Politique des données et de la cybersécurité des Aliments Maple Leaf

Tous les fournisseurs qui ont accès aux données liées aux Aliments Maple Leaf, qui sont fournies par elle ou qui lui appartiennent (« données des AML ») doivent, sur demande, démontrer et certifier leurs politiques, processus et procédures de sécurité et prouver qu'ils sont en mesure de fournir une protection adéquate de ces données, y compris de respecter les critères suivants :

POLITIQUES ET PROCÉDURES

Les fournisseurs doivent établir, mettre en œuvre et entretenir les politiques de sécurité de l'information et un programme de mesures de cybersécurité appropriées afin de prévenir tout accès à l'information confidentielle des Aliments Maple Leaf; ils doivent notamment veiller à ce que toutes les versions de logiciels et les niveaux des correctifs de sécurité, les antivirus gérés et la détection des logiciels malveillants soient à jour.

CONFORMITÉ ET ACCRÉDITATION

Les fournisseurs doivent se conformer à toutes les lois applicables, y compris, sans s'y limiter, aux lois pertinentes sur la protection de la vie privée du Canada et des États-Unis, à la *Sarbanes-Oxley Act* (« SOX » [É.-U.]), au Règlement général sur la protection des données (RGPD [UE]), à la norme *Payment Card Industry Data Security Standard* (PCI DSS) et aux *Statement on Standards for Attestation Engagements* 16 (SSAE16) *Service Organization Controls* (SOC) Type I ou II.

Si l'information confidentielle des ALIMENTS MAPLE LEAF est stockée, les fournisseurs doivent alors effectuer des vérifications et des certifications régulières liées à la sécurité. Les centres de données ou colocations hébergées des fournisseurs doivent avoir récemment effectué une vérification *Statement on Standards for Attestation Engagements* 16 (SSAE16) *Service Organization Controls* (SOC) 2 et doivent fournir tous les rapports correspondants aux Aliments Maple Leaf sur demande. Les fournisseurs qui ont recours à une tierce partie pour conserver les données doivent veiller à ce que tous ces tiers entretiennent des certifications de pointe équivalentes aux normes de vérification SSAE 16, ISAE 3402, SOC 2 et SOC 3 pour les centres de données et doivent être prêts à certifier cette conformité annuellement ou sur demande.

SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Les fournisseurs doivent veiller à ce que tous les systèmes des fournisseurs contenant ou donnant accès aux données des AML comportent des restrictions d'accès et d'autorisation et que toutes les données des AML soient conservées et situées uniquement au Canada ou aux États-Unis ou dans des environnements sous la compétence d'autorités judiciaires canadiennes et des États-Unis.

CONTRÔLE D'ACCÈS

Les fournisseurs doivent maintenir des mots de passe et des protocoles de sécurité afin de contrôler l'accès aux données des AML, y compris, dans le cas d'accès à distance, l'authentification multifactorielle. Les fournisseurs doivent maintenir des procédures raisonnables afin de mettre fin à l'accès de leurs employés aux données des AML lorsqu'il n'est plus nécessaire ou pertinent à l'exécution de leurs obligations. Les fournisseurs doivent avoir des mesures de protection en place afin de veiller à ce qu'aucun employé ou entrepreneur ne puisse copier, déplacer ou conserver l'information confidentielle qui appartient aux Aliments Maple Leaf sur aucun dispositif de stockage des données.

Politique des données et de la cybersécurité des Aliments Maple Leaf

SÉCURITÉ DE SYSTÈME

Les fournisseurs doivent effectuer des analyses internes régulières d'évaluation des vulnérabilités comprenant, sans s'y limiter, les réseaux, serveurs, applications et bases de données, avec des logiciels d'analyse des vulnérabilités de la sécurité standards de l'industrie, afin de révéler les vulnérabilités de la sécurité.

