ENTENTE SUR LE TRAITEMENT DES DONNÉES

Gordon Food Service, Inc. et Gordon Food Service Canada, Ltd.

Dernière mise à jour le 19 février 2024

La présente Entente sur le traitement des données (« **DPA** ») s'applique à tout Fournisseur de marchandises à GFS (« **Fournisseur** ») qui a conclu un ou plusieurs contrats avec Gordon Food Service, Inc. et Gordon Food Service Canada Ltd. (ensemble, « **GFS** »). Le Fournisseur et GFS sont désignés dans le présent document par les termes « **partie** » ou « **parties** », selon le contexte.

1. Définitions clés

1.1 « **Affiliés** » : toute entité qui, directement ou indirectement, contrôle, est contrôlée par ou est sous contrôle commun avec GFS. Aux fins de la présente définition, on entend par « **contrôle** » la propriété ou le contrôle direct ou indirect de plus de 50 % des intérêts avec droit de vote de l'entité concernée.

1.2 « **Accords** » : une ou plusieurs ententes entre le Fournisseur et GFS en vertu desquels le Fournisseur a accès aux RP couverts, les recueille ou les traite d'une autre manière.

1.3 « **RP couverts** »: tous les renseignements personnels fournis au Fournisseur par GFS ou recueillis pour le compte de GFS, recueillis par le Fournisseur pour le compte de GFS ou mis à la disposition du Fournisseur d'une autre manière en vertu des Accords.

1.4 « **Renseignements personnels** » : (a) toute information relative à un consommateur ou à un ménage et (b) toute information relevant des termes « données personnelles », « renseignements personnels » ou « informations personnellement identifiables » (ou tout concept ou définition similaire ou analogue) en vertu des Lois sur la protection des RP.

1.5 « **Format portable** »: dans la mesure où cela est techniquement possible, un format structuré, couramment utilisé, lisible par machine et facilement utilisable, qui permet au consommateur de transmettre les RP couverts à une autre entité ou à un autre responsable du traitement sans entrave, comme le précisent les Lois sur la protection des RP.

1.6. « **Lois sur la protection des RP** » désigne toutes les lois et tous les règlements sur la protection des renseignements personnels et des données applicables au traitement des RP couverts dans le cadre de l'Accord, y compris, mais sans s'y limiter, ceux des États-Unis et du Canada, le California Consumer Privacy Act, le California Privacy Rights Act, le Virginia Consumer Data Protection Act, le Colorado Privacy Act, la Loi sur la protection des renseignements personnels et les documents électroniques (« **LPRPDE** »), le Personal Information Protection Act de la Colombie-Britannique (« **BC PIPA** ») ; le Personal Information

Protection Act de l'Alberta (« **AB PIPA** ») ; et la Loi sur la protection des renseignements personnels dans le secteur privé du Québec (« **Loi sur le privé du Québec** »), lorsqu'elles s'appliquent au traitement des RP couverts par le Fournisseur en vertu de ce DPA.

1.7 Les termes « entreprise », « fins commerciales », « consommateur », « contrôleur », « traitement », « sous-traitant », « vente », « données sensibles », « renseignements personnels sensibles », « Fournisseur de services », « partage » et « demande vérifiable du consommateur » ont le sens qui leur est donné dans les Lois sur la protection des RP. En cas de conflit dans la signification des termes dans les Lois sur la protection des RP, les parties conviennent que les significations de chaque loi s'appliquent.

1.8 « **Services** »: réfère aux services fournis par le Fournisseur à GFS et spécifiés dans les Accords.

2. Conditions du traitement des données

2.1 ***Relations entre les parties***. Les parties conviennent que GFS est la seule partie qui détermine les objectifs et les moyens de traitement des RP couverts en tant qu'"entreprise" ou "contrôleur", et que le Fournisseur traite les RP couverts en tant que "Fournisseur de services" ou "sous-traitant" pour le compte de GFS.

2.2 ***Respect des obligations***. Le Fournisseur déclare et garantit que le Fournisseur, ses employés, spécialistes, sous-traitants et fournisseurs de services (a) se conformeront aux Lois sur la protection des RP et au présent DPA lors du traitement des RP couverts, et (b) fourniront à GFS toute l'assistance raisonnablement requise pour permettre à GFS de remplir ses propres obligations en vertu des Lois sur la protection des RP. Sur demande raisonnable de GFS, le Fournisseur mettra à la disposition de GFS toutes les informations en sa possession raisonnablement nécessaires pour démontrer sa conformité avec le présent paragraphe.

