CONDITIONS GÉNÉRALES DU CONTRAT D'ACCEPTATION AUTOMATE (PAR CARTES DE PAIEMENT)

Le contrat d'acceptation Automate en libre-service (également dénommé « **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 convenues entre Société Générale et l'Accepteur (également dénommées « **Contrat de prestation Automate** »).

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 percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) 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) en Partie 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 Économique Européen (ci-après l'« EEE » - Il comprend les États membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :
– « CRÉDIT » ou « CARTE DE CRÉDIT »,
– « DÉBIT », « PRÉPAYÉ »,
– « COMMERCIAL »,

ou l'équivalent dans une langue étrangère.

1.4 – Par « Catégorie de carte », il faut entendre les catégories de Cartes suivantes :
– la catégorie des cartes de crédit,
– la catégorie des cartes de débit,
– la catégorie des cartes prépayées,
– la catégorie des cartes commerciales.

1.5 – Par « Donnée de sécurité personnalisée », il faut entendre une donnée fournie au titulaire de la Carte par son prestataire de services de paiement à des fins d'authentification. Le code secret de la Carte est une Donnée de sécurité personnalisée.

1.6 – Par « Automate », il faut entendre tout Équipement Électronique agréé ou approuvé par le Schéma dont les marques figurent sur les cartes acceptées par l'Accepteur, permettant la distribution automatique de biens et services, acceptant le paiement par Carte en libre-service en mode sans contact uniquement, impliquant la présence du Titulaire de la Carte au point d'acceptation et sans intervention directe de l'Accepteur.

L'agrément ou l'approbation de l'automate est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par chaque Schéma concerné, qui dispose de la liste des automates agréés ou approuvés.

Définition des classes d'Automates :

Les automates de classe 1 délivrent des biens ou des prestations de services dont le montant est connu avant le déroulement de l'opération.

Les automates de classe 2 délivrent des biens ou des prestations de services dont le montant n'est pas connu avant le déroulement de l'opération. Le calcul du cumul des opérations ne peut se faire qu'à partir du montant réel des opérations précédentes effectuées par le même titulaire de la Carte, le même jour sur le même point de vente (SIRET).

Les automates de classe 2 comprennent deux sous-classes :
– Les Automates de classe 2.1 délivrent des biens ou des prestations de services dont le montant est estimé par le Titulaire de la Carte avant le déroulement de l'opération. Ces appareils sont donc pourvus d'une fonction permettant d'interroger le Titulaire de la Carte, avant la demande d'autorisation, sur sa consommation estimée.
– Les Automates de classe 2.2 délivrent des biens ou des prestations de services dont le montant ne peut pas être connu ou estimé avant le déroulement de l'opération. L'autorisation, lorsqu'elle est requise, est alors demandée pour un montant fixe, défini dans les Conditions Particulières convenues avec l'Acquéreur, et appelé « montant d'autorisation ».

1.7 – Par « Instrument sans contact », il faut entendre une Carte équipée de la technologie « sans contact » ou un autre instrument de paiement disposant de la technologie « sans contact » constitué d'un logiciel de paiement mobile en mode « sans contact » intégré pour partie dans l'élément sécurisé d'un téléphone mobile, pour partie dans le téléphone mobile lui-même, et permettant de réaliser des opérations de paiement quelle qu'en soit la Marque.

1.8 – 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 entrant dans le cadre du Contrat sont les Marques visées en Partie II des présentes.

1.9 – Par « Parties », il faut entendre Société Générale et l'Accepteur.

1.10 – Par « Point d'acceptation », il faut entendre le lieu physique où est initié l'ordre de paiement.

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

1.12 – 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(es) Marque(s) desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

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

ARTICLE 2 – OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

2.1 – Afficher visiblement chaque Marque qu'il accepte notamment en apposant de façon apparente sur son Automate des panonceaux, vitrophanies et enseignes qui lui sont fournis par Société Générale et/ou le Schéma.

Pour la(es) 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 qu'en soit la Catégorie de carte.

2.2 – Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse de façon apparente sur son Automate.

2.3 – Afficher visiblement le montant minimum éventuel à partir duquel la Marque et/ou la Catégorie de carte est(sont) acceptée(s) afin que le titulaire de la Carte en soit préalablement informé.

