LOUISIANA-PACIFIC CORPORATION
ADDENDUM SUR LA SÉCURITÉ DES DONNÉES
(CANADA)

Cette traduction est fournie à titre gracieux. Seule la version originale anglaise du document fait autorité. En cas d'ambiguïté ou de conflit, la version anglaise du document prévaudra/

TABLE DES MATIÈRES

1. **Définitions.** Tous les termes en majuscules non définis dans les présentes ont la signification qui leur est donnée dans le Contrat.

1.1. « Autorité gouvernementale » désigne chaque gouvernement, autorité et agence fédérale, étatique, provinciale et municipale, ainsi que ses agences, départements, autorités et commissions respectifs.

1.2. « Collecter » désigne le fait de réaliser une copie légale des données et de stocker ces données dans un emplacement sécurisé.

1.3. « Contrat » désigne le contrat applicable entre le Prestataire de Services et la Société en vertu duquel le Prestataire de Services fournit ses Services.

1.4. « Données de la Société » désigne toutes les données personnelles, données, informations, représentations visuelles ou graphiques et autres éléments similaires sur tout support ou format électronique, tangible ou autre, qui sont fournis ou accessibles au Prestataire de Services ou à l'une de ses Sociétés affiliées ou à l'un de ses Sous-traitants par ou à la demande de la Société, ou que le Prestataire de Services ou ses Sociétés affiliées ou l'un de ses Sous-traitants créent, collectent, traitent, stockent, génèrent ou transmettent dans le cadre de la fourniture des Services ou de l'exécution des obligations du Prestataire de Services en vertu du Contrat. Les Données de la Société sont considérées et traitées comme des Informations confidentielles de la Société.

1.5. « Données personnelles de la Société » désignent les données et/ou informations que le Prestataire de Services ou l'un de ses Société affiliée ou l'un de ses Sous-traitants peut obtenir ou auxquelles il peut avoir accès, traiter ou transmettre dans le cadre du Contrat ou de tout cahier des charges, qui consistent en des informations ou des données nommant ou identifiant un individu, y compris, mais sans s'y limiter : (a) les informations qui sont explicitement définies comme une catégorie réglementée de données en vertu de toute Loi sur la protection des données applicable à la Société ; (b) les informations personnelles non publiques, y compris, sans s'y limiter, une adresse électronique professionnelle ou personnelle, un numéro d'identification d'employé, une adresse, un numéro d'identification militaire ou d'autres dossiers militaires, des numéros de téléphone, un numéro d'immatriculation de véhicule, une adresse IP, un numéro d'identification national, un numéro de passeport, un numéro TSA, un numéro de sécurité sociale ou d'assurance sociale (en tout ou en partie), ou un numéro de permis de conduire ; (c) les informations médicales ou relatives à la santé, telles que les informations d'assurance, les pronostics médicaux, les informations de diagnostic ou les informations génétiques ; (d) les informations financières, telles que le numéro de police, les Informations de paiement, les antécédents de crédit, le numéro de compte financier ou tout code ou mot de passe permettant d'accéder à un compte financier ; (e) les données personnelles sensibles, telles que le nom, la date de naissance, le nom de jeune fille de la mère, la race, l'état civil, le sexe ou la sexualité, les informations relatives à la vérification des antécédents, les données judiciaires telles que le casier judiciaire, ou les adresses IP liées à l'utilisation de sites web ou attribuées à un individu; (f) les données biométriques ; et/ou (g) les données génétiques. Les Données personnelles de la Société doivent être considérées et traitées comme des Informations confidentielles.

1.6. « Exigences PA DSS » désigne la norme de sécurité des données des applications de paiement maintenue par le PCI qui s'applique aux Personnes qui traitent les transactions par carte de paiement avec les principaux réseaux de cartes de paiement participants.

1.7. « Exigences PCI DSS » désigne la norme de sécurité des données de l'industrie des cartes de paiement maintenue par le PCI qui s'applique aux Personnes qui traitent des transactions par carte de paiement avec les principaux réseaux de cartes de paiement participants.

1.8. « Incident lié à la sécurité des données » désigne : (a) la tentative ou l'acquisition, l'accès, l'utilisation, le Traitement, la perte ou la divulgation non autorisés d'Informations confidentielles ; (b) le doute ou la conviction raisonnable qu'il y a eu une tentative ou une acquisition, un accès, une

utilisation, un Traitement, une perte ou une divulgation non autorisés d'Informations confidentielles ; ou (c) l'utilisation non autorisée ou la tentative d'utilisation de tout Systèmes du Prestataire de Services pour accéder à tout Système de la Société.

1.9. « Informations de paiement » désigne les informations relatives à la carte de paiement (carte de crédit, de débit ou cadeau) collectées auprès d'une personne, y compris le nom et l'adresse de facturation du titulaire de la carte, le numéro et la date d'expiration de la carte de paiement, le code PIN ou le bloc PIN, les données de la bande magnétique, les informations relatives à une transaction par carte de paiement identifiable avec un compte spécifique et le code de vérification externe (par exemple, CVV2) de la carte de paiement.

1.10. « Logiciel antivirus » désigne un logiciel respectant les normes de l'industrie et spécialement conçu pour empêcher l'introduction ou l'intrusion de Logiciels malveillants grâce à un ensemble de Signatures antivirus.

1.11. « Logiciel malveillant » désigne tout type de logiciel ou de programme conçu pour : (a) entraîner un accès non autorisé ou une intrusion ; ou (b) perturber et/ou endommager de toute autre manière le matériel informatique, les logiciels et/ou les données, y compris, mais sans s'y limiter, les virus, vers, chevaux de Troie, logiciels espions, rançongiciels ou autres logiciels destinés à provoquer des pannes de système, des inondations de paquets réseau, l'utilisation non autorisée de privilèges système, l'accès non autorisé à des données sensibles ou l'exécution de codes malveillants qui détruisent des données.

1.12. « Lois sur la protection des données » désignent les lois relatives à la protection des données, aux flux transfrontaliers de données ou à la protection des données, y compris, mais sans s'y limiter : La California Consumer Privacy Act et la California Privacy Rights Act ; la Colorado Privacy Act ; la Connecticut Data Privacy Act ; la Utah Consumer Privacy Act ; la Virginia Consumer Data Protection Act ; la loi fédérale Gramm-Leach-Bliley ; le Règlement général sur la protection des données de l'Union européenne, connu sous le nom de RGPD (y compris les règles ou lois spécifiques à chaque État membre de l'Union européenne émises en vertu du RGPD) ; la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) du Canada ; toutes les règles, règlements et mesures d'application contraignantes émises par la Federal Trade Commission des États-Unis ; toutes les modifications, lois subséquentes ou complémentaires relatives à l'une des lois susmentionnées ; et toutes les lois ou réglementations supplémentaires qui pourraient être promulguées à l'avenir dans toute juridiction applicable.

1.13. « PCI » désigne le Payment Card Industry Security Standards Council (Conseil des normes de sécurité de l'industrie des cartes de paiement) et ses successeurs.

1.14. « Personne » désigne toute personne physique, société, partenariat, société à responsabilité limitée, fiducie, association, entreprise, entité ou Autorité gouvernementale.

1.15. « Poste(s) de travail » désigne tous les ordinateurs portables, ordinateurs de bureau, tablettes, appareils mobiles et tout autre ordinateur (client léger, physique ou virtuel) utilisés par le Prestataire de Services pour fournir les Services ou traiter les Informations confidentielles de la Société.

1.16. « Prestataire de Services » désigne l'entité engagée par la Société pour fournir des Services dans le cadre d'un ou plusieurs contrats.

1.17. « Signatures antivirus » désigne un catalogue de données qui décrit les menaces actuelles liées aux logiciels malveillants (par exemple, virus, vers, logiciels espions) et la manière dont le Logiciel antivirus doit détecter et supprimer la menace d'un système, d'un message ou d'un fichier donné.

1.18. « Société » désigne Louisiana-Pacific Corporation, ainsi que ses filiales et Sociétés affiliées.

1.19. « Sous-traitant » désigne tout sous-traitant du Prestataire de Services fournissant des Services conformément au Contrat.

