Politique de Waste Management

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DES DONNÉES

Octobre 2020

Au cours de la fourniture des produits et de la prestation des services, le fournisseur peut avoir accès à des données de Waste Management (telles que définies ci-dessous) ou les obtenir autrement ou traiter de telles données. Sans limiter les obligations du fournisseur en ce qui a trait aux renseignements confidentiels de Waste Management (« Waste Management » ou « Société ») qu'on retrouve ailleurs dans l'entente, le fournisseur accepte de protéger toutes les données de Waste Management qu'on retrouve dans cette pièce jointe.

1. Définitions et interprétation. Les définitions suivantes s'appliquent aux fins des présentes :

a. « Collecte d'adresses » - Signifie l'utilisation d'un programme informatique conçu ou vendu ou utilisé afin de produire ou chercher et colliger des adresses électroniques; ou utilisation de l'adresse électronique d'un individu obtenue au moyen d'un tel programme informatique.

b. « Données d'un détenteur de carte » - Cette expression possède le sens qu'on lui donne présentement dans les normes de l'ICP (telles qu'elles sont définies ci-dessous).

c. « Message électronique commercial » - Comprend tout message envoyé en lien avec les services vers un compte de courriel, un compte de messagerie instantanée ou de SMS, un compte de téléphone, un compte sur les médias sociaux ou un compte comparable par un moyen de télécommunications quel qu'il soit incluant, un message textuel, sonore, vocal ou sous forme d'image.

d. « Exigences en matière de protection des données » - Signifie collectivement l'ensemble des lois, des règlements, des décisions et des directives nationales, provinciales/territoriales, locales ou d'un état en lien avec les renseignements personnellement identifiables à l'endroit où les entités de Waste Management (telles qu'on les définit ci-dessous) font des affaires et qui s'appliquent à la manutention, par le fournisseur, des données de Waste Management (incluant, sans s'y limiter, aux États-Unis d'Amérique, la Gramm-Leach-Bliley Act et, au Canada, la Loi sur la protection des renseignements personnels et les documents électroniques, ainsi que les lois provinciales essentiellement similaires en matière de protection des renseignements personnels et les versions successives de ces lois).

e. « Données internes » - Signifie tous les renseignements (peu importe leur forme) d'une entité de Waste Management (telle qu'on la définit ci-dessous), qui sont divulgués à un fournisseur ou accessibles à celui-ci en lien avec l'entente, qui ne sont pas accessibles à la population générale, mais qui ne sont pas considérés comme des données personnelles identifiables. Pour éviter tout doute, à moins que ce genre d'information ne réponde autrement à la définition de données personnelles identifiables, les données internes comprennent, sans s'y limiter, toute l'information que les entités de Waste Management peuvent détenir et qui est régie par l'obligation d'assurer leur confidentialité.

f. « Normes de l'ICP » - Signifie les normes de sécurité alors en vigueur dans le but de protéger les données des cartes de paiement auxquelles les sociétés de cartes de paiement exigent que les marchands ou les fournisseurs de services se conforment incluant, sans s'y limiter, les Normes de sécurité des données de l'industrie des cartes de paiement (NSD ICP) alors en vigueur.

g. « Données personnelles identifiables » - Signifie toute l'information (peu importe la forme) d'une entité de Waste Management (telle qu'on la définit ci-dessous) qui identifie, qui concerne, qui décrit ou qu'on peut associer avec ou qu'on peut identifier ou qui pourrait être raisonnablement liée ou qu'on pourrait raisonnablement lier, directement ou indirectement, à un individu ou un ménage en particulier. Les données personnelles identifiables comprennent, sans s'y limiter : (i) les identificateurs, comme le nom véritable, les pseudonymes, la signature, l'adresse postale, le numéro de téléphone, le numéro d'identification personnelle unique, l'adresse du protocole Internet, l'adresse de courriel, le nom de compte ou tout autre identificateur comparable; (ii) les données personnelles identifiables particulières (telles qu'on les définit ci-dessous); (iii) les renseignements commerciaux et les dossiers des clients incluant, sans s'y limiter, les dossiers sur les biens personnels, les produits ou les services achetés, obtenus ou qu'on envisage de se procurer, ou les autres historiques ou tendances en matière d'achats ou de consommation; (iv) l'information au sujet de l'activité sur l'Internet ou sur un autre réseau électronique incluant, sans s'y limiter, l'historique de navigation, l'historique de recherche et les renseignements touchant l'interaction d'un individu avec un site Web, une application ou une publicité; (v) les données de géolocalisation; (vi) les renseignements audio, électroniques, visuels, thermiques, olfactifs ou autres comparables; (vii) les renseignements de nature professionnelle ou en lien avec l'emploi; (viii) les renseignements sur l'éducation, qu'on définit comme étant des renseignements qui ne sont pas des renseignements personnels identifiables publiquement disponibles tels qu'on les définit dans la loi fédérale du droit à l'éducation de la famille et la loi sur la

© 2020 WM Intellectual Property Holdings, LLC.

