Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

1. Définitions

Les modalités définies dans le présent Addenda portant sur la protection des renseignements personnels doivent être interprétées comme ayant la signification indiquée (i) dans le présent Addenda sur la protection des renseignements personnels et (ii) ailleurs dans l'Entente. Si un terme est défini à la fois dans le présent Addenda sur la protection des renseignements personnels et ailleurs dans l'Entente, la définition du présent Addenda sur la protection des renseignements personnels prévaut aux fins du présent Addenda sur la protection des renseignements personnels.

1.1 Par « Lois sur la protection des renseignements personnels applicables », on entend toutes les lois sur la protection des données et de la vie privée applicables au Traitement des données à caractère personnel des clients, y compris, le cas échéant, (a) le GDPR; (b) le R.-U. Data Protection Act 2018; (c) la Directive 2002/58/CE sur la protection de la vie privée et les communications électroniques (telle que mise à jour par la Directive 2009/136/CE), (d) le Règlement de 2003 sur la protection de la vie privée et les communications électroniques (SI 2003/2426); (e) les lois sur la protection des données fédérales et étatiques des U. (e) les lois, règles ou réglementations fédérales et étatiques Américaines en matière de protection des données, y compris, mais sans s'y limiter, le California Consumer Privacy Act de 2018 (« CCPA »); (f) le Personal Information Protection and Electronic Documents Act (« PIPEDA») et la loi canadienne antipourriel « CASL »), et (g) les lois similaires adoptées partout dans le monde concernant la protection ou l'utilisation, la transmission ou tout autre traitement des données à caractère personnel, chacune étant amendée, modifiée et/ou complétée par les orientations ou les décisions réglementaires de toute autorité de contrôle ou autre autorité de réglementation de la protection des données (« autorité de réglementation »).

1.2 Par « Données personnelles du client », on entend les données personnelles fournies à Corporate Traveller (CT) par le client, ses affiliés, ses employés, ses dirigeants, ses contractants, ses représentants, ses travailleurs d'agence ou ses utilisateurs finaux dans le cadre de la fourniture des services ou en relation avec l'Entente.

1.3 « Contrôleur » représente la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les objectifs et les moyens du traitement des données personnelles.

1.4 « Personne concernée », désigne toute personne physique à laquelle se rapportent des données personnelles.

1.5 « Demande de la personne concernée », signifie toute demande d'une personne concernée concernant les données personnelles traitées par un contrôleur dans le cadre de la fourniture des services ou autrement en relation avec l'Entente.

1.6 « GDPR » désigne le General Data Protection Regulation (Règlement général sur la protection des données) UE 2016/679, tel que mis en œuvre dans le droit national et tel que modifié, étendu, réédité ou appliqué par ou en vertu de tout autre statut, loi ou acte législatif.

1.7 « Bonnes pratiques industrielles » : l'exercice du degré de compétence, de diligence, de prudence et de prévoyance que l'on peut raisonnablement et ordinairement attendre d'un opérateur compétent et expérimenté engagé dans le même type d'entreprise dans des circonstances identiques ou similaires.

1.8 « Données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique), ou tel que ce terme (ou des variantes similaires, telles que « informations personnelles ») peut-être défini dans les lois applicables en matière de protection de la vie privée).

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

1.9 On entend par « violation de données personnelles » une violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès à des données personnelles de clients en possession ou sous le contrôle de CT. Les violations de données personnelles comprennent, sans s'y limiter, les éléments suivants (i) l'accès non autorisé, la divulgation, la perte, le téléchargement, le vol, le blocage, le cryptage ou la suppression par des logiciels malveillants ou d'autres actions non autorisées en relation avec les données personnelles des clients par des tiers non autorisés ; (ii) les incidents opérationnels qui ont un impact sur le traitement des données personnelles des clients ; ou (iii) toute violation du présent addenda sur la confidentialité des données ou des lois applicables sur la confidentialité par CT, ses employés ou ses agents, dans la mesure où cette violation affecte l'intégrité et la sécurité des données personnelles des clients ou a un impact négatif important sur les obligations de CT en vertu du présent addenda sur la confidentialité des données.