2.4 – 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. Si l'Accepteur a opté pour une Marque préférée et que le titulaire de la Carte souhaite choisir une autre Marque, il s'engage à informer ce dernier qu'il doit appuyer sur la touche « Correction » de l'Automate pour ce faire.

2.5 – S'abstenir de toute activité illicite telle que la mise en péril de mineurs, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle, le non-respect de la protection des données à caractère personnel, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non-respect des dispositions relatives aux conditions d'exercice de professions réglementées, la vente de produits prohibés.

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 (notamment, le cas échéant, par le biais de son ticket), vérifier avec Société Générale la conformité des informations transmises pour identifier son Point d'acceptation. Les informations doivent indiquer une dénomination commerciale connue du titulaire de la Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (Paiement de proximité, vente à distance, etc…) dans ce Point d'acceptation.

2.7 – Accepter les paiements effectués avec les Cartes portant la(es) Marque(s) et Catégorie(s) de carte qu'il a choisies d'accepter ou qu'il doit accepter en contrepartie

(D)714774 - 07/2022

(i) de vente de biens et/ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même, (ii) de dons.

2.8 – Remettre au titulaire de la Carte un ticket dans tous les cas où l'Automate en édite un qui lui est destiné.

2.9 – Ne pas stocker, sous quelque forme que ce soit, aucune des données de paiement sensibles liées à la Carte suivantes :
– le cryptogramme visuel (trois derniers chiffres du numéro figurant au verso de la Carte) ;
– la piste magnétique dans son intégralité ;
– le code secret.

2.10 – Ne pas collecter au titre des présentes une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement du titulaire de la Carte.

2.11 – Transmettre les enregistrements des opérations de paiement à Société Générale, dans les délais prévus dans les Conditions Particulières convenues avec lui.

2.12 – 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.

2.13 – Utiliser obligatoirement l'Automate et ne pas modifier les paramètres de son fonctionnement. L'Accepteur s'engage également à faire le nécessaire pour que l'Automate soit en permanence conforme aux spécifications techniques et fonctionnelles propres à chaque Schéma concerné. Toute intervention sur ledit Automate (notamment pour assurer sa maintenance) ne devra être effectuée que par des prestataires recommandés par Société Générale.

À défaut, l'Accepteur assumera, vis-à-vis de Société Générale, toutes les éventuelles conséquences préjudiciables qui pourraient en résulter.

2.14 – Prendre toutes les mesures propres à assurer la garde de son Automate et être vigilant quant à l'utilisation qui en est faite.

2.15 – 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 de paiement sensibles liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter tant le Référentiel Sécuritaire PCI/DSS que le Référentiel Sécuritaire Accepteur annexé aux présentes, acceptent que les audits visés à l'article 2.16 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé audit article.

2.16 – Le cas échéant, permettre à Société Générale de faire procéder dans les locaux de l'Accepteur ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du Contrat que des exigences du Référentiel Sécuritaire Accepteur figurant en annexe et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du Contrat et/ou pendant sa durée.

L'Accepteur autorise la communication du rapport à Société Générale et aux Schémas concernés.

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(des) Schéma(s), à une suspension de l'acceptation des Cartes par l'Accepteur, voire à la résiliation du présent Contrat telle que prévue à l'article 9 ci-après, et les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

2.17 – Respecter les exigences du Référentiel Sécuritaire Accepteur annexé aux présentes et les exigences 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.

2.18 – 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.

ARTICLE 3 – OBLIGATIONS DE SOCIÉTÉ GÉNÉRALE

Société Générale s'engage à :

3.1 – Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie II des présentes et son/leur évolution, les Catégories de carte et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de carte et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

3.2 – Respecter le choix de la Marque utilisée pour donner l'ordre de paiement effectué au Point d'acceptation conformément au choix de l'Accepteur ou du titulaire de la Carte.

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

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 modalités définies ci-dessous et dans les Conditions Particulières convenues avec lui :
– 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 :
  - 8h30 pour une télécollecte ;
  - 10h00 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'inter-change.

L'Accepteur peut demander que ces informations soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'inter-change 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'inter-change.

L'Accepteur peut demander que les commissions de service soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'inter-change applicable à l'opération.

ARTICLE 4 – GARANTIE DE PAIEMENT

4.1 – Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 ci-après qu'en Partie II des présentes, ainsi que dans les Conditions Particulières.

4.2 – Toutes les mesures de sécurité sont indépendantes les unes des autres.

Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code secret ou de toute autre Donnée de sécurité personnalisée lorsqu'il ou elle est requis(e).

4.3 – En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement.

Société Générale pourra contre-passer 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 – L'Accepteur doit informer immédiatement Société Générale en cas de fonctionnement anormal de l'automate et pour toutes autres anomalies (absence de reçu ou de mise à jour de la liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par Société Générale, impossibilité de réparation rapide, etc.).

5.2 – Lors du paiement

L'Accepteur s'engage à :

5.2.1 – Vérifier l'acceptabilité de la Carte, c'est-à-dire :
– la Marque et/ou la Catégorie de carte du Schéma concerné par l'acceptation,
– l'hologramme sauf pour les Cartes portant la Marque V PAY,
– la puce sur les Cartes lorsqu'elle y est prévue par le Schéma,
– la Marque et Catégorie de carte définies dans les conditions spécifiques au Schéma concerné figurant dans la partie II des présentes ou dans les Conditions Particulières,
– le cas échéant, la période de validité (fin et éventuellement début).

5.2.2 – Utiliser l'automate selon les modalités techniques qui lui ont été indiquées.

L'automate doit notamment le cas échéant :
– après la lecture de la puce de la Carte lorsqu'elle est présente :
  - permettre le contrôle du code secret ou de toute autre Donnée de sécurité personnalisée lorsque la puce le lui demande,
  - vérifier :
    · le code émetteur de la Carte (BIN),
    · le code service,
    · le cas échéant, la date de fin de validité de la Carte.
– lorsque la puce n'est pas présente sur une Carte, après lecture de la piste ISO 2, vérifier :
  - le code émetteur de la Carte (BIN),
  - le code service,
  - le cas échéant, la date de fin de validité de la Carte.

5.2.3 – Lorsque la puce le demande à l'automate, faire composer par le titulaire de la Carte, dans les meilleures conditions de confidentialité, son code secret (ou lui faire utiliser toute autre Donnée de sécurité personnalisée). La preuve de la frappe du code secret ou de l'utilisation de toute autre Donnée de sécurité personnalisée est apportée par le certificat qui doit figurer sur le ticket émis par l'automate conservé par l'Accepteur (ci-après « Ticket »).

Lorsque le code secret ou toute autre Donnée de sécurité personnalisée n'est pas vérifié(e), l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

(D)714774 - 07/2022

En cas d'opération en mode « sans contact » permise par l'automate, l'opération de paiement est garantie même si le code secret ou toute autre Donnée de sécurité personnalisée n'a pas à être vérifié(e), sous réserve du respect de toutes les autres mesures de sécurité.

5.2.4 – Obtenir une autorisation d'un montant identique à l'opération sous-jacente :
- lorsque le montant de l'opération en cause, ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée et pour le même Point d'acceptation, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec Société Générale, et ceci quelle que soit la méthode d'acquisition des données de la Carte,
- lorsque l'automate ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec Société Générale.

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

Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

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

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

5.2.5 – Interdire une opération supérieure à 1 500 euros.

5.2.6 – Afficher le montant réel de l'opération dès que l'automate peut le définir ou l'estimer et au plus tard, à la délivrance du bien ou du service.

5.3 – Après le paiement

L'Accepteur s'engage à :

5.3.1 – 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. Toute opération ayant fait l'objet d'une autorisation transmise par Société Générale doit être obligatoirement remise à cette dernière.

5.3.2 – Archiver et conserver, à titre de justificatif, pendant quinze (15) mois à compter de la date de l'opération, l'enregistrement magnétique représentatif de chaque opération comprenant l'image du ticket fourni par l'Automate et notamment les numéros de certificat et s'il y a lieu d'autorisations ainsi que tout éléments servant à leur calcul ou le journal de fond lui-même.

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

ARTICLE 6 – PAIEMENT « SANS CONTACT »

Cet article s'applique si l'Accepteur utilise un automate disposant de la technologie « sans contact ».

Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du Contrat sont applicables aux opérations de paiement réalisées avec un automate de paiement sans contact.

Lorsque l'Accepteur utilise un Automate disposant de la technologie dite « sans contact », ledit Automate permet le paiement rapide par les utilisateurs de l'automate sans contact grâce à une lecture à distance dudit automate sans contact.