protection des renseignements personnels (20 U.S.C., article 1232g, 34 C.F.R., partie 99); (ix) l'information au sujet des transactions avec des entités de Waste Management; (x) les conclusions tirées à partir des renseignements énoncés dans les clauses (i) à (ix) de cette définition afin de créer un profil d'un individu reflétant ses préférences, ses caractéristiques, ses tendances psychologiques, ses prédispositions, son comportement, ses attitudes, son intelligence, ses habiletés et ses aptitudes ou d'autres attributs; et (xi) toute autre information du genre qui peut être soumise aux exigences en matière de protection des données.

h. « Renseignements protégés sur la santé » - Cette expression présente le sens qu'on lui donne dans la HIPAA Privacy Rule (45 C.F.R., partie 160 et sous-parties A et E de la partie 164) et doit comprendre les « renseignements personnels sur la santé » ou tout autre terme comparable en vertu d'une loi provinciale ou territoriale qui s'applique à la protection des renseignements personnels.

i. « Données d'authentification délicates » - Cette expression présente le sens qu'on lui donne dans les normes de l'ICP (telles que définies ci-dessus).

j. « Données personnelles identifiables spéciales » - Comprend les types suivants de données personnelles identifiables : (i) numéro de sécurité sociale, numéro d'assurance sociale, numéro d'identification de contribuable, numéro de passeport, numéro de permis de conduire et autres numéros d'identification émis par le gouvernement; (ii) données de détenteur de carte, données d'authentification délicates, numéro de compte financier, numéro de carte de débit, numéro de police d'assurance et information du rapport de crédit, dans chacun des cas, avec ou sans un code ou un mot de passe qui permettrait d'accéder au compte; et (iii) renseignements protégés sur la santé d'un individu, race, religion, ethnicité, données biométriques (comme les empreintes digitales, l'empreinte rétinienne, etc.), les dossiers de signature numérique (comme les clés d'identification numérique, les images non numérisées de la signature d'un individu sur papier), les renseignements d'un contrôle des références et l'orientation sexuelle.

k. « Données de Waste Management » - Signifie, collectivement, les données personnelles identifiables, les données personnelles identifiables spéciales et les données internes.

l. « Entités de Waste Management » - Signifie, collectivement, Waste Management, Inc., ainsi que toutes les entités qui contrôlent, qui sont contrôlées par ou qui font l'objet d'un contrôle commun avec Waste Management, Inc. Aux fins de cette définition : (i) une « entité » est une société, un partenariat, une coentreprise ou toute autre forme d'entreprise, nationale ou étrangère; et (ii) un « contrôle » et les termes dérivés signifient, en ce qui a trait à une entité, la possession, directe ou indirecte, du pouvoir d'orienter ou de provoquer l'orientation de la gestion et des politiques d'une telle entité, que ce soit pas la détention de titres avec droit de vote (ou de tout autre intérêt dans la propriété), en vertu d'un contrat ou autrement.

m. « Systèmes de Waste Management » - Signifie l'équipement, le logiciel et les réseaux exploités par ou au nom d'une entité de Waste Management.

Toutes les références dans cette pièce jointe à des données de Waste Management, des données personnelles identifiables, des données personnelles identifiables spéciales, des données d'un détenteur de carte, des données d'authentification délicates et des données internes constituent une information (peu importe la forme) fournie à, colligée, obtenue, utilisée, consultée, tenue, élaborée, produite, traitée, stockée, transmise ou autrement manipulée par ou au nom du fournisseur en lien avec la fourniture de produits et de services incluant, sans s'y limiter, tout ajout, modification, substitution, mise à niveau ou amélioration des données en question. Dans la mesure où des données ou des renseignements sont qualifiés de données de Waste Management, les données personnelles identifiables, les données personnelles identifiables spéciales ou les données internes dont on fait mention dans cette entente viennent en conflit avec toute définition ou disposition concernant les renseignements confidentiels, exclusifs ou semblables qu'on utilise dans le corps de l'entente ou de toute entente séparée, dans la mesure du possible, un tel conflit doit être interprété comme si cette pièce jointe imposait des responsabilités et des obligations additionnelles ou supplémentaires en lien avec ladite information et non comme si elle était en conflit avec cette information; pourvu, cependant, que si et dans la mesure où un tel conflit ne peut être résolu de la manière décrite aux présentes, la présente pièce jointe ait préséance sur tout conflit et qu'elle contrôle celui-ci.

2. Obligations générales.

a. Le fournisseur doit respecter en tout temps et traiter les données de Waste Management conformément aux exigences présentées dans cette pièce jointe, ainsi qu'aux exigences en matière de protection des données. Le fournisseur, par la présente, affirme et assure qu'il devra s'informer au sujet des exigences en vigueur en matière de protection des données et respecter ces exigences. Le fournisseur devra aviser Waste Management s'il croit que les instructions de Waste Management concernant les données de Waste Management incluant, sans s'y limiter, les exigences présentées dans cette pièce jointe, amènent le fournisseur à contrevenir à une exigence en matière de

© 2020 WM Intellectual Property Holdings, LLC.

protection des données. Le fournisseur affirme et assure qu'il ne prendra aucune mesure compromettant la capacité de Waste Management de respecter quelque exigence que ce soit en matière de protection des données.

