ou de fraude, anormalement élevé ou d'utilisation anormale de Cartes perdues, volées ou contrefaites, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

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

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

présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

10.4 **L'Accepteur s'engage à informer le Bénéficiaire des dispositions prévues à l'article10.**

ARTICLE 11 : NON RENONCIATION

Le fait pour l'Accepteur ou pour l'Acquéreur de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat ne peut en aucun cas être considéré comme constituant de sa part une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

PARTIE 2
DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

ARTICLE 1 – FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas sont :
- VISA Inc,
- MasterCard Europe SA.

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

ARTICLE 2 – OBLIGATION DE L'ACCEPTEUR

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

Les obligations visées dans cet article étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 3 – OBLIGATION DE L'ACQUEREUR

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

DISPOSITIONS SPECIFIQUES AU SCHEMA CB

ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les "Cartes CB") pour le paiement d'achats de biens et/ou de prestations de services ou pour le règlement de dons ou de cotisations auprès des Accepteurs adhérant au Schéma CB et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou solutions de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'acceptation, l'Acquéreur définissant certaines conditions spécifiques de fonctionnement.
Lorsque l'Acquéreur représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à l'Acquéreur, et non la mise en jeu de la garantie du paiement visée à l'article 4 de la Partie 1 du présent Contrat.

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

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

ARTICLE 3 : DISPOSITIONS SUR L'ACCEPTATION DE CARTES CB

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

3.1 Accepter les Cartes CB pour le paiement d'achats de biens et/ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale), même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, à titre de dons en contrepartie du règlement du montant de cotisations.

3.2 Régler, selon les dispositions prévues à l'Annexe 9 Conditions financières, les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du Schéma CB.

3.3 Transmettre les enregistrements des opérations de paiement à l'Acquéreur, au plus tard 7 jours après la date de l'opération. Au-delà d'un délai maximum de six (6) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma CB.

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

- Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'adhésion, voire à une radiation du Schéma CB telle que prévue à l'article 4 ci-après. L'Accepteur autorise la communication du rapport à l'Acquéreur et au GIE CB.

Les obligations visées dans cet article étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 4 : MESURES DE PREVENTION ET DE SANCTION

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

En cas de manquement de l'Accepteur aux dispositions relatives au Schéma CB du présent Contrat ou aux lois en vigueur ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes CB perdues, volées ou contrefaites, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté. Si dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut résilier de plein droit avec effet immédiat le présent Contrat, par lettre recommandée avec demande d'avis de réception.

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

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

En cas de manquement de l'Accepteur aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où l'Accepteur ventile ses remises en paiement entre plusieurs acquéreurs de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE CB peut prendre des mesures de sauvegarde et de sécurité consistant en :

- La suspension de l'acceptation des Cartes CB par l'Accepteur. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de trois (3) mois suivant la mise en demeure d'y remédier.

Ce délai peut être ramené à quelques jours en cas d'urgence et à un (1) mois au cas où l'Accepteur aurait déjà fait l'objet d'une mesure de suspension dans les vingt-quatre (24) mois précédant l'avertissement.

La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la réception de la notification.

● La radiation de l'adhésion de l'Accepteur au Schéma CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis de l'Accepteur concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée avec demande d'avis de réception.

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

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

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

Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par le GIE CB ou l'acquéreur concerné, et portant sur le respect des bonnes pratiques en matière de vente ou prestations réalisées à distance visées à l'article 2 de la Partie 1 et des mesures de sécurité visées à l'article 5 de la Partie 1.

Les obligations visées dans cet article étant également applicables au Bénéficiaire, l'Accepteur s'engage à les reproduire pour les mettre à la charge du Bénéficiaire dans le contrat qui les lie (CGV Agent).

ARTICLE 5 – PROTECTION DES DONNEES A CARACTERE PERSONNEL

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

Ces données à caractère personnel font l'objet de traitements afin de permettre :

1. la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB ;
2. de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte.

L'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés à l'article 14 de la Partie 1 des présentes Conditions Générales par courriel à protegezvosdonnees@cartes-bancaires.com.

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

- Consulter la Politique de protection des données à caractère personnel du GIE CB accessible à www.cartes-bancaires.com/protegezvosdonnees ;
- Contacter le Délégué à la protection des données désigné par le GIE CB par courriel à protegezvosdonnees@cartes-bancaires.com.

