CONDITIONS GÉNÉRALES DU CONTRAT D'ACCEPTATION EN PAIEMENT À DISTANCE (HORS INTERNET) PAR CARTES DE PAIEMENT

Le contrat flux VPC (Vente Par Correspondance – également dénommé « **Contrat Flux VPC** » ou « **Contrat** ») est composé :

- des présentes Conditions Générales qui comportent deux parties :
  - une Partie I : Conditions Générales communes à tous les Schémas,
  - une Partie II : Dispositions spécifiques à chaque Schéma,
  - ainsi qu'une annexe dénommée « Référentiel Sécuritaire Accepteur ».
- des Conditions Particulières (également dénommées « **Contrat de prestation : Flux VPC** » ou « **Contrat de prestation** »).

PARTIE I : CONDITIONS GÉNÉRALES COMMUNES À TOUS LES SCHÉMAS

ARTICLE 1 – DÉFINITIONS

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

1.2 – 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 II des présentes. Dans le cadre du présent Contrat, Société Générale est l'Acquéreur de l'Accepteur.

1.3 – Par « Carte », il faut entendre une catégorie d'instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marque(s).

Lorsque la Carte est émise dans l'Espace Economique 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.

1.4 – 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.

1.5 – 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 II des présentes.

1.6 – Par « Paiement à distance », il faut entendre tout paiement par correspondance et assimilé notamment par fax, e-mail, courrier ou téléphone pour lequel l'opération de paiement est réalisée sur communication du numéro de 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.

1.7 – 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.

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

1.9 – 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.

1.10 – 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.

1.11 – 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 sur la (l'une des) Marque(s) dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément ou d'une approbation par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

ARTICLE 2 – OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

2.1 – 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 en ligne.

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).

2.7 – Accepter les paiements à distance effectués avec la (les) Marque(s) et Catégorie(s) de carte qu'il a choisies d'accepter ou qu'il doit accepter en contrepartie d'actes de vente et/ou de prestations de services offert(e)s 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 concerné et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes, proposées par Société Générale.

2.10 – Régler, selon les conditions convenues avec Société Générale dans le Contrat de prestation, les commissions, frais et d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

(F) 712558 - 07/2022

2.11 – Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter le Référentiel Sécuritaire Accepteur et le Référentiel Sécuritaire PCI DSS, acceptent que les audits visés à l'article 2.13 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé à cet article.

2.12 – Respecter le Référentiel Sécuritaire Accepteur annexé au présent Contrat ainsi que celles du Référentiel Accepteur 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 les locaux de l'Accepteur ou dans ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS. Cette vérification, appelée « procédure d'audit » s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné. Le rapport d'audit fera systématiquement l'objet d'une communication à l'Accepteur et au Schéma concerné.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) à ces clauses et/ou exigences, Société Générale peut procéder, le cas échéant à la demande du(es) Schéma(s) concerné(s), à une suspension de l'acceptation des Cartes portant la (les) Marque(s) dudit (desdits) Schéma(s) concerné(s) par l'audit, voire à la résiliation du présent Contrat, dans les conditions prévues aux articles 8 et 9 de la présente Partie I. 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 quinze (15) mois à compter de la date du dernier paiement,
- donner une information claire au titulaire de la Carte sur les droits dont il dispose et notamment sur la possibilité de retirer à tout moment son consentement,
- ne plus initier de paiements dès lors que le titulaire de la Carte a retiré son consentement à l'exécution de la série d'opérations de paiement considérée.

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

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

2.17 – En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données, coopérer avec Société Générale et, le cas échéant, les autorités compétentes Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire Société Générale à résilier le présent Contrat conformément aux dispositions de l'article 8 de la présente Partie I.

2.18 – Informer immédiatement Société Générale de toute modification des informations communiquées lors de l'ouverture du Contrat, notamment l'activité exercée.

2.19 – Ne pas stocker, sous quelque forme le cryptogramme visuel (trois derniers chiffres du numéro figurant au verso de la Carte). Les numéros des Cartes et leurs dates d'expiration ne pourront être stockés que dans les conditions et pour les finalités prévues par le présent Contrat.

2.20 – Laisser libre accès au Système d'Acceptation à Société Générale et à toute personne désignée par elle pour effectuer, à sa demande, des travaux de maintenance et de mise à niveau dudit Système d'Acceptation.

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 des Schémas visés dans la Partie II des présentes et 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 aux Schémas.

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 pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation 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 modalités définies ci-dessous et dans le Contrat de prestation :

- la date de valeur « J » ouvrée applicable à ces crédits correspond à la date de réception « J » ouvrée de la remise, si ces remises sont reçues par le Centre de traitement de Société Générale avant les heures limites d'acquisition suivantes :
  - 8 h 30 pour une télécollecte ;
  - 10 h 00 pour une remise de fichier(s) ;
  - les remises reçues par le Centre de traitement de Société Générale après ces heures limites d'acquisition sont considérées comme reçues le jour ouvré suivant.

