

(MERCİ DE BIEN VOULOIR PARAPHER TOUTES LES PAGES)

**L'Offre SogeCommerce est composée :**

– d'une prestation de service de paiement par laquelle Société Générale autorise l'Accepteur à accepter des paiements à distance par cartes dans les conditions définies dans :

- les Conditions Générales – Partie 1: Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement et – Partie 3: Conditions communes aux Parties 1 et 2;
- l'Annexe 1: Conditions Particulières, l'Annexe 2: Référentiel Sécuritaire Accepteur;
- Les Conditions Particulières complémentaires à celles figurant en Annexe 1 (également dénommées « Contrat de prestation SogeCommerce »);

(l'ensemble de ces documents étant dénommé le « Contrat d'acceptation en paiement à distance sécurisé par cartes de paiement »)

Les obligations mises à la charge de l'Accepteur au titre de ce service de paiement sont, en partie, mises en œuvre par Société Générale dans le cadre de la prestation technique fournie à l'Accepteur;

– et d'une prestation technique, permettant à l'Accepteur de disposer des logiciels nécessaires à la réalisation de paiements à distance par cartes ainsi que par d'autres moyens de payer disponibles en option. La prestation inclut également l'accès à la plate-forme informatique permettant de gérer ces opérations. Cette prestation est régie par :

- les Conditions Générales – Partie 2: Services SogeCommerce et Partie 3: Conditions communes aux Parties 1 et 2;
- l'Annexe 3: Charte « Protection et Sécurité de votre site SogeCommerce »;
- Les Conditions Particulières (également dénommées « Contrat de prestation SogeCommerce »).

**CONDITIONS GÉNÉRALES – PARTIE 1:****ACCEPTATION EN PAIEMENT À DISTANCE SÉCURISÉ (VADS) PAR CARTES DE PAIEMENT****A. CONDITIONS GÉNÉRALES COMMUNES À TOUS LES SCHÉMAS****ARTICLE 1 – DÉFINITIONS**

**1)** Par « Accepteur », il faut entendre 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, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) et dûment convenu(s) avec Société Générale.

L'Accepteur dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix, membre du Schéma avec lequel il a passé un contrat pour ce faire.

**2)** Par « Acquéreur », il faut entendre tout établissement de crédit ou tout autre établissement habilité à organiser l'acceptation des cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) au B des présentes. Dans le cadre du présent Contrat, Société Générale est l'Acquéreur de l'Accepteur.

**3)** Par « Carte », il faut entendre 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 Économique Européen (ci-après l'« EEE » - Il comprend les États membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), la Carte porte au moins l'une des mentions suivantes :

- « CRÉDIT » ou « CARTE DE CRÉDIT »,
- « DÉBIT »,
- « PRÉPAYÉ »,
- « COMMERCIAL »,

ou l'équivalent dans une langue étrangère.

**4)** Par « Catégorie de carte », il faut entendre :

- soit les cartes de crédit,
- soit les cartes de débit,
- soit les cartes prépayées,
- soit encore les cartes commerciales.

**5)** 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 les Marques CB - Visa, V PAY, Electron - Maestro, Mastercard et dont les conditions de fonctionnement spécifiques figurent au B des présentes.

**6)** 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 déterminées ou déterminables et/ou à des échéances convenues entre l'Accepteur et le titulaire de la Carte.

**7)** Par « Parties », il faut entendre l'Acquéreur (Société Générale) et l'Accepteur.

**8)** Par « Règlement », il faut entendre le Règlement UE n°2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

**9)** 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 CB/Visa/Mastercard reposent sur l'utilisation de Cartes auprès des Accepteurs acceptant la (les) Marque(s) desdits Schémas et cela, dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

**10)** 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 sur 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 ou d'une approbation par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

**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 et/ou 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, et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (ex: mobile et ordinateur).

À 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 Société Générale 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 initiées (par exemple, sur son ticket de paiement), vérifier avec Société Générale la conformité des informations transmises pour identifier son point de vente en ligne.

Les informations doivent indiquer une dénomination commerciale connue des titulaires de Carte et permettre de dissocier ce mode de paiement des autres modes de paiement (ex : automate et règlement en présence du titulaire de la 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 pour le règlement de dons ou de cotisations.

**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 exprès 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 concerné et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes (en ce compris la procédure d'authentification de ces derniers), proposées par Société Générale.

**2.12** – Ne pas stocker sous quelque forme que ce soit le cryptogramme visuel (trois derniers chiffres du numéro figurant au verso de la Carte).

**2.13** – Régler, selon les Conditions Particulières convenues avec Société Générale, les commissions, frais et d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

**2.14** – À la demande de Société Générale, selon les volumes d'opérations Cartes acceptées chez lui, respecter les exigences du Référentiel Sécuritaire Accepteur ainsi que celles du Référentiel Sécuritaire PCI DSS annexées aux présentes.

**2.15** – Permettre à Société Générale et/ou au Schéma concerné de faire procéder dans les locaux de l'Accepteur ou dans 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 » s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné. Le rapport d'audit fera systématiquement l'objet d'une communication à l'Accepteur et au 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) à ces clauses et/ou exigences, Société Générale peut procéder, le cas échéant à la demande du(es) Schéma(s) concerné(s), à une suspension de l'acceptation des Cartes portant la (les) Marque(s) dudit (desdits) Schéma(s) concerné(s) par l'audit, voire à la résiliation du présent Contrat, dans les conditions prévues aux articles 6 de la présente Partie et 1 de la Partie 3. En outre, les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

**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°2013-358 du 14 novembre 2013,
- 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 15 (quinze) 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 considéré.

**2.17** – Faire son affaire personnelle des litiges liés à la relation sous-jacente (ex : contrat de vente) qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.

**2.18** – Informer dans les meilleurs délais Société Générale en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation).

**2.19** – En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données Cartes, coopérer avec Société Générale et, le cas échéant, les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire Société Générale à résilier le présent Contrat conformément aux dispositions de l'article 1 de la Partie 3.

## ARTICLE 3 – OBLIGATIONS DE SOCIÉTÉ GÉNÉRALE

Société Générale s'engage à :

**3.1** – Mettre à la disposition de l'Accepteur, selon les Conditions Particulières convenues avec lui, les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.

**3.2** – Fournir à l'Accepteur les informations le concernant directement, sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie B du présent Contrat et son/leur évolution ainsi que la (les) Marque(s) et la (les) Catégorie(s) de carte dont il assure l'acceptation, et les frais applicables à chaque Marque et Catégorie de carte acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

**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 sur 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 ainsi que les méthodes utilisées pour cette acceptation et lui fournir à sa demande le fichier des codes émetteurs (BIN).

**3.6** – Créditer le compte de l'Accepteur des sommes qui lui sont dues au plus tard le jour ouvrable (un jour ouvrable est un jour au cours duquel l'ensemble des personnes impliquées dans l'exécution d'une opération de paiement exerce une activité permettant d'exécuter l'opération de paiement concernée) suivant le moment de réception des enregistrements des opérations de paiement.

Les Parties conviennent que le moment de réception est le jour ouvrable au cours duquel Société Générale reçoit les enregistrements. Toutefois, les enregistrements reçus après 10h00 sont réputés avoir été reçus le jour ouvrable suivant.

**3.7** – Ne pas débiter, au-delà du délai maximum de 15 (quinze) 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 de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par l'Accepteur et de la commission d'interchange.

L'Accepteur peut demander à ce que les informations soient regroupées par Marque, par Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

**3.9** – Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

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

## ARTICLE 4 – GARANTIE DU PAIEMENT ET MESURES DE SÉCURITÉ

**4.1** – Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant au présent article qu'au B des présentes ainsi que dans les Conditions Particulières figurant en Annexe.

Toutes les mesures de sécurité sont indépendantes les unes des autres. En cas de non-respect d'une seule de ces mesures ou lorsque l'opération ne fait pas l'objet d'une authentification forte sur demande de l'Accepteur conformément à l'article 2 de l'Annexe 1, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestations.

Lors du paiement, l'Accepteur s'engage à obtenir de Société Générale un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement. Les conditions d'obtention du justificatif d'acceptation sont décrites à l'article 2 de l'Annexe 1.

### 4.2 – Lors du paiement

L'Accepteur s'engage à :

**4.2.1** – Appliquer la procédure de sécurisation des ordres de paiement (en ce compris la procédure d'authentification) décrite dans les Conditions Générales et en annexe.

**4.2.2** – Vérifier l'acceptabilité de la Carte c'est-à-dire :

- la période de validité (fin et éventuellement début),
- que la Marque est indiquée dans le Contrat de prestation SogeCommerce.

**4.2.3** – Obtenir une autorisation d'un montant identique à l'opération sous-jacente. La demande d'autorisation doit obligatoirement mentionner le CVX2 (cryptogramme visuel, cf. Définition à l'article 2.12). Une réponse de type « interdit », faite par le Système d'Acceptation, annule la garantie pour toutes les transactions faites postérieurement, le même jour avec la même Carte, dans le même point de vente en ligne.

### 4.3 – Après le paiement

L'Accepteur s'engage à :

4.3.1 – Transmettre à Société Générale dans un délai maximum de 6 (six) jours à compter de la transaction, les enregistrements électroniques des opérations et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévues dans le Contrat de prestation SogeCommerce conclu avec Société Générale.

L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par Société Générale doit être obligatoirement remise à cette dernière.

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

4.3.3 – Communiquer par fax ou courrier postal, au plus tard 8 (huit) jours calendaires à compter de leur demande par Société Générale, tout justificatif des opérations de paiement.

4.4 – Les mesures de sécurité énumérées aux articles 4.2 et 4.3 ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 2 de la Partie 3.

## ARTICLE 5 – MODALITÉS ANNEXES DE FONCTIONNEMENT

### 5.1 – Réclamation

Toute réclamation doit être formulée par écrit à Société Générale, dans un délai maximum de 6 (six) mois à compter de la date de l'opération contestée, sous peine de forclusion.

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

En cas de mauvaise exécution, il appartient à l'Accepteur d'établir l'erreur imputable à Société Générale. Si la preuve de l'erreur de Société Générale est démontrée par l'Accepteur, Société Générale remboursera immédiatement ce dernier et rétablira le compte débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu.

### 5.2 – Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à Société Générale.

En cas de conflit entre ces enregistrements, les enregistrements électroniques produits par Société Générale 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 Société Générale et/ou le Schéma.

### 5.3 – 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 ou dans les Conditions Particulières convenues avec Société Générale, effectuer la remise correspondante à Société Générale à qui il avait remis l'opération initiale. Le montant de la « transaction crédit » ne doit pas dépasser le montant de l'opération initiale.

## ARTICLE 6 – SUSPENSION DE L'ACCEPTATION

6.1 – Pour des raisons de sécurité, Société Générale peut procéder, 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.