2.3 ***Suppression ou restitution des RP couverts***. Sur demande écrite de GFS ou en cas de résiliation d'un contrat, le Fournisseur cessera de traiter les RP couverts dans les plus brefs délais. Dans les soixante (60) jours suivant une demande écrite de GFS ou la résiliation d'un contrat, le Fournisseur détruira les RP couverts, sauf instruction contraire de GFS ; à condition qu'avant cette destruction, le Fournisseur renvoie ou mette à la disposition de GFS pendant une période de soixante (60) jours, pour un téléchargement complet et sécurisé, tous les RP couverts en sa possession. Le Fournisseur peut conserver les RP couverts dans la mesure et pour la durée requises par le droit applicable, à condition que le Fournisseur (a) informe GFS de ces obligations (sauf interdiction) et (b) garantisse la confidentialité permanente de tous ces RP couverts. Sur demande écrite de GFS ou dans les 60 jours suivant la résiliation d'un contrat, le Fournisseur fournira à GFS une attestation écrite certifiant qu'il s'est conformé à ces obligations de suppression.

2.4 ***Évaluations***. Le cas échéant, le Fournisseur fournira à GFS, à la demande raisonnable de ce dernier, l'assistance et les informations raisonnablement nécessaires pour permettre à GFS d'effectuer des évaluations des facteurs relatifs à la vie privée en vertu des Lois sur la protection des RP.

3. Limitation de l'utilisation des RP couverts

3.1 ***Portée limitée du traitement***. Le Fournisseur traitera les RP couverts uniquement selon les instructions données dans les Accords, le présent DPA et toute autre instruction écrite fournie par GFS qui est compatible avec les termes de l'Accord, dans chaque cas pour la durée de la fourniture des Services à GFS.

3.2 ***Restrictions concernant les données***. Le Fournisseur ne doit pas (a) vendre ou partager les RP couverts, (b) collecter, conserver, utiliser ou divulguer les RP couverts à des fins autres que les fins commerciales spécifiées dans les Accords, telles que la fourniture des Services à GFS, (c) conserver, utiliser ou divulguer les RP couverts en dehors de la relation commerciale directe avec GFS, (d) combiner les RP couverts avec d'autres Renseignements personnels, (d) combiner les RP couverts avec d'autres Renseignements personnels, y compris pour procéder à l'augmentation des données ou au profilage, à moins que les Lois sur la protection des RP ne l'autorisent expressément pour les fonctions du Fournisseur (par exemple, à des fins de prévention de la fraude ou lorsque la loi l'exige), et/ou (e) exporter les RP couverts en dehors du pays à partir duquel ils ont été fournis ou collectées sans l'accord écrit préalable de GFS. Le Fournisseur a le droit d'utiliser les données agrégées (telles que définies ci-dessous) à des fins commerciales internes avec le consentement écrit de GFS (courriel suffisant), à condition que le Fournisseur n'utilise ni ne divulgue les données agrégées à des fins commerciales. Par « **données agrégées** », on entend les RP couverts qui sont dépersonnalisés et agrégés conformément aux Lois sur la protection des RP, de sorte que les informations ne sont pas liées ou ne peuvent raisonnablement être liées à GFS ou à ses clients.

3.3 ***Droits d'audit***. GFS ou, au choix de GFS, un tiers raisonnablement désigné par GFS pour agir au nom de GFS et acceptable pour le Fournisseur, a le droit de contrôler la conformité du Fournisseur avec le présent DPA par des mesures pouvant inclure des examens manuels, des analyses automatisées, des tests de pénétration, des évaluations régulières, des audits ou des tests techniques ou opérationnels. Le Fournisseur coopérera pleinement à tout audit initié par GFS, à condition que cet audit n'interfère pas de manière déraisonnable avec la conduite normale des affaires du Fournisseur. Le Fournisseur doit fournir des résultats audités avec suffisamment de détails pour comprendre les conclusions, les risques connexes et les exigences en matière de remédiation. Sauf obligation contraire de la loi, GFS doit avertir le Fournisseur au moins 10 jours à l'avance d'un tel audit et ne doit pas auditer le Fournisseur plus de deux fois par période de douze mois, étant entendu que GFS peut procéder à un audit à tout moment en cas d'incident de sécurité, à la demande d'une autorité de réglementation ou dans le cadre de la défense des droits légaux de GFS.

