(MERCI DE BIEN VOULOIR PARAPHER TOUTES LES PAGES)

L'offre VPC e-Gestion 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 :
  • l'Annexe 1 : Référentiel Sécuritaire Accepteur,
  • l'Annexe 2 : Charte des bonnes pratiques à destination des Accepteurs en paiement à distance (hors Internet) par cartes de paiement.
  (l'ensemble de ces documents étant dénommé le « Contrat d'acceptation en paiement à distance (hors Internet) 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, consistant à mettre à disposition de l'Accepteur une plate-forme informatique lui permettant d'enregistrer et de gérer des ordres de paiements par cartes ainsi que par les moyens de paiement disponibles en option. Cette prestation est régie par les Conditions Générales - Partie 2 : « Services VPC e-Gestion » et Partie 3 « Conditions communes au Parties 1 et 2 ».

CONDITIONS GÉNÉRALES - PARTIE 1: ACCEPTATION EN PAIEMENT À DISTANCE (HORS INTERNET) PAR CARTES DE PAIEMENT

A. CONDITIONS GÉNÉRALES COMMUNES À TOUS LES SCHÉMAS

ARTICLE 1 – DÉFINITIONS

1) L'« Accepteur » peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens et/ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou à percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) et dûment convenu(s) avec Société Générale.

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 », on entend une catégorie d'instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marque(s).
Lorsque la Carte est émise dans l'Espace 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 visées au B des présentes.

6) Par « Paiement à distance », il faut entendre tout paiement par correspondance et assimilé, notamment fax, e-mail, courrier, téléphone, pour lequel l'opération de paiement est réalisée sur communication du numéro de la Carte, de sa date de fin de validité et de son cryptogramme visuel et, à chaque fois que cela est possible et/ou nécessaire, les nom et prénom du titulaire de la Carte.

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

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

9) 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.

10) 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.

11) Par « Système d'Acceptation », il faut entendre les logiciels et protocoles conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant la (l'une des) Marque(s) dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément 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 – Signaler au public de façon apparente sur les supports de vente chaque Marque qu'il accepte, chaque Catégorie de Carte qu'il accepte ou refuse et le montant minimum éventuel à partir duquel la Carte est acceptée.
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 – 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.

2.3 – 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 : télévision et téléphonie). À cet effet, l'Accepteur organise la traçabilité adéquate des informations liées au paiement à distance.

2.4 – 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.

2.5 – 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 2.4.

2.6 – Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a initiées, vérifier avec Société Générale la conformité des informations transmises pour identifier son point de vente.
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).

(O) 713189 - 09/2021

2.7 – Accepter les paiements à distance effectués avec les Cartes portant la(les) Marque(s) et Catégorie(s) de carte qu'il a choisie(s) 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.

2.8 – 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.

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

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

2.11 – 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.

2.12 – À la demande de Société Générale selon les volumes d'opérations Cartes acceptées chez lui, à respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat ainsi que celles du Référentiel Sécuritaire PCI DSS dont il peut prendre connaissance à l'adresse suivante : http//fr.pcisecuritystandards.org/minisite/en/ ou qui lui sera communiqué par Société Générale à première demande.

2.13 – Permettre à Société Générale et/ou au Schéma concerné de faire procéder dans ses locaux ou ceux de ses prestataires, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement en fonction des risques de sécurité liés au Système d'Acceptation utilisé. Cette vérification, appelée « procédure d'audit » s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.
Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, Société Générale peut procéder le cas échéant, à la demande du(des) Schéma(s) concerné(s), à une suspension de l'acceptation par l'Accepteur des Cartes portant la(les) Marque(s) du(des) 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 1 et de la présente Partie 3. L'Accepteur autorise la communication du rapport à Société Générale et au(x) Schéma(s) concerné(s). En outre, les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

2.14 – 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 considérée.

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

2.16 – Informer dans les meilleurs délais Société Générale en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies.

2.17 – En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte/utilisation frauduleuse des données liées au paiement, coopérer avec Société Générale et, le cas échéant, avec 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 à l'article 1 de la Partie 1.

2.18 – Laisser libre accès au Système d'Acceptation à Société Générale et à toute personne désignée par cette dernière pour effectuer, si nécessaire, des travaux de maintenance et de mise à niveau du Système d'Acceptation.