b. Le fournisseur devra assurer la plus stricte confidentialité des données de Waste Management. Sauf lorsqu'autorisé en vertu du présent article, le fournisseur ne devra divulguer les données de Waste Management à aucun tiers ou entreprise incluant, sans s'y limiter, ses sociétés affiliées. Sauf lorsqu'autorisé en vertu du présent article, le fournisseur ne devra pas utiliser (directement ou indirectement) les données de Waste Management à une fin autre que pour offrir des produits et des services.

c. Avant de remettre les données de Waste Management à un tiers incluant, sans s'y limiter, une société affiliée ou un éventuel sous-traitant ou fournisseur de services, le fournisseur devra obtenir auprès d'un administrateur de Waste Management une approbation écrite afin de pouvoir procéder à ladite divulgation et cette approbation sera remise à la discrétion exclusive de Waste Management. Si le fournisseur est autorisé à divulguer les données de Waste Management à ce tiers, ladite divulgation devra se limiter à la quantité minimale de données de Waste Management nécessaire afin de permettre au tiers de s'acquitter de ses obligations à l'endroit du fournisseur. Avant d'effectuer ladite divulgation, le fournisseur accepte, si Waste Management consent à ce qu'il divulgue ses renseignements au tiers en question, de signer avec le tiers une entente écrite comportant des obligations dont la portée est au moins aussi vaste et qui sont au moins aussi restrictives que celles qu'on retrouve dans la présente pièce jointe. Néanmoins, le fournisseur restera en tout temps imputable et responsable de tous les actes et omissions par des tiers en ce qui concerne les données divulguées de Waste Management comme si les tiers étaient des parties à cette entente incluant, sans s'y limiter, le respect des dispositions de la présente pièce jointe et leur violation des exigences en vigueur en matière de protection des données. Waste Management devra avoir le droit d'exiger que le fournisseur fasse appel aux fournisseurs accrédités par elle en ce qui concerne l'endroit où, la façon dont et la manière dont les données de Waste Management sont utilisées et stockées.

d. Le fournisseur ne devra pas être autorisé à utiliser les données de Waste Management à ses propres fins ou aux fins d'un tiers. Sans avoir obtenu au préalable l'approbation écrite d'un administrateur de Waste Management, qui sera donnée à la discrétion exclusive de Waste Management, les données de Waste Management ne pourront, autrement que pour offrir les produits et les services, être utilisées, surveillées, analysées, individualisées, anonymisées, agrégées, vendues, louées ou exploitées commercialement d'une autre manière, quelle qu'elle soit (incluant, sans s'y limiter, dans une forme individualisée, anonymisée ou agrégée).

e. Le fournisseur ne devra en aucun temps acquérir la propriété, la licence, les droits, le titre ou tout autre intérêt à l'égard des données de Waste Management qui devront toutes, comme c'est le cas entre Waste Management et le fournisseur, être des renseignements exclusifs et confidentiels de Waste Management. Par la présente, le fournisseur cède et fera en sorte que ses employés, ses sous-traitants et ses fournisseurs de services cèdent à Waste Management de manière irrévocable, inconditionnelle et à perpétuité, sans autres considérations, tous les droits, le titre et l'intérêt que chacun peut détenir à l'endroit des données de Waste Management incluant toute propriété intellectuelle et tout autre droit de propriété à l'égard des données de Waste Management. Ces droits seront dévolus à Waste Management au moment de créer les données pertinentes de cette dernière. De plus, dans la mesure où le fournisseur ou des membres de son personnel, des sous-traitants et des fournisseurs de services acquièrent des droits moraux à l'endroit des données de Waste Management, le fournisseur devra renoncer et s'assurer que ces membres de son personnel, ces sous-traitants et des fournisseurs renoncent à ces droits.

f. Sans limiter les obligations du fournisseur en vertu de l'entente, celui-ci devra élaborer, mettre en œuvre, surveiller, entretenir et respecter des procédures et des procédés écrits pour la sauvegarde, le stockage et la correction des erreurs, ainsi qu'en cas de destruction, perte ou altération des données de Waste Management qui sont en sa possession ou sous son contrôle. Le fournisseur devra aviser rapidement Waste Management de toute erreur, destruction, perte ou modification des données de cette dernière dont il a connaissance et corriger rapidement toute erreur, destruction, perte ou modification, et ce, gratuitement et sans frais pour Waste Management.

g. Au moment de recevoir un avis, le fournisseur devra rapidement aider et soutenir Waste Management advenant qu'une autorité gouvernementale fasse enquête si et dans la mesure où une telle enquête concerne les données de Waste Management qui sont traitées par le fournisseur. Waste Management assumera les frais d'une telle aide et d'un tel soutien, sauf si l'enquête est rendue nécessaire en raison d'actes ou d'omissions de la part du fournisseur ou de ceux d'employés, de sous-traitants ou de fournisseurs de services du fournisseur. Dans ce cas, l'aide et le soutien seront défrayés exclusivement par le fournisseur.

h. À moins d'obligation contraire dans la loi en vigueur, le fournisseur devra aviser Waste Management dans les vingt-quatre (24) heures après avoir reçu une ordonnance judiciaire ou administrative, une demande de renseignements ou autre d'une autorité gouvernementale ou d'un plaideur (que ce soit au moyen de questions verbales, d'interrogatoires, de demandes de renseignements ou de documents dans le cadre de procédures judiciaires,

© 2020 WM Intellectual Property Holdings, LLC.