1.20. « Supports physiques » désigne les supports de stockage électroniques et les supports tangibles utilisés pour stocker les Données de la Société, y compris, mais sans s'y limiter, les disques durs externes, les clés USB sous toutes leurs formes, les bandes (bobines, cassettes), les cartouches, les disques, les tambours, les CD, les DVD, le papier, les microfilms et les microfiches.

1.21. « Systèmes de la Société » désignent les réseaux, équipements, matériels, logiciels et systèmes de communication, ainsi que leurs composants et éléments, détenus, utilisés ou exploités par la Société.

1.22. « Systèmes du Prestataire de Services » désigne les équipements, logiciels et systèmes de communication et composants utilisés, fournis et/ou développés par le Prestataire de Services ou l'un de ses Sociétés affiliées ou Sous-traitants pour la fourniture des Services, y compris, sans limitation, les passerelles de paiement par carte ou les processeurs de carte.

1.23. « Traitement » ou « traiter » désigne toute opération ou ensemble d'opérations effectuées ou à effectuer en rapport avec les Données personnelles de la Société, que ce soit par des moyens automatiques ou non, telles que la création, la saisie, la collecte, l'obtention, l'accès, l'enregistrement, l'organisation, le stockage, l'adaptation, la modification, la récupération, la consultation, l'utilisation, la transmission, le transfert, la divulgation ou la destruction des Données personnelles de la Société.

1.24. « Utilisateur(s) final(aux) » désigne toute personne physique autorisée par la Société à utiliser les Services, ce qui peut inclure, sans s'y limiter, les employés, agents, sous-traitants, consultants, prestataires externes, fournisseurs ou autres personnes physiques (y compris des tiers).

2. **Application et avancées technologiques**. Les Parties comprennent et conviennent que les technologies et les pratiques évoluent au fil du temps et que les mesures et contrôles administratifs, physiques, techniques et organisationnels énoncés dans le présent Addendum sur la sécurité des données peuvent faire l'objet d'améliorations et de développements. À cet égard, le Prestataire de Services, ses Sociétés affiliées et son Personnel peuvent, dans certains cas et avec l'accord écrit préalable de la Société, mettre en œuvre des mesures alternatives mais équivalentes (ou fonctionnellement supérieures) à celles énoncées dans le présent Addendum sur la sécurité des données, à condition toutefois que la mise en œuvre de ces alternatives n'entraîne aucune dégradation ou réduction de l'efficacité des mesures et contrôles associés ; et à condition également que l'approbation de la Société à cet égard ne soit pas considérée comme une renonciation à l'une quelconque des obligations du Prestataire de Services en vertu du présent Addendum sur la sécurité des données. Le Prestataire de Services sera responsable et indemnisera la Société pour tout manquement des Sociétés affiliées du Prestataire de Services et du Personnel du Prestataire de Services à se conformer aux conditions générales du présent Addendum sur la sécurité des données dans la même mesure que si ce manquement était imputable au Prestataire de Services lui-même. La Société peut demander, et le Prestataire de Services ne peut refuser sans motif valable, un engagement écrit visant à protéger la confidentialité et la sécurité des Systèmes de la Société en cas d'accès physique ou en ligne aux locaux et/ou aux Systèmes de la Société.

3. **Obligations de sécurité du Prestataire de Services**. Le Prestataire de Services élaborera, maintiendra et mettra en œuvre un programme complet de sécurité de l'information écrit conforme aux Lois sur la protection des données, y compris une formation obligatoire pour le Personnel du Prestataire de Services qui a accès aux Informations confidentielles de la Société concernant les exigences en matière de confidentialité, de secret et de sécurité de l'information énoncées dans le Contrat et dans le présent Addendum sur la sécurité des données. Le programme de sécurité de l'information du Prestataire de Services et les programmes de sécurité de l'information de ses Sociétés affiliées et de tous ses Sous-traitants comprendront des mesures de protection administratives, techniques, physiques, organisationnelles et opérationnelles appropriées, ainsi que d'autres mesures de sécurité conçues pour : (a) garantir la sécurité et la confidentialité des Informations confidentielles de la Société ; (b) protéger contre toute menace ou tout danger anticipé pour la sécurité et l'intégrité des Informations confidentielles de la Société et (c) protéger contre tout Incident lié à la sécurité des données.

4. **Normes de sécurité**. Le Prestataire de Services s'engage, et, le cas échéant, fera en sorte que ses Sociétés affiliées et Sous-traitants, maintiennent en tout temps (ou toute certification ou tout rapport subséquent applicable accepté par la Société):

   a. une certification ISO/IEC ISO 27001 (« Certification ISO ») ; ou
   b. un rapport annuel Service Organization Control (« SOC ») 2 Type II (« SOC 2 ») ; ou
   c. si disponible, un rapport SOC 3 (« SOC 3 ») (les rapports SOC 1, SOC 2 et SOC 3 sont collectivement nommés les « Rapports SOC ») ; ou
   d. une certification NIST SP 800-53 Revision 5 (« Certification NIST »).

   Les rapports SOC 2 doivent être préparés conformément à la norme SSAE19 ou à une norme supérieure. Les rapports SOC 2 et SOC 3 doivent couvrir intégralement les contrôles liés à la sécurité, à la disponibilité, à l'intégrité, à la confidentialité et à la vie privée des systèmes d'information (y compris les procédures, les personnes, les logiciels, les données et l'infrastructure) utilisés par le Prestataire de Services et ses Sociétés affiliées et Sous-traitants dans le traitement des Données de la Société. Le Prestataire de Services et ses Sociétés affiliées et Sous-traitants fourniront sans délai une copie du rapport de Certification NSIT, SOC ou ISO à la Société dès la signature du Contrat et au plus tard trente (30) jours après réception par l'auditeur indépendant pour chaque période annuelle au cours de laquelle le Prestataire de Services, ses Sociétés affiliées ou ses Sous-traitants reçoivent ce rapport. Le Prestataire de Services informera rapidement la Société de toute lacune identifiée dans les rapports. Le Prestataire de Services traitera et résoudra rapidement toute lacune dans la mesure nécessaire pour se conformer à ses obligations en vertu du Contrat et de l'Annexe 1 (Sécurité) et informera la Société lorsque cette lacune aura été résolue. Si une lacune n'est pas résolue rapidement, elle sera considérée comme une violation substantielle du Contrat par le Prestataire de Services.

5. **Tests d'intrusion**. Lorsque des informations confidentielles, des services d'infrastructure ou des développements d'applications sont fournis à la Société, le Prestataire de Services engagera, à ses propres frais, un tiers indépendant pour effectuer chaque année des tests d'intrusion, y compris des tests manuels (c'est-à-dire pas seulement des analyses automatisées de vulnérabilité), afin d'évaluer les contrôles de sécurité des systèmes, des logiciels, des applications, des hôtes et des couches réseau du Prestataire de Services utilisés pour fournir les Services, conformément aux méthodologies standard du secteur (par exemple, OWASP et OSSTMM). À ses propres frais, le Prestataire de Services documentera et fera en sorte que ses Sociétés affiliées et Sous-traitants documentent la manière dont ils protégeront toutes les Informations confidentielles de la Société découvertes lors des tests. Le Prestataire de Services fournira à la Société des copies de son rapport dès qu'elles seront disponibles et au plus tard trente (30) jours après réception pour chaque période annuelle. Le Prestataire de Services utilisera, et fera en sorte que ses Sociétés affiliées et Sous-traitants utilisent, un document intitulé « Règles d'engagement » (RE) afin de clarifier les attentes en matière d'horaires des tests d'intrusion, de procédures d'escalade, de portée, de méthode de communication et de tout autre élément raisonnablement lié, et le soumettra à la Société pour approbation avant de procéder aux tests d'intrusion. Le Prestataire de Services informera rapidement la Société de toute lacune identifiée ainsi que des mesures correctives nécessaires pour corriger toutes les vulnérabilités. Si une faiblesse critique est identifiée, le Prestataire de Services, ainsi que ses Sociétés affiliées et Sous-traitants (le cas échéant), prendront des mesures correctives dans les sept (7) jours calendaires suivant la réception du rapport. Si une faiblesse importante est identifiée, des mesures correctives seront prises par le Prestataire de Services, ses Sociétés affiliées ou Sous-traitants (le cas échéant) dans les trente (30) jours calendaires suivant la réception du rapport. À ses propres frais, le Prestataire de Services, ainsi que ses Sociétés affiliées et Sous-traitants, retesteront toute faiblesse élevée et fourniront à la Société des preuves tangibles que ces faiblesses ont été corrigées à la satisfaction raisonnable de la Société. La Société ne sera pas responsable des défaillances, impacts négatifs, dégradations du système, défaillances de produits ou défaillances du système liés aux Systèmes du Prestataire de Services en raison de la conformité à la présente section 5 .