VÉRIFICATION ET SURVEILLANCE

Les fournisseurs doivent maintenir une piste de vérification automatisée qui documente les évènements de sécurité de système, ainsi que tout évènement de gestion de changement qui donne lieu à l'accès, la modification et (ou) la suppression d'information appartenant aux Aliments Maple Leaf.

SÉCURITÉ DE RÉSEAU

Les fournisseurs doivent maintenir un processus officiel pour l'approbation, l'essai et la documentation de toutes les connexions de réseau et les changements apportés aux configurations de pare-feu et de routeur. Les fournisseurs doivent configurer les pare-feux afin qu'ils interdisent et enregistrent les suspects et limitent les connexions de réseau ne permettant que le trafic approprié et autorisé, interdisant tout autre trafic à travers le pare-feu. Les règles du pare-feu doivent être examinées de façon récurrente.

PROTECTION, ASSAINISSEMENT ET DESTRUCTION DES DONNÉES

Les fournisseurs doivent se servir de cryptage pour protéger les données des AML qui sont conservées hors de leur environnement de réseau, y compris dans le cas de données des AML qui sont sur un dispositif de stockage tel qu'une bande de sauvegarde, un ordinateur portatif, une clé USB, un dvd ou un cd. Les fournisseurs ne doivent pas conserver d'information confidentielle des Aliments Maple Leaf sur un support amovible (p. ex., clés USB, bandes, CD ou lecteur de disque dur externe), sauf : (a) aux fins de sauvegarde, de continuité des activités, de reprise après sinistre et d'échange de données, tel que permis et exigé en vertu de l'Entente et (b) en utilisant un cryptage très robuste.

INTERVENTION ET NOTIFICATION EN CAS D'INCIDENT

Les fournisseurs doivent maintenir une procédure de gestion en cas d'incident qui comprends la notification immédiate des Aliments Maple Leaf aussitôt qu'ils prennent connaissance de toute destruction, perte, altération, divulgation non autorisée ou accès potentiel aux systèmes du fournisseur ou de destruction, perte, altération, divulgation non autorisée ou accès accidentel ou réel aux systèmes du fournisseur. Les fournisseurs doivent suivre les pratiques exemplaires d'intervention en cas d'incident et faire des efforts raisonnables pour identifier la cause des incidents et de prendre les mesures nécessaires afin de remédier à la cause de tout incident.
Un fournisseur ne doit en aucun cas, sans avoir obtenu le consentement préalable écrit des Aliments Maple Leaf, faire un énoncé publique concernant les systèmes de technologie de l'information des Aliments Maple Leaf ou tout incident ou infraction concernant les systèmes d'information ou autres ressources des Aliments Maple Leaf.

Politique des données et de la cybersécurité des Aliments Maple Leaf

ASSURANCE CYBERSÉCURITÉ

Les fournisseurs devront divulguer aux Aliments Maple Leaf s'ils gardent en vigueur une police d'assurance cybersécurité et le cas échéant, fournir aux Aliments Maple Leaf les détails pertinents de la police. À la discrétion des Aliments Maple Leaf, les fournisseurs devront maintenir une police d'assurance cybersécurité dont la couverture et les limites sont acceptables aux Aliments Maple Leaf.

GESTION DE LA CONTINUITÉ DES ACTIVITÉS ET REPRISE APRÈS SINISTRE

Les fournisseurs doivent élaborer, opérer, gérer et réviser des plans de continuité des activités et de reprise après sinistre qui sont caractérisées par la sauvegarde quotidienne des données et des systèmes, le stockage hors-site des supports et dossiers de stockage, la protection des dossiers et les plans d'intervention appropriés. Les fournisseurs doivent avoir documenté les procédures de sauvegarde sécuritaire et de récupération des données et de l'information qui doivent comprendre, au minimum, les procédures pour le transport, le stockage et l'élimination des copies de sauvegarde des données et, à la demande des Aliments Maple Leaf, fournir ces procédures documentées.