2.19 – Informer immédiatement Société Générale en cas de modification des informations le concernant communiquées à Société Générale pour l'ouverture du présent Contrat, notamment celles figurant dans les Conditions Particulières (également dénommées « Contrat de prestation VPC e-Gestion »).

ARTICLE 3 – OBLIGATIONS DE SOCIÉTÉ GÉNÉRALE

Société Générale s'engage à :

3.1 – Mettre à la disposition de l'Accepteur toute information relative à la sécurité des opérations de paiement.

3.2 – Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie B du présent Contrat et son(leur) évolution, les Catégories de carte, les Marques dont il assure l'acceptation, ainsi que les frais applicables à chacune des Marques et Catégories 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 – Indiquer à l'Accepteur la liste et les caractéristiques des Cartes (Marques et Catégories de carte) pouvant être acceptées, et lui fournir à sa demande le fichier des codes émetteurs (BIN).

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

3.6 – 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.

3.7 – 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.

3.8 – 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 que les commissions de service soient regroupées par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 4 – GARANTIE DU PAIEMENT ET MESURES DE SÉCURITÉ

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées au présent Contrat sauf en cas :
- de réclamation du titulaire de la Carte qui conteste la réalité même ou le montant de l'opération de paiement,
- d'opération de paiement réalisée au moyen d'une Carte non valide, périmée ou bloquée.

À ce titre, l'Accepteur autorise expressément Société Générale à débiter d'office son compte du montant de toute opération de paiement dont la réalité même ou le montant serait contesté par le titulaire de la Carte.
Toutes les mesures de sécurité sont indépendantes les unes des autres.
En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement, et ce en l'absence de contestations.

4.1 – Lors du paiement :
L'Accepteur s'engage à :

4.1.1 - Effectuer tous les contrôles à partir des indications (numéro de Carte et date d'échéance) fournies par le client lors de la commande.

4.1.2 - Contrôler la longueur (de 13 à 19 caractères) et la vraisemblance mathématique du numéro de la Carte au moyen de la méthode de calcul communiquée par Société Générale. En cas de système de paiement interactif, bloquer la commande au bout de trois saisies erronées.

4.1.3 - Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la période de validité suivant indication fournie par le titulaire de la Carte (fin et éventuellement début),
- que la Marque utilisée est indiquée dans les Conditions Particulières.

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

4.2 – Après le paiement :
L'Accepteur s'engage à :

4.2.1 - Transmettre à Société Générale, dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec Société Générale, 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 prévus dans les Conditions Particulières convenues 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.

4.2.2 - Envoyer au titulaire de la Carte, à sa demande, un justificatif de l'opération de paiement.

(O) 713189 - 09/2021

4.2.3 - Archiver et conserver, à titre de justificatif, pendant 15 (quinze) mois, les bons ainsi que les relevés détaillés des commandes reçues des titulaires de Cartes.

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

4.2.5 - 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 et/ou le Schéma prévaudront sur ceux produits 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 2.13 ci-dessus au cas où le rapport révélerait un ou plusieurs manquements 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 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

7.1 – En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés 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.

7.2 – 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.

7.3 – 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.

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 les communiquer 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 lutte contre la fraude à la carte de paiement et la gestion des éventuels recours en justice ;
- 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 sous une forme couramment utilisée et lisible par un appareil électronique ;

(O) 713189 - 09/2021

– introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

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

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° 2017-222 du 20 juillet 2017 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 oeuvre toutes les mesures techniques et organisationnelles appropriées pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux 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 peut/peuvent 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 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 2 (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 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 2.3 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 sécurisé 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.

(O) 713189 - 09/2021

Ces données à caractère personnel font l'objet de traitements afin de permettre :
– la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB ;
– de répondre aux obligations réglementaires ou légales, notamment en matière pénale ou administrative liées à l'utilisation de la Carte ; Les données à caractère personnel traitées par le GIE CB sont conservées pour les durées suivantes :
– en matière 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.

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 par courriel à protegezvosdonnees@cartes-bancaires.com

Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :
– consulter la Charte de protection des données à caractère personnel du GIE CB accessible à www.cartes-bancaires.com/protegezvosdonnees ;
– contacter le Délégué à la protection des données désigné par le GIE CB par courriel à protegezvosdonnees@cartes-bancaires.com

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 SOCIÉTÉ GÉNÉRALE

Par dérogation à l'article 3.6 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 3 – 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 4 – 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 1 – RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR » annexé aux présentes, Société Générale appliquera à l'Accepteur :

4.1 – Un forfait de 103 000 €,

4.2 – 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.