6. **Identifiants et authentification des Utilisateurs finaux**. Le Prestataire de Services veillera à ce que chaque Utilisateur final se voie attribuer un identifiant et un mot de passe, un jeton ou un identifiant biométrique (« Identifiants ») uniques, ainsi qu'un facteur secondaire d'authentification (authentification multifactorielle), et fera en sorte que ses Sociétés affiliées et Sous-traitants veillent également à ce qu'il en soit ainsi. Cela permettra aux Utilisateurs finaux d'accéder aux Services uniquement après s'être authentifiés à l'aide d'Identifiants multifactoriels valides. Les Identifiants seront stockés au repos à l'aide d'un algorithme de hachage à sens unique (SHA-256 ou équivalent) et seront cryptés chaque fois qu'ils seront transmis sur Internet, conformément aux exigences en matière de chiffrement des données énoncées à la section 20. Une fois l'authentification effectuée, les Services permettront de suivre l'activité de chaque Utilisateur final grâce à l'utilisation d'un Identifiant de session unique associé aux Identifiants et à chaque session de connexion.

7. **Mots de passe ou authentification sans mot de passe**. Tous les mots de passe, qu'ils soient créés manuellement par l'Utilisateur final ou générés automatiquement, doivent respecter des exigences minimales de complexité, notamment, sans s'y limiter, l'exigence que tous les mots de passe comportent au moins douze (12) caractères alphanumériques et comprennent des lettres, des caractères spéciaux et des chiffres. Tous les systèmes et postes de travail du Prestataire de Services : (a) comprendront des contrôles de l'historique des mots de passe afin d'interdire l'utilisation des trois (3) derniers mots de passe utilisés ; (b) exigeront une question de vérification avant de réinitialiser le mot de passe ; (c) n'enregistreront en aucun cas les mots de passe ; (d) vont chiffrer les mots de passe lors de leur stockage et de leur transmission ; et (e) disposeront de contrôles pour forcer l'expiration d'un mot de passe après une période définie, mais au moins dans les 90 jours (tout ce qui précède étant appelé « Exigences de sécurité des mots de passe »). En aucun cas, le Personnel du Prestataire de Services ne sélectionnera et n'attribuera manuellement un mot de passe à un Utilisateur final des Services. Tout mot de passe généré automatiquement pour les Services sera : (i) généré automatiquement de manière à produire une valeur aléatoire ; (ii) envoyé automatiquement par e-mail à l'Utilisateur final qui en a fait la demande ; et (iii) valable pour une seule connexion réussie, l'Utilisateur final destinataire devant sélectionner manuellement un mot de passe de substitution lors de la connexion avec le mot de passe généré automatiquement. L'authentification sans mot de passe est acceptable, à condition que deux facteurs d'authentification soient appliqués (certificats, SMS, fourniture d'un code PIN à 6 chiffres par l'application, etc.).

8. **Gestion des identités et des accès**. Les Services doivent pouvoir utiliser des normes de gestion des identités et des accès telles que : (a) SCIM et/ou permettre l'intégration d'API pour la création, la modification et la suppression de comptes d'Utilisateurs finaux et d'autorisations d'accès, ainsi que

l'échange de données d'identité ; et (b) des normes de gestion des identités et des accès telles que SAML, OAuth, OpenID Connect afin de prendre des décisions d'authentification et d'autorisation.

9. **Sécurité des applications**. Les Services et les Systèmes du Prestataire de Services fourniront, le cas échéant, des contrôles de sécurité configurables, comprenant au minimum : (a) la possibilité de révoquer l'accès aux Services après un nombre défini de tentatives de connexion consécutives infructueuses (« Verrouillage ») ; (b) la possibilité de spécifier la durée du Verrouillage ; (c) la possibilité de spécifier le nombre de demandes de connexion invalides avant de déclencher le Verrouillage ; (d) la conformité aux Exigences de sécurité des mots de passe ; (e) des contrôles permettant de mettre fin à une session d'Utilisateur final après une période d'inactivité définie ; (f) la possibilité d'accepter les connexions aux Services à partir de certaines plages d'adresses IP uniquement ; (g) la possibilité de limiter les connexions aux Services à des périodes spécifiques ; (h) la possibilité de déléguer l'authentification des Utilisateurs finaux ou de fédérer l'authentification via SAML ; et (i) la mise à jour, via l'automatisation ou un processus contrôlé de manière centralisée, des correctifs et des *service packs* des applications et des systèmes d'exploitation.

10. **Accès aux Systèmes de la Société**. Le Prestataire de Services reconnaît que la Société se réserve le droit de résilier l'accès du Prestataire de Services à tout ou partie des Systèmes de la Société à tout moment, à sa seule discrétion et sans aucune responsabilité. Si le Prestataire de Services bénéficie d'un accès à distance aux Systèmes de la Société, il doit se conformer à toutes les exigences de sécurité applicables énoncées dans les présentes. En outre, le Prestataire de Services, ses Sociétés affiliées, ses employés, ses Sous-traitants et ses agents doivent s'assurer que tous les accès à distance entrants et sortants vers et depuis les Systèmes de la Société et tout système qui Traite, transmet ou stocke les Données personnelles de la Société utilisent une méthode de chiffrement de bout en bout conformément aux exigences en matière de chiffrement des données énoncées à la section 20.

11. **Sécurité des systèmes et des postes de travail du Prestataire de Services**. Toutes les installations contenant les Systèmes du Prestataire de Services doivent, au minimum : (a) être conçues structurellement pour résister aux intempéries et autres conditions naturelles raisonnablement prévisibles ; (b) mettre en œuvre des mesures de protection physiques appropriées pour protéger les systèmes contre les dommages liés à la fumée, à la chaleur, au froid, à l'eau, au feu, à l'humidité ou aux fluctuations de l'alimentation électrique ; (c) être alimentées par des onduleurs et des systèmes de secours sur site ; (d) mettre en œuvre des contrôles appropriés pour garantir que seul le personnel autorisé est autorisé à accéder physiquement à l'installation ; (e) utiliser des processus conformes aux normes de l'industrie pour éliminer les composants physiques contenant des Informations confidentielles de la Société ; et (f) utiliser, au minimum, le protocole WPA2 pour toute la sécurité du réseau sans fil. Le Système du Prestataire de Services maintiendra des pare-feu à toutes les zones démilitarisées logiques et à tous les points de connexion Internet et comprendra des mesures de protection conçues pour empêcher tout pontage éventuel entre les Systèmes de la Société et des réseaux n'appartenant pas à la Société, y compris la prévention de la connectivité logique entre les Systèmes du Prestataire de Services et les réseaux n'appartenant pas à la Société (par exemple, Internet) lorsqu'ils sont simultanément connectés aux Systèmes de la Société (par exemple, les VPN à fractionnement de tunnel). Toutes les stations de travail utilisées par le Prestataire de Services pour accéder aux Informations confidentielles de la Société : (i) seront documentées et suivies dans un système officiel de gestion des actifs ; (ii) utiliseront des disques durs chiffrés ; (iii) disposeront d'un pare-feu logiciel installé et fonctionnel ; (iv) garantiront que les systèmes d'exploitation sont pris en charge par le Prestataire de Services et que les applications et les systèmes d'exploitation disposent de tous les correctifs critiques installés dans un délai d'une (1) semaine ; (v) n'accepteront que les mots de passe conformes aux exigences de sécurité des mots de passe ; et (vi) disposeront d'un économiseur d'écran ou d'une autre méthode de verrouillage qui s'active après quinze (15) minutes d'inactivité au maximum.

12. **Supports physiques**.