1.10 « Traitement » désigne toute opération ou ensemble d›opérations effectuées sur des données à caractère personnel ou sur des ensembles de données à caractère personnel, que ce soit ou non par des moyens automatisés, tels que la collecte, l›enregistrement, l›organisation, la structuration, le stockage, l›adaptation ou la modification, l›extraction, l›accès, la consultation, l›utilisation, l›acquisition, le transfert, l›hébergement (via un serveur, un site web, un nuage ou autre), la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l›alignement ou la combinaison, la restriction, l›effacement ou la destruction. Toute activité définie comme un traitement par les lois applicables en matière de protection de la vie privée ou soumise à leurs exigences relève de la présente définition. Les termes « traité », « processus » et toute autre variante du terme « traitement » sont également définis comme indiqué ci-dessus.

1.11 « Processeur » désigne la personne physique ou morale, l›autorité publique, l›agence ou tout autre organisme qui traite les données personnelles pour le compte du Contrôleur.

1.12 « Autorité de surveillance » : toute autorité de protection des données ou autre agence gouvernementale, réglementaire, administrative, judiciaire ou autre, ou organisme similaire, qui a le pouvoir de mettre en œuvre, d'appliquer et/ou de superviser le respect des lois applicables en matière de protection de la vie privée.

1.13 « Fournisseur » : le transport, l›hébergement, le logiciel de réservation et d›autres fournisseurs de services de gros tel que les compagnies aériennes, les autocars, les chemins de fer, les loueurs de voitures et les opérateurs d›outils de réservation en ligne tiers que la CT engage au nom du Client pour fournir des produits et des services liés aux voyages au Client.

Dans le présent Addenda sur la protection des renseignements personnels, les références aux lois applicables en matière de protection de la vie privée et aux termes qui y sont définis sont remplacées par des références aux lois applicables en matière de protection de la vie privée qui remplacent, modifient, étendent, réadoptent ou consolident ces lois applicables en matière de protection de la vie privée et les termes équivalents définis dans ces lois applicables en matière de protection de la vie privée, une fois qu'elles sont en vigueur et applicables, ou intègrent ces références (selon le cas).

2. Les parties à titre de responsables du traitement et respect des lois applicables en matière de protection des renseignements personnels.

Les parties reconnaissent que, pour fournir les services, CT doit nécessairement traiter les données personnelles des clients à titre de contrôleur. Chaque partie agira comme contrôleur séparé et indépendant (et non en tant que contrôleur conjoint) en ce qui concerne toutes les données personnelles des clients qu'elle traite en vertu de et/ou en relation avec le présent Entente et les services. Chaque partie doit se conformer à toutes les lois applicables en matière de protection de la vie privée en ce qui concerne le traitement des données personnelles des clients et doit s'assurer qu'elle dispose d'une base légale pour ce traitement, le cas échéant. Lorsqu'un affilié d'une partie est un contrôleur ou un processeur de données personnelles du client en vertu du présent Entente, cette partie doit s'assurer que son affilié respecte ses obligations en vertu des lois sur la protection de la vie privée applicables et du présent Addenda sur la protection des renseignements personnels, le cas échéant.

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Sans limiter ce qui précède, chaque partie s'abstiendra de « vendre » (tel que défini par la CCPA à Cal. Civ. Code § 1798.140(t), tel qu›il peut être modifié) ou de transférer les données personnelles des clients autrement qu›en conformité avec les lois applicables en matière de protection des renseignements personnels.

3. Informations fournies aux personnes concernées.

Avant de partager les renseignements personnels du client avec CT, le client fournira toutes les notifications requises par les lois sur la protection de la vie privée applicables à la personne concernée dans chaque cas en ce qui concerne le partage des données personnelles du client avec CT. Lorsque CT recueille des données personnelles de clients directement auprès de personnes concernées, il lui incombe de s'assurer qu'il fournit des informations claires et transparentes aux personnes concernées, comme l'exigent les lois applicables sur la protection de la vie privée, en ce qui concerne le traitement en question.

4. Coopération et assistance.

Chaque partie fournit à l'autre partie une coopération, une assistance et des informations raisonnables afin de l'aider à se conformer aux lois applicables en matière de protection de la vie privée.

5. Notifications.

Chaque partie notifie rapidement à l'autre (dans la mesure permise par la loi) par écrit, en fournissant des détails raisonnables, toute plainte, audit, enquête ou demande de tiers (que ce soit par une autorité de contrôle, une personne concernée ou autre) établissant, alléguant ou demandant des informations sur un éventuel non-respect des lois applicables en matière de protection de la vie privée en rapport avec les données personnelles des clients conservées par ou pour cette partie, et les parties coopèrent raisonnablement l'une avec l'autre à cet égard.