d'assignations à comparaître, de demandes d'enquêtes civiles ou d'autres procédés comparables) tentant d'avoir accès ou de divulguer des renseignements de Waste Management. Waste Management aura le droit, à ses propres frais, de contester toute réclamation connexe à la place et au nom du fournisseur. Le fournisseur devra collaborer de manière raisonnable avec Waste Management à cette défense à la demande de Waste Management. Si et dans la mesure où le fournisseur est forcé de divulguer des données de Waste Management en vertu d'une ordonnance judiciaire ou administrative obligatoire, il devra faire appel à tous les efforts raisonnables sur le plan commercial afin de prévenir et limiter ladite divulgation uniquement aux données de Waste Management dont le conseiller juridique du fournisseur a déterminé qu'il est tenu de produire et préserver autrement la confidentialité des données de Waste Management incluant, sans s'y limiter, en collaborant avec Waste Management afin d'obtenir une ordonnance de protection appropriée ou toute autre assurance fiable à l'effet que les données de Waste Management seront traitées de manière confidentielle.

3. Obligations spécifiques. Sans limiter les obligations du fournisseur en vertu de l'article 2 de la présente pièce jointe :

a. Le fournisseur devra élaborer, mettre en œuvre, surveiller, entretenir et respecter l'ensemble du programme de sécurité du système et de l'information dans sa version écrite (« mesures de protection des données ») incluant les protocoles et les contrôles administratifs, électroniques et physiques visant à protéger la sécurité, la confidentialité, la précision et l'intégrité, ainsi qu'à prévenir la destruction, les dommages, la perte, la modification et l'utilisation accidentels ou non autorisés; ainsi qu'à prévenir tout accès physique ou électronique non autorisé ou l'acquisition des systèmes de Waste Management et des données de Waste Management. Les mesures de protection des données devront être conformes aux politiques, aux pratiques et aux exigences de Waste Management en matière de sécurité de l'information que Waste Management peut transmettre de temps à autre au fournisseur (incluant, sans s'y limiter, les dispositions de sécurité accrue régissant l'utilisation de données personnelles identifiables spéciales afin de respecter les exigences en matière de protection des données) et devront être au moins aussi rigoureuses que les plus strictes (i) des directives et des exigences en matière de sécurité des données qui sont présentées dans cette pièce jointe, (ii) des normes industrielles adoptées ou exigées par Waste Management incluant, sans s'y limiter, les normes de l'ICP (dans la mesure où les données d'un détenteur de carte ou les données d'authentification sensibles sont consultées, utilisées, traitées, stockées, transmises ou manipulées autrement par ou au nom du fournisseur en lien avec la fourniture des produits et des services), les normes ISO 27001:2013 (Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Exigences), ISO 27002:2013 (Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information) et dans la mesure où l'on fait appel à une forme quelconque de technologie en nuage pour offrir les services, ISO 27017:2015 (Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage) et ISO 27018:2014 (Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des informations personnellement identifiables (PII) dans les nuages publics agissant comme processeurs de PII), (iii) les exigences en matière de protection des données; et (iv) les pratiques prédominantes dans l'industrie. Le fournisseur doit entretenir et appliquer les mesures de protection des données à chaque endroit à partir duquel il ou ses employés, ses sous-traitants ou ses fournisseurs de services offrent des produits ou des services. De plus, le fournisseur doit s'assurer que les mesures de protection des données couvrent tous les réseaux, les systèmes, les serveurs, les ordinateurs, les blocs-notes, les ordinateurs portatifs, les dispositifs de stockage, ainsi que les autres appareils et supports qui permettent de traiter ou de manipuler les données de Waste Management ou qui donnent accès aux données de Waste Management ou aux systèmes de Waste Management. Le fournisseur doit remettre à Waste Management les documents sur les mesures de protection des données en tout temps sur demande de celle-ci. Le fournisseur ne doit pas modifier les mesures de protection des données de manière à réduire ou à compromettre la confidentialité et la sécurité des données de Waste Management ou les systèmes de Waste Management ou faire en sorte qu'il ne réponde plus aux exigences présentées dans cette pièce jointe.

b. Les mesures de protection des données doivent comprendre, sans s'y limiter : (i) les mesures de contrôle d'accès appropriées et conformes aux pratiques en vigueur dans l'industrie, qui, au moment de créer la présente entente consistent, entre autres, à limiter l'accès à la quantité minimale de données de Waste Management par le nombre le moins élevé possible de membres du personnel du fournisseur qui ont besoin de les consulter afin de pouvoir offrir les produits et les services; et (ii) des protections par mot de passe éprouvées, à jour et conformes aux normes de l'industrie, des pare-feu et des protections antivirus et contre les logiciels malveillants pour protéger les données de Waste Management stockées sur les ordinateurs du fournisseur.

c. Le fournisseur doit chiffrer, en faisant appel aux outils de chiffrement standard, tous les registres et les dossiers contenant les données de Waste Management que le fournisseur : (i) transmet ou envoie sans fil ou sur les réseaux publics; (ii) stocke sur des ordinateurs portables ou sur des supports de stockage; (iii) lorsque c'est possible du point de vue technique, stocke sur des dispositifs portables; et (iv) stocke sur un appareil quelconque qu'on transporte hors du contrôle physique ou logique du fournisseur. Le fournisseur doit assurer la sécurité et la confidentialité de toutes les clés de chiffrement qui sont associées aux données chiffrées de Waste Management. La simple protection des mots de passe ne répond pas aux exigences énoncées dans ce présent paragraphe.