    12.1 Généralités. Le Prestataire de Services mettra tout en œuvre pour ne transférer les Données de la Société que par voie électronique, en utilisant des méthodes conformes au présent Addendum sur la sécurité des données. Si le Prestataire de Services détermine que les Données de la Société ne peuvent pas être envoyées de manière sécurisée par voie électronique, il en informera la Société et obtiendra son consentement pour transporter les Données de la Société à l'aide de Supports physique. Tout transport de Supports physique contenant des Données de la Société doit être conforme à la présente section 12.

    12.2. Inventaire et chaîne de contrôle. Le Prestataire de Services désignera un interlocuteur unique chargé de créer et de tenir à jour un inventaire des Supports physique et de vérifier périodiquement l'exactitude de cet inventaire. L'inventaire doit inclure, au minimum, un numéro de suivi ou tout autre numéro d'identification associé à chaque expédition de Supports physique et indiquer si les Supports physique reçus ont été stockés, renvoyés, détruits ou effacés. Le Prestataire de Services mettra à jour l'inventaire lors de la réception, du transport ou de l'élimination des Supports physique. Tous les Supports physique contenant des Données de la Société doivent être stockés dans une pièce ou une armoire verrouillée dont l'accès est limité au personnel qui a besoin d'accéder à ces zones pour exercer ses fonctions. Le Prestataire de Services doit tenir une chaîne de contrôle entièrement documentée, en suivant toutes les manipulations et tous les retraits de Supports physique, qui comprend au minimum l'état des Supports physique au moment de l'accès ou de l'enlèvement, l'identification de l'individu qui les a manipulés, le but, la date, l'heure, la destination prévue et la date de retour prévue, le cas échéant.

    12.3. Emballage et transport. Si la Société consent au transport des Données de la Société à l'aide de Supports physiques, tous les Supports physiques doivent être chiffrés conformément aux meilleures pratiques de l'industrie qui intègrent, au minimum, les pratiques de chiffrage des données énoncées à la section 20 avant le transport. Avant de transporter les Supports physique, le Prestataire de Services contactera la Personne responsable de la réception au sein de la Société afin de confirmer la date et l'heure du transport et, après la livraison, obtiendra une confirmation écrite de la réception des Supports physique par le destinataire. L'extérieur de tout conteneur contenant des Supports physique doit être adressé à un destinataire spécifique, avec son nom et son adresse professionnelle. Aucune autre marque ou information d'identification ne doit être apposée sur le conteneur. Au minimum, les conditions suivantes seront requises pour le transport des Supports physique : (a) ne seront pas transportés via un centre de distribution majeur et ne feront pas l'objet d'une manutention de masse ou d'un tri automatisé ; (b) feront l'objet d'une surveillance point à point (par exemple, signatures indiquant tout changement de garde - expéditeur, transporteur ou destinataire, lecture de codes-barres, numéros de contrôle de livraison, enregistrement) ; (c) feront l'objet d'un suivi GPS ; et (d) feront l'objet de manifestes d'expédition comprenant les signatures de l'expéditeur, du destinataire et du chauffeur, ainsi que l'heure de livraison et de retrait. En aucun cas, le Prestataire de Services n'autorisera que les Supports physique soient laissés sans surveillance ou dans un véhicule non sécurisé.

13. **Fiabilité du système de production.** Le Prestataire de services s'assurera, et fera en sorte que, le cas échéant, ses Sociétés affiliées et ses Sous-traitants s'assurent, que tous les composants réseau, accélérateurs SSL, équilibreurs de charge, serveurs web, serveurs d'application, serveurs de bases de données et dispositifs de stockage utilisés pour fournir les Services soient configurés selon une méthodologie de conception redondante reconnue dans le secteur, comprenant, au minimum : (a) la mise en grappe de serveurs et l'équilibrage de charge des serveurs web et de bases de données ; (b) la mise en miroir, la réplication ou toute autre technologie équivalente des systèmes de fichiers et des bases de données ; et (c) le stockage sur disque de niveau opérateur utilisant des disques RAID et plusieurs chemins d'accès aux données.

14. **Procédures de sauvegarde et de récupération des données.** Le Prestataire de Services : (a) veillera à ce que les Informations confidentielles de la Société soient sauvegardées, chiffrées et stockées dans un emplacement et un format permettant leur récupération en cas de besoin jusqu'à la dernière transaction engagée ; (b) stockera des copies des Informations confidentielles de la Société et des procédures de récupération des données dans un endroit différent de celui où se trouve l'équipement informatique principal traitant les Informations confidentielles de la Société ; (c) mettre en place des procédures spécifiques régissant la création et l'accès aux copies des Informations confidentielles de la Société ; (d) révisera les procédures de récupération des données au moins tous les six (6) mois ; et (e) tiendra un registre de tous les efforts de restauration, de la description des données restaurées, de la Personne responsable de la restauration et des données (le cas échéant) qui ont nécessité une saisie manuelle pendant le processus de récupération des données.

15. **Reprise après sinistre et continuité des activités.** Le Prestataire de Services dispose actuellement et maintiendra à tout moment un plan approprié de reprise après sinistre, de continuité des activités et d'urgence, ainsi que les politiques et procédures connexes (collectivement, le « Plan de reprise après sinistre ») convenus par écrit entre le Prestataire de Services et la Société, et fournira un résumé de son Plan de reprise après sinistre à la Société par écrit lors de la signature du présent Addendum sur la sécurité des données. Le Plan de reprise après sinistre permettra d'assurer la continuité des opérations en cas de sinistre affectant les activités commerciales du Prestataire de Services et sera conforme aux normes, procédures et pratiques internationalement reconnues en matière de continuité des activités, de planification d'urgence et de reprise après sinistre, y compris, mais sans s'y limiter, les exigences minimales suivantes : (a) une installation de reprise après sinistre géographiquement éloignée de son centre de données principal, ainsi que tout le matériel, les logiciels et la connectivité Internet nécessaires pour fournir les Services sans réduction ou dégradation substantielle de leur fonctionnalité ou de leur disponibilité, dans le cas où le centre de données principal serait rendu indisponible ; (b) des copies de sauvegarde sécurisées des Informations confidentielles de la Société qui ne sont pas stockées sur un Système de la Société ; (c) la restauration des Services dans les douze (12) heures suivant la déclaration d'un sinistre par le Prestataire de Services ; et (d) une perte de données maximale de quatre (4) heures. Le Prestataire de Services informera la Société dès que possible après avoir considéré une interruption de service comme un sinistre et traitera toute interruption de ce type conformément aux conditions de son Plan de reprise après sinistre. Le Prestataire de Services testera toutes les fonctionnalités de son Plan de reprise après sinistre au moins une fois par année civile et fournira les résultats de ces tests à la Société sur demande.

16. **Journalisation.** Les systèmes et postes de travail du Prestataire de Services utilisés pour l'exécution des Services devront, le cas échéant, fournir les fonctionnalités et capacités de journalisation minimales suivantes : (a) pare-feu, routeurs, commutateurs réseau, serveurs, postes de travail et systèmes d'exploitation activés, actifs et configurés avec des capacités de journalisation permettant d'enregistrer les événements avec un niveau de détail suffisant, vers la destination de journalisation par défaut correspondante ou vers un serveur *syslog* centralisé (pour les systèmes réseau), à des fins de diagnostic et d'analyse en cas d'Incident lié à la sécurité des données; (b) des entrées de journal d'accès enregistrées contenant, au minimum, la date, l'heure, l'Identifiant de l'utilisateur, l'URL demandée ou l'identifiant de l'entité manipulée, l'opération effectuée (consultation, modification, etc.) et la source de l'adresse IP ; et (c) la capacité de suivre certaines modifications administratives apportées aux systèmes et postes de travail du Prestataire utilisés pour l'exécution des Services (telles que les modifications de mot de passe et l'ajout de champs personnalisés) dans un « journal d'audit de configuration » (l'ensemble des éléments ci-dessus désigné collectivement par « les journaux »). Tous les journaux doivent être mis à disposition de la Société pour consultation, téléchargement et stockage local, et conservés pendant une durée minimale de deux (2) ans dans un emplacement sécurisé physiquement et logiquement. Le Prestataire, ainsi que ses Sociétés affiliées et le Personnel du Prestataire, fourniront sur demande à la Société des copies de tous les journaux.