Si les résultats de l'audit révèlent un manquement important au respect du présent DPA par le Fournisseur, ce dernier travaillera de bonne foi avec GFS pour remédier à ces problèmes à la satisfaction de GFS.

3.4 ***Remédiation à la conformité ; droits de résiliation***. Le Fournisseur s'engage à informer GFS dans les meilleurs délais s'il détermine qu'il n'est plus en mesure de respecter ses obligations en vertu des Lois sur la protection des RP. Dès réception de la notification du Fournisseur conformément au présent paragraphe, GFS peut demander au Fournisseur de prendre les mesures raisonnables et appropriées pour remédier à l'utilisation non autorisée des RP couverts ou résilier les Accords.

3.5 ***Sous-traitants ; fournisseurs de services.***

1. ***Nomination de sous-traitants***. Le Fournisseur a le droit d'engager des sous-traitants dans le cadre de l'exécution de ses Services en vertu des présentes (« Sous-traitants »). Avant le début de tout traitement de RP couverts par le Fournisseur en vertu des présentes, le Fournisseur doit fournir à GFS la liste actuelle des Sous-traitants engagés dans le traitement de RP couverts pour chaque service applicable, y compris une description de leurs activités de traitement et des pays où ils se trouvent. Le Fournisseur doit informer GFS par écrit (courriel suffisant) de tout changement concernant l'ajout ou le remplacement de Sous-traitants engagés dans le traitement des RP couverts. En outre, le Fournisseur doit s'assurer que les Sous-traitants du Fournisseur qui traitent les RP couverts pour le compte du Fournisseur acceptent par écrit les mêmes restrictions et exigences que celles qui s'appliquent au Fournisseur dans le présent DPA et les Accords en ce qui concerne les RP couverts. Le Fournisseur demeure entièrement responsable envers GFS des actes et omissions de ses Sous-traitants.

2. ***Droit d'opposition***. GFS peut s'opposer par écrit à la désignation par le Fournisseur d'un nouveau Sous-traitant ou fournisseur de services pour des motifs raisonnables liés à la protection des données en le notifiant par écrit au Fournisseur dans un délai de 30 jours à compter de la réception de la notification conformément à l'article 3.5. Si GFS s'y oppose, les parties discuteront de bonne foi des préoccupations de GFS en vue de parvenir à une résolution commercialement raisonnable. Si aucune solution ne peut être trouvée, le Fournisseur, à sa seule discrétion, aura le choix entre : i) ne pas désigner le Sous-traitant ou le fournisseur de services ou; ii) autorisera GFS à résilier les Accords, en remboursant dans ce dernier cas à GFS tous les frais non utilisés et payés d'avance.

3.6 *Réidentification*. Le Fournisseur ne réidentifiera pas, et n'autorisera pas ses Sous-traitants ou fournisseurs de services à réidentifier, les données dépersonnalisées, anonymisées ou pseudonymisées dérivées des RP couverts traités par le Fournisseur pour le compte de GFS, sauf instruction écrite de GFS (un courrier électronique suffit).

4. Demandes des consommateurs

4.1 ***Répondre aux demandes des consommateurs***. Le Fournisseur met en œuvre et maintient des processus et des procédures suffisants pour répondre aux demandes d'accès, de correction et/ou de suppression des RP couverts détenus par le Fournisseur que peut recevoir GFS. Dans les dix (10) jours suivant une demande écrite de GFS (un courriel suffit), le Fournisseur doit, le cas échéant : (a) effacer ou détruire en toute sécurité, ou faire effacer ou détruire, des éléments spécifiques des RP couverts, y compris toute copie de ces RP couverts conservée par le(s) Sous-traitant(s) ou le(s) fournisseur(s) de services du Fournisseur ; (b) fournir les informations demandées par GFS sur le traitement des RP couverts par le Fournisseur ; (e) modifier, et ordonner à ses sous-traitants ou fournisseurs de services de modifier, des éléments spécifiques des RP couverts ; ou (f) limiter le traitement des RP couverts qui sont « sensibles » en vertu des Lois sur la protection des RP, conformément aux instructions de GFS.