6. Violation de données à caractère personnel.

Les parties sont conscientes que les lois applicables en matière de protection des renseignements personnels peuvent imposer à une partie l'obligation d'informer une autorité de contrôle et la personne concernée en cas de violation de données personnelles affectant les données personnelles du client. En plus de se conformer à ses obligations de notification en vertu des lois applicables sur la protection de la vie privée, CT notifiera rapidement au client tout incident technique, organisationnel ou autre (y compris les incidents chez les sous-traitants) ayant entraîné une violation de données à caractère personnel au sens de l'article 33, paragraphe 1, de la loi sur la protection de la vie privée. 33 par.1 GDPR, affectant les données personnelles du client. La notification par CT d'une violation de données à caractère personnel au client doit être complète et inclure toutes les informations requises en vertu de l'art. 33 par. 3 GDPR et/ou requises par les lois applicables en matière de protection de la vie privée, dans la mesure où ces informations sont disponibles.

En cas de violation de données personnelles, CT prendra rapidement toutes les mesures requises et appropriées en vertu des lois sur la protection de la vie privée et des normes techniques applicables pour rétablir la confidentialité, l'intégrité et la disponibilité des données personnelles du client et la résilience des systèmes de traitement et des services de CT et pour atténuer le risque de préjudice et/ou toute conséquence préjudiciable pour les personnes concernées affectées ou potentiellement affectées par la violation de données personnelles.

7. Demandes des personnes concernées.

Chaque partie fournira à l'autre partie une assistance raisonnable pour se conformer à toute demande de la personne concernée.

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

8. Sécurité.

Conformément aux bonnes pratiques industrielles et aux lois applicables en matière de protection des renseignements personnels, chaque partie met en œuvre des mesures de sécurité techniques et organisationnelles appropriées (y compris le maintien de tout contrôle de sécurité) afin de garantir un niveau de sécurité des données à caractère personnel en sa possession ou sous son contrôle qui soit adapté au risque présenté par le traitement, en tenant compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que du risque de probabilité et de gravité variables pour les droits et les libertés des personnes concernées. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques présentés par le traitement, notamment la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée de données à caractère personnel concernant le client transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à ces données.

Sans préjudice du caractère général de ce qui précède, les mesures de sécurité techniques et organisationnelles minimales que CT mettra en œuvre et maintiendra sont énoncées à l'annexe 1 du présent Addenda sur la confidentialité des données. CT peut, de temps à autre, mettre en œuvre d'autres mesures techniques et organisationnelles adéquates, à condition toutefois que ces mesures ne soient pas matériellement inférieures au niveau de sécurité défini dans le présent document.

9. Exigences relatives au personnel.

CT s'assurera que tout le personnel impliqué dans le traitement des renseignements personnels des clients est correctement qualifié et formé et qu'il s'est engagé à garder les données personnelles des clients confidentielles ou qu'il est soumis à une obligation statutaire appropriée de confidentialité conformément aux lois applicables sur la protection de la vie privée.

10. Désignation du personnel chargé de la protection des données.

Le cas échéant, chaque partie désignera des personnes de contact autorisées en matière de confidentialité et de sécurité des données.

11. Désignation des sous-traitants.

Si CT engage un sous-traitant tiers pour traiter les données personnelles du client dans le but de fournir les services, CT acceptera des conditions écrites avec le sous-traitant qui : (i) exigent que le sous-traitant traite les données personnelles du client uniquement dans le but de fournir les services ; (ii) exigent que le sous-traitant mette en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données personnelles du client contre une violation des données personnelles ; et (iii) se conforment aux exigences des lois applicables en matière de protection des renseignements personnels. CT demeurera responsable envers le client de toute violation des données personnelles du client.

12. Transferts restreints à partir de l'EEE et du Royaume-Uni.

Afin de permettre une prestation efficace et efficiente de ses services, CT peut traiter les données personnelles des clients de l'Espace économique européen et du Royaume-Uni dans d'autres juridictions. Cela n'est autorisé que dans les cas suivants (i) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt du voyageur (par exemple, pour réserver un voyage ou un hébergement par l'intermédiaire d'un vendeur dans un pays non européen) ou lorsque le transfert est requis par la loi applicable; ou (ii) CT a pris toutes les mesures nécessaires pour garantir que les données personnelles du client transférées en dehors de l'Espace économique européen et du Royaume-Uni (que ce soit à une société affiliée de CT, à un sous-traitant ou autre) resteront protégées de manière adéquate conformément aux exigences des lois applicables en matière de protection de la vie privée. Pour les transferts de l'EEE, le Client reconnaît que CT peut assurer cette protection adéquate en exécutant les Clauses contractuelles Types (CCN) énoncées dans l'annexe