17. **Détection et prévention des intrusions.** Le Prestataire de Services surveillera les Services et les Systèmes du Prestataire de Services afin de détecter tout accès non autorisé, interception ou interruption à l'aide de mécanismes de détection et de prévention des intrusions basés sur le réseau et conformes aux normes industrielles en vigueur.

18. **Logiciels malveillants ; protection contre les virus.** Le Prestataire de Services et, le cas échéant, ses Sociétés affiliées et Sous-traitants installeront et maintiendront sur tous les Postes de travail et Systèmes du Prestataire de Services un Logiciel antivirus (y compris des fonctionnalités de protection contre les logiciels malveillants et de protection des terminaux) qui utilise des fonctionnalités de protection en temps réel maintenues conformément aux pratiques recommandées par le Prestataire de Services du Logiciel antivirus. En outre, le Prestataire de Services veillera et, le cas échéant, fera en sorte que ses Sociétés affiliées et Sous-traitants veillent à ce que : (a) le Logiciel antivirus vérifie au moins une fois par jour les nouvelles Signatures antivirus ; et (b) les Signatures antivirus soient à jour. Le Prestataire de Services veillera et, le cas échéant, fera en sorte que ses Sociétés affiliées et son Personnel suppriment immédiatement tout Logiciel malveillant découvert ou susceptible d'être présent dans les Systèmes du Prestataire de Services, les Postes de travail ou au sein des Services. Tous les Services effectueront, le cas échéant, une analyse en temps réel des fichiers et autres données téléchargés dans les Services concernés afin d'identifier et d'éliminer tout fichier ou autre donnée contenant un Logiciel malveillant.

19. **Aucun dispositif de désactivation**. Ni les Services ni les Systèmes du Prestataire de Services n'utiliseront, n'introduiront ou n'autoriseront de quelque manière que ce soit des routines ou des éléments logiciels susceptibles de provoquer ou de permettre un accès non autorisé, la désactivation, la suppression ou tout autre dommage ou interférence avec les Systèmes de la Société.

20. **Chiffrement des données.** Le Prestataire de Services veillera, le cas échéant, à ce que ses Sociétés affiliées et Sous-traitants mettent en œuvre et utilisent les meilleures pratiques standard du secteur qui intègrent au minimum la certification SSL VeriSign 256 bits et des clés publiques RSA 2048 bits afin de protéger les Informations confidentielles de la Société, y compris lors des transmissions entre le réseau de la Société et les Systèmes du Prestataire de Services. Les Informations confidentielles de la Société et toutes les sauvegardes des Informations confidentielles de la Société au repos seront chiffrées conformément aux meilleures pratiques standard de l'industrie qui intègrent, au minimum, le chiffrement de disque Advanced Encryption Standard (AES) avec une longueur de clé minimale de 128 bits. Tous les appareils portables, y compris, sans limitation, les smartphones et les tablettes, contenant ou accédant aux Informations confidentielles de la Société doivent utiliser un chiffrement de bout en bout pour les transmissions à partir de l'appareil portable et toutes les données au repos stockées ou accessibles à partir de l'appareil.

21. **Audits du système.** À tout moment après le premier anniversaire de la date d'entrée en vigueur, la Société peut choisir de procéder à un audit de la sécurité des données, moyennant un préavis d'au moins dix jours ouvrables au Prestataire de Services, afin de comparer les pratiques actuelles du Prestataire de Services en matière de sécurité des données aux meilleures pratiques des principaux prestataires de services identiques ou similaires à ceux fournis par le Prestataire de Services. Si un tel audit révèle que les pratiques et processus de sécurité des données alors utilisés par le Prestataire de Services sont en contradiction flagrante avec les meilleures pratiques du secteur ou ne sont pas conformes aux obligations requises en vertu des présentes, le Prestataire de Services remboursera à la Société le coût de cet audit et la Société et le Prestataire de Services établiront et mettront en œuvre sans délai un plan visant à mettre en œuvre les meilleures pratiques identifiées dans les Services. La Société ne sera pas responsable des défaillances, des impacts négatifs, des dégradations du système, des défaillances de produits ou des pannes de système liés aux Systèmes du Prestataire de Services en raison de la conformité à la présente section 21.

22. **Droit de surveillance.** La Société aura le droit de surveiller la conformité du Prestataire de Services au présent Addendum sur la sécurité des données. Pendant les heures normales de bureau et sans préavis, la Société ou ses représentants autorisés respectifs peuvent inspecter les installations et les équipements du Prestataire de Services, ainsi que toute information ou tout matériel en possession, sous la garde ou sous le contrôle du Prestataire de Services, en rapport avec les obligations du Prestataire de Services en vertu du Contrat ou du présent Addendum sur la sécurité des données. Une inspection effectuée conformément au présent Addendum sur la sécurité des données n'interférera pas de manière déraisonnable avec la conduite normale des activités du Prestataire de Services. Le Prestataire de Services coopérera pleinement à toute inspection initiée par la Société. Le Prestataire de Services répondra rapidement et de manière appropriée à toute demande de la Société relative au Traitement des Données personnelles de la Société.

23. **Sous-traitants.** Le Prestataire de Services fera preuve d'une diligence raisonnable suffisante avant de retenir les services d'un Sous-traitant afin de s'assurer que ce dernier ne compromettra en aucune manière la sécurité, la confidentialité, la disponibilité ou l'intégrité des Informations confidentielles de la Société. En outre, le Prestataire de Services s'assurera que les conditions de son contrat de sous-traitance avec tout Sous-traitant sont conformes aux responsabilités et obligations du Contrat et du présent Addendum sur la sécurité des données. Le Prestataire de Services prendra les mesures appropriées pour que ses Sociétés affiliées et son Personnel soient informés et se conforment aux conditions générales applicables du Contrat et veillera à ce que le Personnel du Prestataire de Services soit formé au traitement des Informations confidentielles de la Société et aux obligations associées en vertu du présent Contrat.

24. **Accès aux informations confidentielles.** Le Prestataire de Services veillera à ce que tout membre de son Personnel ayant accès aux Informations confidentielles de la Société se voie accorder cet accès sur la base d'une approche de privilège minimal/du principe du besoin d'en connaître. Le Prestataire de Services mettra également en place des politiques interdisant au Prestataire de Services, aux Sociétés affiliées du Prestataire de Services ou au Personnel du Prestataire de Services d'utiliser des postes de travail personnels pour le traitement des Informations confidentielles de la Société. Le Prestataire de Services ne retirera pas les Informations confidentielles de la Société de son emplacement ni ne copiera les Informations confidentielles de la Société, sauf si ce retrait ou cette conservation est raisonnablement nécessaire pour fournir les Services. Les Informations confidentielles de la Société doivent toujours être anonymisées/masquées avant d'être transférées vers des environnements non actifs.

25. **Droits sur les Données de la Société.** Les Données de la Société sont et resteront à tout moment la propriété de la Société. Le Prestataire de Services renonce par la présente à tous les privilèges légaux et de droit commun qu'il pourrait avoir actuellement ou à l'avenir en ce qui concerne les Données de la Société. Le Prestataire de Services veillera à ce que toutes les Données de la Société soient strictement séparées des données du Prestataire de Services et des données de tout autre client par des moyens techniques appropriés. Sans limiter la portée générale des obligations prévues par le Contrat ou le présent Addendum sur la sécurité des données, le Prestataire de Services ne doit pas utiliser ou permettre l'utilisation des Données de la Société pour commercialiser ou solliciter des affaires pour les produits ou services du Prestataire de Services, de ses Sociétés affiliées ou de son Personnel, ni utiliser les Données de la Société à d'autres fins que la prestation des Services prévus par le Contrat. Sauf accord écrit exprès de la Société, ni le Prestataire de Services, ni ses Sociétés affiliées, ni le personnel du Prestataire de Services n'ont le droit d'agréger les Données de la Société, ni d'utiliser, de vendre, de créer des œuvres dérivées ou d'exploiter de quelque manière que ce soit les données agrégées de la Société.