ANNEXE 8-3.1 : REFERENTIEL SECURITAIRE ACCEPTEUR

Les exigences constituant le Référentiel Sécuritaire Accepteur sont présentées ci-après :

EXIGENCE 1 (E1) : GERER LA SECURITE DU SYSTEME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE

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

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

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

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

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

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

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

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

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

EXIGENCE 4 (E4) : ASSURER LA PROTECTION LOGIQUE DU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.
Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

EXIGENCE 5 (E5) : CONTROLER L'ACCES AU SYSTEME 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) : GERER LES ACCES AUTORISES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates.

Les autorisations données doivent être archivées et contrôlées régulièrement.

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

L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.

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

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

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

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

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

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

EXIGENCE 7 (E7) : SURVEILLER LES ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

EXIGENCE 8 (E8) : CONTROLER 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 SECURITE (PATCHES DE SECURITE) 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'INTEGRITE DES LOGICIELS APPLICATIFS RELATIFS AU SYSTEME 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 TRAÇABILITE DES OPERATIONS 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'INTEGRITE DES INFORMATIONS RELATIVES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

EXIGENCE 14 (E14) : PROTEGER LA CONFIDENTIALITE DES DONNEES BANCAIRES

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

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

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

EXIGENCE 15 (E15) : PROTEGER LA CONFIDENTIALITE DES IDENTIFIANTS – AUTHENTIFIANTS DES UTILISATEURS ET ADMINISTRATEUR

La confidentialité des identifiants-authentifiants doit être protégée lors de leur stockage et de leur circulation.

Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.

Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.

ANNEXE 8-3.2 : REFERENTIEL SECURITAIRE PCI-DSS

Les exigences constituant le Référentiel Sécuritaire PCI-DSS sont organisées autour d'un ensemble de 12 familles d'exigences regroupant 250 règles réparties en six grands domaines présentés ci-après :

1° *Mettre en place et gérer un réseau sécurisé*

1ère exigence	Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires des Cartes
2ème exigence	Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système

2° *Protéger les données des titulaires de Cartes*

3ème exigence	Protéger les données des titulaires de Cartes stockées
4ème exigence	Crypter la transmission des données des titulaires de Cartes sur les réseaux publics ouverts

3° *Disposer d'un programme de gestion de la vulnérabilité*

5ème exigence	Utiliser et mettre à jour régulièrement un logiciel antivirus
6ème exigence	Développer et gérer des applications et systèmes sécurisés

4° *Mettre en œuvre des mesures de contrôle d'accès efficaces*

7ème exigence	Limiter l'accès aux données des titulaires de Cartes aux cas de nécessité professionnelle absolue
8ème exigence	Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique
9ème exigence	Limiter l'accès physique aux données des titulaires de Cartes

5° *Surveiller et tester régulièrement les réseaux*

10ème exigence	Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de Cartes
11ème exigence	Tester régulièrement les systèmes et procédures de sécurité

6° *Disposer d'une politique en matière de sécurité de l'information*

12ème exigence	Disposer d'une politique régissant la sécurité de l'information

ANNEXE 8-3.3 : Procédure de sécurisation des ordres de paiement

1. La procédure comporte obligatoirement une demande d'autorisation lorsqu'elle s'applique à l'acceptation d'un ordre de paiement transmis par Internet.

   Dans une infrastructure 3D Secure, la transaction de paiement à distance impose au porteur une deuxième phase d'authentification, en plus de la saisie des données cartes. Celle-ci intervient avant la demande d'autorisation. Ce protocole est la première version du 3D Secure (3DS).

2. **La procédure d'utilisation du CVX2** : L'Accepteur s'engage à contrôler (ou faire contrôler) le CVX2 donné par le Titulaire de la Carte.

3. **Processus d'authentification 3D Secure :**

   Prérequis techniques :
   La mise en œuvre du paiement sécurisé nécessite :
   - un enregistrement préalable 3DS de l'Accepteur par l'Acquéreur auprès des schémas VISA et MasterCard et, d'une solution technique.
   - l'installation par l'Accepteur pour recevoir des paiements à distance sécurisés via Internet. L'installation de cette solution est à la charge de l'Accepteur. Ce dernier doit utiliser une solution accepteur 3DS agrée par les schémas.