6.2 – La suspension peut être décidée en raison notamment :

6.2.1 – 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,

6.2.2 – d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,

6.2.3 – 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,

6.2.4 – de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,

6.2.5 – de retard volontaire ou non motivé de transmission des justificatifs,

6.2.6 – d'un risque aggravé en raison des activités de l'Accepteur,

6.2.7 – d'une utilisation d'un Système d'Acceptation non agréé ou non approuvé,

6.2.8 – d'une utilisation anormale ou détournée du Système d'Acceptation.

6.3 – L'Accepteur s'engage alors à restituer à Société Générale les dispositifs techniques et sécuritaires et les documents en sa possession dont Société Générale est propriétaire, et à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes du Schéma concerné.

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

## ARTICLE 7 – MESURES DE PRÉVENTION ET DE SANCTION PRISES PAR SOCIÉTÉ GÉNÉRALE

En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes perdues, volées ou contrefaites, Société Générale 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.

7.1 – Si dans un délai de 30 (trente) 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, Société Générale peut soit procéder à une suspension de l'acceptation des Cartes, dans les conditions précisées à l'article 6 ci-dessus, soit résilier de plein droit avec effet immédiat, le présent Contrat par lettre recommandée avec demande d'avis de réception sous réserve du dénouement des opérations en cours.

7.2 – De même, si dans un délai de 3 (trois) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, Société Générale 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.

7.3 – En cas de suspension ou de résiliation, l'Accepteur s'engage à restituer à Société Générale les dispositifs techniques et sécuritaires et les documents en sa possession dont Société Générale est propriétaire et, à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes, sauf dans le cas où il a conclu un ou plusieurs autre(s) contrat(s) d'acceptation.

## ARTICLE 8 – SECRET BANCAIRE ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

### 8.1 – Secret bancaire

De convention expresse, l'Accepteur autorise Société Générale à stocker, le cas échéant, des données secrètes ou confidentielles portant sur lui et le cas échéant à des entités impliquées dans le fonctionnement du (des) Schéma(s) aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations, qu'elles émanent des titulaires de Cartes ou d'autres entités.

### 8.2 – Protection des données à caractère personnel

Lors de la signature et de l'exécution des présentes, chacune des Parties peut avoir accès à des données à caractère personnel.

Ainsi, en application de la réglementation française et européenne sur la protection des données à caractère personnel, et en particulier du Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel, il est précisé que :

8.2.1 – Les données à caractère personnel relatives à l'Accepteur, collectées par Société Générale nécessaires à l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées que pour les finalités suivantes :

– le traitement des opérations de paiement par Carte. Ce traitement est nécessaire à la bonne exécution du présent Contrat et, à défaut, le Contrat ne pourra être exécuté ;

– la poursuite des intérêts légitimes de Société Générale que constituent la prévention et la lutte contre la fraude à la carte de paiement, la gestion des éventuels recours en justice ainsi que l'élaboration de statistiques anonymes ne permettant pas l'identification du titulaire de la Carte ;

– la réponse aux obligations légales et réglementaires.

Ces données à caractère personnel traitées par Société Générale sont conservées pour les durées suivantes :

– les données nécessaires à l'exécution des opérations de paiement par Carte sont conservées pour une durée de 5 (cinq) ans à compter de la fin de la relation commerciale, le cas échéant, la fin du recouvrement ;

– les données nécessaires à la lutte contre la fraude sont conservées pour une durée maximum de 10 (dix) ans à compter de la clôture du dossier fraude ;

– les données nécessaires à la gestion d'un éventuel recours en justice sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées selon les durées légales de prescription applicables.

Pour satisfaire les finalités précisées ci-dessus, les données à caractère personnel relatives à l'Accepteur pourront être communiquées aux émetteurs, aux Schémas de cartes de paiement dont les marques sont acceptées par l'Accepteur ainsi qu'à toute entité impliquée dans le fonctionnement des Schémas.

Conformément à la réglementation applicable et notamment au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :

- demander à accéder aux données à caractère personnel le concernant et / ou en demander la rectification ou l'effacement;
- définir des directives relatives au sort des données à caractère personnel le concernant après son décès;
- s'opposer au traitement de données à caractère personnel le concernant réalisé aux fins de lutte contre la fraude et / ou de gestion des éventuels recours en justice, sous réserve que Société Générale n'invoque pas de motifs légitimes et impérieux;
- demander des limitations au traitement des données à caractère personnel le concernant dans les conditions prévues à l'article 18 du Règlement (UE) 2016/679 du 27 avril 2016;
- demander à recevoir et / ou transmettre à un autre responsable du traitement les données à caractère personnel le concernant, nécessaires à l'exécution des présentes, sous une forme couramment utilisée et lisible par un appareil électronique.

Ces droits peuvent être exercés et le Délégué à la protection des données peut être contacté :

- à l'agence où est ouvert le compte courant de l'Accepteur associé aux présentes;
- par courrier électronique à l'adresse suivante :  
protectiondesdonnees@societegenerale.fr

Lorsque, après avoir contacté Société Générale, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) estime que ses droits ne sont pas respectés, il peut introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

8.2.2 - À l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les titulaires de Cartes.

L'Accepteur s'engage à respecter la réglementation française et européenne applicable en matière de protection des données à caractère personnel et notamment le Règlement (UE) 2016/679 du 27 avril 2016.

L'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte ainsi que pour les finalités prévues par la Délibération n° 2018-303 du 6 septembre 2018 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat.

L'Accepteur s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour que soient assurées la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de l'article 32 du Règlement (UE) 2016/679 du 27 avril 2016.

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès de Société Générale, de l'intégralité des droits prévus par la réglementation française et européenne applicable en matière de protection des données à caractère personnel, et notamment de leurs droits d'accès, de rectification, d'effacement, d'opposition, de limitation ainsi que de leur droit à la portabilité. À cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

## B. DISPOSITIONS SPÉCIFIQUES À CHAQUE SCHÉMA

### DISPOSITIONS SPÉCIFIQUES AU SCHÉMA CB

#### ARTICLE 1 – DÉFINITION DU SCHÉMA 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 et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'acceptation, Société Générale définissant certaines conditions spécifiques de fonctionnement.

Lorsque Société Générale 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 Société Générale, 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 A 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, même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, pour le paiement de dons ou en contrepartie du règlement du montant de cotisations.

**3.2** - Transmettre les enregistrements des opérations de paiement à Société Générale, dans les délais prévus dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 (six) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma CB.

**3.3** - En cas d'audit par le GIE CB, permettre à Société Générale de faire procéder dans les locaux de l'Accepteur ou dans 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. Le rapport d'audit fera systématiquement l'objet d'une communication à l'Accepteur et au GIE CB.

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) à ces clauses et/ou exigences, Le GIE CB et/ou Société Générale peu(t)(vent) procéder à une suspension de l'acceptation des Cartes CB, voire à la résiliation du présent Contrat, dans les conditions prévues à l'article 4 de la présente Partie. En outre, les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

#### ARTICLE 4 – MESURES DE PRÉVENTION ET DE SANCTION

**4.1** - Mesures de prévention et de sanction mises en œuvre par Société Générale. En cas de manquement de l'Accepteur aux dispositions relatives au Schéma CB du présent Contrat ou aux lois et réglementations 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, Société Générale 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 30 (trente) 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, Société Générale 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 3 (trois) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, Société Générale peut décider de plein droit la résiliation 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 3 (trois) mois suivant la mise en demeure d'y remédier.

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

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

- La radiation de l'adhésion 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 Société Générale les dispositifs techniques et sécuritaires et les documents en sa possession dont Société Générale est propriétaire et à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes CB.

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

À 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 Société Générale, ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son choix.

Cette reprise d'effet ou cette nouvelle adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par le GIE CB ou Société Générale, et portant sur le respect des bonnes pratiques en matière de vente ou de prestations réalisées à distance visées à l'article 2.4 de la Partie A et des mesures de sécurité visées à l'article 4 de la Partie A.

## ARTICLE 5 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Société Générale, au titre de l'acceptation en paiement à distance sécurisée par Cartes, informe que le GIE CB traite des données à caractère personnel de l'Accepteur (personne physique ou personne physique le représentant) qui concernent notamment son identité et ses fonctions.

Ces données à caractère personnel font l'objet de traitements afin de permettre :  
– la prévention et la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB (intérêt légitime) ;

– de répondre aux obligations réglementaires ou légales, notamment en matière pénale ou administrative liées à l'utilisation de la Carte (obligation légale) ;

Les données à caractère personnel traitées par le GIE CB sont conservées pour les durées suivantes :

– en matière de prévention et de lutte contre la fraude, les données utilisées pour l'émission d'alertes sont conservées pour une durée maximale de 12 (douze) mois à compter de l'émission des alertes. En cas de qualification de fraude avérée, les données relatives à la fraude sont conservées au maximum 5 (cinq) années, conformément à la réglementation de la CNIL ;

– les données nécessaires à la gestion d'un éventuel recours en justice sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées selon les durées légales de prescription applicables.

Vous pouvez retrouver le détail des données à caractère personnel traitées par le GIE CB, de leurs durées de conservation, des destinataires de ces données et des mesures de sécurité mises en œuvre pour les protéger dans la Politique de protection des données à caractère personnel du GIE CB accessible à l'adresse suivante : [www.cartesbancaires.com/protegezvosdonnees](http://www.cartesbancaires.com/protegezvosdonnees).

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 8.2.1 de la Partie A en contactant le Délégué par courriel à [protegezvosdonnees@cartes-bancaires.com](mailto:protegezvosdonnees@cartes-bancaires.com).

Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut également contacter son Délégué à la protection des données désigné par le GIE CB par courriel à [protegezvosdonnees@cartes-bancaires.com](mailto:protegezvosdonnees@cartes-bancaires.com).

## DISPOSITIONS SPÉCIFIQUES AUX SCHÉMAS VISA ET MASTERCARD

### ARTICLE 1 – FONCTIONNEMENT DES SCHÉMAS

Les entités responsables des Schémas VISA et MASTERCARD sont :

- VISA Europe et Visa Inc,
- Mastercard Europe S.A.

Les Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes :

- Pour VISA Europe et VISA Inc. :
  - Visa,
  - V PAY,
  - Electron.
- Pour Mastercard Europe S.A. :
  - Mastercard,
  - Maestro.

### ARTICLE 2 – OBLIGATION DE L'ACCEPTEUR

En complément de l'article 2.7 de la Partie A, 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.

### ARTICLE 3 – OBLIGATION DE SOCIÉTÉ GÉNÉRALE

Par dérogation à l'article 3.7 de la Partie A, Société Générale 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.

### ARTICLE 4 – GARANTIE DE PAIEMENT

Pour les opérations de paiement réalisées à l'aide d'une Carte émise hors de l'EEE, la garantie de paiement n'est pas acquise en cas de contestation du titulaire de la Carte liée à la relation sous-jacente.