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

de la Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 (« CCN »). Pour les transferts du Royaume-Uni, le Client reconnaît que CT peut assurer une protection adéquate en signant l'Entente international de transfert de données publié par le Bureau du Commissaire à l'information du Royaume-Uni en vertu de S119A (1) Data Protection Act 2018 et en vigueur le 21 mars 2022 (« IDTA »).

13. Renvoi des données.

Le Client peut, à son entière discrétion, demander par écrit à CT de lui retourner une copie complète de toutes les données personnelles du Client (ou de son représentant) par transfert de fichier sécurisé dans le format raisonnablement notifié par le Client. Il incombe au client de fournir aux personnes concernées tout avis requis en vertu des lois applicables en matière de protection de la vie privée en rapport avec cette demande.

14. Conservation des données.

CT reconnaît qu'en règle générale, les données personnelles ne peuvent être conservées indéfiniment ou plus longtemps que nécessaires pour le traitement prévu. Les données personnelles des clients ne peuvent être conservées que pendant la durée nécessaire pour satisfaire toutes les bases légales applicables au traitement énoncé à l'article 6 du GDPR, le cas échéant, et pendant la durée requise par les lois sur la protection de la vie privée applicable, et toujours à condition que CT veille à ce que les données personnelles conservées (i) restent confidentielles et soient protégées contre l'accès, la divulgation ou l'utilisation non autorisés et (ii) ne soient traitées que dans la mesure nécessaire aux fins spécifiées dans les lois sur la protection de la vie privée applicables autorisant leur stockage et d'autres traitements, et à aucune autre fin.

15. Droit d'audit du client.

CT conservera ou fera conserver les informations raisonnablement nécessaires pour démontrer qu'il respecte ses obligations en vertu du présent addenda sur la confidentialité des données et, moyennant un préavis raisonnable pendant la durée de l'Entente, mettra à la disposition du client les informations nécessaires pour démontrer qu'il respecte ses obligations en vertu du présent addenda sur la confidentialité des données, lorsque ces informations ne sont pas soumises à des restrictions de confidentialité dues à de tierces parties. Sans limiter la portée de ce qui précède, CT mettra à la disposition du Client, sur demande : (i) une liste de tous les sous-traitants désignés par CT pour traiter les données personnelles du Client ; (ii) une copie de son attestation de conformité PCI DSS la plus récente, dans la mesure où les données personnelles du Client comprennent des données de titulaires de cartes de paiement ; et (iii) un résumé des résultats du dernier audit interne de sécurité des données de CT pour les systèmes qui sont utilisés pour traiter les données personnelles du Client. Toute documentation et information non publique divulguée au client conformément au présent paragraphe sera considérée comme une information exclusive et confidentielle de CT. Le client ne divulguera pas cette documentation ou ces informations à un tiers et ne les utilisera pas à d'autres fins que l'évaluation de la conformité de CT avec le présent Addenda sur la confidentialité des données.

16. Maintien en vigueur.

Les engagements pris dans le présent Addenda sur la confidentialité des données restent en vigueur même après la résiliation ou l'expiration de l'Entente.

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Annexe 1 à l'Addenda sur la protection des données : mesures techniques et organisationnelles de CT

Mesures de pseudonymisation et de cryptage des données à caractère personnel	• Les outils de chiffrement sont déployés conformément à une politique centrale de chiffrement. • Les outils de chiffrement utilisent des algorithmes non obsolètes et des produits approuvés. • Les utilisateurs sont formés à l'utilisation des outils de chiffrement conformément à une politique de chiffrement. • Chiffrement des données en transit à l'aide de TLS 1.2; • Les données critiques au repos sont cryptées à l'aide de l'algorithme AES 256; • Les données de l'alimentation RH sont également cryptées à l'aide de PGP pendant la transmission et au repos sur notre serveur SFTP; • Cryptage au niveau du disque et cryptage au niveau de la colonne; • Intégration d'un tiers à la solution de tokenisation pour certaines données critiques; • Les clés cryptographiques sont protégées contre la modification, la perte et la destruction grâce à : o des profils d'utilisateurs centralisés pour l'authentification. - Pas de décryptage ou de recryptage en cas de rotation ou d'expiration des clés. - Maintien de journaux et de pistes d'audit complet. - Solution commune de chiffrement/déchiffrement pour l'ensemble de l'application. - Principe du moindre privilège. - Sauvegardes fréquentes.