4.3 – 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

4.4 – 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 4.2 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 €

4.5 – 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€.

4.6 – 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 VPC E-GESTION

VPC e-Gestion est une offre de services (également dénommée les « Services VPC e-Gestion ») consistant en la mise à disposition de l'Accepteur d'un ensemble de moyens logistiques et humains permettant le traitement des ordres de paiement par Carte donnés par téléphone ou par tout autre moyen de communication à distance hors Internet.

Toute autre utilisation des Services VPC e-Gestion devra faire l'objet d'une convention séparée.

ARTICLE 1 – MOYENS NÉCESSAIRES À L'UTILISATION DES SERVICES VPC E-GESTION

VPC e-Gestion repose sur une plate-forme de paiements sécurisée, élaborée à partir de la solution de paiement sécurisée SIPS dont Worldline est propriétaire.

L'utilisation de VPC e-Gestion 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 VPC e-Gestion se fait via l'utilisation d'un navigateur Internet répondant à des normes de sécurité (notamment en termes de chiffrement) nécessaires audit accès.

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 Internet et du bon fonctionnement de son équipement informatique.

L'Accepteur doit s'être assuré, sous sa responsabilité, de la compatibilité du matériel et des logiciels destinés à utiliser VPC e-Gestion.

La plate-forme de paiement VPC e-Gestion est accessible via l'adresse Internet : https://office.sogenactif.com

L'accès au service VPC e-Gestion n'est possible qu'au moyen d'un identifiant et d'un mot de passe.

(O) 713189 - 09/2021

L'identifiant est envoyé à l'adresse électronique indiquée dans le Contrat de prestation. 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.

ARTICLE 2 – DESCRIPTION DES SERVICES

Une documentation technique décrivant les fonctionnalités et les paramétrages de VPC e-Gestion est mise à disposition de l'Accepteur à l'adresse suivante : https://documentation.sogenactif.com (site Internet en libre accès).
Les services VPC e-Gestion reposent sur :

2.1 – Un service de création d'opérations de paiement, par Carte des Schémas CB, Visa, Mastercard et, en option, par certaines cartes privatives.

2.1.1 - VPC e-Gestion permet à l'Accepteur de transmettre à Société Générale une opération de paiement qu'il a constituée à partir des données que son client lui a communiquées par téléphone ou par tout autre moyen de communication à distance à l'exception d'Internet.
À cet égard, il est rappelé que l'Accepteur ne doit constituer que des opérations pour lesquelles un ordre de paiement par Carte lui a été préalablement donné.

2.1.2 - Lors d'une demande de paiement par Carte CB, Visa ou 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 de 13 à 19 caractères numériques.
Si l'un de ces contrôles se révèle négatif, l'opération de paiement ne peut être enregistrée.
Pour constituer une opération de paiement, l'Accepteur doit donc obtenir le numéro de la Carte, sa date de validité et le cryptogramme visuel.
Si les contrôles sont positifs, une demande d'autorisation est systématiquement transmise vers la banque de l'acheteur sur la base des informations (numéro de Carte, date de validité et cryptogramme visuel) communiquées.
L'Accepteur est informé du résultat des contrôles.

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

2.1.4 - Société Générale attire l'attention de l'Accepteur sur le fait, qu'en application des dispositions des Conditions Générales - Partie 1, **les opérations ne pourront pas être garanties en cas de contestation.**