### ARTICLE 5 – PÉNALITÉS EN CAS DE COMPROMISSION

En cas de compromission (constitue une compromission un événement qui entraîne, directement ou indirectement, l'accès, la divulgation ou la manipulation non autorisé(e) des données des Cartes – ci-après dénommée « Compromission ») résultant d'un manquement de l'Accepteur et/ou d'un/de ses prestataires autre(s) que Société Générale aux exigences du Référentiel Sécuritaire PCI DSS telles que décrites dans le document « ANNEXE 2 - RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR » annexé aux présentes, Société Générale appliquera à l'Accepteur :

**5.1** – Un forfait de 103 000 €,

**5.2** – auquel viendra s'ajouter :

– une pénalité de 3€ par carte dans l'hypothèse où seul le numéro de Carte serait compromis ;

– ou une pénalité de 18€ par carte dans l'hypothèse où le numéro de la Carte ainsi que le cryptogramme visuel seraient compromis.

**5.3** – Dans l'hypothèse où l'Accepteur ne régulariserait pas la situation dans le délai imparti par Société Générale pour ce faire, cette dernière appliquera à l'Accepteur une pénalité supplémentaire de 25 000€ par jour de retard

**5.4** – Toutefois, dans le cas particulier où l'Accepteur répartit ses remises de paiements auprès d'au moins 3 (trois) acquéreurs, Société Générale appliquera, en remplacement de la pénalité complémentaire prévue à l'article 5.2 *supra* un forfait complémentaire conformément à la grille ci-dessous :

Forfait initial	50 000 €
Forfait complémentaire en cas de non régularisation dans les 90 jours	+ 30 000 €
Forfait complémentaire en cas de non régularisation dans les 120 jours	+ 50 000 €
Forfait complémentaire en cas de non régularisation dans les 150 jours	+ 50 000 €
Forfait complémentaire en cas de non régularisation dans les 180 jours	+ 75 000 €

**5.5** – En cas de nouvelle Compromission imputable à l'Accepteur et/ou à un de/ses prestataires autre(s) que Société Générale dans les 36 (trente-six) mois suivant le constat d'une Compromission résultant d'un manquement de sa part et/ou d'un de/ses prestataires autre(s) que Société Générale, Société Générale appliquera à l'Accepteur un forfait supplémentaire de 60 000€.

**5.6** – L'inexécution des exigences issues du Référentiel Sécuritaire PCI DSS sera réputée définitive en cas de survenance d'une Compromission. Dès lors, les pénalités seront dues sans qu'une mise en demeure soit nécessaire. En outre, toutes les pénalités dues au titre d'une Compromission seront débitées sur le compte de l'Accepteur. Société Générale informera au préalable celui-ci afin de lui permettre, le cas échéant, de constituer une provision suffisante.

## CONDITIONS GÉNÉRALES - PARTIE 2: SERVICES SOGECOMMERCE

SogeCommerce est une offre de services (également dénommée les « Services SogeCommerce ») consistant en la mise à disposition de l'Accepteur d'un ensemble de moyens logistiques et humains pour accueillir les paiements lors d'une vente électronique à distance conclue via Internet.

### ARTICLE 1 – MOYENS NÉCESSAIRES À L'UTILISATION DES SERVICES SOGECOMMERCE

SogeCommerce repose sur une plate-forme de paiements sécurisée, élaborée à partir de la solution de paiement sécurisée Payzen dont Lyra Network est propriétaire. Payzen met en œuvre des formulaires adaptés au protocole de paiement par Carte et de certains autres moyens de payer (PayPal, American Express...) disponibles en option.

#### 1.1 – Pré-requis

L'utilisation de SogeCommerce nécessite l'utilisation d'un micro-ordinateur équipé d'un système d'exploitation, d'une connexion à un réseau de communication électronique pour le transport des informations, et des logiciels de communication et de navigation que l'Accepteur installe sur son micro-ordinateur.

L'accès à la plate-forme SogeCommerce se fait via l'utilisation d'un navigateur Internet présentant des normes de sécurité (cryptage notamment) nécessaires audit accès.

Dans le cas où l'Accepteur ne dispose pas de site Internet, SogeCommerce peut être utilisée dans sa version « Lite » (cf. descriptif à l'article 1.2.3) qui ne nécessite aucune intégration ni même de logiciel spécifique à installer sur son ordinateur. L'Accepteur fait son affaire personnelle de son accès à Internet (notamment choix d'un fournisseur d'accès), du choix et de l'installation de son navigateur et du bon fonctionnement de son équipement informatique.

#### 1.2 – Installation

L'Accepteur reçoit par e-mail, après l'ouverture de son Contrat, un identifiant lui permettant d'accéder à son outil de gestion en ligne (dénommé « Back-Office SogeCommerce »). À la première connexion, il lui sera demandé d'entrer son code de première connexion afin de changer nécessairement le mot de passe associé à son identifiant.

##### 1.2.1 – Intégration de SogeCommerce sur le site marchand de l'Accepteur

L'Accepteur devra mettre en place une liaison sécurisée avec la plate-forme, conformément aux instructions figurant dans les guides techniques qui sont mis à sa disposition. Cette liaison est établie par l'intermédiaire de redirections permettant la communication et l'échange de données entre l'Accepteur et la plate-forme SogeCommerce.

Le dialogue entre le site marchand de l'Accepteur et la plate-forme de paiement SogeCommerce s'effectue par un échange de données. Pour créer un paiement, ces données sont envoyées au moyen d'un formulaire HTML via le navigateur de l'acheteur.

La documentation technique et fonctionnelle mise à sa disposition est disponible en libre accès à l'adresse : <https://sogecommerce.societegenerale.eu/doc/>.

À la fin du paiement, le résultat est transmis au site marchand de deux manières :

- automatiquement au moyen de notifications appelées URL de notification instantanée (également appelée IPN pour Instant Payment Notification),
- par le navigateur lorsque l'acheteur clique sur le bouton pour revenir au site marchand.

Pour assurer la sécurité des échanges, les données sont signées au moyen d'un certificat connu uniquement de l'Accepteur et de la plate-forme SogeCommerce. Le certificat est propre à l'Accepteur et à l'environnement utilisé. Il permet, dans les conditions définies dans la documentation technique, d'assurer la confidentialité et l'intégrité des paiements et de vérifier l'identité de l'Acquéreur de la transaction. Chaque certificat est rattaché à un contrat de mise à disposition de la plate-forme de paiement et à un Accepteur.

L'Accepteur devra mettre en œuvre les paramètres décrits dans la documentation technique afin de mettre en place une liaison sécurisée avec la plate-forme SogeCommerce.

L'installation est effectuée par l'Accepteur ou un prestataire technique désigné par l'Accepteur. Il appartient à l'Accepteur de s'assurer que la personne en charge de l'installation dispose des compétences informatiques nécessaires.

Une assistance téléphonique ouverte tous les jours ouvrés (par « jour ouvré », on entend un jour du lundi au vendredi, hors jours fériés) de 9 heures à 18 heures et une assistance par courrier électronique (cf. adresse indiquée dans la documentation technique et fonctionnelle) sont mises à disposition de l'Accepteur ou de son prestataire technique.

Société Générale décline toute responsabilité quant à l'implémentation des Services SogeCommerce, en particulier en cas de bug, virus ou de dysfonctionnement du matériel de l'Accepteur consécutif à la mise en place des redirections requises, à moins de démontrer que ce fait est imputable à Société Générale.

L'Accepteur a la garde juridique de son certificat. À cet égard, il s'engage notamment à les conserver de manière strictement confidentielle et à mettre en place toute mesure de sécurité nécessaire à sa protection.

##### 1.2.2 – Tests et passage en production

L'Accepteur peut effectuer des tests selon la procédure décrite dans la documentation technique mise à sa disposition (cf. modalités décrites ci-dessus). Lorsque l'Accepteur a interfacé la page de paiement de SogeCommerce avec son site marchand, qu'il a effectué les tests de pré-production sur le compte de test, et renvoyé le procès-verbal de recette dûment complété - ou demandé via son Back-Office SogeCommerce à passer en production - Lyra Network s'engage à activer le compte de production dans un délai d'une journée ouvrée complète sous réserve d'absence d'anomalie constatée par Lyra Network.

Les mises en production sont réalisées du lundi au vendredi de 9h30 à 16h30. Société Générale recommande de ne pas utiliser SogeCommerce pour le traitement de véritables opérations de paiement avant que les tests n'aient été réalisés avec succès.

##### 1.2.3 – Mise en place de la version « Lite » de SogeCommerce

L'Accepteur reçoit par e-mail, après l'ouverture de son Contrat, un identifiant lui permettant d'accéder à son outil de gestion en ligne (dénommé « Back-Office SogeCommerce »). À la première connexion, il lui sera demandé d'entrer son code de première connexion afin de changer nécessairement le mot de passe associé à son identifiant.

Cette version permet à l'Accepteur d'accéder aux seules fonctionnalités de paiement suivantes :

- le paiement par e-mail qui permet à l'Accepteur, par le biais de son Back-Office SogeCommerce, d'envoyer un e-mail à son client dans lequel ce dernier trouvera un lien pour accéder à la page de paiement sécurisée SogeCommerce ;
- le paiement par SMS qui permet à l'Accepteur, par le biais de son Back-Office SogeCommerce, d'envoyer un SMS à son client dans lequel ce dernier trouvera un lien pour accéder à la page de paiement sécurisée SogeCommerce ;
- le paiement par URL qui permet à l'Accepteur de créer à partir de son Back-Office SogeCommerce, uniquement un lien de paiement à copier où il le souhaite ;
- le paiement par formulaire hébergé qui permet à l'Accepteur de créer son propre formulaire Web par le biais de son Back-Office SogeCommerce. Hébergé par la plate-forme SogeCommerce, il peut y insérer autant de champs qu'il le souhaite (champs obligatoires, facultatifs, préremplis...). Il suffit ensuite à l'Accepteur de communiquer l'adresse URL de ce formulaire à ses clients pour leur proposer de payer en ligne.

Les modalités de mise en œuvre de ces fonctionnalités sont décrites dans les guides utilisateurs disponibles sur le site Internet documentaire <https://sogecommerce.societegenerale.eu/doc/>.

## ARTICLE 2 – DESCRIPTION DES SERVICES

### Les Services SogeCommerce reposent sur un socle standard composé :

**2.1 – d'un service de paiement en ligne responsive Web design**, (en français : conception de sites Web adaptatifs, c'est-à-dire s'adaptant aux différents canaux de communication comme les Smartphones et tablettes) par Carte des Schémas CB, Visa, Mastercard, en option, par d'autres instruments de paiement, dans un environnement sécurisé par la technologie Transport Layer Security (TLS).