L'Accepteur s'engage à signaler au public l'acceptation du paiement « sans contact » par l'apposition sur l'Automate, au niveau du lecteur « sans contact », de façon apparente, d'un pictogramme permettant d'identifier le paiement « sans contact ».

En toutes circonstances, l'Accepteur doit se conformer aux directives qui apparaissent sur l'Automate, notamment la frappe du code secret dans les meilleures conditions de confidentialité.

Le montant unitaire maximum de chaque opération de paiement en mode « sans contact » est limité à cinquante (50) euros lorsque l'opération de paiement est réalisée au moyen d'une Carte équipée de la technologie « sans contact » dont le plafond aura été mis à jour (si ce plafond n'a pas été mis à jour, le montant unitaire maximum de chaque opération de paiement en mode « sans contact » est limité à trente (30) euros). Au-delà de ce montant unitaire maximum, les conditions de l'opération de paiement telles que prévues dans les Conditions Générales de la présente Partie restent inchangées.

Lorsqu'un certain nombre de règlements successifs en mode « sans contact » est atteint, l'Accepteur peut être amené à passer en mode contact même pour une opération d'un montant inférieur au montant unitaire maximum d'une opération en mode « sans contact ».

Lorsque l'opération de paiement est réalisée à l'aide d'un Automate sans contact autre que la Carte équipée de la technologie « sans contact », les articles 5.2.1, 7.3, 7.4 et 7.6 de la présente Partie ne sont pas applicables.

ARTICLE 7 – MODALITÉS ANNEXES DE FONCTIONNEMENT

7.1 – 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 une durée de quinze (15) jours calendaires à compter de la date de débit en compte résultant d'une opération non garantie.

Dès lors que le caractère mal exécuté d'une opération sera établi 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.

7.2 – 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, les enregistrements électroniques produits par Société Générale et/ou le Schéma dont les règles s'appliquent à l'opération de paiement concernée 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.

7.3 – Dysfonctionnement

Société Générale et l'Accepteur ne peuvent être tenus pour responsable de l'impossibilité d'effectuer le paiement en cas de dysfonctionnement de la Carte et/ou de son support.

ARTICLE 8 – MODIFICATIONS

8.1 – Société Générale peut modifier à tout moment les présentes Conditions Générales ainsi que les Conditions Particulières.

8.2 – 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 état de l'automate à la suite d'un dysfonctionnement, etc.
- des modifications sécuritaires telles que :
  - la modification du seuil de demande d'autorisation,
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptabilité des Cartes portant certaines Marques.

8.3 – 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.

8.4 – Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque Société Générale ou le Schéma concerné constate, dans le Point d'acceptation, une utilisation anormale de Cartes/automates sans contact perdu(e)s, volé(e)s ou contrefait(e)s.

8.5 – 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.

8.6 – Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat.

ARTICLE 9 – DURÉE ET RÉSILIATION DU CONTRAT

9.1 – Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

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.

9.2 – 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 10.2 ci-dessous. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

9.3 – 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.

9.4 – L'Accepteur sera 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 son Point d'acceptation tout signe d'acceptation des Cartes du(des) Schéma(s) concerné(s).

(D)714774 - 07/2022

ARTICLE 10 – SUSPENSION DE L'ACCEPTATION

10.1 – Société Générale peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes/d'Automates sans contact 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 2.16 de la présente Partie, 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.

10.2 – La suspension peut être décidée en raison notamment :

10.2.1 – du non-respect répété des obligations du présent Contrat et du refus d'y remédier, notamment d'une utilisation d'un Automate non agréé permettant à l'Accepteur d'accéder au Système d'Acceptation et d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma,

10.2.2 – d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes/Automates sans contact perdu(e)s, volé(e)s ou contrefait(e)s,

10.2.3 – d'un refus d'acceptation répété et non motivé des Cartes du Schéma qu'il a choisies d'accepter ou qu'il doit accepter,

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

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

10.2.6 – d'un risque aggravé en raison des activités de l'Accepteur.

10.3 – L'Accepteur s'engage alors à restituer à Société Générale les dispositifs techniques et sécuritaires et les documents en sa possession dont Société Générale est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes du(des) Schéma(s) concerné(s).

10.4 – 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 auprès de Société Générale ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son choix.