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

3.7 – 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 service à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

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

ARTICLE 4 – GARANTIE DU PAIEMENT

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées au présent article 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 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.

Société Générale pourra contrepasser le montant des opérations non garanties qui n'ont pu être imputées sur le compte sur lequel fonctionne la Carte ou qui ont fait l'objet d'une contestation de la part du titulaire de la Carte.

Les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par la banque du titulaire de la Carte à Société Générale.

ARTICLE 5 – MESURES DE SÉCURITÉ

5.1 – Lors du paiement :

L'Accepteur s'engage à :

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

5.1.2 – Contrôler la longueur (de 13 à 19 caractères).

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

- la période de validité (fin et éventuellement début) suivant les indications du titulaire de la Carte,
- que la Marque utilisée est indiquée dans le Contrat de prestation.

5.1.4 – Obtenir une autorisation d'un montant identique à l'opération sous jacente.

5.2 – Après le paiement :

L'Accepteur s'engage à :

5.2.1 – Transmettre à Société Générale dans les délais et selon les modalités prévus dans le Contrat de prestation les enregistrements électroniques des opérations et s'assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans le Contrat de prestation. L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit et

(F) 712558 - 07/2022

dont le montant est identique à celle de l'ordre de paiement. Toute opération ayant fait l'objet d'une autorisation transmise par Société Générale doit obligatoirement lui être remise.

5.2.2 – Envoyer au Titulaire de la Carte, à sa demande, un justificatif de l'opération de paiement.

5.2.3 – Archiver et conserver pendant quinze (15) mois tout justificatif des opérations de paiement et les communiquer, par courrier postal ou par fax, au plus tard huit (8) jours calendaires à compter de leur demande par Société Générale.

5.2.4 – Les mesures de sécurité énumérées au présent article 5 pourront être modifiées et complétées pendant toute la durée du Contrat, selon la procédure prévue à l'article 7.

ARTICLE 6 – MODALITÉS ANNEXES DE FONCTIONNEMENT

6.1 – Réclamation

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

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

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.

6.2 – 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.

6.3 – Transaction crédit (service optionnel)

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 » et 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. La mise en oeuvre de la fonctionnalité « transaction crédit » est subordonnée à l'accord préalable de Société Générale.

ARTICLE 7 – MODIFICATIONS

7.1 – Société Générale peut modifier à tout moment les présentes Conditions Générales ainsi que le Contrat de prestation.

Société Générale peut notamment apporter :

- des modifications techniques telles que l'acceptation de nouvelles Cartes, des 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 des Cartes portant certaines Marques,
  - la désactivation de la fonctionnalité Transaction crédit.

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

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

7.4 – Passés les délais visés au présent article, les modifications sont réputées acceptées par l'Accepteur s'il n'a pas résilié le présent Contrat, sans que Société Générale ait à lui rappeler cette faculté. Elles lui sont donc opposables.

7.5 – 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 9 de la présente Partie I, voire la résiliation du Contrat dans les conditions prévues à l'article 8 de la présente Partie I.

ARTICLE 8 – DURÉE ET RÉSILIATION DU CONTRAT

8.1 – Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans le Contrat de prestation. 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 du Schéma de son choix en utilisant des moyens sécurisés d'acceptation avec tout autre acquéreur de son choix.

8.2 – 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 9.2 ci-dessous. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

8.3 – Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat, sous réserve du dénouement des opérations en cours. Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

8.4 – L'Accepteur est tenu de restituer à Société Générale les dispositifs techniques et sécuritaires 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.

ARTICLE 9 – SUSPENSION DE L'ACCEPTATION

9.1 – 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 manquement(s) tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS.

9.2 – La suspension peut être décidée en raison notamment :

9.2.1 – du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation d'un Schéma,

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

9.2.3 – d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,

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

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

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

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

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

9.3 – 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.

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

ARTICLE 10 – MESURES DE PRÉVENTION ET DE SANCTION PRISES PAR SOCIÉTÉ GÉNÉRALE

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

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

10.3 – De même, si dans un délai de trois (3) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, Société Générale peut décider la résiliation de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

(F) 712558 - 07/2022

ARTICLE 11 – SECRET BANCAIRE ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

11.1 – Secret bancaire

De convention expresse l'Accepteur autorise Société Générale à stocker, le cas échéant, des données secrètes ou confidentielles portant sur lui et à 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.

11.2 – Protection des données à caractère personnel

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

Ainsi, en application de la réglementation française et européenne applicable en matière de 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 :

11.2.1 – Les données à caractère personnel relatives à l'Accepteur, collectées par Société Générale nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées que pour les seules 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 cinq (5) 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 dix (10) 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 le 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 ;
- 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.