Le cas échéant, l'appel à la plate-forme SogeCommerce permet à l'Accepteur d'intégrer sur son site Internet des boutons permettant à l'internaute de sélectionner le type de moyens de payer qu'il souhaite proposer (Cartes des Schémas CB, Visa et Mastercard, et, en option, d'autres moyens de payer : American Express, Paypal, Prélèvement SEPA...). Une fois la solution de paiement sélectionnée, l'internaute est redirigé vers la page de saisie des informations de paiement correspondante.

#### Paiements par Carte

Lors d'une demande de paiement par Carte des Schémas CB, Visa, Mastercard, les éléments suivants sont contrôlés :

- date de validité égale ou postérieure à la date du jour,
- présence du cryptogramme visuel,
- présence d'un numéro de Carte comportant de 10 à 19 caractères.

Si l'un de ces contrôles se révèle négatif, l'acheteur est invité à recommencer. Après 3 tentatives infructueuses, la transaction est refusée.

Si les contrôles sont positifs, une demande d'authentification est effectuée, dans le cadre du programme 3D Secure. Si l'authentification est possible, l'internaute est redirigé vers la page de saisie de la donnée d'authentification que lui a communiquée sa banque.

La réponse à la demande d'authentification générée par le programme 3-D Secure est systématiquement transmise, quelle qu'en soit l'issue, à l'Accepteur, dans le journal des transactions envoyé chaque matin (le champ prévu à cet effet indique « Yes », « No » ou « n'est pas renseigné »). Elle est également disponible sur l'outil de back-office dans le mode « consultation de transaction ».

Si les contrôles visés ci-dessus sont positifs, et même si l'authentification de l'internaute a échoué, une demande d'autorisation est systématiquement transmise de Société Générale vers la banque de l'acheteur sur la base des

informations (numéro de Carte, date de validité et cryptogramme visuel) communiquées par l'acheteur.

L'Accepteur et l'acheteur sont informés en temps réel du résultat de la demande d'autorisation via un message informatique transmis sur le serveur de l'Accepteur et affiché sur l'écran de l'acheteur.

La transaction autorisée sera envoyée sous forme de remise à Société Générale. À moins que l'Accepteur effectue un paramétrage différent, les remises sont adressées à Société Générale le soir chaque jour ouvré (par « jour ouvré », on entend un jour du lundi au vendredi, hors jours fériés). En cas d'impossibilité d'envoi liée à un problème technique le soir même, la remise est envoyée au plus tard à 10 h 00 le lendemain matin.

**2.2 – d'un Back-Office Sogecommerce** qui permet notamment à l'Accepteur, de consulter, créer (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce), annuler partiellement ou totalement, ou rembourser partiellement ou totalement des transactions effectuées sur son site et de paramétrer l'heure de remise des opérations à Société Générale. L'accès au Back-Office Sogecommerce n'est possible qu'au moyen d'un identifiant et d'un mot de passe. L'identifiant est envoyé à l'adresse électronique indiquée dans le Contrat de prestation Sogecommerce. Le mot de passe est transmis dans un deuxième e-mail adressé à l'Accepteur. L'Accepteur doit prendre toutes les mesures propres à assurer la confidentialité de son identifiant et de son mot de passe.

Le Back-Office Sogecommerce comporte également un outil d'administration des règles de lutte contre la fraude (dénommé « Module de gestion de risque avancée »), un outil de gestion des utilisateurs (accessible sous réserve de l'autorisation préalable de Société Générale).

Le module de gestion de risque avancée (cf. article 2.5 ci-dessous) : il permet à l'Accepteur de gérer les règles de lutte contre la fraude qui pourront s'appliquer à l'un ou plusieurs des moyens de payer de sa boutique, conformément aux instructions figurant dans les guides techniques dont il peut disposer.

L'outil de gestion des utilisateurs : il permet notamment à l'Accepteur de créer, modifier, activer ou désactiver un utilisateur, et de gérer les droits de l'ensemble des utilisateurs.

### 2.3 – d'outils de reporting

Deux journaux de fonds peuvent être transmis quotidiennement par courrier électronique à l'Accepteur :

- le journal des transactions contient l'ensemble des transactions de paiement effectuées par les clients,
- le journal des opérations comprend l'ensemble des opérations (validation, remboursement, annulation, etc.) effectuées par l'Accepteur.

Deux journaux de rapprochement peuvent également être transmis quotidiennement :

- le Journal de Rapprochement Bancaire (JRB), permet de rapprocher les montants crédités ou débités sur le compte de l'Accepteur des transactions initialement saisies.
- le Journal de Rapprochement des Impayés (JRI), permet de rapprocher les impayés débités du compte bancaire de l'Accepteur des transactions initialement saisies.

À cette fin, l'Accepteur autorise via le document figurant à la suite du Contrat de prestation Société Générale à mettre chaque jour à la disposition de Lyra Network les différentes données enregistrées portant sur les transactions traitées et les impayés reçus...

Dans l'hypothèse où l'Accepteur est titulaire de plusieurs Contrats de prestation (autrement dit, dispose de plusieurs sites), il pourra recevoir chaque jour deux journaux de fonds par contrat.

Les données autres que bancaires transitant par Internet ne sont pas protégées et peuvent être falsifiées. Par conséquent, une partie du contenu des journaux de fonds n'est pas garanti et la responsabilité de Société Générale ne pourra donc être engagée à ce titre.

### 2.4 – de modules de paiement open Source

**(excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce)**

L'Accepteur peut télécharger à partir du site <https://sogecommerce.societegenerale.eu/doc/> le Module de paiement Sogecommerce disponible pour la solution E-commerce Open Source utilisée lors de la conception de son site marchand. Les modalités d'installation du module comprennent une documentation complète ainsi que les sources techniques du module de paiement Sogecommerce.

### 2.5 – d'outils sécuritaires via le Module de gestion de risque avancée

Les 21 contrôles opérés sur les transactions doivent être paramétrés par l'Accepteur, via son Back-Office Sogecommerce, en vue de déclencher les actions suivantes :

- bloquer une transaction (entraîne le refus immédiat du paiement),
- déclencher ou désactiver (sous réserve d'acceptation de Société Générale) le recours au dispositif 3D Secure pour le paiement concerné,
- lever une alerte (avertit l'Accepteur selon des cas définis pour mettre en œuvre certains traitements spécifiques ou lancer des vérifications complémentaires sur la/les transaction(s) concernée(s) comme par exemple, la mise en attente d'une livraison),
- Valider manuellement une transaction (permet de bloquer temporairement la remise du paiement afin de vérifier la transaction et décider ou non sa validation ou son annulation si cette dernière est jugée à risque).

Les critères pris en compte par le Module de gestion de risque avancée sont de différentes natures :

- critères issus des données du paiement (informations sur la transaction comme le montant, la devise, le panier, l'acheteur, le pays, l'adresse IP, l'e-mail ...),
- critères issus de l'analyse du type de Carte (CB, Visa, Mastercard, ...), du produit de la carte (consommateur, commerciale, prépayée), du pays émetteur,
- critères issus du résultat de 3D Secure (enrôlement du titulaire de la Carte, statut d'authentification),
- critères issus du résultat de l'autorisation (code retour de l'autorisation, résultat du transfert de responsabilité),
- listes grises pour bloquer le paiement (peuvent être établies sur des Cartes, des adresses IP, des codes BIN, les pays émetteurs de la Carte et le pays des adresses IP).

L'Accepteur a accès à la configuration des contrôles en temps réel via son Back-Office Sogecommerce :

- Contrôles sur le résultat 3D Secure
  - paiement 3D Secure avec un titulaire de Carte dont l'authentification ne peut pas être vérifiée
  - Carte non enrôlée au programme 3D Secure
  - paiement 3D Secure avec une Carte dont l'enrôlement ne peut pas être vérifié
  - transfert de responsabilité
- Contrôle sur le montant
  - contrôle sur le montant (permet de déclencher une(des) action(s) lorsque la transaction est comprise entre un montant minimum et un montant maximum
- Contrôles sur le moyen de paiement
  - contrôle des cartes commerciales
  - contrôle des cartes commerciales suivant leur provenance
  - contrôle des cartes prépayées
  - contrôle des cartes à autorisation systématique
  - contrôle des e-Carte-Bleue
- Contrôles sur le panier
  - contrôle sur le nombre de produits du panier
  - contrôle des produits du panier
- Contrôles sur le pays
  - contrôle du pays de l'acheteur (adresse de facturation)
  - contrôle du pays de livraison
  - contrôle de la variété des pays
  - contrôle sur des produits Carte provenant de certains pays
  - contrôle des pays pour les paiements par prélèvement SEPA
- Contrôles sur la fréquence d'utilisation
  - contrôle sur la fréquence d'utilisation d'une adresse e-mail sur une semaine
  - contrôle sur la fréquence d'utilisation d'une adresse IP sur une semaine
  - contrôle sur la fréquence d'utilisation d'un moyen de paiement sur une semaine
- Contrôle sur le média (canal de communication)
  - contrôle sur le type de média utilisé (ordinateur, tablette, téléphone mobile)

Un ordre de priorité est défini entre certaines actions, comme par exemple :

- l'action « refuser une transaction » est prioritaire sur l'action « valider manuellement »
- l'action « activer 3D Secure » annule les actions de type « désactiver 3D Secure ». Par ailleurs, l'Accepteur a la possibilité de souscrire l'option « Gestion des risques sur-mesure ». Cette option lui permettra d'obtenir une analyse des transactions par des experts de la fraude aux fins de création et mise en place de règles sécuritaires spécifiques à son activité.

### 2.6 – d'un site internet d'information concernant l'état de fonctionnement des services de la plateforme de paiement Sogecommerce.

Ce site, accessible à l'adresse <https://sogecommerce.status.lyra.com/>, permet à l'Accepteur de disposer en temps réel d'un outil de surveillance des performances et du bon fonctionnement de chacun des composants de la plateforme de paiement Sogecommerce (3D Secure, Back-Office marchand, Centre de notifications, Journaux et remises, Moyens de paiement, Paiement par redirection, Service SFTP, Webservices).

Ce site affiche également les informations relatives à la survenue d'incidents et la progression de leur résolution, aux opérations de maintenance en cours ou planifiées.

Les informations se rafraîchissent en temps réel. Un historique des 5 derniers incidents survenus est aussi disponible.

En outre, une fonctionnalité d'abonnement est proposée à l'Accepteur afin qu'il puisse recevoir automatiquement par email (à l'adresse renseignée lors de la souscription du présent contrat) les notifications concernant les informations publiées sur ce site dans le but d'en être systématiquement informé dans les meilleurs délais. Société Générale recommande vivement l'utilisation de cette fonctionnalité accessible en cliquant sur le bouton « S'abonner aux mises à jour » présent sur le site. L'Accepteur peut à tout moment modifier les paramètres des notifications qu'il souhaite recevoir en cliquant sur ce même bouton.»