2.2 – Un portail de gestion extranet en ligne qui permet notamment à l'Accepteur de consulter, créer, 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. Ce portail de gestion permet aussi l'accès à différents outils de gestion pour l'Accepteur : un outil d'administration des règles de lutte contre la fraude, un outil de gestion des utilisateurs.
L'accès au portail de gestion n'est possible qu'au moyen d'un identifiant et d'un mot de passe. Un e-mail, envoyé à l'adresse électronique indiqué dans le Contrat de prestation comprend d'une part, l'identifiant et, d'autre part, un lien permettant de créer le mot de passe. L'Accepteur doit prendre toutes les mesures propres à assurer la confidentialité de son identifiant et de son mot de passe.
– L'outil d'administration des outils de lutte contre la fraude (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 – Des outils de reporting : deux journaux de fonds sont 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 sont également 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.
Dans l'hypothèse où l'Accepteur est titulaire de plusieurs Contrats de prestation, il recevra chaque jour 2 (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 – Des outils sécuritaires/des règles anti-fraude
Les 9 règles anti-fraude proposées en standard sont décrites ci-dessous. Elles impliquent d'effectuer une vérification sur l'un des critères de la transaction.
Les règles sont de type « GO » (détectant une condition favorable à la poursuite de la transaction) ou « NOGO » (détectant une condition défavorable à la poursuite de la transaction). La règle de type « GO » retourne un résultat positif si la condition est remplie et un résultat neutre dans le cas contraire. La règle de type « NOGO » retourne un résultat négatif si la condition est remplie et un résultat neutre dans le cas contraire.
Les règles peuvent être paramétrées en mode décisif ou en mode informatif.
En mode décisif, 3 types de résultat peuvent en découler s'agissant de l'acceptation de la transaction :
– Résultat positif : le critère contrôlé est favorable à l'acceptation de la transaction ;
– Résultat négatif : le critère contrôlé est défavorable à l'acceptation de la transaction ;
– Résultat neutre : le critère contrôlé n'est ni favorable ni défavorable à l'acceptation de la transaction.
En mode informatif, la règle paramétrée n'a pas d'impact sur le déroulement de la transaction. Le résultat de la règle est restitué à l'Accepteur pour analyse.
– En cas de pluralité de contrôles sélectionnés par l'Accepteur, ceux-ci sont effectués les uns après les autres dans l'ordre déterminé par l'Accepteur. Si un contrôle paramétré en mode décisif retourne un résultat non neutre, les contrôles décisifs suivants ne sont pas déroulés. Quel que soit le résultat des contrôles décisifs, l'ensemble des contrôles paramétrés en informatif sera déroulé.
Leur activation et leur paramétrage sont placés sous la responsabilité de l'Accepteur grâce à l'extranet de gestion de la lutte contre la fraude accessible à partir du portail extranet de gestion. Il appartient à l'Accepteur de s'assurer de la régularité des contrôles qu'il met en place, notamment au regard de la réglementation sur les données à caractère personnel. Une documentation technique détaillant les contrôles et leurs paramétrages est mise à disposition de l'Accepteur dans le portail de gestion.
En outre, si les traitements des données à caractère personnel réalisés dans le cadre de la lutte anti-fraude aboutissent à un refus de la transaction, l'Accepteur proposera un moyen de paiement alternatif à son client conformément à la Délibération de la CNIL n° 2013-358 du 14 novembre 2013.

2.4.1 - Contrôle d'encours de Cartes
Cette règle permet à l'Accepteur de mesurer le risque sur une transaction par le contrôle de l'activité (le nombre et/ou le montant des transactions cumulé) de la Carte sur une période.
La règle est exécutée sur toutes les transactions effectuées avec une Carte.
L'Accepteur doit paramétrer le nombre maximal de transactions et/ou le montant cumulé maximal, ainsi que la période concernée.

2.4.2 - Contrôle du pays de la Carte (BIN étranger)
Cette règle permet à l'Accepteur de mesurer le risque sur une transaction en fonction du pays d'émission de la Carte du porteur.
L'Accepteur doit paramétrer la liste des pays de la carte autorisés ou interdits ou transmettre cette liste directement dans la requête de paiement. En l'absence de liste de pays autorisés ou interdits, le contrôle considère le code pays Accepteur comme le seul autorisé.

2.4.3 - Contrôle d'encours identifiant client
Cette règle permet à l'Accepteur de mesurer le risque sur une transaction par le contrôle de l'activité (le nombre de transactions et/ou le montant des transactions cumulé) d'un acheteur à partir d'un identifiant client sur une période donnée.
La règle est exécutée sur toutes les transactions de paiement dans lesquelles l'identifiant client (« customer id ») est transmis.
L'Accepteur doit paramétrer le nombre maximal de transactions effectuées et/ou le montant cumulé maximal et la durée du cumul et transmettre l'identifiant client de l'acheteur dans la requête.