Processus d'authentification :

eZyness impose à ses clients l'utilisation du processus d'authentification 3D Secure.

Le programme 3D Secure a été retenu par les réseaux VISA, Mastercard et CB. Il s'agit d'un protocole permettant de réaliser l'authentification d'un paiement en ligne effectué par un porteur de carte déjà enrôlé. 3D Secure est un moyen de lutte contre la fraude de contestation par l'internaute des transactions faites en ligne. En cas de fraude, il y a transfert de la responsabilité de l'acquéreur à l'émetteur (liability schift).

Toutefois 3D Secure ne couvre pas les contestations et paiement ci-après :

Contestations non couvertes par 3D Secure :

- le montant : différence entre le montant annoncé et le montant facturé par le commerçant
- la livraison des biens et services : non réception de la commande, totale ou partielle
- la conformité des biens ou services : marchandise non conforme à la commande
- la présentation tardive en compensation : suivant délais dans le contrat commerçant.

Paiements non protégés par 3D Secure :

- paiement fractionnés à l'expédition : cas lors d'un achat de la non disponibilité de certains produits ou quantités de la commande. L'accord pour cette transaction est valable pour l'intégralité du montant de la commande mais seul le premier paiement est couvert par 3D Secure.
- paiement en « n » fois : seul le premier paiement est couvert par 3D Secure
- paiement agrégé
- paiement périodique.

Annexe 8-3.4 : DSP 2 - la sécurisation renforcée des paiements

La seconde Directive sur les Services de Paiement (DSP2) en vigueur depuis le 14 Septembre 2019 vise à renforcer la sécurité des paiements et accroître les droits des consommateurs au sein de la zone euro.

Dans ce cadre, les normes techniques de règlementation (dites aussi RTS : Regulatory Technical Standards) de la DSP 2 imposent l'authentification forte pour les paiements électroniques (SCA : Strong Customer Authentication). Autrement dit, les paiements par carte en ligne sont la cible principale de la DSP2.

L'authentification forte est permise par l'utilisation du protocole 3D Secure ce qui permet de s'assurer que le client est bien à l'origine du paiement en ligne. Il s'agit de la seconde version du 3D Secure (3DS V2)

Seuls trois types de paiements à distance sont jugés hors champs d'application de la DSP2 :

- Les paiements initiés par le marchand en opposition à ceux à l'initiative du porteur (MIT Merchant Initiated Transactions) ;
- Les paiements dits MO/TO (mail order / telephone order) ;
- Les paiements « one leg » c'est-à-dire dont l'acquéreur ou l'émetteur se trouve en dehors de l'Union Européenne.

Afin que l'authentification puisse être réalisée par l'émetteur de la carte, le commerçant procède à une demande d'authentification 3D Secure avant toute autorisation.

Il est à noter qu'avec les dernières versions du protocole 3DS (EMV 3DS ou autrement appelé 3DS V2), l'émetteur peut procéder à une authentification passive (aussi dit frictionless).

Dans ce cadre, le commerçant a la possibilité d'exprimer sa préférence quant à l'application ou non du frictionless par l'émetteur qui est seul décisionnaire au final.

Les trois choix disponibles et applicables pour chaque opération de paiement sont :

- Souhait d'une authentification passive (« Sans demande d'AF » ou « Frictionless » ci-après)
- Souhait d'une authentification forte (« Demande d'AF » ou « Demande de friction » ci-après)
- Pas de préférence (« Sans avis » ci-après)

Par défaut, eZyness applique le choix suivant : Pas de préférence / Sans avis.

Annexe 8-3.5 : DSP 2 évolutions du transfert de responsabilité

La DSP 2 induit de nouvelles règles de transfert de responsabilité qui s'appliqueront au niveau européen.

Demande du marchand	Réponse de l'émetteur	Responsable en cas de fraude
Demande d'AF / demande de friction	Demande d'AF / demande de friction	Emetteur
Demande d'AF / demande de friction	Sans demande d'AF / Frictionless	Emetteur
Sans avis	Demande d'AF / demande de friction	Emetteur
Sans avis	Sans demande d'AF / Frictionless	Emetteur
Sans demande d'AF / Frictionless	Demande d'AF / demande de friction	Emetteur
Sans demande d'AF / Frictionless	Sans demande d'AF / Frictionless	Marchand

AF = Authentification Forte