## ARTICLE 3 – PARTICULARITÉS DE SOGECOMMERCE POUR LES AUTRES SOLUTIONS DE PAIEMENT ET AUTRES OPTIONS

### 3.1 – Acceptation d'autres moyens de payer

L'Accepteur peut, en option, demander à utiliser la plate-forme Sogecommerce pour accepter des moyens de payer autres que des Cartes des Schémas CB, Visa et Mastercard : prélèvement SEPA, Cartes du Schéma American Express, cartes privatives (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce), PayPal, e-Chèques Vacances (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce) notamment.

L'accès à ce service nécessite l'accord de Société Générale (et, dans l'affirmative, la signature d'un avenant au Contrat Sogecommerce) et peut, pour certains d'entre eux, impliquer la conclusion d'un contrat avec un Prestataire de Services de Paiement (ci-après « PSP »).

#### 3.1.1 – Installation

Pour proposer l'un de ces moyens de payer à ses clients, l'Accepteur doit réaliser les paramétrages exposés dans le guide technique dédié mis à sa disposition (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce).

#### 3.1.2 – Description des services optionnels

Pour les cartes privatives (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce), les fonctions du service de paiement en ligne sont détaillées dans la documentation technique mise à disposition de l'Accepteur.

Pour les autres moyens de payer, Sogecommerce consiste à rediriger les clients de l'Accepteur, qui sélectionnent le moyen de payer, soit vers la page de paiement du PSP proposant ce moyen de payer (étant précisé que cette page de paiement n'est pas hébergée par Société Générale), soit vers la page de paiement Société Générale dédiée.

L'Accepteur dispose également d'un outil de gestion et d'outils de reporting tels que décrits à l'article 2. Toutefois, seules les fonctions de l'outil de gestion et les outils reporting mentionnés dans le guide technique pour chaque moyen de payer seront mis à la disposition de l'Accepteur.

### 3.2 – Autres options

En fonction des besoins exprimés par l'Accepteur, Société Générale pourra lui proposer d'autres options.

## ARTICLE 4 – OBLIGATIONS DE SOCIÉTÉ GÉNÉRALE

Société Générale s'engage (à) :

**4.1** – mettre à la disposition de l'Accepteur les services décrits à l'article 2 et, en option, à l'article 3 ;

**4.2** – assurer la maintenance des logiciels utilisés dans le cadre des Services Sogecommerce ;

**4.3** – en cas de dysfonctionnement des moyens de télécommunication mis en œuvre par Société Générale, à intervenir pour rétablir le service dans les meilleurs délais ;

**4.4** – mettre en œuvre dans les délais prévus par le GIE « CB » les évolutions demandées par la communauté des établissements de crédit et de paiement relatives :

– au paiement par Carte, conformément aux règles opérationnelles et aux normes applicables en matière de vente à distance,

– aux raccordements au réseau d'autorisation,

– aux procédures d'authentification des titulaires de cartes et des Accepteurs, conformément aux spécifications techniques approuvées par le GIE « CB » ;

**4.5** – mettre en place les moyens nécessaires pour préserver la confidentialité des informations transmises par l'Accepteur ;

**4.6** – favoriser une disponibilité du service 24h/24 et 7j/7. Sogecommerce pourra toutefois être interrompu temporairement pour des besoins de maintenance et d'évolution. Une information préalable sera publiée en ce sens sur le site internet d'information concernant l'état de fonctionnement des services de la plateforme de paiement Sogecommerce accessible à l'adresse <https://sogecommerce.status.lyra.com/> ; cf article 2.6 de la présente Partie II (Conditions Générales des Services Sogecommerce).

## ARTICLE 5 – OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

**5.1** – collaborer activement et régulièrement avec Société Générale dans l'intérêt du bon fonctionnement des Services Sogecommerce ;

**5.2** – se doter des moyens nécessaires à la bonne exécution de Sogecommerce et à utiliser les moyens mis à sa disposition conformément à ce qui est prévu au présent Contrat ;

**5.3** – s'assurer que les paramétrages des Services Sogecommerce qu'il réalise ainsi que les utilisations qu'il en fait, répond à ses besoins. En cas de doute, l'Accepteur prendra contact avec Société Générale ;

**5.4** – concernant l'ensemble des Services Sogecommerce mis à sa disposition, à ne pas les utiliser pour un autre usage que celui prévu par le présent Contrat, à ne pas les décompiler en dehors de l'exception prévue à l'article L.122-6-1 du Code de la propriété intellectuelle, à respecter les consignes d'utilisation, à installer les mises à jour fournies par Société Générale dans un délai maximum de 6 (six) mois et à informer Société Générale en cas de dysfonctionnement ;

**5.5** – respecter les règles de protection et sécurité des Services Sogecommerce figurant en Annexe 3 ainsi que toute autre mesure de protection dont Société Générale informerait l'Accepteur.

## ARTICLE 6 – RESPONSABILITÉ DE SOCIÉTÉ GÉNÉRALE

**6.1** – Société Générale est responsable de la bonne exécution des prestations, objet des présentes Conditions Générales. Société Générale assume une obligation de mise en œuvre en ce qui concerne la réception des informations. La responsabilité de Société Générale, limitée aux dommages directs, ne pourra être recherchée que s'il est établi qu'elle a commis une faute ou s'est rendue coupable d'une négligence. De convention expresse entre les Parties, est notamment considéré comme préjudice indirect, tout préjudice commercial, perte de chiffre d'affaires, de bénéfice, de commande ou de clientèle.

**6.2** – Les réclamations relatives aux opérations bancaires peuvent être effectuées dans les conditions prévues dans la Partie 1.A. Au cas où la responsabilité de la Banque serait retenue, les Parties conviennent expressément que, toutes sommes confondues, la Banque ne sera pas tenue de payer un montant supérieur aux sommes payées par l'Accepteur au titre des Services Sogecommerce au cours des 12 (douze) derniers mois. Les réclamations relatives au fonctionnement de la plate-forme de paiement ou de l'ensemble des logiciels doivent être formulées dans un délai d'un an, sous peine de prescription des actions y afférentes.

**6.3** – Au cas où la responsabilité de Société Générale serait retenue pour les services techniques, les Parties conviennent expressément que, toutes sommes confondues, Société Générale ne sera pas tenue de payer un montant supérieur aux sommes payées par l'Accepteur au titre du présent Contrat au cours des 12 (douze) derniers mois.

**6.4** – La responsabilité de la Banque ne pourra jamais être engagée :

– pour tout dommage lié au non respect par l'Accepteur des préconisations d'installation des logiciels, et tout dommage lié à leur utilisation ;

– pour tout dommage lié au fait que les services ne sont pas conformes à des besoins spécifiques envisagés par l'Accepteur ;

– pour tout dommage lié au non respect par l'Accepteur de dispositions légales ou du droit des tiers sur son site Internet ;

– pour tout dommage lié à l'inexécution de ses obligations tenant à un cas de force majeure.

Outre les cas habituellement retenus par la jurisprudence française, les Parties conviennent expressément de considérer comme cas de force majeure : les grèves totales ou partielles des prestataires de la Banque, les intempéries, les épidémies, incendies, tempêtes, inondations, dégâts des eaux, les blocages des réseaux de télécommunications et tous autres cas indépendants de la volonté expresse des Parties empêchant l'exécution normale du Contrat.



## **ARTICLE 7 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL**

L'expression « Données à caractère personnel » désigne toute information se rapportant à une personne identifiée ou identifiable, directement ou indirectement, en particulier par référence à un numéro d'identification ou à un ou plusieurs élément(s) spécifique(s) la concernant.

Société Générale et l'Accepteur s'engagent à respecter l'ensemble des obligations résultant de la réglementation relative à la protection des données à caractère personnel et de la vie privée applicables dans le cadre des présentes, spécialement les obligations issues du Règlement (UE) 2016/679 du 27 avril 2016. Société Générale et l'Accepteur s'engagent à collaborer activement afin de permettre l'accomplissement des formalités leur incombant. Chaque Partie s'abstient de toute action susceptible de mettre l'autre Partie en situation de manquement au Règlement précité.

Par ailleurs, l'Accepteur s'engage à :

- se conformer à l'obligation d'information des personnes concernées telle que prévue aux articles 13 et 14 du Règlement susmentionné et faire figurer sur tout document ayant pour objet la collecte de Données à caractère personnel (questionnaire ou formulaire, par exemple) les informations prévues par ledit article, dont les modalités d'exercice des droits d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition et à la portabilité, ainsi que les éventuels transferts de données en dehors de l'Espace Économique Européen. Par ailleurs, l'Accepteur s'engage d'ores et déjà à permettre l'exercice de ces droits;
- prendre, et s'assurer que son personnel et toute personne agissant en son nom et pour son compte prend, dans le strict respect de ses obligations contractuelles, toute mesure nécessaire pour préserver et faire respecter l'intégrité, la sécurité et la confidentialité des Données à caractère personnel ;
- satisfaire avec diligence par écrit aux demandes d'information de Société Générale, dans un délai de 5 (cinq) jours ouvrés (par « jour ouvré », on entend un jour du lundi au vendredi, hors jours fériés) à compter de la demande, afin de lui permettre de répondre (i) aux demandes d'exercice de leurs droits présentées par les personnes concernées ou (ii) aux demandes présentées par les autorités de protection des données ou par ses délégués à la protection des données (« data protection officers »);
- informer sans délai Société Générale de toute demande ayant trait aux Données à caractère personnel.

## **ARTICLE 8 – DROITS DE PROPRIÉTÉ INTELLECTUELLE**

Il n'y a pas de transfert des droits de propriété intellectuelle sur l'ensemble des logiciels (versions actuelles et futures) et les documentations mis à disposition de l'Accepteur par Société Générale dans le cadre du présent Contrat. Leur utilisation par l'Accepteur est impérativement limitée aux fonctions décrites et nécessaires à l'exécution du présent Contrat. Le droit d'utilisation de l'ensemble des logiciels susvisés n'emporte pas le droit de faire toute opération interdite telle qu'indiquée ci-après, y compris dans le cadre de sa destination contractuelle. Par « opération interdite » les Parties entendent la reproduction permanente ou provisoire de l'ensemble des logiciels autre qu'une copie de sauvegarde, en tout ou en partie par tout moyen et sous toute forme, ainsi que la traduction, l'adaptation, l'arrangement ou toute autre modification de l'ensemble des logiciels et la reproduction de l'ensemble des logiciels en résultant, la correction desdits éléments par soi-même ou par des tiers des éventuelles anomalies des éléments de l'ensemble des logiciels, la mise sur le marché à titre onéreux ou gratuit. L'Accepteur est responsable de l'ensemble des services, informations, signes, images ou de toutes autres données figurant sur son site Internet.