11.2.2 – 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. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat.

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

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès de l'Accepteur, 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.

ARTICLE 12 – NON RENONCIATION

Le fait pour 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'elle soit, à l'exécution de celle-ci.

ARTICLE 13 – LOI APPLICABLE/TRIBUNAUX COMPÉTENTS

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

ARTICLE 14 – LANGUE DU PRÉSENT CONTRAT

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

PARTIE II : 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 I 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 I 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.

(F) 712558 - 07/2022

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

3.3 – En cas d'audit par le GIE CB, permettre à Société Générale de faire procéder dans les locaux de l'Accepteur ou dans ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée. Le rapport d'audit fera systématiquement l'objet d'une communication à l'Accepteur et au GIE CB.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) à ces clauses et/ou exigences, Le GIE CB et/ou Société Générale peu(t)(vent) procéder à une suspension de l'acceptation des Cartes CB, voire à la résiliation du présent Contrat, dans les conditions prévues à l'article 4 de la présente Partie. En outre, les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

ARTICLE 4 – MESURES DE PRÉVENTION ET DE SANCTION

4.1 – Mesures de prévention et de sanction mises en œuvre par Société Générale.

En cas de manquement de l'Accepteur aux dispositions relatives au Schéma CB du présent Contrat ou aux lois 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 trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, 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 trois (3) 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 trois (3) mois suivant la mise en demeure d'y remédier.

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

  La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la réception de la notification.
- la radiation de l'adhésion de l'Accepteur au Schéma CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis de l'Accepteur concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée avec demande d'avis de réception.

4.3 – En cas de suspension ou de radiation, l'Accepteur s'engage alors à restituer à 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 six (6) 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 I et des mesures de sécurité visées à l'article 4 de la Partie I.

ARTICLE 5 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

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

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

- la 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 douze (12) 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 cinq (5) 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 11.2.2 de la Partie I 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 I, 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

4.1 – 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 »).

4.2 – En cas de Compromission résultant d'un manquement de l'Accepteur et/ou d'un de ses prestataires autres que Société Générale aux exigences du Référentiel Sécuritaire PCI DSS telles que décrites dans le document

« Référentiel Sécuritaire Accepteur » annexé aux présentes, Société Générale appliquera à l'Accepteur :

a) Un forfait de 103 000 €,

b) 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 trois (3) acquéreurs, Société Générale appliquera, en remplacement de la pénalité complémentaire prévue à l'article 4.2.b 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 trente-six (36) 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.

NOTE D'INFORMATION SUR LE PAIEMENT À DISTANCE (HORS INTERNET) PAR CARTES

Vous venez de souscrire un contrat de Vente à Distance auprès de notre établissement, et nous vous en remercions. Nous espérons que l'accès au paiement par Carte contribuera au développement de votre chiffre d'affaires. Aussi, soucieux du bon déroulement de vos opérations de paiement, nous attirons votre attention sur les particularités de la Vente à Distance et sur les précautions que nous vous conseillons vivement d'observer.

Nous vous rappelons que le fait d'obtenir une autorisation du centre d'appel bancaire vous indique seulement que la Carte présentée n'a pas fait l'objet d'une demande de blocage au moment de la transaction et que le montant demandé est dans la limite autorisée du titulaire de la Carte.

Ainsi, comme indiqué à l'article 4 de la Partie I des présentes, 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, la simple communication du numéro de Carte, de la date d'échéance et du cryptogramme visuel (trois derniers chiffres au dos de la carte bancaire) autorise le titulaire, en l'absence de frappe du code secret ou de signature, à contester une opération. Aussi, afin de limiter le risque de fraude et d'impayé, nous vous conseillons, dans la mesure du possible, d'authentifier vos clients potentiels avant toute expédition de marchandises ou commencement d'exécution de prestations de services, notamment lors d'une première commande, par exemple en envoyant un courrier de confirmation de commande.

Par ailleurs, une vigilance toute particulière s'impose 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 de tout autre lieu à caractère public ;
- s'il s'agit de commandes répétitives émanant d'un même client, qui plus est si celui-ci est un nouveau client ;
- si l'on vous demande, pour des montants importants, de fractionner la somme due (sans doute pour obtenir plus facilement une autorisation), attention ces opérations fractionnées ne sont pas garanties ;
- 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,
- si la commande est d'un montant inhabituel ou si l'adresse de résidence est dans des pays avec lequel vous n'avez pas l'habitude de réaliser des opérations commerciales.

Pour toute question complémentaire en matière de Vente à Distance, nous vous invitons à téléphoner au 0825 067 068(1).

En attendant, nous espérons que ces recommandations seront de nature à améliorer la sécurité de vos opérations commerciales.

