Addenda relatif à la protection des données

Le présent Addenda s'applique à la collecte, à l'utilisation, à la divulgation, au stockage, et à tout autre type de traitement (collectivement, le « **Traitement** ») des renseignements personnels transférés à Fundserv par le Client en vue de leur traitement pour le compte du Client (« **Renseignements Personnels du Client** ») afin de fournir des services (« **Services** ») à ce dernier conformément à l'entente, désignée comme le « Fundserv Customer Contract », conclue entre les parties (« Entente »).

Les parties conviennent de ce qui suit :

1. **Respect des Lois sur la Protection des Renseignements Personnels.** Le Client et Fundserv doivent se conformer aux lois, ordonnances et règlements fédéraux et provinciaux canadiens régissant le traitement des renseignements personnels, y compris la *Loi sur la protection des renseignements personnels et les documents électroniques* et les lois provinciales analogues (les « **Lois sur la Protection des Renseignements Personnels** »), et se fournir mutuellement une coopération raisonnable dans la mesure où celle-ci est nécessaire pour permettre à chaque partie de se conformer aux Lois sur la Protection des Renseignements Personnels.
2. **Limitation de la Finalité ; Propriété.** Tout traitement des Renseignements Personnels du Client par Fundserv doit être limité à ce qui est nécessaire pour fournir les Services ou à toute autre fin autorisée par le Client ou requise ou permise en vertu des Lois sur la Protection des Renseignements Personnels applicables. Les Renseignements Personnels du Client seront et demeureront en tout temps la propriété exclusive du Client.
3. **Consentement.** Le Client déclare et garantit que, conformément aux lois applicables, le consentement des personnes concernées a été obtenu, dans la mesure où cela est nécessaire pour que Fundserv puisse traiter les renseignements requis afin de fournir les services envisagés par les parties dans le cadre de la présente Politique et du Contrat de Membre Actuel. Les parties reconnaissent et conviennent que le consentement susmentionné puisse ne pas être requis pour certains traitements lorsqu'ils sont nécessaires ou autorisés en vertu des Lois sur la Protection des Renseignements Personnels.
4. **Conformité.** Le Client doit maintenir des mesures de contrôle pour s'assurer que les Autorités Locales d'Enregistrement et les utilisateurs finaux se conforment à toutes les exigences raisonnablement imposées par Fundserv pour protéger la confidentialité et la sécurité des Renseignements Personnels des Clients et des systèmes de Fundserv, y compris celles énoncées dans la Politique de Confidentialité de Fundserv, le Guide des Autorités Locales d'Enregistrement et toutes les communications de Fundserv. De plus, le Client doit restreindre l'accès aux utilisateurs finaux nécessitant un tel accès pour accomplir leurs tâches et doit immédiatement aviser Fundserv de tout accès non autorisé aux Renseignements Personnels du Client ou aux renseignements concernant d'autres clients de Fundserv.
5. **Sous-traitants.** Le Client autorise Fundserv à nommer des sous-traitants pour le traitement des Renseignements Personnels du Client en son nom. Fundserv doit s'assurer que l'entente entre Fundserv et le sous-traitant est régie par un contrat écrit offrant une protection des Renseignements Personnels du Client équivalente ou supérieure à celle prévue à la présente Politique.
6. **Transferts Transfrontaliers.** Fundserv ne peut traiter, et doit s'assurer que ses sous-traitants ne traitent, les Renseignements Personnels du Client qu'au Canada et aux États-Unis, à moins que Fundserv ne donne un préavis raisonnable au client.

7. **Demandes des Personnes Concernées en vertu des Lois sur la Protection des Renseignements Personnels.** Si Fundserv reçoit une demande d'une personne visant les Renseignements Personnels du Client en vertu des Lois sur la Protection des Renseignements Personnels, Fundserv doit promptement rediriger cette demande au Client, et accepte de coopérer raisonnablement avec le Client pour répondre à cette demande conformément aux Lois sur la Protection des Renseignements Personnels.