## **ARTICLE 9 – SUSPENSION DES SERVICES**

Société Générale se réserve la possibilité à tout moment, sans préavis et sans formalité particulière, de suspendre l'accès à tout ou partie des fonctionnalités de la plate-forme SogeCommerce ou de fermer l'accès à la plate-forme pour des raisons de sécurité, notamment en cas de risque de fraude ou de risque d'atteinte à la confidentialité des données. Société Générale prendra contact avec l'Accepteur dans les plus brefs délais pour l'informer des raisons de ces modifications ou de la fermeture d'accès.

## **ARTICLE 10 – PROTECTION DES FICHIERS ET DOCUMENTS**

L'Accepteur se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à Société Générale en constituant un double de ceux-ci. L'Accepteur se déclare à cet égard pleinement informé de la nécessité d'une part, de vérifier la qualité et l'exhaustivité de ses sauvegardes informatiques, d'autre part, de réaliser des sauvegardes multiples. Pour sa part, et sous réserve du respect de ces obligations de sauvegarde par l'Accepteur, Société Générale s'engage à reconstituer dans les meilleurs délais les documents et fichiers qui auraient été confiés, et qui viendraient à être perdus ou auraient été rendus inutilisables par sa faute, sous réserve que l'Accepteur lui fournisse les données nécessaires à leur reconstitution. Dans ce cas, l'Accepteur renonce à tout autre recours contre Société Générale hormis cette reconstitution.

## **ARTICLE 11 – SÉCURITÉ**

La sécurité du paiement entre le poste acheteur de l'internaute et le service de paiement SogeCommerce repose sur la mise en œuvre d'une technologie sécurisée appelée Transport Layer Security (TLS). Les informations relatives au paiement sont systématiquement chiffrées lorsqu'elles circulent sur Internet. Société Générale gère la sécurité des échanges et s'assure de la protection des secrets (clés de chiffrement) et de leur gestion (tirage, affectation, constitution de certificat, changement périodique...) selon les niveaux spécifiés par les Schémas (GIE « CB », Visa, Mastercard, American Express...). La plate-forme de paiement sécurisée qui assure le Traitement des données des cartes bancaires répond aux exigences du standard PCI-DSS.

Le transport des informations entre l'Accepteur, Société Générale et la plate-forme de paiement Lyra Network est effectué par l'intermédiaire d'un réseau de transmission de données qui n'est pas géré par Société Générale. Elle n'assume donc aucune responsabilité en ce qui concerne le transport des informations.

## **ARTICLE 12 – CONVENTION SUR LA PREUVE**

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à Société Générale. En cas de conflit, les enregistrements électroniques produits par Société Générale ou le GIE « CB » prévaudront sur ceux produits par l'Accepteur « CB », à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par Société Générale ou le GIE « CB ».

## **ARTICLE 13 – APPROBATION DES DOCUMENTS**

Tous documents, comptes rendus, rapports d'analyse fonctionnelle ou organique, applications ou autres adressés par Société Générale à l'Accepteur dans le cadre de l'exécution de l'intervention, seront considérés comme approuvés sans réserve s'ils n'ont fait l'objet d'une contestation par écrit dans les 15 (quinze) jours de leur réception. L'Accepteur s'oblige, en conséquence, à les examiner avec tout le soin et la diligence requis.

## **ARTICLE 14 – RÉFÉRENCIEMENT ET MARQUES**

Sauf convention contraire, Société Générale est autorisée au seul droit, non exclusif, pour la durée du présent Contrat, à citer à titre de référence le nom de l'Accepteur et les prestations réalisées.

Les marques SogeCommerce et Société Générale étant déposées, elles ne peuvent être utilisées sans l'autorisation préalable et écrite de Société Générale. Toutefois, Société Générale accorde à l'Accepteur, le seul droit, non exclusif, pour la durée du présent Contrat, de faire figurer les éléments du logo SogeCommerce et Société Générale, sur les pages réservées au paiement dans le cadre de la mise en place de la solution SogeCommerce. Dans le cas où l'Accepteur utilise les éléments du logo, la mise en exploitation de SogeCommerce se fait après accord de Société Générale.

## CONDITIONS GÉNÉRALES - PARTIE 3: CONDITIONS COMMUNES AUX PARTIES 1 ET 2

Les dispositions ci-dessous s'appliquent à l'ensemble des prestations rendues par Société Générale dans le cadre de l'Offre SogeCommerce.

### ARTICLE 1 – DURÉE ET RÉSILIATION DU CONTRAT

**1.1** – Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans le Contrat de prestation SogeCommerce.

L'Accepteur d'une part, Société Générale d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les Parties), sous réserve du dénouement des opérations en cours, mettre fin au présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. Par ailleurs, le présent Contrat sera automatiquement résilié en cas de clôture du compte courant de l'Accepteur qui y est associé. L'Accepteur garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.

**1.2** – En outre, à la demande de tout Schéma, Société Générale 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 aux articles 7.1 et 7.2 de la Partie 1. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

**1.3** – 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 révélerait des impayés, ceux-ci seront à la charge de l'Accepteur et pourront faire l'objet d'une déclaration de créances.

**1.4** – L'Accepteur est tenu de restituer à Société Générale les dispositifs techniques et sécuritaires, les logiciels et les documents en sa possession dont Société Générale est propriétaire.

Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation, l'Accepteur s'engage à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes et toute éventuelle référence à Société Générale.

**1.5** – La résiliation de la prestation de service de paiement décrite en Partie 1 ou de la prestation de service technique décrite en Partie 2 emporte résiliation du présent Contrat.

**1.6** – Société Générale peut suspendre ou résilier le Contrat sans préavis, sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception, dès lors qu'il est informé de l'illicéité du contenu du site Internet de l'Accepteur.

**1.7** – Aucune indemnité ne pourra être demandée du fait de l'exercice régulier par l'une des Parties des droits de résiliation que lui confère le présent article.

### ARTICLE 2 – MODIFICATIONS

**2.1** – Société Générale peut modifier à tout moment les dispositions du présent Contrat.

Société Générale peut notamment apporter :

- des modifications techniques telles que l'acceptation de nouvelles Cartes, les modifications de logiciels, le changement de certains paramètres, la remise en l'état du Système d'Acceptation à la suite d'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.

**2.2** – Les nouvelles conditions entrent en vigueur au terme d'un délai minimum fixé à 1 (un) mois à compter de la notification sur support papier ou sur tout autre support durable.

**2.3** – Ce délai est exceptionnellement réduit à 5 (cinq) jours calendaires lorsque Société Générale ou le Schéma constate une utilisation anormale de Cartes perdues, volées ou contrefaites, ou encore détecte un risque particulier de fraude.

**2.4** – En cas de désaccord, l'Accepteur a la possibilité de résilier son Contrat, selon les modalités prévues à l'article 1. Passé le délai de préavis, l'Accepteur est réputé avoir accepté les modifications s'il n'a pas résilié le Contrat, sans que Société Générale ait à lui rappeler cette faculté.

**2.5** – Le non-respect des nouvelles conditions techniques et sécuritaires, dans les délais impartis, peut entraîner la suspension par Société Générale de l'acceptation des Cartes portant la (les) Marque(s) du (des) Schéma(s) concerné(s), dans les conditions prévues à l'article 6 de la partie 1 du présent Contrat, voire à la résiliation du Contrat, dans les conditions prévues à l'article 1 de la présente Partie.

### ARTICLE 3 – CONDITIONS FINANCIÈRES

Les conditions financières sont déterminées dans le Contrat de Prestation SogeCommerce ou dans tout autre document approuvé par les Parties. Sauf disposition contraire, les prix sont exprimés hors taxes, hors éventuels frais de transport et d'expédition.

Lorsque les conditions financières font référence au tarif en vigueur selon la brochure tarifaire applicable à l'Accepteur, ce tarif peut être modifié selon les modalités prévues dans les conditions générales de fonctionnement du compte sur lequel les opérations sont facturées.

Les sommes dues au titre de SogeCommerce sont débitées sur le compte de l'Accepteur. L'abonnement mensuel est débité au début de chaque mois.

Sauf accord contraire des Parties, les commissions sont imputées sur le montant des opérations créditées.

Tout mois commencé est entièrement dû.

Dans le cas où des frais ou commissions ne seraient pas réglés dans les 30 (trente) jours de leur exigibilité, Société Générale, après une relance de l'Accepteur par lettre recommandée avec demande d'avis de réception restée vaine pendant 8 (huit) jours, aura la faculté de suspendre les Services SogeCommerce jusqu'au règlement des sommes dues, sans que cette suspension puisse être considérée comme une résiliation de Contrat du fait de Société Générale ouvre un quelconque droit à indemnisation pour l'Accepteur. En outre, à compter du 31<sup>e</sup> (trente et unième) jour, la somme due portera intérêt au taux de 3 fois le taux d'intérêt légal sans qu'une mise en demeure préalable ne soit nécessaire.

### ARTICLE 4 – NON-RENONCIATION

Le fait par l'Accepteur ou pour Société Générale 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'en soit, à l'exécution de celle-ci.

### ARTICLE 5 – LOI APPLICABLE/TRIBUNAUX COMPÉTENTS

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

### ARTICLE 6 – LANGUE DU PRÉSENT CONTRAT

Les présentes Conditions Générales et Particulières (en ce compris le Contrat de prestation) constituent le Contrat original rédigé en langue française qui est le seul qui fait foi.

## ANNEXE 1 - CONDITIONS PARTICULIÈRES

Les Conditions Particulières du Contrat Sogecommerce comprennent les dispositions figurant dans le présent document ainsi que celles figurant dans le Contrat de prestation Sogecommerce ainsi que tout autre document émanant de Société Générale et approuvé par l'Accepteur.

### 1 – ACCEPTATION DES CARTES AUTRES QUE LES CARTES DES SCHÉMAS CB, VISA ET MASTERCARD

Pour pouvoir accepter des Cartes telles que des Cartes American Express, l'Accepteur doit conclure un contrat d'acceptation avec le Schéma concerné.

Les règlements des transactions par American Express sont effectués dans les conditions convenues dans ce contrat.

### 2 – JUSTIFICATIF D'ACCEPTATION

En adhérant aux Services Sogecommerce, l'Accepteur demande à être inscrit dans le programme 3D Secure auprès des Schémas CB (Paiement sécurisé CB), Visa (VisaSecure©) et Mastercard (Mastercard Identity Check©).

Ce dernier génère, pour les paiements effectués au moyen de Cartes portant les marques CB, Visa, V PAY, Electron, Mastercard ou Maestro par un internaute à partir de la page de paiement Sogecommerce de l'Accepteur, en complément de la demande d'autorisation, une demande d'authentification du titulaire de la Carte. L'Accepteur peut toutefois demander à l'émetteur (uniquement au titre de 3D Secure V2 et dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30 € ou d'un Paiement Récurrent de rang supérieur à 1) de ne pas appliquer de procédure d'authentification forte du titulaire de la carte. L'émetteur est libre d'accepter ou non la demande.