ANNEXE : RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR

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

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

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

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

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

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

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

EXIGENCE 2 (E2) – GÉRER L'ACTIVITÉ HUMAINE ET INTERNE

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

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

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

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

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

EXIGENCE 3 (E3) – GÉRER LES ACCÈS AUX LOCAUX ET AUX INFORMATIONS

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

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

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

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

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

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

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

(1) Service 0,15€ / min + prix appel.

(F) 712558 - 07/2022

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

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

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

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

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

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

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

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

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

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

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

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

Les autorisations données doivent être archivées et contrôlées régulièrement.

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

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

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

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

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

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

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXIGENCE 15 (E15) – PROTÉGER LA CONFIDENTIALITÉ DES IDENTIFIANTS – AUTHENTIFIANTS DES UTILISATEURS ET ADMINISTRATEUR

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

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

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

(F) 712558 - 07/2022

NIVEAUX ET ACTIONS À MENER PAR LE COMMERCANT POUR LA CONFORMITÉ ET VALIDATION

Sources : programmes PCI-DSS des Schémas Visa et Mastercard
AIS : Account Information Security, SDP : Site Data Protection.
https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp#2
https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html

CATÉGORIE	CRITÈRES	ACTIONS À MENER PAR LE COMMERÇANT/BASE ANNUELLE
	VISA	
NIVEAU 1	■ Commerçant ayant un volume annuel de transactions Visa tous canaux (à proximité et à distance) > 6 millions ou commerçant Global (i.e. opérant sur plusieurs pays)	■ Déposer un Rapport de conformité (« ROC ») réalisé par un QSA (Qualified Security Assessor) ou une ressource interne si signé par un représentant de l'entreprise ■ Soumettre un Formulaire d'Attestation de Conformité (« AOC »)
NIVEAU 2	■ Commerçant ayant un volume annuel de transactions Visa tous canaux de 1 à 6 million(s) tous canaux	■ Remplir un Questionnaire de l'Auto-Audit (« SAQ ») ■ Soumettre un Formulaire d'Attestation de Conformité (« AOC »)
NIVEAU 3	■ Commerçant ayant un volume annuel de transactions Visa e-com de 20k à 1 million	■ Remplir un Questionnaire de l'Auto-Audit (« SAQ ») ■ Soumettre un Formulaire d'Attestation de Conformité (« AOC »)
NIVEAU 4	■ Commerçant ayant un volume annuel de transactions Visa e-com < 20k ou tout autre commerçant ayant un volume annuel de transactions Visa jusqu'à 1 million	■ Remplir un Questionnaire de l'Auto-Audit (« SAQ ») ou procéder à un exercice de validation alternative comme défini par l'acquéreur
	MASTERCARD	
NIVEAU 1	■ Commerçant qui a subi un piratage ou une attaque ayant déclenché un événement de compromission dite "Account Data Compromise" (« ADC ») ■ Commerçant ayant un volume annuel total de transactions combinées Mastercard et Maestro > 6 millions ■ Commerçant ayant un volume annuel de transactions Visa tous canaux (à proximité et à distance) > 6 millions ou commerçant Global (i.e. opérant sur plusieurs pays) ■ Commerçant portant plusieurs failles de sécurité devant recevoir une autre qualification que « ADC » et présentant un risque pour le système de paiement	■ PCI DSS audit annuel visant à accomplir un Rapport de Conformité ((« ROC ») par un « QSA » (PCI SSC-approved Qualified Security Assecssor) ou un auditeur interne (Internal Secuirty Assessor ou « ISA ») certifié « PCI SSC » N.B. : Le ROC doit être conduit par un « QSA » (PCI SSC-approved Qualified Security Assecssor) ou un auditeur interne (Internal Secuirty Assessor ou « ISA ») certifié « PCI SSC »
NIVEAU 2	■ Commerçant ayant un volume annuel total de transactions combinées Mastercard et Maestro > 1 million mais < = 6 millions ■ Commerçant ayant un volume annuel de transactions Visa tous canaux de 1 à 6 million(s) tous canaux	■ Questionnaire de l'Auto-Audit (« SAQ »)* N.B. : Les commerçants remplissant le SAQ A, SAQ A-EP ou SAQ D doivent en outre engager un QSA ou auditeur interne certifié « PCI SSC » pour la validation de conformité
NIVEAU 3	■ Commerçant ayant un volume annuel total de transactions e-com combinées Mastercard et Maestro > 20k mais < = 1 million ■ Commerçant répondant aux critères de niveau 3 de Visa	■ Questionnaire de l'Auto-Audit (« SAQ »)*
NIVEAU 4	■ Tout autre commerçant**	■ Questionnaire de l'Auto-Audit (« SAQ »)*

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

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

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

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

(F) 712558 - 07/2022