© 2020 WM Intellectual Property Holdings, LLC.

d. Le fournisseur doit prendre des mesures raisonnables pour assurer la fiabilité du personnel qui aura accès ou qui viendra autrement en contact avec les données de Waste Management en s'assurant, dans chacun des cas, que l'accès se limite strictement à ces individus qui ont absolument besoin de connaître les données pertinentes de Waste Management afin de pouvoir offrir les produits et les services, ainsi qu'en s'assurant que tous ces individus sont régis par des ententes de confidentialité écrites ou par des obligations professionnelles ou légales en matière de confidentialité. Sans limiter l'application de la phrase précédente en ce qui concerne le personnel du fournisseur qui doit avoir accès ou venir autrement en contact avec les données de Waste Management, le fournisseur doit : (i) exiger de ces employés qu'ils protègent les données de Waste Management conformément aux exigences des articles 2(b) et 2(c) de la présente pièce jointe au cours de leur période d'embauche ou de maintien en poste et même après; (ii) offrir à ces employés la formation appropriée en ce qui concerne la sécurité de l'information et la protection des renseignements personnels; et (iii) s'assurer que ces employés possèdent les qualifications et les références nécessaires afin de pouvoir traiter et protéger les données de Waste Management conformément aux exigences de la présente pièce jointe (incluant, sans s'y limiter, conformément à la loi en vigueur, à l'exigence selon laquelle le fournisseur doit procéder à des contrôles des drogues et des antécédents de ces employés avant qu'ils n'aient accès ou qu'ils ne viennent autrement en contact avec des données de Waste Management de la manière décrite dans la déclaration de santé et sécurité du fournisseur).

e. Si le fournisseur se connecte ou se voit accorder l'accès à un système de Waste Management, celui-ci accepte : (i) de ne pas accéder et de ne permettre à aucune autre entité d'accéder à un système de Waste Management sans avoir obtenu au préalable l'autorisation d'un agent responsable de Waste Management, qui lui sera accordée à la discrétion exclusive de Waste Management, alors que l'accès ou la tentative d'accès devra se dérouler de la manière prévue dans cette autorisation; (ii) toute connexion par le fournisseur au système de Waste Management et toutes les tentatives de connexion devront se dérouler uniquement par l'entremise des passerelles/pare-feu de Waste Management; et (iii) le fournisseur devra utiliser des programmes de détection/recherche de virus et de logiciels malveillants éprouvés, à jour et conformes aux normes de l'industrie afin de détecter et empêcher le transfert de logiciels malveillants des systèmes informatiques du fournisseur vers à n'importe quel système de Waste Management. De plus, le fournisseur doit obtenir l'autorisation préalable de Waste Management, que cette dernière devra accorder à sa discrétion exclusive, pour tous les employés du fournisseur qui ont accès à un système de Waste Management, alors que cet accès devra se dérouler de la manière décrite dans ladite autorisation.

4. Données personnelles identifiables. Sans limiter les autres obligations du fournisseur qui sont présentées dans cette pièce jointe, les dispositions suivantes doivent s'appliquer aux données personnelles identifiables. Si et dans la mesure où certaines des autres dispositions de cette pièce jointe conçues pour s'appliquer aux données personnelles identifiables contredisent ou ne sont pas conformes aux dispositions du présent article, les dispositions du présent article auront préséance.

a. À moins d'une approbation écrite contraire expresse par un agent responsable de Waste Management (qui sera accordée à la discrétion exclusive de Waste Management) ou si et dans la mesure prévue dans les exigences en matière de protection des données, autrement demandée par le sujet des données individuelles, le fournisseur devra utiliser, consulter, traiter, gérer, transférer et divulguer uniquement les données personnelles identifiables nécessaires afin de fournir les produits et les services et uniquement la quantité minimale et au nombre minimal d'individus nécessaires afin d'offrir les produits et les services. Le fournisseur ne devra pas utiliser, consulter, traiter, gérer, transférer ou divulguer des données personnelles identifiables dans la mesure où cette utilisation, cette consultation, ce traitement, cette gestion, ce transfert ou cette divulgation violerait toute exigence en matière de protection des données si elle était effectuée par Waste Management. Dans la mesure où la fourniture de produits et de services implique ou requiert le traitement de données personnelles identifiables, le fournisseur devra agir uniquement en vertu des instructions et des directives de Waste Management incluant, sans s'y limiter, celles qui sont présentées dans cette entente. Le fournisseur devra rapidement se conformer (c'est-à-dire en aucun cas après le délai de conformité prévu dans les exigences en vigueur en matière de protection des données) à une demande de Waste Management afin de consulter ou modifier des données personnelles identifiables ou à toute mesure nécessaire afin de permettre à Waste Management de se conformer aux exigences en vigueur en matière de protection des données.