Si l'émetteur accepte, les opérations réalisées sans authentification forte sont effectuées sans justificatif d'acceptation.

La réponse à la demande d'authentification forte ou à la demande d'exemption à l'authentification forte est systématiquement transmise à l'Accepteur dans le journal des transactions envoyé chaque matin. Elle est également disponible via le Back-Office Sogecommerce, menu « Gestion » / onglet « Transactions en cours ». L'Accepteur s'interdit de demander au titulaire de la Carte de lui communiquer le code d'authentification ou de sécurité que lui a transmis l'émetteur de la Carte, à l'exception du cryptogramme visuel.

**L'obtention du justificatif d'acceptation visé à l'article 4.1 des Conditions Générales – Partie 1 – Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement - A - Conditions générales communes à tous les schémas se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.**

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement. Lorsque la Carte n'est pas émise par Société Générale, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'émetteur à Société Générale.

Société Générale pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

### 3 – MODALITÉS PARTICULIÈRES DE PAIEMENT À DISTANCE PAR CARTES DES SCHÉMAS CB, VISA OU MASTERCARD

#### 3.1 – Dispositions communes à l'ensemble des modalités particulières

Les modalités particulières de paiement à distance par Cartes des Schémas CB, Visa ou Mastercard visées au présent article sont accessibles sur demande expresse de l'Accepteur et sous réserve de l'acceptation de Société Générale.

L'Accepteur reconnaît avoir été informé que ces modalités ne constituent pas un mode normal d'utilisation du Système d'Acceptation et accepte de supporter les risques y afférents.

#### 3.2 – La création à partir d'un numéro de Carte (excepté dans le cadre de l'utilisation de la version « Lite » de Sogecommerce)

L'Accepteur peut transmettre à Société Générale une opération de paiement qu'il a constituée à partir des données que son client lui communique par téléphone, fax, e-mail ou autre canal de communication. Pour constituer une transaction, l'Accepteur doit obtenir le numéro de la Carte, sa date de validité et le cryptogramme visuel. L'Accepteur s'engage à ne constituer que des opérations pour lesquelles un ordre de paiement par Carte lui a été préalablement donné. Par dérogation à l'article 4 des Conditions Générales – Partie 1: Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les paiements à distance réalisés selon ces modalités ne sont pas garantis en cas de contestation du titulaire de la Carte.

#### 3.3 – L'annulation

L'Accepteur peut annuler totalement ou partiellement une transaction avant que celle-ci ne soit transmise à Société Générale.

L'accepteur s'engage à obtenir l'accord du titulaire de la Carte avant d'annuler totalement ou partiellement une opération. Par dérogation à l'article 4 des Conditions Générales – Partie 1: Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les opérations partiellement annulées ne sont pas garanties si le titulaire de la Carte conteste le montant de l'opération.

#### 3.4 – Le paiement différé supérieur à 6 jours

L'Accepteur peut prévoir, par l'intermédiaire de Sogecommerce, de transmettre à Société Générale une opération de plus de 6 (six) jours après qu'elle ait été effectuée. Dans ce cas, la demande d'autorisation pour le montant total de l'opération est effectuée avant la transmission de l'opération à Société Générale. Par dérogation à l'article 4 des Conditions Générales – Partie 1: Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les paiements à distance réalisés selon ces modalités ne sont pas garantis si le titulaire de la Carte conteste avoir donné un ordre de paiement ou le montant de l'opération.

## ANNEXE 2 – RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR

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

### EXIGENCE 1 (E1)

#### GÉRER LA SÉCURITÉ DU SYSTÈME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE

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

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

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

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

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

### EXIGENCE 2 (E2)

#### GÉRER L'ACTIVITÉ HUMAINE ET INTERNE

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

Les obligations et les responsabilités du personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.

Le personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.

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

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

### EXIGENCE 3 (E3)

#### GÉRER LES ACCÈS AUX LOCAUX ET AUX INFORMATIONS

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

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

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

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

### EXIGENCE 4 (E4)

#### ASSURER LA PROTECTION LOGIQUE DU SYSTÈME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

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

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

### EXIGENCE 5 (E5)

#### CONTRÔLER L'ACCÈS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION

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

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

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

### EXIGENCE 6 (E6)

#### GÉRER LES ACCÈS AUTORISÉS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

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

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

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

### EXIGENCE 7 (E7)

#### SURVEILLER LES ACCÈS AU SYSTÈME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée. Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

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

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

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

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

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

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

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

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

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

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

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

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

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions du Règlement (UE) 2016/679 du 27 avril 2016 et aux recommandations de la CNIL.

Il en est de même pour l'authentifiant de l'Accepteur et les éléments secrets servant à chiffrer.

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

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

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

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

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

## **EXIGENCE 16 (E16) RESPECTER LE STANDARD « PAYMENT CARD INDUSTRY – DATA SECURITY SYSTEM (PCI DSS) »**

En souscrivant le contrat SogeCommerce, vous adhérez également à ce standard intitulé PCI DSS dont le détail peut être obtenu sur le site Internet: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Les obligations ou recommandations qui incombent aux commerçants sont fonction du nombre de transactions annuelles effectuées sur le site marchand. Quatre niveaux ont été définis. Nous vous invitons à vous reporter au document « Programme PCI/DSS – SOGECOMMERCE » ci-après afin de prendre connaissance du niveau de votre entreprise.

# PROGRAMME PAYMENT CARD INDUSTRY DATA SECURITY SYSTEM (PCI- DSS) DE VISA ET MASTERCARD

## NIVEAUX ET ACTIONS À MENER PAR LE COMMERÇANT POUR LA CONFORMITÉ ET VALIDATION

Sources : programmes PCI-DSS des Schémas Visa et Mastercard

AIS: Account Information Security, SDP: Site Data Protection.

[https://usa.visa.com/support/small-business/security-compliance.html?ep=v\\_sym\\_cisp#2](https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp#2)

<https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html>

CATÉGORIE	CRITÈRES	ACTIONS À MENER PAR LE COMMERÇANT/BASE ANNUELLE
<b>VISA</b>		
<b>NIVEAU 1</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel de transactions Visa tous canaux (à proximité et à distance) &gt; 6 millions ou commerçant Global (i.e. opérant sur plusieurs pays)</li> </ul>	<ul style="list-style-type: none"> <li>Déposer un Rapport de conformité (« ROC ») réalisé par un QSA (Qualified Security Assessor) ou une ressource interne si signé par un représentant de l'entreprise</li> <li>Soumettre un Formulaire d'Attestation de Conformité (« AOC »)</li> </ul>
<b>NIVEAU 2</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel de transactions Visa tous canaux de 1 à 6 million(s) tous canaux</li> </ul>	<ul style="list-style-type: none"> <li>Remplir un Questionnaire de l'Auto-Audit (« SAQ »)</li> <li>Soumettre un Formulaire d'Attestation de Conformité (« AOC »)</li> </ul>
<b>NIVEAU 3</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel de transactions Visa e-com de 20k à 1 million</li> </ul>	<ul style="list-style-type: none"> <li>Remplir un Questionnaire de l'Auto-Audit (« SAQ »)</li> <li>Soumettre un Formulaire d'Attestation de Conformité (« AOC »)</li> </ul>
<b>NIVEAU 4</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel de transactions Visa e-com &lt; 20k ou tout autre commerçant ayant un volume annuel de transactions Visa jusqu'à 1 million</li> </ul>	<ul style="list-style-type: none"> <li>Remplir un Questionnaire de l'Auto-Audit (« SAQ ») ou procéder à un exercice de validation alternative comme défini par l'acquéreur</li> </ul>
<b>MASTERCARD</b>		
<b>NIVEAU 1</b>	<ul style="list-style-type: none"> <li>Commerçant qui a subi un piratage ou une attaque ayant déclenché un événement de compromission dite "Account Data Compromise" (« ADC »)</li> <li>Commerçant ayant un volume annuel total de transactions combinées Mastercard et Maestro &gt; 6 millions</li> <li>Commerçant ayant un volume annuel de transactions Visa tous canaux (à proximité et à distance) &gt; 6 millions ou commerçant Global (i.e. opérant sur plusieurs pays)</li> <li>Commerçant portant plusieurs failles de sécurité devant recevoir une autre qualification que « ADC » et présentant un risque pour le système de paiement</li> </ul>	<ul style="list-style-type: none"> <li>PCI DSS audit annuel visant à accomplir un Rapport de Conformité ("ROC")</li> </ul> <p>N.B. : Le ROC doit être conduit par un « QSA » (PCI SSC-approved Qualified Security Assessor) ou un auditeur interne (Internal Security Assessor ou « ISA ») certifié « PCI SSC »</p>
<b>NIVEAU 2</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel total de transactions combinées Mastercard et Maestro &gt; 1 million mais &lt;= 6 millions</li> <li>Commerçant ayant un volume annuel de transactions Visa tous canaux de 1 à 6 million(s) tous canaux</li> </ul>	<ul style="list-style-type: none"> <li>Questionnaire de l'Auto-Audit (« SAQ »)*</li> </ul> <p>N.B. : Les commerçants remplissant le SAQ A, SAQ A-EP ou SAQ D doivent en outre engager un QSA ou auditeur interne certifié « PCI SSC » pour la validation de conformité</p>
<b>NIVEAU 3</b>	<ul style="list-style-type: none"> <li>Commerçant ayant un volume annuel total de transactions e-com combinées Mastercard et Maestro &gt; 20k mais &lt;= 1 million</li> <li>Commerçant répondant aux critères de niveau 3 de Visa</li> </ul>	<ul style="list-style-type: none"> <li>Questionnaire de l'Auto-Audit (« SAQ »)*</li> </ul>
<b>NIVEAU 4</b>	<ul style="list-style-type: none"> <li>Tout autre commerçant**</li> </ul>	<ul style="list-style-type: none"> <li>Questionnaire de l'Auto-Audit (« SAQ »)*</li> </ul>

\* Les commerçants du niveau 2, 3 ou 4 peuvent alternativement, à leur discrétion, engager un QSA ou un ISA certifié PCI DSS à réaliser un ROC.

\*\* Les commerçants du niveau 4 doivent se conformer à PCI DSS. Ils doivent consulter leur acquéreur afin de déterminer si la validation de la conformité est aussi requise.

La documentation relative à PCI DSS (ROC, SAQ etc.) : [https://www.pcisecuritystandards.org/document\\_library](https://www.pcisecuritystandards.org/document_library)

QSA (Qualified Security Assessor) = prestataire spécialisée dans la sécurité informatique certifié pour la réalisation d'audits PCI-DSS. La liste des QSA certifiés par PCI DSS : [https://www.pcisecuritystandards.org/assessors\\_and\\_solutions/qualified\\_security\\_assessors](https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors).