2.4.4 - Liste de numéros de Cartes
L'Accepteur peut gérer une liste de numéros de Cartes, pour lui permettre de mesurer le risque.
3 (trois) types de règles peuvent être appliqués :
– Vérification dans une liste noire : liste de type NOGO. Si la Carte est présente dans cette liste, un résultat négatif sera retourné.
– Vérification dans une liste grise : liste de type NOGO. Si la Carte est présente dans cette liste, un résultat négatif sera retourné.
– Vérification dans une liste blanche : liste de type GO. Si la Carte est présente dans cette liste, un résultat positif sera retourné.
L'Accepteur doit paramétrer la ou les liste(s) qu'il souhaite.

2.4.5 - Contrôle de Cartes en opposition
Cette règle permet à l'Accepteur de décider de donner suite ou non à un achat effectué au moyen d'une Carte en opposition. Ce contrôle est réalisé sur toutes les transactions de paiement avec Carte CB , Visa et Mastercard. La règle vérifie si la Carte est présente dans la base des Cartes en opposition. Le fichier des Cartes en opposition est alimenté en se basant sur la liste des Cartes de l'opposition du Schéma CB dont la mise à jour est effectuée plusieurs fois par jour.

(O) 713189 - 09/2021

2.4.6 - Contrôle montant
Cette règle permet à l'Accepteur de mesurer le risque sur un achat par le contrôle du montant. La règle va vérifier si le montant de la transaction est dans la plage de montant défini par l'Accepteur.L'Accepteur devra paramétrer le montant minimum et/ou le montant maximum. En l'absence de paramétrage, la règle retourne un résultat neutre.

2.4.7 - Contrôle d'association Carte/client
Cette règle permet à l'Accepteur de vérifier qu'un acheteur donné n'utilise pas un nombre trop élevé de Cartes différentes sur une période.
La règle est exécutée sur toutes les transactions de paiement dans lesquelles l'identifiant client (« customer id ») est transmis. La règle contrôle l'activité à partir du numéro de Carte et de l'identifiant client sur une période donnée.
L'Accepteur devra paramétrer le nombre de cartes maximum et la durée du cumul et transmettre l'identifiant client dans la requête de paiement.

2.4.8 - Contrôle d'association client/Carte
Cette règle permet à l'Accepteur de vérifier qu'une Carte donnée n'est pas utilisée pas un nombre trop élevé d'acheteurs différents sur une période.
La règle est exécutée sur toutes les transactions de paiement dans lesquelles l'identifiant client (« customer id ») est transmis. La règle contrôle l'activité à partir du numéro de Carte et de l'identifiant client sur une période donnée.
L'Accepteur devra paramétrer le nombre d'acheteurs maximum et la durée du cumul et transmettre l'identifiant client dans la requête de paiement.

2.4.9 - Contrôle de la date d'expiration du PAN (i.e du numéro de Carte)
Cette règle permet à l'Accepteur de détecter les paiements dont la Carte arrive à expiration dans les prochains mois.
La règle est exécutée sur toutes les transactions Carte. Elle vérifie si le nombre de mois avant expiration de la Carte est supérieur au nombre de mois indiqué par l'Accepteur.
L'Accepteur devra paramétrer le nombre de mois minimum avant expiration de la Carte.
En l'absence de paramétrage du nombre de mois minimum avant expiration, la règle considère que ce nombre est égal à zéro.

2.5 – Option de traitement et de suivi
L'Accepteur a la possibilité de souscrire à l'option « Confirmation de paiement par e-mail ». Cette option permet d'envoyer un e-mail de confirmation à l'acheteur en même temps que la réponse automatique.
L'Accepteur peut demander à être copie de l'e-mail envoyé à l'acheteur.

ARTICLE 3 – PARTICULARITÉS DE VPC-E GESTION POUR LES CARTES AMERICAN EXPRESS

L'Accepteur peut, en option, demander à utiliser la plate-forme VPC e-gestion pour accepter les cartes American Express.
L'accès à ce service nécessite l'accord de Société Générale (et, dans l'affirmative, la signature d'un avenant au Contrat VPC e-gestion) et implique la conclusion d'un contrat d'acceptation avec American Express France.