b. Le fournisseur ne devra pas transférer physiquement des données personnelles identifiables ou permettre l'accès à des données personnelles identifiables aux membres de son personnel ou à un tiers (incluant, sans s'y limiter, les sociétés affiliées du fournisseur) à l'intérieur ou à partir d'un endroit situé aux États-Unis d'Amérique ou au Canada, sans avoir obtenu au préalable l'approbation écrite d'un agent de Waste Management, qui sera accordée à la discrétion exclusive de Waste Management.

c. Le fournisseur devra aviser Waste Management rapidement par écrit (et, dans tous les cas, moins de cinq (5) jours après la réception) de toute communication reçue d'un individu en lien avec sa demande d'accès, de modification ou de correction de données personnelles identifiables en lien avec l'individu ou de sa demande de fournir les détails touchant le traitement ou la divulgation de données personnelles identifiables touchant l'industrie (incluant, sans s'y

© 2020 WM Intellectual Property Holdings, LLC.

limiter, le sujet, la durée, la nature et le but du traitement ou de la divulgation, les types de données personnelles identifiables, ainsi que les catégories de sujets ou de destinataires des données) et le fournisseur devra, dans chacun des cas, se conformer à toutes les instructions de Waste Management avant de répondre à ce genre de communications.

d. Le fournisseur devra documenter les divulgations à des tiers de données personnelles identifiables et l'information en lien avec de telles divulgations, au besoin, afin de permettre à Waste Management de répondre à une demande de la part d'un individu désirant obtenir un rapport des divulgations de ses données personnelles identifiables.

e. Le fournisseur ne devra pas stocker des données personnelles identifiables sur des ordinateurs portables, des mémoires portatives ou d'autres appareils portatifs ou sur tout appareil transporté hors du contrôle physique ou logique du fournisseur. Dans chacun des cas, l'approbation écrite d'un agent de Waste Management devra être accordée à la discrétion exclusive de Waste Management.

f. Le fournisseur ne devra pas transférer de données personnelles identifiables directement à partir d'un pays de l'Espace économique européen ou des données personnelles identifiables provenant d'un tel pays (même si ces données sont stockées à l'extérieur de l'Espace économique européen) vers des pays dont l'Union européenne considère qu'ils ne possèdent pas un niveau de protection adéquat des données personnelles identifiables (et les fournisseurs ne pourront accéder aux données personnelles identifiables provenant de tels pays) sans s'assurer au préalable qu'un tel transfert répond aux exigences des clauses contractuelles standard approuvées par la Commission européenne en vertu de décisions rendues par la Commission européenne, puisque les clauses contractuelles standard en matière de transfert de données personnelles à des « processeurs » de données dans des pays tiers en vertu de la Directive 95/46/EC de la Commission européenne sont en place entre l'exportateur de données (qui pourrait être Waste Management ou toute autre entité de Waste Management désignée par cette dernière) et l'importateur de données, dans chacun des cas, dans la mesure concernant le transfert pertinent. Les parties acceptent de se conformer aux exigences de ces clauses contractuelles standard. En cas de divergence entre les conditions énoncées dans cette pièce jointe, d'une part, et les clauses contractuelles standard, d'autre part, les modalités qui protègent le mieux les données personnelles identifiables doivent avoir préséance. En cas de doute à savoir quelles sont les conditions qui assurent la meilleure protection, les exigences des clauses contractuelles standard doivent prévaloir. Si, en vertu de la loi (en particulier la loi qui remplace la Directive 95/46/EC de la Commission européenne, comme le règlement (UE) 2016/679), d'une décision d'un tribunal, de la Commission européenne ou d'un énoncé officiel d'une autorité responsable de la protection des données au sein de l'Union européenne, les clauses contractuelles standard n'assurent pas une protection adéquate permettant le transfert intégral des données personnelles identifiables, les parties devront s'entendre sur un mécanisme différent (excluant cependant l'obligation pour une entité responsable de Waste Management d'obtenir le consentement d'individus) en vertu duquel le fournisseur devra pouvoir recevoir et consulter des données personnelles identifiables sans que Waste Management ne doivent encourir de coûts ou de dépenses.

g. Les parties reconnaissent, aux fins de la Directive 95/46/EC de la Commission européenne et de la mise en œuvre des lois promulguées par des états membres de la Commission européenne, ainsi que du règlement (UE) 2016/679, que le fournisseur sera un « processeur » des données personnelles identifiables en sa possession et que Waste Management agira à titre de « contrôleur » des données personnelles identifiables, et ce, conformément à la définition des termes « processeur » et « contrôleur » qu'on présente dans le règlement (UE) 2016/679. Waste Management assumera seule la responsabilité qui consiste à déterminer les fins pour lesquelles et la manière dont les données personnelles identifiables doivent être traitées.

h. Si des renseignements protégés sur la santé sont consultés, utilisés, traités, stockés, transmis ou manipulés autrement par le fournisseur ou en son nom en lien avec la fourniture de produits et la prestation de services, le fournisseur devra alors, si Waste Management le demande, signer une entente d'associé en affaires contenant à tout le moins les modalités contenues dans les exigences en matière de protection des données. Les parties acceptent de respecter cette entente d'associés en affaires. En cas de divergence entre les modalités de la présente pièce jointe et celles de l'entente d'associé en affaires, les modalités qui protègent le mieux les renseignements protégés sur la santé auront préséance. En cas de doutes à savoir quelles sont celles qui offrent la meilleure protection, les exigences de l'entente d'associé en affaires devront prévaloir.