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Mesures visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement	• Ententes de confidentialité dans les contrats des employés comme condition d'embauche; • Le maintien d'un SGSI complet de politiques et de procédures. Ces politiques et procédures couvrent tous les aspects de la confidentialité, de l'intégrité et de la disponibilité des données. Les politiques incluent (mais ne sont pas limitées à) : - le contrôle d'accès, l'utilisation acceptable, la sécurité physique, la sécurité du réseau, le cryptage, la sauvegarde, la conservation des données, la gestion des incidents, le contrôle des changements, etc.; • Les systèmes sont sauvegardés au moins une fois par jour. • Les fichiers de données sont sauvegardés sur un système distinct afin de protéger l'intégrité et la disponibilité des données. • Toute la technologie de CT est protégée par un logiciel antivirus/antimalware de qualité commerciale, dont les signatures sont mises à jour quotidiennement. • Des plans de reprise après sinistre ont été mis en place et testés pour les systèmes clés afin de permettre une reprise conforme aux tolérances de risque de l'entreprise. • Surveillance 24 heures sur 24, 7 jours sur 7 et 365 jours par an des données d'événements reçues des postes de travail du personnel de CT, des serveurs, des courriers électroniques et des sources d'enregistrement sur le web. • Des plans de gestion des vulnérabilités sont en place pour assurer la détection et la correction en temps utile des vulnérabilités au sein de l'écosystème technologique de CT. • Des pare-feux et des IDS/IPS sont mis en œuvre pour détecter et prévenir toute activité malveillante au niveau du réseau.
Mesures visant à garantir la capacité de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci en temps utile en cas d'incident physique ou technique	• Plan de continuité des activités révisé au moins une fois par an; • Plan de réponse aux incidents revu au moins une fois par an; • Les fichiers de données et les systèmes sont sauvegardés sur un système distinct afin de protéger l'intégrité des données. Tous les sites de CT sont protégés par un logiciel de détection des virus; • Plan de reprise après sinistre pour les systèmes avec une architecture N+1 lorsque cela est nécessaire pour répondre aux exigences de continuité.

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Procédures permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement.	• Programme d'audit interne et externe, rapports d'audit et documentation. • Test des processus de sauvegarde, de reprise après sinistre et des procédures de continuité des activités; • Évaluation des risques et surveillance du système sur une base régulière. • Tests de pénétration internes, externes et applicatifs effectués au moins une fois par an ou après tout changement significatif. • Analyse des vulnérabilités internes, externes et applicatives au moins une fois par mois. • Une analyse statique régulière du code est effectuée sur les applications importantes, et tous les ingénieurs logiciels suivent périodiquement une formation sur le code sécurisé. • Un programme privé de recherche de bogues a été mis en place pour surveiller en permanence la position de la CT en matière de sécurité externe. • Recherche continue et proactive des menaces dans l'ensemble du domaine technologique par des chasseurs de menaces experts, informés des menaces de l'industrie. • Surveillance de la sécurité 24 heures sur 24, 7 jours sur 7, 365 jours par an, au moyen d'une solution SIEM, surveillant les serveurs clés, l'infrastructure du réseau, les postes de travail et la télémétrie du comportement des utilisateurs.
Mesures d'identification et d'autorisation des utilisateurs	• Politique de contrôle d'accès qui définit les rôles et les responsabilités en matière de contrôle d'accès physique et logique; • Enregistrement des utilisateurs pour les nouveaux venus et les changements de rôle, et la suppression de l'enregistrement pour les personnes qui quittent l'entreprise; • Les droits d'accès privilégiés sont restreints. Les accès privilégiés sont fournis en fonction des besoins et doivent être approuvés par le service de sécurité de l'entreprise avant d'être créés. • Examen trimestriel de tous les accès aux comptes privilégiés/super-utilisateurs; • Les comptes partagés et génériques sont contraires à la politique de FCTG. Chaque personne se voit attribuer un identifiant personnel lui permettant d'accéder aux applications et aux ressources système autorisées. • L'accès à distance au réseau de l'entreprise nécessite un AMF. L'accès à l'environnement de production et l'exécution de fonctions administratives requièrent également l'utilisation de l'AMF; • Les sessions inactives sont automatiquement fermées au bout de 15 minutes; • L'accès est bloqué après un certain nombre d'échecs d'authentification; • L'accès est accordé sur la base d'un besoin de savoir établi en fonction des rôles, conformément aux politiques d›accès; • Droits d'accès différenciés en fonction du rôle (profils, rôles, transactions et objets); • Surveillance et enregistrement des accès et des changements de rôle; moteur d'analyse du comportement des entités et des utilisateurs en place au sein du SOC. • Mesures disciplinaires à l'encontre des employés qui accèdent à des données à caractère personnel sans autorisation;