ARTICLE 4 – OBLIGATIONS DE SOCIÉTÉ GÉNÉRALE

Société Générale s'engage :

4.1 – à mettre à la disposition de l'Accepteur les Service décrits à l'article 2 ;

4.2 – à assurer la maintenance de la plate-forme de paiement utilisée dans le cadre des Services VPC e-Gestion ;

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

4.4 – à mettre en œuvre dans les délais prévus par le GIE CB les évolutions demandées par la communauté des établissements de crédit 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 ;

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

4.6 – à favoriser une disponibilité des Services 24h/24 et 7j/7. Les Services VPC e-Gestion pourront toutefois être interrompus temporairement pour des besoins de maintenance et/ou d'évolution, sous réserve d'une information préalable de l'Accepteur. Cette information pourra être réalisée par l'insertion d'un message sur le site Internet de la plate-forme de paiement.

ARTICLE 5 – OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage :

5.1 – à collaborer activement et régulièrement avec la Banque dans l'intérêt du bon fonctionnement des Services ;

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

5.3 – afin de limiter les risques de détournement des données liées aux Cartes de ses clients, à créer des opérations de paiement par l'intermédiaire des Services VPC e-Gestion dès réception des ordres de paiement correspondants ;

5.4 – s'assurer que les paramétrages des Services VPC e-Gestion qu'il réalise ainsi que les utilisations qu'il en fait, répondent à ses besoins. En cas de doute, l'Accepteur prendra contact avec Société Générale.

ARTICLE 6 – RESPONSABILITÉ DE SOCIÉTÉ GÉNÉRALE

6.1 – Société Générale est responsable de la bonne exécution des prestations objet des présentes Conditions Générales. Elle assume une obligation de mise en œuvre de moyens 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. 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 – Au cas où la responsabilité de Société Générale serait retenue, 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.

6.3 – La responsabilité de la Banque ne pourra jamais être engagée :
– 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 tout autre cas indépendant 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 Economique 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 la plateforme VPC e-Gestion et les documentations mises 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.

(O) 713189 - 09/2021

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 certaines fonctions de la plate-forme 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 entre le poste de l'Accepteur et les Services VPC e-Gestion repose sur la mise en œuvre d'une technologie sécurisée Transport Layer Security (TLS). Les informations relatives au paiement sont systématiquement chiffrées lorsqu'elles circulent sur Internet.
La Banque 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 différents émetteurs de Cartes (GIE CB, VISA, MASTERCARD, AMERICAN EXPRESS CARTE FRANCE…).
La plate-forme de paiement sécurisée qui assure le Traitement des données des Cartes répond aux exigences du standard PCI DSS.
Le transport des informations entre l'Accepteur, Société Générale et la plate-forme de paiement Worldline 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 , 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, logiciels ou autres adressés par la Banque 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 – RÉFÉRENCEMENT ET MARQUES

14.1 – 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.
14.2 Les marques VPC e-Gestion et Société Générale étant déposées, elles ne peuvent être utilisées sans l'autorisation préalable et écrite de Société Générale

CONDITIONS GÉNÉRALES – PARTIE 3 : CONDITIONS COMMUNES AUX PARTIES 1 ET 2

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 VPC e-Gestion.
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 à l'article 6.2 de la Partie 1.A. 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.

1.4 – 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, sans que Société Générale ait à lui rappeler cette faculté.

1.5 – 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.

1.6 – 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.

1.7 – 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 autre(s) contrat(s) d'acceptation, l'Accepteur s'engage à retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes et toute éventuelle référence à Société Générale.

1.8 – 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 logiciel, 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 ci-dessus. 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.A 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 VPC e-Gestion 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.

(O) 713189 - 09/2021

Les sommes dues au titre des Services VPC e-Gestion 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 VPC e-Gestion 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 31e (trente et unième) jour, la somme due portera intérêt au taux de 3 (trois) 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 - RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR

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

RECOMMANDATION 1 (R1)
GÉRER LA SÉCURITÉ DU SYSTÈME COMMERCIAL ET DE PAIEMENT AU SEIN DE L'ENTREPRISE

Pour assurer la sécurité des données des transactions et notamment, des données des porteurs, une organisation, des procédures et des responsabilités doivent être établies. En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données nominatives et des données bancaires dans le cadre de leur utilisation et de leur environnement. Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système. Le contrôle du respect des exigences de sécurité relatives au système commercial et de paiement doit être assuré. Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

RECOMMANDATION 2 (R2)
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 les personnels reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

RECOMMANDATION 3 (R3)
GÉRER LES ACCÈS AUX LOCAUX ET AUX INFORMATIONS

Tout dispositif (équipement réseau, serveur,) qui stocke ou qui traite des données relatives à une transaction et notamment, des données de paiement sensibles liées à la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les recommandations de la CNIL. Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre. Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie. La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