4.2 ***Renvoi des demandes directes***. Le Fournisseur doit renvoyer à GFS toutes les demandes des consommateurs soumises directement au Fournisseur concernant les RP couverts. Le Fournisseur ne doit pas répondre à ces demandes autrement qu'en informant le demandeur que la demande est renvoyée à GFS.

5. Contrôles de sécurité

5.1 ***Obligation de confidentialité***. Le Fournisseur, ses employés, ses spécialistes, ses sous-traitants et ses fournisseurs de service sont soumis à une obligation de confidentialité en ce qui concerne les RP couverts.

5.2 ***Mesures de sécurité***. Le Fournisseur met en œuvre et maintient des mesures, procédures et pratiques de sécurité techniques et organisationnelles raisonnables, adaptées à la nature des RP couverts, afin de protéger ces RP couverts contre l'accès, la destruction, l'utilisation, la modification ou la divulgation non autorisés (« Mesures de sécurité »). Ces Mesures de sécurité doivent respecter ou dépasser les normes industrielles applicables (par exemple, le NIST Cybersecurity Framework) et toutes les obligations énoncées dans les Accords ou dans les lois applicables. Le Fournisseur se conformera aux exigences de l'Annexe sur la sécurité jointe aux présentes.

5.3 ***Incident de sécurité.***

(a) ***Notification***. Le Fournisseur doit informer GFS dans les vingt-quatre (24) heures de l'accès, de la destruction, de l'utilisation, de la modification ou de la divulgation non autorisés soupçonnés par le Fournisseur (chacun étant un « **Incident de sécurité** ») de tout RP couvert. Le Fournisseur informera GFS par courrier électronique avec accusé de réception à **privacy@gfs.com** en mettant en copie **legal@gfs.com** et le principal contact commercial du Fournisseur chez GFS. Le Fournisseur doit : (i) fournir à GFS le nom et les coordonnées d'un employé du Fournisseur qui servira de contact principal de GFS en matière de sécurité et sera

disponible pour aider GFS vingt-quatre (24) heures par jour, sept (7) jours par semaine en tant que contact pour résoudre les obligations associées à un Incident de sécurité. La notification écrite fournie conformément au présent paragraphe comprendra un bref résumé des faits disponibles, l'état d'avancement de l'enquête du Fournisseur et, s'il est connu et applicable, le nombre potentiel de personnes affectées par l'Incident de sécurité.

(b) ***Gestion et remédiation***. Le Fournisseur fournira à GFS toute information et coopération raisonnablement demandée par GFS concernant tout Incident de sécurité, y compris en fournissant à GFS ou à son enquêteur désigné raisonnablement acceptable par le Fournisseur un accès physique aux installations et opérations concernées, en facilitant les entretiens et en mettant à disposition les dossiers, journaux et autres documents pertinents raisonnablement requis par GFS. Le Fournisseur doit immédiatement remédier à tout Incident de sécurité à ses propres frais, conformément aux lois applicables. Le Fournisseur remboursera à GFS les coûts réels encourus par GFS pour répondre à un Incident de sécurité et atténuer les dommages causés par celui-ci, y compris tous les coûts de notification et de remédiation. Sauf si la loi l'exige, le Fournisseur n'informera aucun tiers d'un Incident de sécurité sans l'accord écrit de GFS. En outre, le Fournisseur accepte que GFS ait le droit exclusif de déterminer si l'Incident de sécurité doit être notifié, le contenu de cette notification, ainsi que la nature et l'étendue des mesures correctives.

5.4 ***Contrôle***. Sur demande et sur une base annuelle, le Fournisseur fournira à GFS les résultats de tout audit effectué (par exemple, SOC1, SOC2, ISO27001, etc.) par ou au nom du Fournisseur qui évalue l'efficacité du programme de sécurité de l'information du Fournisseur en ce qui concerne la sécurité et la confidentialité des RP couverts (« **Rapport sur les contrôles** »). Le Fournisseur doit veiller à ce que chaque Sous-traitant ou fournisseur de service mette à la disposition de GFS un Rapport sur les contrôles sur une base annuelle ou à la suite d'un Incident de sécurité.