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Mesures de protection des données lors de leur transmission	• Les données des flux RH des clients sont cryptées à l'aide de PGP pendant la transmission et au repos sur notre serveur SFTP; • Les données sont transférées à l'aide des protocoles suivants : SFTP, HTTPS ou API sécurisée via TLS 1.2 ou supérieur; • Systèmes de détection et de prévention des intrusions en place. Des systèmes de détection et de prévention des intrusions sont en place. Une protection active des points d'extrémité ainsi qu'un antivirus est en place sur tous les points d'extrémité et les serveurs; • Contrôles de journalisation et de surveillance 24 heures sur 24, 7 jours sur 7 et 365 jours par an pour toutes les infrastructures critiques; • Tous les accès aux composants du système sont liés à un utilisateur unique dans les journaux d'audit et les actions sont consignées dans les journaux.
Mesures de protection des données pendant le stockage	• La norme de chiffrement nécessite l'utilisation d'algorithmes non obsolètes et de produits approuvés. • Utilisateurs formés à l'utilisation des outils de chiffrement conformes à la norme de chiffrement. • Données critiques chiffrées au repos à l'aide d'AES 256 ; • Certaines données critiques tokénisées via le service de tokénisation tiers. • Le chiffrement au niveau du disque et au niveau des colonnes est utilisé ; • Les clés cryptographiques sont protégées contre la modification, la perte et la destruction par : • o Profils d'utilisateurs centralisés pour l'authentification. • o Pas de décryptage ou de rechiffrement en cas de rotation ou d'expiration de la clé. • o Tenir des journaux complets et des pistes d'audit. • o Solution commune de cryptage/déchiffrement pour l'ensemble de l'application. • o Principe du moindre privilège. • Sauvegardes fréquentes. • Contrôles d'accès basés sur le principe du moindre privilège; • Segmentation logique des données personnelles des clients à partir des données d'autres clients ; • Ségrégation des fonctions (production/tests); • Modalités de stockage, de modification, de suppression, de transmission des données à différentes fins;

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Mesures visant à assurer la sécurité physique des lieux où les données personnelles sont traitées	• L'établissement d'autorisations d'accès pour les employés et les tiers ayant besoin de savoir ; • La politique de sécurité physique, qui établit les règles d'octroi, de contrôle, de surveillance et de suppression de l'accès physique aux installations des ressources d'information, y compris l'accès aux bureaux, aux salles et aux installations. Notre politique de sécurité physique contient des lignes directrices pour le travail dans les zones sécurisées, y compris les armoires techniques et les centres de données. Les zones abritant des actifs critiques ou sensibles sont désignées comme des zones sécurisées. Des contrôles appropriés sont en place, y compris (mais sans s'y limiter) : l'accès par carte à puce, les registres d'accès et la supervision, le cas échéant. • Notre infrastructure informatique est hébergée par un grand fournisseur mondial dans des installations réparties géographiquement. Chaque installation est conçue pour fonctionner 24 heures sur 24, 7 jours sur 7 et 365 jours par an et utilise diverses mesures pour protéger les opérations contre les pannes de courant, les intrusions physiques, les catastrophes naturelles et les pannes de réseau. Ces centres de données sont conformes aux normes industrielles en matière de sécurité physique et de disponibilité. • Exigences de sécurité avec nos sous-traitants et sous-fournisseurs, acceptation totale de la conformité avec les exigences législatives applicables en matière de protection de l'information, y compris la sécurité physique.
Mesures pour assurer l'enregistrement des événements	• SIEM nouvelle génération avec analyse du comportement des utilisateurs et des entités, • Flux de journaux de surveillance du centre d'opérations de sécurité 24 heures sur 24, 7 jours sur 7, 365 jours par an, SIEM et surveillance plus large de l'état de santé, • Sources de journalisation d'événements conformes à PCI-DSS; • Agents de détection et de réponse des points finaux fournissant une télémétrie des événements à partir de l'ensemble du domaine technologique, • Procédures d'identification et d'authentification des utilisateurs; • Procédures de sécurité identifiant/mot de passe (caractères spéciaux, longueur minimale, changement de mot de passe); • Blocage automatique (par exemple, mot de passe ou délai d'attente); • Surveillance des tentatives d'effraction et désactivation automatique de l'identifiant en cas de plusieurs tentatives de saisie de mots de passe erronés;