## **1 – INFORMATIONS IMPORTANTES RELATIVES AU CERTIFICAT ET À LA SÉCURITÉ DES ÉCHANGES**

Le dialogue entre le site marchand de l'Accepteur et la plate-forme de paiement SogeCommerce s'effectue par un échange de données. Pour créer un paiement, ces données sont envoyées au moyen d'un formulaire HTML via le navigateur de l'acheteur. À la fin du paiement, le résultat est transmis au site marchand de deux manières :

- automatiquement au moyen de notifications appelées URL de notification instantanée (également appelée IPN pour Instant Payment Notification) ;
- par le navigateur lorsque l'acheteur clique sur le bouton pour revenir au site marchand.

Pour assurer la sécurité des échanges, les données sont signées au moyen d'un certificat connu uniquement de l'Accepteur et de la plate-forme de paiement (cf. article 1.2 des Conditions générales – Partie 2 : Services SogeCommerce).

Deux types de certificat sont mis à disposition :

- le certificat de test qui permet de générer la signature d'un formulaire en mode test.
- le certificat de production qui permet de générer la signature d'un formulaire en mode production.

## **2 – RÈGLES ÉLÉMENTAIRES DE PROTECTION DU CERTIFICAT**

L'intégrité des informations échangées est garantie par un échange de signatures numériques entre la plate-forme de paiement SogeCommerce et le site marchand de l'Accepteur.

Dès le premier paiement réalisé avec une Carte réelle, le certificat de production est masqué pour des raisons de sécurité. L'Accepteur s'engage à ne pas stocker son certificat dans un fichier facilement accessible et notamment via Internet. En cas de perte, l'Accepteur aura la possibilité d'en générer un nouveau depuis son Back-Office SogeCommerce (cf. article 2.2 des Conditions Générales – Partie 2 : Services SogeCommerce).

# NOTE D'INFORMATION

## ACCEPTATION EN PAIEMENT À DISTANCE SÉCURISÉ VIA SOGECOMMERCE

Vous venez de souscrire un contrat Sogecommerce auprès de notre établissement, et nous vous en remercions. Nous espérons que l'accès au paiement par Carte sur Internet contribuera au développement de votre chiffre d'affaires. Aussi, afin que cette activité se déroule dans de bonnes conditions, nous souhaitons vous faire quelques recommandations s'agissant de l'encaissement des transactions et des Services Sogecommerce et vous livrer de plus amples informations concernant la procédure de sécurisation des ordres de paiement et les journaux de transactions.

### RECOMMANDATIONS CONCERNANT L'ENCAISSEMENT DES TRANSACTIONS

Afin de limiter le risque de fraude et d'impayé, nous vous recommandons la plus grande vigilance vis-à-vis des transactions qui seront effectuées sur votre site, notamment dans les cas suivants :

- si l'adresse de livraison est différente de l'adresse de résidence ou bien s'il s'agit d'une poste restante, d'un hôtel, d'un hôpital ou tout autre lieu à caractère public ;
- s'il s'agit de commandes répétitives émanant d'un même client, qui plus est si celui-ci est un nouveau client ;
- si l'on vous demande, pour des montants importants, de fractionner la somme due (sans doute pour obtenir plus facilement une autorisation) ;
- s'il s'agit d'un règlement effectué avec une Carte étrangère pour une livraison vers un pays différent de celui de la Carte ou bien si l'origine de la Carte correspond à un pays dit « à risque » en matière de transactions internationales ;
- si le client vous propose une autre Carte alors qu'une demande d'autorisation a été refusée sur une (ou plusieurs) Carte(s) utilisée(s) précédemment.

Dès lors qu'une transaction vous semble suspecte, nous vous invitons soit à proposer à votre client un autre moyen de paiement, soit à annuler la transaction à l'aide de votre Back-Office Sogecommerce.

Vous devez également prévoir la saisie obligatoire de l'adresse e-mail de vos clients sur les bons de commande en ligne et envoyer systématiquement un accusé de réception afin de repérer les e-mails non délivrés.

### RECOMMANDATIONS CONCERNANT LES SERVICES SOGECOMMERCE

#### – Généralités.

Vous disposez aussi de la « remontée d'information du code ISO » de la Carte qui vous permet d'identifier le pays d'origine de la Carte utilisée sur votre site.

De plus, nous vous conseillons vivement de mettre en place les outils sécuritaires mis à votre disposition et détaillés dans le Contrat de prestation Sogecommerce.

Votre Back-Office Sogecommerce vous permet d'annuler une transaction totalement ou partiellement avant son envoi en compensation, c'est-à-dire tant que le délai de capture n'est pas atteint. Par défaut, le délai de capture est fixé à zéro, ce qui signifie que les transactions sont transmises à la banque le soir même.

Si vous avez besoin d'allonger le délai vous permettant d'annuler une transaction, vous devez paramétrer un délai de capture supérieur à zéro.

Attention, au-delà de 6 (six) jours, la demande d'autorisation pour le montant total de l'opération n'est effectuée qu'avant la transmission de l'opération à la Banque.

#### – Informations concernant la procédure de sécurisation des ordres de paiement.

Le protocole 3D Secure (ci-après dénommé « 3DS » et, dans sa première version, « 3DS V1 ») a pour objet la mise en œuvre, par l'émetteur de la Carte (ci-après dénommé « l'Émetteur »), de moyens techniques aux fins d'authentification forte du titulaire de la Carte.

Ce protocole a évolué (ci-après dénommé « 3DS V2 ») dans le but notamment de se conformer aux exigences de la Directive (UE) 2015/2366 dite « DSP2 » et des normes techniques en découlant (Règlement Délégué (UE) 2018/389) dites « RTS SCA ».

Dans le cadre de 3DS V2, la décision d'authentification du titulaire de la Carte appartient à l'Émetteur. Cette authentification est réalisée soit en interaction avec le titulaire de la Carte (il y a alors authentification forte), soit sans interaction avec ce dernier (dans les cas où une exemption à l'authentification forte est possible), au moyen d'un certain nombre d'informations relatives au contexte de l'opération de paiement (à minima nom et adresse électronique du titulaire de la Carte ainsi que l'adresse de facturation). Votre attention est attirée sur le fait que certaines opérations de paiement ne peuvent être réalisées dans le cadre de 3DS en raison notamment de la catégorie de la Carte avec laquelle l'opération de paiement est effectuée (ex: cartes prépayées anonymes) ou du mode de paiement utilisé (ex: paiement en l'absence du titulaire de la Carte comme le paiement récurrent).

Par ailleurs, vous vous interdisez de demander au titulaire de la Carte la communication du code d'authentification ou de sécurité que lui a transmis l'Émetteur, à l'exception du cryptogramme visuel.

#### • Pré-requis

La mise en œuvre de 3DS V2, comme de 3DS V1 (possible en présence d'une opération de paiement VISA ou MASTERCARD), requiert :

- (i) Votre enrôlement préalable par Société Générale auprès des Schémas CB (Paiement sécurisé CB – seulement pour 3DS V2), VISA (VisaSecure©) et MASTERCARD (Mastercard Identity Check©).
- (ii) L'utilisation de logiciels spécifiques compris dans les Services Sogecommerce.

#### • Authentification du titulaire de la Carte

- Authentification forte

Lors de l'opération de paiement, le titulaire de la Carte est redirigé vers la page d'authentification de l'Émetteur. L'authentification est effectuée conformément à une des/la méthode(s) d'authentification que ce dernier a choisie(s).

- Exemption à l'authentification forte dans le cadre de 3DS V2 (également dénommée « frictionless »)

L'exemption à l'authentification forte est mise en œuvre à partir des informations que vous avez collectées envoyées par Sogecommerce (cf documentation technique dédiée mise à la disposition de ce dernier pour connaître le détail de ces informations) et des informations connues par la base de gestion de risque (ex: historique des transactions du titulaire de la Carte) sans interaction avec le titulaire de la Carte.

L'exemption à l'authentification forte est appliquée :

- (i) soit sur votre demande expresse (uniquement dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30€ ou d'un paiement récurrent de rang supérieur à 1) validée par l'Émetteur (en présence d'une telle demande, l'Émetteur peut l'accueillir favorablement – outre la communication des informations obligatoires à Sogecommerce, la communication d'informations facultatives y concourt fortement - ou la refuser et décider d'appliquer une authentification forte).
- (ii) soit à l'initiative de l'Émetteur.

#### • Conséquences de l'authentification forte et de l'exemption à l'authentification forte du titulaire de la Carte

La réponse à la demande d'authentification forte ou à la demande d'exemption à l'authentification forte vous est systématiquement transmise dans le journal des transactions envoyé chaque matin. Elle est également disponible via le Back-Office Sogecommerce, menu « Gestion » / onglet « Transactions en cours ».

#### L'obtention du justificatif d'acceptation visé à l'article 4.1 des Conditions Générales - Partie 1 - Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement - A - Conditions générales communes à tous les schémas se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement (le titulaire de la Carte peut contester ou répudier – c'est-à-dire nier être l'auteur – une transaction auprès de l'Émetteur, à tout moment, et ce, pendant les 13 (treize) mois qui suivent la date initiale de la transaction). Lorsque la Carte n'est pas émise par Société Générale, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'Émetteur à Société Générale.

Société Générale pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

#### • Demande d'autorisation

À la suite de l'authentification forte ou de l'exemption à l'authentification forte du titulaire de la Carte, une autorisation doit être demandée pour chaque opération de paiement.

La demande d'autorisation doit comporter le cryptogramme visuel (s'il est présent) et les éléments relatifs à la demande d'authentification du titulaire de la Carte concernée.

#### • Matrice de responsabilité dans le cadre de 3DS V2

Dans le cadre de 3DS V2, les règles applicables en matière de responsabilité sont les suivantes :

		VOTRE SOUHAIT		
		Pas de souhait	Frictionless	Authentification forte
DÉCISION DE L'ÉMETTEUR	Frictionless	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	<b>Impossibilité d'obtenir un justificatif d'acceptation (Opération de paiement non garantie)</b>	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)
	Authentification forte	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)

### INFORMATIONS CONCERNANT LES JOURNAUX DE TRANSACTIONS

Les journaux de transactions, reçus quotidiennement par e-mail, ne se substituent pas aux relevés de compte. Seuls les relevés de compte permettent de confirmer que les transactions envoyées en compensation ont bien été créditées. Nous vous invitons à contrôler régulièrement vos relevés de compte afin de vérifier les opérations portées au crédit de votre compte.

Pour tout renseignement complémentaire sur l'Offre Sogecommerce, vous pouvez téléphoner au 0811 900 480 depuis la France (numéro Azur - coût d'un appel local depuis un poste fixe) ou au +33 567 223 329 depuis l'étranger, ou envoyer un mail à [support@sogecommerce.societegenerale.eu](mailto:support@sogecommerce.societegenerale.eu).

Nous espérons que ces recommandations seront de nature à améliorer la sécurité de vos opérations commerciales.