RECOMMANDATION 4 (R4)
ASSURER LA PROTECTION LOGIQUE DU SYSTÈME COMMERCIAL ET DE PAIEMENT

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement doivent être établies et leur respect doit être contrôlé. Seul le serveur supportant l'application commerciale doit être accessible par les internautes. Le serveur de base de données client ainsi que le serveur hébergeant le système de paiement ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu. Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu. L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées. Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables. Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité. Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

RECOMMANDATION 5 (R5)
CONTRÔLER L'ACCÈS AU SYSTÈME COMMERCIAL ET DE PAIEMENT

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés. Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et de paiement. Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

RECOMMANDATION 6 (R6)
GÉRER LES ACCÈS AUTORISÉS AU SYSTÈME COMMERCIAL ET DE PAIEMENT

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement. Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification. L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées. L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué. Les changements de situation (changement de poste, départ,) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués. La suppression des droits d'accès doit être immédiate en cas de départ d'une personne. Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données. Les tentatives d'accès doivent être limitées en nombre. Les mots de passe doivent être changés régulièrement. Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

(O) 713189 - 09/2021

RECOMMANDATION 7 (R7)
SURVEILLER LES ACCÈS AU SYSTÈME COMMERCIAL ET DE PAIEMENT

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit. L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine. Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées. Les systèmes assurant l'enregistrement doivent au minimum être le pare-feu, le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements. Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées. Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

RECOMMANDATION 8 (R8)
CONTRÔLER L'INTRODUCTION DE LOGICIELS PERNICIEUX

Les procédures et les responsabilités de gestion ayant trait à la protection antivirus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées. L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et de paiement. La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

RECOMMANDATION 9 (R9)
APPLIQUER LES CORRECTIFS DE SÉCURITÉ (PATCHES DE SÉCURITÉ) SUR LES LOGICIELS D'EXPLOITATION

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettent des accès non autorisés et non visibles. Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

RECOMMANDATION 10 (R10)
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.

RECOMMANDATION 11 (R11)
MAINTENIR L'INTÉGRITÉ DES LOGICIELS APPLICATIFS RELATIFS AU SYSTÈME COMMERCIAL ET DE PAIEMENT

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications. Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise. La demande de modification doit être approuvée par le responsable fonctionnel du système. Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

RECOMMANDATION 12 (R12)
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.

RECOMMANDATION 13 (R13)
MAINTENIR L'INTÉGRITÉ DES INFORMATIONS RELATIVES AU SYSTÈME COMMERCIAL ET DE PAIEMENT

La protection et l'intégrité des éléments de la transaction doivent être assurées ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments. Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

RECOMMANDATION 14 (R14)
PROTÉGER LA CONFIDENTIALITÉ DES DONNÉES BANCAIRES

Les données du porteur ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations. Le cryptogramme visuel d'un porteur ne doit en aucun cas être stocké par le commerçant. Les données bancaires et nominatives relatives à une transaction, et notamment les données du porteur doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions du Règlement (UE) 2016/679 du 27 avril 2016 et aux recommandations de la CNIL. Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer. Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

RECOMMANDATION 15 (R15)
PROTÉGER LA CONFIDENTIALITÉ DES IDENTIFIANTS – AUTHENTIFIANTS DES UTILISATEURS ET DES ADMINISTRATEURS

La confidentialité des identifiants authentifiant 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.

RECOMMANDATION 16 (R16)
RESPECTER LE STANDARD « PAYMENT CARD INDUSTRY – DATA SECURITY SYSTEM » (PCI-DSS)

En souscrivant le contrat VPC e-Gestion, vous adhérez également à ce standard intitulé PCI-DSS dont le détail peut être obtenu sur le site internet www.pcisecuritystandards.org

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

(O) 713189 - 09/2021

NIVEAUX ET ACTIONS À MENER SELON LE NOMBRE DE TRANSACTIONS

Sources : programmes PCI-DSS des Réseaux Visa Europe (AIS) et Mastercard (SDP)
AIS : Account Information Security, SDP : Site Data Protection.
http://www.visaeurope.com/receiving-payments/security/merchants
http://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html