i. Si des données d'un détenteur de carte ou des données d'authentification délicates sont consultées, utilisées, traitées, stockées, transmises ou manipulées autrement par ou au nom du fournisseur, ou si le fournisseur pourrait influencer la sécurité dans un environnement de données d'un détenteur de carte ou des données d'authentification délicates de Waste Management, dans chacun des cas en lien avec la fourniture de produits et la prestation de services, le fournisseur devra alors respecter les normes de l'ICP, s'assurer que les mesures de protection des données répondent aux exigences des normes de l'ICP, tenir un registre de vérification complet de toutes les transactions et activités associées aux données du détenteur de carte et aux données d'authentification délicates et ne pas stocker les données d'authentification délicates sur un appareil incluant, sans s'y limiter, des ordinateurs portables, des supports de stockage portatifs ou d'autres appareils portatifs ou sur tout appareil transporté hors du contrôle physique ou logique du

© 2020 WM Intellectual Property Holdings, LLC.

fournisseur. Le fournisseur déclare et garantit qu'il ne prendra aucune mesure capable de compromettre la capacité de Waste Management de respecter les normes de l'ICP. Le fournisseur déclare et garantit également qu'il maintiendra la certification de sa conformité aux normes de l'ICP, ladite certification étant démontrée par un tiers indépendant reconnu à cette fin dans l'industrie des cartes de paiement. Sans limiter la généralité des exigences précédentes du présent paragraphe :

i. Le fournisseur devra réaliser tous les examens, les tâches, les évaluations, les essais de pénétration, les analyses et autres activités nécessaires en vertu des normes de l'ICP pour les marchands ou les fournisseurs de services de niveau 1, qui s'appliquent (incluant, sans s'y limiter, toute directive de conformité émise par le Conseil des normes de sécurité de l'ICP ou par des organismes subalternes) ou autrement pour valider sa conformité aux normes de l'ICP dans la mesure où elles concernent des éléments du système et des parties de l'environnement des données des détenteurs de cartes ou des données d'authentification délicates de Waste Management dont le fournisseur est responsable (« environnement de l'ICP »).

ii. Le fournisseur devra remettre à Waste Management des copies de tous les documents nécessaires afin de vérifier sa conformité aux exigences de la clause (i) dans le présent paragraphe (« Documents de vérification »). Si Waste Management détermine que d'autres documents de vérification sont nécessaires en vertu des normes de l'ICP ou qu'il est probable qu'ils soient nécessaires afin de vérifier la conformité, incluant un « rapport de conformité » et une « attestation de conformité » non qualifiée connexe, le fournisseur devra fournir ces documents de vérification additionnelle à Waste Management dans les six (6) mois après avoir reçu la demande de Waste Management ou à l'intérieur du délai imposé pour que Waste Management se conforme, selon la première éventualité. Au moins une fois l'an par la suite, tant que ces documents sont exigés en vertu des normes de l'ICP, le fournisseur devra remettre à Waste Management une copie des documents de vérification concernant l'environnement de l'ICP.

iii. Au moins une fois par trimestre, le fournisseur devra remettre à Waste Management la preuve d'une analyse de vulnérabilité de l'environnement de l'ICP réalisée au cours des trois (3) mois précédents par un tiers indépendant et reconnu par l'industrie des cartes de paiement à cette fin.

iv. Le fournisseur devra aviser Waste Management dans les vingt-quatre (24) heures en cas d'exception touchant un rapport de conformité, une attestation de conformité ou une analyse de vulnérabilité trimestrielle ou s'il apprend qu'il ne répond plus aux normes de l'ICP ou s'il prévoit raisonnablement qu'il ne répondra plus à ces normes, alors qu'il devra préciser dans cet avis les mesures prises afin de corriger ladite exception ou non-conformité.

5. Violation de données.

a. Si le fournisseur découvre ou est avisé qu'on a consulté, acquis, détruit, modifié, divulgué, copié, perdu ou utilisé des données de Waste Management en sa possession ou sous son contrôle (chaque cas étant une « violation de données »), le fournisseur devra, dans chacun des cas, à ses frais et ses dépens exclusifs :

i. aviser immédiatement Waste Management (dans tous les cas, moins de vingt-quatre (24) heures après en avoir été avisé) de la date et des circonstances de la violation de données, de la nature et du contenu des données de Waste Management touchées (incluant, s'il s'agit d'une violation de données personnelles (qu'on définit ci-dessous), des catégories et du nombre approximatif d'éléments de données concernés, des instances responsables des éléments de données concernés, ainsi que des catégories et du nombre approximatif des registres concernés), en plus de donner une description des conséquences probables de la violation de données et de fournir tout nouveau renseignement dont il pourrait être informé;

ii. enquêter et déterminer les expositions qui ont donné lieu à la violation de données;

iii. prendre toutes les mesures nécessaires afin d'éliminer ou contenir les expositions qui ont mené à la violation de données et éliminer, atténuer ou limiter toutes les conséquences découlant de la violation de données;

iv. procéder à un examen après coup de tous les événements et de toutes les mesures prises, le cas échéant, dans le but d'apporter les modifications nécessaires aux systèmes informatiques ou aux pratiques d'affaires du fournisseur en lien avec la protection des données de Waste Management;

v. dans les trente (30) jours après qu'on ait constaté la violation de données, fournir à Waste

© 2020 WM Intellectual Property Holdings, LLC.