ARTICLE 11 – MESURES DE PRÉVENTION ET DE SANCTION PRISES PAR SOCIÉTÉ GÉNÉRALE

En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes/d'Automates sans contact perdu(e)s, volé(e)s ou contrefait(e)s, 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.

11.1 – 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 dans les conditions précisées à l'article 10 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.

11.2 – 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 des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

ARTICLE 12 – SECRET BANCAIRE ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

12.1 – 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.

12.2 – 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 :

12.2.1 – 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.

12.2.2 – 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 13 – 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 14 – 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 présent Contrat est soumise 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 15 – LANGUE DU PRÉSENT CONTRAT

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

(D)714774 - 07/2022

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 ») auprès des Accepteurs adhérant au Schéma CB dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou solution de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'adhésion, 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 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 des articles 2.7, 2.11 et 2.16 de la Partie I du présent Contrat, l'Accepteur s'engage :
– à accepter les Cartes CB pour le paiement d'achats de biens et/ou de prestations de services offerts à sa clientèle et réellement effectués,
– à 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 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,
– en cas de demande d'audit par le GIE CB, à permettre à Société Générale de faire procéder dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

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

ARTICLE 4 – SUSPENSION DE L'ADHÉSION ET RADIATION DU SCHÉMA CB

4.1 – Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au Schéma CB. Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen. Son effet est immédiat.

Elle peut être décidée en raison notamment :
– d'une utilisation anormale de Cartes/d'Instruments de paiement sans contact perdu(e)s, volé(e)s ou contrefait(e)s,
– d'une utilisation d'Automates non agréé,
– d'un risque de dysfonctionnement important du Schéma CB,
– d'une utilisation anormale ou détournée de l'Automate.

4.2 – L'Accepteur s'engage alors à restituer à Société Générale l'Automate, les dispositifs techniques et sécuritaires et les documents en sa possession dont Société Générale est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes CB.

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

4.4 – 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'adhésion avec un autre acquéreur de son choix.

4.5 – En cas de comportement frauduleux de la part de l'Accepteur, il peut être immédiatement radié du Schéma CB ou la suspension être convertie en radiation.

ARTICLE 5 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Société Générale, au titre de l'acceptation en paiement de proximité 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 deux (2) années 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 ;
– 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 12.2.2 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 Inc et Visa Europe ;
– Mastercard International Inc.

Les Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes :
– Pour VISA Inc. :
  - Visa ;
  - V PAY ;
  - ELECTRON.
– Pour Mastercard International Inc. :
  - Mastercard ;
  - Maestro.

ARTICLE 2 – OBLIGATION DE SOCIÉTÉ GÉNÉRALE

Par dérogation à l'article 3.6 de la Partie I du présent Contrat, Société Générale s'engage à ne pas débiter au-delà du délai maximum de vingt-quatre (24) mois à partir de la date de crédit initial porté au compte de l'Accepteur les opérations de paiement non garanties et qui n'ont pu être imputées sur le compte sur lequel fonctionne la Carte.

ARTICLE 3 – GARANTIE DE PAIEMENT

Une opération de paiement réalisée en lecture puce « EMV » est garantie, même s'il n'y a pas eu frappe du code secret par le titulaire de la Carte, à condition d'avoir obtenu une autorisation d'un montant identique à ladite opération.

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 « Programme PCI/DSS » 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 :

	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Forfait initial	50 000 €	25 000 €	10 000 €	10 000 €
Forfait complémentaire en cas de non régularisation dans les 90 jours	+ 30 000 €	+ 15 000 €	+ 5 000 €	+ 5 000 €
Forfait complémentaire en cas de non régularisation dans les 120 jours	+ 50 000 €	+ 25 000 €	+ 10 000 €	+ 10 000 €
Forfait complémentaire en cas de non régularisation dans les 150 jours	+ 75 000 €	+ 50 000 €	+ 15 000 €	+ 15 000 €
Forfait complémentaire en cas de non régularisation dans les 180 jours	+ 75 000 €	+ 50 000 €	+ 15 000 €	+ 15 000 €

N.B : Les niveaux précisés ci-dessus correspondent à ceux définis par le Standard PCI DSS détaillé dans le document « Programme PCI/DSS – AUTOMATE » annexé aux présentes

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 réputé 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.

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.

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.

(D)714774 - 07/2022

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-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.

(D)714774 - 07/2022

PROGRAMME PCI/DSS

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.

(D)714774 - 07/2022