26. **Développement et gestion des vulnérabilités.** Pour tout processus de développement logiciel lié à la fourniture des Services en vertu du Contrat, le Prestataire de Services doit traiter les vulnérabilités courantes en matière de programmation : (a) en utilisant des directives de programmation sécurisé et les dernières pratiques reconnues par l'industrie en matière de gestion des vulnérabilités, telles que le guide Open Web Application Security Project (OWASP), le guide SANS CWE Top 25 Most Dangerous Software Errors et CERT Secure Coding ; et (b) formant au moins une fois par an le Personnel du Prestataire de services chargé de développer les logiciels fournis dans le cadre des Services aux techniques de programmation sécurisé les plus récentes, y compris, mais sans s'y limiter, la manière d'éviter les vulnérabilités courantes en matière de programmation. Le Prestataire de Services doit mettre en place un programme complet de gestion des vulnérabilités pour l'identification régulière (au moins une fois par mois), la catégorisation et la correction en temps opportun des vulnérabilités techniques et de processus au niveau des couches infrastructure et application du ou des Systèmes du Prestataire de Services fournis. Les correctifs logiciels destinés à corriger les vulnérabilités doivent être installés et activés dans les délais suivants :

Gravité	Score CVSS	Exigences en matière de remédiation
Critique	9,0 ou plus	<= 1 semaine
Élevé	7,0 à 8,9	<=30 jours
Moyen	4,0 à 6,9	<=60 jours
Faible	0,1 à 3,9	<=90 jours

27. **Conformité PCI.**

27.1. Documentation relative à la conformité PCI. Si le Prestataire de Services fournit des services de traitement des paiements ou si les Services incluent une fonctionnalité de traitement des paiements, le Prestataire de Services déclare et garantit que : (a) il est actuellement conforme à toutes les Exigences PCI DSS et PA DSS applicables ; (b) il s'est enregistré en tant que Prestataire de Services auprès de toutes les entités requises (par exemple, Visa, MasterCard, etc.) ; (c) dans la mesure requise par les Exigences PCI DSS et/ou PA DSS (c'est-à-dire après avoir atteint les seuils de transaction appropriés), a fait l'objet d'une évaluation par rapport aux Exigences PCI DSS et PA DSS réalisée par un évaluateur de sécurité qualifié indépendant (un « QSA ») au cours des douze (12) derniers mois ; (d) dispose d'un certificat d'attestation de conformité à jour et conforme, d'un rapport de validation, d'un rapport de conformité et de toute exception qui y est mentionnée (collectivement, la « documentation de conformité »), conformément aux Exigences PCI DSS ; et (e) mettra la documentation de conformité à la disposition de la Société pour examen sur demande.

27.2. Événement de non-conformité PCI. Le Prestataire de Services s'engage et accepte d'être et de rester en conformité avec toutes les Exigences PCI DSS et PA DSS applicables et de prendre les mesures nécessaires pour valider sa conformité avec les Exigences PCI DSS et PA DSS. Il doit informer immédiatement la Société dans l'un des cas suivants (individuellement, un « Événement de non-conformité ») : (a) le Prestataire de Services apprend ou a des raisons de croire qu'il n'est plus conforme aux Exigences PCI DSS et/ou PA DSS ; ou (b) le Prestataire de Services subit un changement défavorable dans son statut de certification ou de conformité par rapport aux Exigences PCI DSS et/ou PA DSS. En cas d'événement de non-conformité, le Prestataire de Services fournira immédiatement à la Société un plan détaillé pour remédier à cet événement de non-conformité. Si, après un préavis raisonnable de la part de la Société, le Prestataire de Services n'est pas en mesure de fournir la validation de sa conformité aux Exigences PCI DSS et/ou PA DSS et les documents de conformité nécessaires requis en vertu du Contrat, la Société aura le droit de faire appel à un QSA pour effectuer un audit du Prestataire de Services afin de déterminer sa conformité aux Exigences PCI DSS et PA DSS, et

le Prestataire de Services devra prendre en charge tous les coûts liés à cet audit. Tout audit de ce type sera réalisé par un QSA pour le compte de la Société et sera mené de manière à minimiser raisonnablement toute perturbation des activités du Prestataire de Services. Le Prestataire de Services coopérera raisonnablement avec ce QSA, notamment en lui fournissant un accès raisonnable à ses installations et au Personnel nécessaire pour auditer et tester la conformité. Le Prestataire de Services mettra en œuvre toutes les mesures correctives recommandées par ce QSA dès que cela sera raisonnablement possible afin de conserver sa certification de conformité aux Exigences PCI DSS et PA DSS ou de la réobtenir, et fournira un plan détaillé concernant toutes les mesures correctives recommandées. Le Prestataire de Services reconnaît qu'il est seul responsable à tout moment de la sécurité de toute Information de paiement ou donnée de titulaire de carte en transit, au repos ou en sa possession. Le fait pour le Prestataire de Services de ne pas maintenir sa certification de conformité aux Exigences PCI DSS et/ou PA DSS sera considéré comme une violation substantielle du Contrat par le Prestataire de Services.

27.3. Enquête sur les Incident lié à la sécurité des données PCI. En cas d'Incident lié à la sécurité des données et en plus des autres obligations découlant d'un tel événement, le Prestataire de Services doit fournir un accès complet aux membres PCI et/ou aux entités approuvées par PCI afin que cet incident puisse faire l'objet d'une enquête approfondie sans restriction. Le Prestataire de Services doit maintenir la sécurité de toutes les Informations de paiement qui lui sont fournies pendant toute la durée du Contrat et pendant toute la durée de vie des Informations de paiement après l'expiration ou la résiliation anticipée du Contrat. Le Prestataire de Services s'engage à intégrer les meilleures pratiques en matière de sécurité dans ses logiciels afin d'empêcher l'interception des données de transaction, y compris les Informations de paiement.

28. **Autorité de Traitement des Données personnelles de la Société.** Le Prestataire de Services, ses Sociétés affiliées et son Personnel Traiteront les Données personnelles de la Société uniquement pour le compte et au profit de la Société, aux fins du Traitement des Données personnelles de la Société dans le cadre du Contrat, et afin de remplir leurs obligations en vertu du Contrat et des instructions écrites de la Société. La Société aura le pouvoir exclusif de déterminer les finalités et les moyens du Traitement des Données personnelles de la Société. Le Prestataire de Services veillera à ce que son Personnel ayant accès aux Informations confidentielles de la Société ou aux Données personnelles de la Société soit informé de la nature confidentielle des Informations confidentielles de la Société ou des Données personnelles de la Société par le biais d'une formation appropriée sur ses responsabilités en matière d'accès à ce type d'informations.

29. **Données transfrontalières.** Le Prestataire de Services s'engage à ne pas, et à veiller à ce que ses Sociétés affiliées et son Personnel s'engagent à ne pas traiter, diffuser ou transférer les Données personnelles de la Société en dehors du pays (ou, si elles ont été initialement livrées à un endroit situé dans l'Espace économique européen (« EEE ») ou en Suisse, en dehors de l'EEE ou de la Suisse) où la Société ou son personnel respectif les a initialement livrées pour Traitement (un « Transfert transfrontalier de données ») sans le consentement écrit préalable explicite de la Société ou de la Société affiliée appropriée de la Société, qui peut être refusé à sa seule discrétion. Le Prestataire de Services conclura tous les accords écrits nécessaires (selon la détermination raisonnable de la Société) pour se conformer aux Lois sur la protection des données concernant tout Transfert transfrontalier de Données personnelles de la Société, que ce soit vers ou depuis le Prestataire de Services.