	CRITÈRES	ACTIONS À MENER PAR LE COMMERÇANT	PÉRIODICITÉ
NIVEAU 1	Accepteur ayant un volume annuel de transactions Visa et/ou Mastercard supérieur à 6 000 000 ou ayant fait l'objet d'une compromission l'année précédente.	☑ Rapport de conformité suite à audit sur site réalisé par un QSA* (Qualified Security Assessor) ou une ressource interne agréée auditeur PCI-DSS ☑ Scan de vulnérabilité par un ASV* (Approved Scan Vendor) ☑ Formulaire d'attestation de conformité **OBLIGATION**	→ ANNUELLE → TRIMESTRIELLE
NIVEAU 2	Accepteur ayant un volume annuel de transactions Visa et/ou Mastercard compris entre 1 000 000 et 6 000 000.	☑ Questionnaire de self audit ☑ Scan de vulnérabilité par un ASV* (Approved Scan Vendor) ☑ Formulaire d'attestation de conformité **OBLIGATION**	→ ANNUELLE → TRIMESTRIELLE
NIVEAU 3	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard compris entre 20 000 et 1 000 000.	☑ Questionnaire de self audit ☑ Scan de vulnérabilité par un ASV* (Approved Scan Vendor) **OBLIGATION**	→ ANNUELLE → TRIMESTRIELLE
NIVEAU 4	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard inférieur à 20 000.	☑ Questionnaire de self audit ☑ Scan de vulnérabilité par un ASV* (Approved Scan Vendor) **RECOMMANDATION**	→ ANNUELLE → TRIMESTRIELLE

* Prestataires agréés ou certifiés par PCI-DSS (Conseil des normes de sécurité PCI https://fr.pcisecuritystandards.org/minisite/en/) :

- ASV (Approved Scan Vendor) = prestataire spécialisé dans la sécurité informatique agréé pour la réalisation de scan de vulnérabilité
  Liste des ASV agréés par PCI-DSS : https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
- QSA (Qualified Security Assessor) = prestataire spécialisé dans la sécurité informatique certifié pour la réalisation d'audits PCI-DSS
  Liste des QSA certifiés par PCI-DSS : https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Questionnaire de self audit et formulaire d'attestation de conformité disponibles sur le site PCI-DSS : https://fr.pcisecuritystandards.org/minisite/en

(O) 713189 - 09/2021

Vous venez de souscrire un Contrat VPC e-Gestion auprès de notre établissement, et nous vous en remercions. Nous espérons que l'accès à un service permettant de traiter des ordres de paiement par Carte donnés par téléphone contribuera au développement de votre chiffre d'affaires. Afin que cette activité se déroule dans de bonnes conditions, nous souhaitons attirer votre attention sur certains points.
Comme indiqué dans les Conditions Générales – Partie 1, vous ne bénéficiez d'aucune garantie de paiement en cas de réclamation du titulaire de la Carte lorsque celui-ci conteste la réalité même ou le montant d'une transaction. En effet, le titulaire de la Carte peut contester ou répudier[1] une transaction auprès de sa banque, au plus tard, dans les 13 (treize) mois suivant la date de débit de la transaction. Dans ce cas, nous devrons restituer le montant des opérations contestées à cette banque et débiter, par conséquent, votre compte.
C'est pourquoi, 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 auprès de vous, 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 (alors que les Conditions Générales - Partie 1 prévoient que l'autorisation doit être demandée pour le montant total de l'opération sous jacente) ;
- 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 l'outil de back-office Sogenactif Gestion.

RECOMMANDATION DE SÉCURITÉ CONCERNANT LE SERVICE VPC E-GESTION

Pour vous aider à lutter contre la fraude et les impayés, vous disposez, par l'intermédiaire du service VPC e-Gestion de la « remontée d'information du code ISO » de la Carte qui vous permet d'identifier le pays d'origine de la Carte utilisée.
Nous vous conseillons également de mettre en place les outils sécuritaires mis à votre disposition et détaillés dans le Contrat de prestation.
Votre Portail de gestion 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 LES JOURNAUX :

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 VPC e-Gestion,
vous pouvez téléphoner au 0825 090 095 (Service 0,15 € TTC/min + prix appel – Tarif en vigueur au 01/01/2021) ou envoyer un e-mail à supportsogenactif@worldline.com
Nous espérons que ces recommandations seront de nature à améliorer la sécurité de vos opérations commerciales.

(O) 713189 - 09/2021