8. **Programme de Protection des Renseignements Personnels.** Fundserv doit maintenir un programme exhaustif de protection des renseignements personnels qui contient des mesures de protection administratives, techniques et physiques adaptées aux exigences en matière de protection et de confidentialité de ces renseignements, tel qu'indiqué à l'Annexe A (le « **Programme de Protection des Renseignements Personnels** »). Le Programme de Protection des Renseignements Personnels de Fundserv doit être conçu pour : (a) assurer la confidentialité, l'intégrité et la disponibilité des Renseignements Personnels du Client en la possession ou sous le contrôle de Fundserv ou auxquels Fundserv a accès ; (b) protéger contre toute menace ou tout risque anticipé pour la confidentialité, l'intégrité et la disponibilité des Renseignements Personnels du Client ; (c) protéger contre l'accès, l'utilisation, la divulgation, la modification ou la destruction non autorisé ou illicite des Renseignements Personnels du Client ; (d) protéger contre la perte, la destruction ou l'endommagement accidentel des Renseignements Personnels du Client ; et (e) préserver les Renseignements Personnels du Client conformément aux Lois sur la Protection des Renseignements Personnels.

9. **Incidents de confidentialité**

9.1. **Informer le Client d'un incident de confidentialité.** Fundserv doit sans délai aviser le Client de toute perte, accès non autorisé, utilisation ou divulgation des Renseignements Personnels du Client ou de toute autre violation ou tentative de violation, par toute personne, du Programme de Protection des Renseignements Personnels de Fundserv ou d'autres mesures de protection des renseignements personnels du Client (« **Incident de Confidentialité** »). Fundserv doit rapidement prendre toutes les mesures raisonnablement nécessaires pour atténuer les conséquences négatives de l'incident de confidentialité. Le Client est responsable des exigences applicables en matière de notification et/ou de rapport en vertu des Lois sur la Protection des Renseignements Personnels. Fundserv doit fournir une coopération raisonnable au Client en ce qui concerne les exigences applicables en matière de notification et/ou de rapport en vertu des Lois sur la Protection des Renseignements Personnels.

10. **Examen et vérification de la sécurité**

10.1. À la demande raisonnable du Client et pour répondre à son besoin d'entreprendre une vérification relative aux exigences de confidentialité, Fundserv fournira au Client des copies (i) de ses politiques et procédures en matière de protection des renseignements personnels, de confidentialité et de sécurité qui s'appliquent aux Renseignements Personnels du Client, et (ii) de l'assurance d'une tierce partie de Fundserv traitant, entre autres, de la confidentialité, de la sécurité, et de l'intégrité des renseignements personnels. Le Client doit traiter tous ces renseignements divulgués par Fundserv comme des renseignements confidentiels tels que définis dans la Politique.

11. **Environnement de test d'acceptation utilisateur**

11.1. Fundserv met à la disposition de ses clients un environnement de test d'acceptation utilisateur (TAU) afin de faciliter la formation des nouveaux clients à ses systèmes et de donner aux clients existants l'occasion de tester de nouvelles fonctions avant qu'elles ne soient mises en production. Le client ne peut télécharger dans l'environnement TAU que des données ne contenant pas de renseignements personnels. Toute donnée téléchargée dans l'environnement UAT n'est pas soumise aux protections du présent Addenda.

12. Interprétation et traitement sécurisé

12.1. Dès sa signature par les parties, la présente Politique devient partie intégrante de l'Entente et constitue l'intégralité de l'accord entre les parties à cet égard, et toutes les représentations, déclarations et ententes antérieures s'y rapportant sont remplacées par les termes de l'Entente. Pour plus de clarté, l'exclusion de la responsabilité en vertu de l'Entente est réputée conforme aux dispositions du présent Addenda et exclut toute responsabilité de Fundserv en cas de violation de l'une des dispositions de l'Addenda.

12.2. Fundserv doit restituer en toute sécurité ou disposer de tous les Renseignements Personnels du Client en sa possession ou en la possession de tout tiers à qui il a transféré des Renseignements Personnels du Client dans un délai raisonnable suivant l'expiration ou la résiliation de l'Entente, conformément au calendrier de conservation de Fundserv, à moins que la conservation de ces renseignements personnels transférés ne soit permise ou exigée par les lois applicables.