30. **Réponse aux Incidents liés à la sécurité des donnés.** Le Prestataire de Services doit maintenir des politiques et des procédures de gestion des incidents de sécurité, y compris des procédures détaillées d'escalade des incidents de sécurité. En cas d'Incident lié à la sécurité des données, le Prestataire de Services, à ses frais exclusifs : (a) signalera rapidement (et en aucun cas plus de vingt-quatre (24) heures après que le Prestataire de Services, une Société affiliée du Prestataire de Services ou le Personnel du Prestataire de Services ait pris connaissance d'un Incident lié à la sécurité des données) cet incident à la Société, en résumant de manière raisonnablement détaillée son impact sur la Société, les Systèmes de la Société ou la réputation commerciale de la Société, s'il est connu ; (b) enquêter (avec la participation de la Société ou la participation d'un enquêteur judiciaire tiers indépendant si la Société le demande) cet Incident lié à la sécurité des données et coopérer avec la Société et ses représentants désignés dans le cadre de toute enquête menée par la Société ou toute Personne concernée relative à la sécurité ou à l'Incident lié à la sécurité des données, y compris, mais sans s'y limiter, fournir toute information ou tout document pertinent relatif à cette violation de la sécurité en possession ou sous le contrôle du Prestataire de Services ou en possession ou sous le contrôle de tout membre du Personnel du Prestataire de Services ou de tout Sous-traitant ; (c) effectuer une évaluation des risques et élaborer un plan d'actions correctives, puis fournir à la Société un rapport écrit sur cette évaluation des risques et sur les mesures prises ou à prendre par le Prestataire de Services ; (d) préparer et (après approbation de la Société) mettre en œuvre un plan de remédiation afin de prendre toutes les mesures correctives nécessaires et recommandées, et coopérer pleinement avec la Société dans tous les efforts raisonnables et légaux visant à prévenir, atténuer, rectifier et remédier aux effets de l'Incident lié à la sécurité des données ; (e) s'assurer que ce rapport contient toutes les informations nécessaires pour : (i) mener une analyse juridique appropriée afin de déterminer la conformité avec toutes les lois, règles, réglementations, directives et exigences gouvernementales internationales, fédérales, étatiques, provinciales et locales applicables actuellement en vigueur et dès leur entrée en vigueur (y compris, sans limitation, les Lois sur la protection des données) ; et (ii) déterminer dans quelle mesure la notification et la communication aux personnes concernées (définies ci-dessous) sont recommandées ou requises par les lois applicables ; (f) mettre à disposition tout le personnel du Prestataire de Services concerné pour un entretien ; (g) atténuer, aussi rapidement que possible et dans la mesure du possible, tout effet néfaste de cet Incident lié à la sécurité des données connu du Prestataire de Services, des Sociétés affiliées du Prestataire de Services ou du personnel du Prestataire de Services ; (h) coopérer avec la Société et son personnel respectif pour fournir tout document, communication, avis, communiqué de presse ou rapport lié à tout Incident lié à la sécurité des données ; et (i) coopérer avec la Société et ses représentants désignés en ce qui concerne la mise en œuvre de nouvelles mesures de sécurité visant à empêcher que de tels incidents ne se reproduisent. Le contenu de tout document, communication, avis, communiqué de presse ou rapport lié à tout Incident lié à la sécurité des données doit être approuvé par la Société avant toute publication ou communication.

31. **Frais liés aux Incidents liés à la sécurité des données.** Outre les obligations d'indemnisation du Prestataire de Services énoncées dans le Contrat, le Prestataire de Services défendra, indemnisera et dégagera la Société, ainsi que ses dirigeants, administrateurs, employés et agents respectifs, de toute responsabilité à l'égard de toute réclamation, poursuite, cause d'action, responsabilité, perte, frais et dommages, y compris les honoraires raisonnables d'avocat, découlant de ou liés à tout Incident lié à la sécurité des données, y compris, mais sans s'y limiter : (a) les frais engagés pour avertir ou informer les anciens et actuels employés, fournisseurs, clients et autres personnes de la Société dont les Données personnelles de la Société ont pu être divulguées ou compromises à la suite de l'Incident lié à la sécurité des données (les « personnes concernées ») et les organismes chargés de l'application de la loi, les organismes de réglementation ou d'autres tiers, conformément à la loi, y compris les Lois sur la protection des données, ou selon les instructions de la Société ; (b) les dépenses engagées soit par la Société, soit par l'intermédiaire d'un enquêteur judiciaire indépendant, d'un conseiller juridique ou de tout autre tiers engagé par la Société, pour enquêter, évaluer ou remédier à l'Incident lié à la sécurité des données et se conformer aux lois applicables et/ou aux normes industrielles pertinentes ; (c) les dépenses liées aux efforts raisonnablement prévus et commercialement reconnus pour atténuer les conséquences de la violation des données des consommateurs, y compris, mais sans s'y limiter, les coûts associés à l'offre d'une surveillance du crédit pendant une période d'au moins douze (12) mois ou toute période plus longue requise par les lois applicables ou recommandée par un ou plusieurs organismes de réglementation de la Société, ou toute autre mesure de protection similaire visant à atténuer les dommages causés aux personnes concernées ; (d) les dépenses engagées pour faire appel à un centre d'appels ou pour élaborer des supports de communication internes

ou externes afin de répondre aux demandes de renseignements concernant l'Incident lié à la sécurité des données pendant une période d'au moins cent quatre-vingts (180) jours ou toute période plus longue requise par la loi ; (e) les amendes, pénalités ou intérêts que la Société paie à toute Autorité gouvernementale ou réglementaire ; (f) les frais juridiques engagés en relation avec un Incident lié à la sécurité des données ou pour traiter toute réclamation de tiers résultant de l'Incident lié à la sécurité des données ou de l'enquête menée par les forces de l'ordre ou les organismes de réglementation ; (g) les dépenses engagées pour faire appel à une société de relations publiques ou de gestion de crise afin de gérer les communications au nom de la Société en rapport avec tout Incident lié à la sécurité des données, et (h) les coûts liés aux demandes de rançon, aux efforts de récupération après une attaque par rançongiciel et aux pertes commerciales résultant d'une attaque par rançongiciel. Sans limiter, exclure ou réduire le droit de la Société à des dommages-intérêts de quelque nature que ce soit en vertu du Contrat ou des obligations d'indemnisation ou de la responsabilité du Prestataire de Services envers la Société, les frais mentionnés aux points (a) à (h) ci-dessus sont considérés comme des dommages directs supplémentaires de la Société.

32. **Aucune violation des exigences en matière de confidentialité et de sécurité de l'information.** Le Prestataire de Services déclare et garantit qu'aucune loi applicable, exigence légale, mesure d'application de la confidentialité ou de la sécurité de l'information, enquête, litige ou réclamation n'interdit au Prestataire de Services : (a) de remplir ses obligations en vertu du Contrat ; ou (b) de se conformer aux instructions qu'il reçoit de la Société concernant les Informations confidentielles de la Société. Le Prestataire de Services déclare et garantit en outre que ni lui, ni aucun Sous-traitant ou Société affiliée n'accédera ou n'obtiendra de quelque manière que ce soit les Informations confidentielles de la Société, ni ne se connectera de quelque manière que ce soit aux Systèmes de la Société, à moins que les mesures de protection et de sécurité décrites dans le présent Addendum sur la sécurité des données n'aient été pleinement mises en œuvre et ne soient effectives. Le Prestataire de Services conclura tout autre accord de confidentialité ou de sécurité des informations raisonnablement demandé par la Société.

33. **Informations confidentielles de la Société perdues ou détruites de manière inappropriée.** Le Prestataire de Services s'engage à ne pas supprimer ou détruire, et à ne pas permettre à ses Sociétés affiliées ou à son Personnel de supprimer ou détruire, les Informations confidentielles de la Société ou les supports sur lesquels elles sont stockées sans l'autorisation préalable de la Société. La Société autorise par la présente le Prestataire de Services à supprimer ou détruire les Informations confidentielles de la Société conformément à toute politique de conservation des documents de la Société ou à toute autre instruction écrite de la Société. Le Prestataire de Services s'engage, et fera en sorte que ses Sociétés affiliées et son Personnel s'engage, à conserver et à fournir à la Société un ou plusieurs rapports identifiant les Informations confidentielles de la Société, y compris les supports, qui ont été détruits et nettoyés, le cas échéant, conformément à la version la plus récente de la publication spéciale 800-88 Rev. 1 du National Institute of Standards and Technology (NIST) intitulée « Guidelines for Media Sanitization » (Directives pour le nettoyage des supports). En cas de perte ou de destruction d'informations confidentielles de la Société due à un acte ou une omission du Prestataire de Services, de ses Sociétés affiliées ou de son Personnel, y compris tout Incident lié à la sécurité de l'information, le Prestataire de Services restaurera ou fera en sorte que la Société affiliée ou le Sous-traitant concerné du Prestataire de Services restaure ces Informations confidentielles de la Société à l'aide de la sauvegarde la plus récente disponible. Le Prestataire de Services accordera la priorité à cet effort afin de minimiser tout effet négatif sur les activités de la Société et l'utilisation des Services et des Systèmes du Prestataire de Services. La Société s'engage à coopérer avec le Prestataire de Services afin de fournir toutes les informations, fichiers ou données brutes disponibles nécessaires à la régénération, la reconstruction ou le remplacement des Informations confidentielles de la Société. Si le Prestataire de Services ou la Société Affiliée ou le Sous-traitant du Prestataire de Services concerné ne parvient pas à régénérer, reconstruire et/ou remplacer intégralement les Informations confidentielles de la Société perdues ou détruites dans le délai raisonnablement fixé par la Société, celle-ci pourra alors, aux frais du Prestataire de Services, obtenir des services de reconstruction des données auprès d'un tiers, et le Prestataire de Services coopérera et fera en sorte que la Société affiliée, le Sous-traitant ou le Personnel du Prestataire de Services concerné coopère avec ce tiers, à la demande de la Société. S'il est déterminé que les Informations confidentielles de la Société ont été perdues ou détruites à la suite d'actes ou d'omissions délibérés, intentionnels ou négligents du Prestataire de Services, d'une Société affiliée du Prestataire de Services, d'un Sous-traitant ou du Personnel du Prestataire de Services, la Société peut résilier le Contrat pour motif valable et intenter toute action civile et pénale à sa disposition.