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Mesures pour garantir la configuration du système, y compris la configuration par défaut	• Politique formelle de contrôle des changements pour établir les règles de création, d'évaluation, de mise en œuvre et de suivi des modifications apportées aux ressources d'information de l'entreprise. • Les processus de contrôle des modifications suivent le document de gestion des modifications et s'appliquent aux conceptions et configurations d'applications et d'interfaces système système (API), ainsi qu'aux composants de réseau et de systèmes d'infrastructure. • Toutes les modifications sont testées dans un environnement hors production avant d'être mises en œuvre. • Les versions sont gérées via un processus Release to Production pour capturer la configuration du système et les processus de support au moment de la publication. • Tous les changements doivent être approuvés par les parties prenantes concernées et impactées avant le déploiement, évitant ainsi tout impact sur la disponibilité des services fournis au Groupe; • Normes de configuration de sécurité de base maintenues et actifs analysés pour valider la conformité
Mesures de gouvernance et de gestion de l'informatique interne et de la sécurité informatique	• Politiques et procédures de sécurité de l'information; • Plan de réponse aux incidents; • Audit interne et externe régulier; • Examen et supervision du programme de sécurité de l'information; • Rapports réguliers sur les risques de sécurité, les mesures et la mise en œuvre de la stratégie de sécurité au conseil d'administration et à l'équipe de direction.
Mesures pour certification/ assurance des processus et produits	• ISO27001 (opérations Royaume-Uni) • PCI DSS • Cyber Essentials + (opérations Royaume-Uni)
Mesures visant à garantir la minimisation des données •	• Évaluations d›impact sur la protection des données entreprises • Documentation concernant les catégories de données qui doivent être traitées ; • Veiller à ce que la quantité minimale de données soit traitée pour atteindre la finalité du traitement;
Mesures pour garantir la qualité des données	• Les données personnelles sont conservées exactes et à jour; • Les données sont corrigées sur demande ou lorsque cela est nécessaire; • Processus de demande d'accès au sujet utilisé à l'échelle mondiale; • Les individus ont donné accès à leurs données personnelles pour apporter des modifications/mises à jour/corrections;
Mesures visant à garantir une conservation limitée des données	• Calendrier de conservation des données; • Politique de conservation des données; • Les données personnelles sont supprimées ou anonymisées de manière irréversible ou autrement supprimées après l'expiration de la période de conservation;

Addenda sur la protection des renseignements personnels (Contrôleur à Contrôleur)

Mesures visant à assurer la responsabilité	• Confidentialité dès la conception et par défaut; • Enregistrements des activités de traitement des données; • Évaluations d›impact sur la protection des données, le cas échéant; • Évaluations des intérêts légitimes, le cas échéant; • Des Ententes adéquatees avec des tiers; • Critères de sélection des processeurs; • Processus d'intégration des fournisseurs et questionnaire; • Suivi de l'exécution des contrats; • Programme de formation RGPD et InfoSec;
Mesures permettant la portabilité des données et garantissant leur effacement	• Les données personnelles sont mises à disposition sur demande dans un format électronique portable utilisant les normes de l'industrie; • Élimination sécurisée des informations stockées sur des supports magnétiques et non magnétiques qui empêchent une récupération potentielle des informations;
Mesures supplémentaires relatives aux données sensibles (toutes les mesures énumérées ci-dessus s'appliquent)	
Mesures supplémentaires mises en œuvre spécifiquement pour les transferts de données sensibles pour compléter celles énumérées ci-dessus	• Utilisation des données limitée uniquement à des fins de réservation de voyage; • Formation de tout le personnel au traitement des données personnelles sensibles relatives à l'emploi et annuellement par la suite; • Journalisation des accès aux données; • Accès au personnel limité par un accès fondé sur les rôles.