Annexe A

Exigences minimales du programme de protection des renseignements personnels

Le Programme de Protection des Renseignements Personnels de Fundserv comprend les éléments suivants :

a) **Sensibilisation et Formation à la Sécurité.** Un programme obligatoire de sensibilisation et de formation à la sécurité destiné à tous les membres du personnel de Fundserv (y compris la direction), comprenant : (i) une formation sur la manière de mettre en œuvre et de respecter son Programme de Protection des Renseignements Personnels ; et (ii) la promotion d'une culture de sensibilisation à la sécurité par le biais de communications périodiques de la direction générale avec les employés.

b) **Évaluation et Contrôle des Antécédents.** Politiques et procédures visant à effectuer des évaluations appropriées de tous les membres actuels et potentiels du personnel de Fundserv qui ont accès aux Renseignements Personnels des Clients.

c) **Contrôles d'Accès.** Politiques, procédures et contrôles logiques : (i) pour limiter l'accès à ses systèmes d'information et à l'installation ou aux installations dans lesquelles ils sont hébergés aux personnes dûment autorisées ayant un besoin de savoir ; (ii) pour limiter la quantité de Renseignements Personnels des Clients accessibles aux personnes autorisées dans le cadre de leurs fonctions professionnelles ; (iii) pour limiter l'accès aux membres du personnel et aux autres personnes qui ne devraient pas y avoir accès ; et (iv) pour supprimer l'accès en temps opportun en cas de changement de responsabilités ou de statut professionnel ou à la suite d'un échec de l'évaluation des antécédents. Dans le cadre de son ensemble de contrôles d'accès, Fundserv délègue le rôle d'Autorité locale d'enregistrement (ALE) à une ou plusieurs personnes dans chaque organisation. Chaque ALE a certaines responsabilités, notamment celle de fournir aux utilisateurs finaux l'accès à l'environnement de Fundserv. Pour obtenir de plus amples renseignements sur les rôles et les responsabilités d'une ALE, veuillez consulter le guide ALE de votre gestionnaire d'accès.

d) **Sécurité Physique et Environnementale.** Les mesures de sécurité qui fournissent une assurance raisonnable que l'accès physique aux installations où sont stockées les Renseignements Personnels des Clients, y compris les serveurs physiques, est limité aux personnes dûment autorisées et que des mesures de sécurité environnementale sont mises en place pour détecter, prévenir et contrôler les destructions dues à des conditions environnementales extrêmes. Ces mesures de sécurité comprennent : (i) l'enregistrement et la surveillance des tentatives d'accès non autorisé aux installations de Fundserv par le personnel de sécurité ; (ii) des systèmes de surveillance par caméra aux points d'entrée internes et externes critiques des installations de Fundserv ; (iii) des systèmes de surveillance et de contrôle de la température et de l'humidité de l'air à des niveaux appropriés pour l'équipement informatique ; et (d) des modules d'alimentation sans coupure (UPS) et des générateurs de secours qui fournissent une alimentation de secours en cas de défaillance électrique.

e) **Procédures en cas d'Incident de Confidentialité.** Un plan d'intervention comprenant les procédures à suivre en cas d'incident de confidentialité réel ou présumé. Ces procédures comprennent (i) la formation d'une équipe interne d'intervention en cas d'incident, avec un responsable de l'intervention ; (ii) l'évaluation du risque de préjudice que pose l'incident et la détermination des personnes susceptibles d'être affectées ; (iii) l'établissement de rapports internes ; (iv) l'enregistrement de ce qui a été fait et par qui, afin de faciliter l'analyse ultérieure et une éventuelle action en justice ; et (v) la réalisation et la documentation d'une analyse des causes principales et d'un plan de redressement.

f) **Plan d'Urgence.** Politiques et procédures visant à répondre à une situation d'urgence ou à tout autre événement (par exemple, incendie, vandalisme, panne de système, pandémie et catastrophe naturelle) susceptible d'endommager les Renseignements Personnels des Clients ou les systèmes de production qui contiennent des Renseignements Personnels des Clients. Ces procédures comprennent (i) une politique de sauvegarde périodique des systèmes de fichiers de production et des bases de données contenant les Renseignements Personnels des Clients, selon un calendrier défini ; (ii) un plan formel de reprise après sinistre pour les installations de Fundserv où les Renseignements Personnels des Clients sont stockés ; et (iii) un processus formel pour aborder le cadre par lequel un événement imprévu pourrait être géré pour minimiser la perte de ressources vitales.