6. Enquêtes

6.1 ***Notification d'une enquête réglementaire***. Le Fournisseur doit notifier à GFS toute enquête ou correspondance réglementaire concernant les RP couverts (une « Enquête ») dans les trois (3) jours suivant la notification de l'Enquête. Le Fournisseur doit fournir à GFS toutes les copies des documents et de la correspondance relatifs à l'Enquête sans retard injustifié.

6.2 ***Réponse à une Enquête***. Le Fournisseur ne divulguera aucune information confidentielle de GFS ou d'une partie affiliée à l'autorité compétente sans l'accord écrit préalable de GFS. Le Fournisseur prendra toutes les autres mesures nécessaires pour répondre à l'Enquête de manière adéquate et dans les délais impartis.

7. Divers

7.1 ***Divisibilité***. Si une disposition du présent DPA est jugée nulle par un tribunal, cette disposition est réputée dissociable des autres dispositions du présent DPA, et le reste du DPA prend effet, comme si les parties n'avaient pas inclus la disposition retirée.

7.2 ***Saisie ou confiscation***. Si un RP couvert peut être visé par une saisie ou une confiscation, une procédure d'insolvabilité (y compris une vente) ou une procédure de concordat, ou tout autre événement ou mesure pris par un tiers, le Fournisseur doit en informer GFS avec un préavis raisonnable. En outre, le Fournisseur informera ce tiers que la souveraineté et la propriété des RP couverts appartiennent à GFS.

7.3 ***Survie***. Toutes les déclarations, garanties et indemnisations survivent à la résiliation et/ou à l'expiration du présent DPA et restent pleinement en vigueur. Tous les droits et privilèges d'une partie, dans la mesure où ils sont équitablement attribuables à des événements ou conditions survenant ou existant au moment de la résiliation et/ou de l'expiration du présent DPA ou avant, survivent à la résiliation et peuvent être appliqués par cette partie.

7.4. ***Généralités***. Sauf mention expresse dans le présent document, les dispositions des Accords restent inchangées et pleinement applicables. En cas de conflit entre les termes des Accords et les termes de ce DPA, les termes de ce DPA prévaudront, à moins que le(s) Accord(s) ne contienne(nt) une référence croisée spécifique à la section du DPA devant être modifiée. Les en-têtes sont utilisés pour des raisons de commodité et n'affectent pas l'interprétation des termes de ce DPA.

ANNEXE SUR LA SÉCURITÉ

1. ***Politiques et procédures***. Le Fournisseur doit maintenir et assurer la conformité avec ses politiques et procédures écrites de gestion de la sécurité (« **Politiques du Fournisseur** ») afin de prévenir, détecter, contenir et corriger les violations des mesures prises pour protéger la confidentialité, l'intégrité ou la disponibilité des systèmes d'information du Fournisseur qui stockent, traitent, transfèrent ou accèdent aux informations confidentielles de GFS (« **Systèmes du Fournisseur** »). Les Politiques du Fournisseur doivent au minimum : (i) dans la mesure où le Fournisseur a accès à des RP couverts, traiter ces RP couverts à tout moment comme des renseignements très sensibles ; (ii) inclure un programme formel de gestion des risques, comprenant des évaluations périodiques des risques ; et (iii) fournir un cadre adéquat de contrôles qui protègent les Systèmes du Fournisseur, y compris, sans s'y limiter, tout matériel ou logiciel prenant en charge GFS et les informations confidentielles de GFS.

2. ***Évaluations de la sécurité***. Le Fournisseur doit effectuer et documenter chaque année une évaluation de la sécurité technique des Politiques du Fournisseur et des Systèmes du Fournisseur afin de s'assurer qu'il continue à se conformer aux obligations énoncées dans la présente Annexe et à celles imposées par la loi. Ces évaluations doivent garantir que

les informations confidentielles de GFS sont stockées de manière confidentielle et sécurisée dans les Systèmes du Fournisseur et évaluer la maintenance et la structure des Systèmes du Fournisseur.