34. **Restitution ou destruction intentionnelle des Informations confidentielles de la Société.** Le Prestataire de Services s'engage, et fera en sorte que ses Sociétés affiliées et son Personnel s'engagent, à supprimer et détruire définitivement les Informations confidentielles de la Société (ou la partie de ces Informations confidentielles spécifiée par la Société) et/ou à restituer ces informations confidentielles à la Société ou à ses représentants, dans le format et sur le support prescrits par la Société, comme suit : (a) dans les trente (30) jours suivant l'expiration ou la résiliation du Contrat et l'exécution des obligations de chaque Partie en vertu des présentes ; et (b) à tout moment où la Société demande les Informations confidentielles de la Société ou dans les trente (30) jours suivant la demande de la Société. Le Prestataire de Services remettra à la Société une attestation écrite de sa conformité au présent paragraphe et de la conformité de ses Sociétés affiliées et du Personnel du Prestataire de Services, signée par un représentant autorisé du Prestataire de Services. Lorsqu'il n'est pas techniquement possible et/ou commercialement réalisable pour le Prestataire de Services ou une Société affiliée ou un Sous-traitant du Prestataire de Services de supprimer ou de détruire définitivement les Informations confidentielles de la Société détenues sous forme électronique, le Prestataire de Services supprimera ou détruira définitivement les Informations confidentielles de la Société dès qu'il sera techniquement possible et/ou commercialement raisonnable de le faire. Dans l'intervalle, le Prestataire de Services veillera, et fera en sorte que ses Sociétés affiliées et son Personnel veillent, à ce que toute Information confidentielle de la Société résiduelle conservée sous sa garde ou son contrôle soit définitivement mise hors d'usage et ne soit plus traitée, sauf pour la simple conservation de ces informations résiduelles. S'il n'est pas techniquement possible et/ou commercialement viable de rendre définitivement inutilisables les Informations confidentielles de la Société et de ne plus les traiter, le Prestataire de Services, ses Sociétés affiliées et son Personnel continueront d'appliquer les mesures de protection prévues dans les présentes pour les Informations confidentielles de la Société jusqu'à ce que ces Informations confidentielles soient rendues inutilisables. En aucun cas, le Prestataire de Services, ses Sociétés affiliées ou ses Sous-traitants ne retiendront des Informations confidentielles de la Société afin de résoudre un litige.

35. **Indemnisation.** Outre toute autre obligation d'indemnisation prévue dans le Contrat, le Prestataire de Services indemnisera, défendra et dégagera la Société, ses dirigeants, administrateurs, employés, Société mère et Sociétés affiliées de toute responsabilité en cas de réclamations, demandes, pertes, responsabilités, coûts et dépenses, y compris les honoraires d'avocats et les frais de conseil juridique interne, résultant d'une violation du présent Addendum sur la sécurité des données par le Prestataire de Services, ses employés, agents, représentants ou le Personnel du Prestataire de Services, suite à des actes ou omissions du Prestataire de Services ou du Personnel du Prestataire de Services en rapport avec les Informations confidentielles de la Société.

36. **Divulgation électronique.** Le Prestataire de Services doit maintenir des capacités de divulgation électronique de bout en bout conformes aux normes généralement acceptées et à toutes les réglementations et lois en vigueur. Au minimum, le Prestataire de Services doit remplir les fonctions suivantes : (a) dès réception d'un avis écrit de la Société lui demandant de conserver et de Collecter les données électroniques pertinentes pour une affaire, le Prestataire de Services doit prendre des mesures raisonnables et immédiates pour conserver et Collecter toutes les données électroniques pertinentes pour une affaire ; (b) le Prestataire de Services doit conserver une documentation détaillée de toutes les activités liées à la conservation et à la collecte

des données électroniques ; et (c) à la demande du conseiller juridique de la Société ou de son représentant désigné, le Prestataire de Services doit rechercher les données collectées et fournir les résultats à la Société ou à son tiers désigné.

37. **Demandes d'accès, de correction et de portabilité des données.** Le Prestataire de Services informera rapidement la Société par écrit, et dans tous les cas dans les deux (2) jours suivant leur réception à l'adresse security@lpcorp.com, s'il reçoit : (a) toute demande d'un individu concernant les Données personnelles de la Société, y compris, mais sans s'y limiter, les demandes de désinscription, les demandes d'accès et/ou de rectification, de blocage, d'effacement, et les demandes de portabilité des données ; ou (b) toute plainte, objection, notification ou autre communication relative aux Données personnelles de la Société ou au respect par l'une ou l'autre des parties de la législation applicable en matière de Données personnelles de la Société, y compris, sans s'y limiter, les allégations selon lesquelles le Traitement enfreint les droits d'un individu en vertu de la législation applicable. Le Prestataire de Services ne répondra pas directement à une telle demande, plainte, notification ou autre communication, sauf s'il y est expressément autorisé par la Société ou si la loi applicable l'exige, et il apportera à la Société une coopération et une assistance raisonnables en ce qui concerne une telle demande, plainte, notification ou communication. En outre, le Prestataire de Services veillera à avoir mis en œuvre les mesures techniques et organisationnelles nécessaires pour aider la Société à remplir ses obligations de réponse à toute demande d'un individu concernant les Données personnelles de la Société.

38. **Nouveaux produits.** Le Prestataire de Services ne peut fournir aucun nouveau service ou produit en rapport avec les Services sans avoir préalablement obtenu : (a) le consentement de la Société autorisant un tel changement ; ou (b) un avenant dûment signé au présent Addendum sur la sécurité des données traitant de ce changement. La Société ne sera pas responsable envers le Prestataire de Services ou ses Sociétés affiliées et n'aura aucune obligation de paiement pour les produits ou services non acceptés en raison de l'absence des éléments (a) et (b). L'acceptation d'un nouveau produit ou service sans les éléments (a) ou (b) ci-dessus ne constitue pas une renonciation aux droits ou obligations prévus par le Contrat et le présent Addendum sur la sécurité des données. Toute violation de la présente section par le Prestataire de Services est considérée comme une violation substantielle du Contrat.

39. **Modifications des conditions.** Le présent Addendum sur la sécurité des données ne peut être modifié que par un avenant écrit signé par les Parties.

40. **Garanties supplémentaires.** Le Prestataire de Services prendra toutes les autres mesures raisonnablement demandées par la Société pour aider celle-ci à se conformer à toute obligation de notification, d'enregistrement ou autre applicable à la Société en vertu des lois, règles et réglementations applicables en matière de Données de la Société. Ces mesures peuvent inclure, sans s'y limiter, la signature d'accords supplémentaires ou complémentaires requis par les lois et réglementations applicables.

41. **Titres ; interprétation.** Les titres descriptifs des sections du présent Addendum sur la sécurité des données sont insérés uniquement pour des raisons de commodité et ne doivent pas contrôler ou affecter la signification ou l'interprétation de toute disposition des présentes. Dans le présent Addendum sur la sécurité des données, sauf si le contexte l'exige autrement : (a) le terme « jours » désigne les jours calendaires ; et (b) le terme « y compris » signifie « y compris, sans limitation ».