g) **Contrôles d'Audit.** Mécanismes matériels, logiciels et/ou procéduraux qui enregistrent et examinent l'activité des systèmes d'information qui contiennent ou utilisent des informations électroniques. Ces mécanismes doivent garantir que les actions sont attribuables à une personne identifiable.

h) **Intégrité des Renseignements Personnels.** Politiques et procédures visant à préserver la confidentialité, l'intégrité et la disponibilité des Renseignements Personnels des Clients et à les protéger contre la divulgation, la modification ou la destruction des Renseignements Personnels des Clients.

i) **Sécurité du Stockage et de la Transmission.** Mesures de sécurité visant à empêcher tout accès non autorisé aux Renseignements Personnels des Clients transmis sur un réseau public de communications électroniques ou stockés électroniquement. Ces mesures comprennent (i) limiter l'utilisation de dispositifs de stockage portables, tels que les lecteurs USB (Universal Serial Bus), pour stocker ou transférer les Renseignements Personnels des Clients dans la mesure où cela est manifestement nécessaire pour répondre à un objectif spécifique ; et (ii) le cryptage pendant la transmission.

j) **Ségrégation.** Mesures garantissant la ségrégation des Renseignements Personnels des Clients avec les renseignements d'autrui.

k) **Responsabilité en matière de Sécurité.** Attribution de la responsabilité de l'élaboration, de la mise en œuvre et de la gestion de son Programme de Protection des Renseignements Personnels, y compris : (i) la désignation d'un responsable de la sécurité ayant une responsabilité globale ; et (ii) la définition des rôles et des responsabilités en matière de sécurité pour les personnes ayant des responsabilités dans ce domaine.

l) **Tests.** Tester périodiquement les contrôles, systèmes, et procédures clés de son Programme de Protection des Renseignements Personnels afin de s'assurer qu'ils sont correctement mis en œuvre et qu'ils permettent de faire face aux menaces et aux risques identifiés. Ces tests sont effectués par des tiers indépendants qualifiés.

m) **Journalisation et Surveillance.** Surveillance du réseau et des systèmes, y compris les journaux d'erreurs sur les serveurs, les disques et les événements de sécurité, afin de détecter tout problème potentiel. Cette surveillance comprend (i) l'examen des modifications matérielles affectant les systèmes d'authentification, d'autorisation et d'audit ; (ii) l'examen de l'accès privilégié aux systèmes de production de Fundserv ; et (iii) l'engagement de tiers pour effectuer des évaluations de la vulnérabilité du réseau et des tests de piratage sur une base régulière.

n) **Gestion des Changements et de la Configuration.** Maintien de politiques et de procédures pour la gestion des modifications apportées par Fundserv aux systèmes de production, aux applications et aux bases de données. Ces politiques et procédures doivent comprendre (i) un processus de documentation, de test et d'approbation des correctifs et de la maintenance du service ; (ii) un processus de correctifs de

sécurité qui exige que les systèmes soient corrigés en temps utile sur la base d'une analyse des risques ; et (iii) un processus permettant à Fundserv d'utiliser une tierce partie pour effectuer des évaluations de la sécurité au niveau des applications web.

o) **Ajustements du Programme.** Fundserv surveillera, évaluera et pourra ajuster, le cas échéant, le Programme de Protection des Renseignements Personnels à la lumière de : (i) tout changement technologique pertinent et de toute menace interne ou externe à l'égard de Fundserv ou des Renseignements Personnels du Client ; (ii) de la réglementation en matière de protection de la sécurité et de la confidentialité des renseignements applicable au Client et/ou à Fundserv ; et (iii) de l'évolution des arrangements commerciaux de Fundserv, tels que les fusions et les acquisitions, les alliances et les coentreprises, les arrangements d'impartition et les changements apportés aux systèmes d'information.

p) **Appareils.** Tous les ordinateurs portables et de bureau utilisés par Fundserv et ses sous-traitants pour accéder aux Renseignements Personnels des Clients doivent : (i) être équipés d'un système de cryptage : (i) être munis d'un dispositif de chiffrement ; et (ii) utiliser des mesures de sécurité raisonnables pour protéger ces appareils conformément aux normes de l'industrie.