3. ***Certifications***. Sur demande écrite de GFS, le Fournisseur fournit à GFS les résultats de tout audit réalisé par le Fournisseur ou en son nom, qui évalue l'efficacité du programme de sécurité de l'information du Fournisseur en ce qui concerne la sécurité et la confidentialité des RP couverts partagés au cours de l'exécution du contrat (« **Rapport sur les contrôles** »). Le Fournisseur doit s'assurer que chaque Sous-traitant prépare et met à la disposition de GFS un Rapport sur les contrôles sur une base annuelle ou à la suite d'un Incident de Sécurité.

4. ***Sécurité physique***. Le Fournisseur doit maintenir des contrôles de sécurité physique appropriés (y compris des contrôles des installations et de l'environnement) afin d'empêcher l'accès physique non autorisé aux Systèmes du Fournisseur.

5. ***Limitation de l'accès***. Le Fournisseur met en œuvre des contrôles d'accès appropriés limitant l'accès aux RP couverts aux seuls employés, spécialistes, sous-traitants et fournisseurs de services qui ont besoin de connaître ces informations pour s'acquitter de leurs obligations dans le cadre des Accords.

6. ***Registres d'accès des visiteurs***. Le Fournisseur tiendra des registres d'accès pour les visiteurs et les invités (« **Registre des invités du Fournisseur** ») et veillera à ce que ces visiteurs et invités soient escortés lorsqu'ils se trouvent dans toute installation permettant un accès physique ou virtuel aux Systèmes du Fournisseur et conservera le Registre des invités du Fournisseur dans un endroit sûr pendant au moins trois (3) mois.

7. ***Contrôles du périmètre***. Le Fournisseur maintiendra des contrôles raisonnables du périmètre du réseau, tels que des pares-feux, à toutes les connexions du périmètre aux Systèmes du Fournisseur.

8. ***Gestion de la vulnérabilité et tests***. Le Fournisseur doit utiliser des processus raisonnables de gestion des vulnérabilités afin d'atténuer les risques liés à la sécurité des données, y compris, mais sans s'y limiter, des mesures d'atténuation visant à résoudre les problèmes identifiés par le Fournisseur, GFS ou conformément aux lois applicables. Le Fournisseur autorise GFS et ses tiers agréés à effectuer des tests de vulnérabilité en matière de sécurité dans le but d'identifier les failles de sécurité dans la fonctionnalité web du Fournisseur utilisée par GFS et les clients de GFS, les clients et les Sous-traitants du Fournisseur, sous réserve que GFS fournisse un préavis raisonnable et que le Fournisseur obtienne tous les consentements nécessaires de la part de son fournisseur de

services d'hébergement web.

9. ***Durcissement du système***. Les paramètres de configuration du Fournisseur pour les Systèmes du Fournisseur comprendront des procédures visant à désactiver tous les services inutiles sur les appareils et les serveurs et seront appliqués à tous les Systèmes du Fournisseur qui accèdent aux informations confidentielles de GFS, les transmettent ou les stockent.

10. ***Gestion des correctifs***. Le Fournisseur doit établir et respecter des politiques de correction des systèmes internes qui garantissent que tous les Systèmes du Fournisseur sont maintenus à un niveau de correction stable et actuel.

11. ***Détection de virus***. Le Fournisseur installera un logiciel de détection de codes malveillants commercialement raisonnable, comprenant des détecteurs de virus et de logiciels malveillants, sur tous les systèmes vulnérables aux logiciels malveillants qui sont utilisés pour accéder aux informations confidentielles de GFS, les traiter ou les stocker, et le Fournisseur maintiendra à jour les signatures de virus antimalware.

12. ***Journalisation des accès aux Systèmes***. Le Fournisseur tient des journaux de système qui permettent d'identifier de manière unique les utilisateurs individuels et leur accès aux systèmes associés, et d'identifier les activités tentées ou exécutées par ces utilisateurs. Tous les systèmes créant des journaux d'accès aux systèmes doivent être synchronisés avec une source de temps centrale. Le Fournisseur identifiera, examinera et répondra à toute activité suspecte ou malveillante identifiée dans le journal du système du Fournisseur. Le Fournisseur doit conserver une piste d'audit des journaux de sécurité pour le système du Fournisseur. Le Fournisseur conservera ces journaux pendant toute la durée de l'Accord ou pendant un (1) an, selon la durée la plus longue, ou selon les exigences des lois applicables.

13. ***Vérification des antécédents***. Le Fournisseur doit exiger que tout le personnel ayant accès aux informations confidentielles de GFS via les Systèmes du Fournisseur fasse l'objet d'une vérification de ses antécédents. Le Fournisseur doit en outre veiller à ce que son personnel chargé du traitement des informations confidentielles de GFS soit informé de la nature confidentielle des RP couverts, ait reçu une formation appropriée sur ses responsabilités et ait signé des ententes de confidentialité écrites. Le Fournisseur doit veiller à ce que ces obligations de confidentialité survivent à la fin de l'engagement du personnel.

14. ***Processus de contrôle des modifications***. Le Fournisseur doit maintenir des processus raisonnables de contrôle des modifications pour approuver et suivre les changements

dans l'environnement informatique du Fournisseur.

15. ***Protection des supports de stockage***. Le Fournisseur doit s'assurer que les supports de stockage contenant les informations confidentielles de GFS sont correctement nettoyés de toutes les informations confidentielles de GFS ou sont détruits avant d'être éliminés ou réutilisés pour un traitement ne relevant pas du Fournisseur. Tous les supports sur lesquels les informations confidentielles de GFS sont stockées doivent être protégés contre tout accès ou modification non autorisés. Le Fournisseur doit maintenir des processus et des mécanismes raisonnables et appropriés pour assurer la responsabilité et le suivi de la réception, du retrait et du transfert des supports de stockage utilisés pour les systèmes d'information du Fournisseur ou sur lesquels sont stockées les informations confidentielles de GFS.

16. ***Comptes de système***. Le Fournisseur doit maintenir des Politiques du Fournisseur appropriées en matière de demande, d'approbation, d'audit et d'administration des comptes et des privilèges d'accès aux Systèmes du Fournisseur et aux informations confidentielles de GFS. Le personnel du Fournisseur qui accède aux Systèmes du Fournisseur qui stockent, transmettent ou traitent les informations confidentielles de GFS se verra attribuer des comptes système individuels afin de garantir la responsabilité de l'accès accordé.

17. ***Mots de passe***. Le Fournisseur doit mettre en œuvre des paramètres de mot de passe appropriés pour les systèmes qui accèdent aux informations confidentielles de GFS, les transmettent ou les stockent (« **Systèmes connexes** »). Le Fournisseur doit mettre en œuvre une authentification forte à deux facteurs et des mots de passe complexes (« **Mots de passe** ») pour tous les réseaux et systèmes d'accès aux Systèmes connexes. Le Fournisseur doit respecter les pratiques de l'industrie en matière de Mots de passe. Les Mots de passe par défaut du fabricant utilisés dans les produits du Fournisseur doivent être modifiés lors de l'installation.

18. ***Continuité des activités***. Le Fournisseur doit s'assurer qu'il dispose de processus et de procédures adéquats permettant à une entreprise de maintenir le service en cas de catastrophe (« **Plans de continuité des activités** ») afin de garantir sa conformité avec les conditions du présent DPA et doit revoir et tester les Plans de continuité des activités au moins une fois par an.

19. ***Destruction des données***. Toutes les informations confidentielles de GFS doivent être détruites en toute sécurité une fois qu'elles ne sont plus nécessaires, par le biais de processus commercialement raisonnables. La stratégie du Fournisseur en matière de destruction des données doit être documentée et inclure des registres pour toutes les

informations confidentielles de GFS détruites, qui doivent être disponibles pour examen par GFS.

20. ***Conformité aux normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS)***. En ce qui concerne les Services, dans la mesure où cela est applicable, le Fournisseur maintiendra le niveau requis de conformité et de certification PCI DSS et fournira la documentation correspondante à la demande de GFS. Le Fournisseur est responsable de la sécurité des données des titulaires de cartes qu'il rencontre, utilise et/ou conserve conformément au présent DPA ou afin de fournir les Services. Le Fournisseur est tenu de mettre en œuvre et de maintenir des mesures de sécurité raisonnables. Ces mesures de sécurité doivent être appropriées à la lumière de la sensibilité des informations et doivent protéger les informations contre l'accès, l'utilisation ou la divulgation non autorisés.