Management un rapport détaillé décrivant les expositions ayant mené à la violation de données et soumettre à l'approbation de Waste Management un plan d'action décrivant ces expositions et ces mesures correctives, incluant des mesures préventives appropriées afin que les expositions qui ont donné lieu à la violation de données ne se reproduisent pas;

vi. mettre en place le plan d'action approuvé par Waste Management conformément aux modalités;

vii. réunir, documenter et conserver toute l'information recueillie dans le cadre de son enquête sur la violation de données, ainsi que toutes les mesures prises en réaction à la violation de données, et ce, dans chacun des cas, en donnant suffisamment de détails pour répondre aux attentes raisonnables d'admissibilité pour des raisons légales;

viii. collaborer à toute enquête en lien avec la violation de données réalisée à la discrétion d'une entité gouvernementale, quelle qu'elle soit;

ix. aider et collaborer avec Waste Management dans le cadre de ses efforts et de ceux des individus désignés, afin d'enquêter sur la violation de données, réagir à celle-ci, empêcher qu'elle ne se reproduise, atténuer ses effets et corriger la situation; et

x. tenir Waste Management régulièrement (mais dans tous les cas sur demande de celle-ci) informée quant à l'état de la violation de données et de toutes les questions qui la concernent incluant, sans s'y limiter, les efforts que déploie le fournisseur en vertu du présent paragraphe.

b. En plus de ses obligations en vertu du paragraphe (a) du présent article, si la violation de données implique des données personnelles identifiables (« violation de données personnelles »), le fournisseur devra alors à ses propres frais et dépenses, si et dans la mesure exigée par Waste Management :

i. aider et collaborer avec Waste Management à tous les avis et communications destinés aux individus concernés, aux individus possiblement touchés, aux autorités gouvernementales, ainsi qu'aux tiers que Waste Management jugera appropriés;

ii. créer et tenir pendant au moins deux (2) ans à compter de la date de la découverte de la violation de données personnelles, un site Web d'information présentant la forme et le contenu choisis par Waste Management avant qu'il ne soit affiché, afin d'informer les individus touchés et possiblement touchés par la violation de données concernant, sans s'y limiter, tout l'équipement connexe, le logiciel, la connectivité à l'Internet et la sécurité du site Web;

iii. créer et entretenir un centre d'appel téléphonique disponible vingt-quatre (24) heures sur 24, sept (7) jours sur sept afin de répondre aux questions des individus touchés et possiblement touchés par la violation des données personnelles, et ce, pour une période d'au moins six (6) mois après que le dernier avis de violation des données personnelles ait été acheminé aux individus touchés et possiblement touchés, pourvu que ce centre d'appel doive utiliser les textes fournis par Waste Management; et

iv. pour une période d'au moins deux (2) ans à compter de la date de la découverte de la violation de données personnelles, fournir à tous les individus touchés et possiblement touchés par l'incident une protection contre le vol d'identité qui équivaut ou qui est supérieure à la surveillance du crédit ou à un service de protection et qui comprend la surveillance automatique quotidienne par les trois bureaux de crédit, l'aide aux victimes de fraude et une assurance d'une valeur de 1 million de dollars (1 000 000 $) en cas de vol d'identité, sans franchise, un bureau d'aide accessible vingt-quatre (24) heures sur 24, sept (7) jours sur sept, ainsi que des rapports de crédit gratuits.

c. Le fournisseur ne devra pas divulguer l'existence d'une violation de données ou toute information connexe à quiconque ou à un tiers sans avoir premièrement consulté Waste Management et obtenu sa permission, sauf dans la mesure nécessaire pour aviser Waste Management, les autorités responsables de l'application de la loi, ainsi que les assureurs, le conseiller juridique et les firmes de relations publiques du fournisseur ou lorsqu'exigé de manière expresse dans les exigences en matière de protection des données. Waste Management devra assurer le contrôle éditorial final du contenu des documents déposés, communications, avis, communiqués de presse, rapports et autres divulgations en lien avec une violation de données.

d. Le fournisseur devra rembourser à Waste Management tous les coûts et dépenses encourus par cette dernière en lien avec une enquête, une réponse, les mesures visant à prévenir la répétition, les mesures d'atténuation et de

© 2020 WM Intellectual Property Holdings, LLC.

correction suite à une violation de données incluant, sans s'y limiter : (i) les services judiciaires et d'enquête ayant pour but d'enquêter sur la cause de l'événement et sur la mesure dans laquelle des données personnelles identifiables étaient concernées; (ii) la préparation et l'envoi par la poste ou par d'autres moyens d'avis ou d'autres communiqués à des individus concernés, des individus possiblement touchés, des autorités gouvernementales ou des tiers, selon ce que Waste Management juge approprié; (iii) des services de relations publiques ou d'autres services de gestion de crise comparables; (iv) des frais juridiques, de consultation et de comptabilité associés à l'enquête de Waste Management et aux mesures prises en réponse à l'événement; (v) les amendes et les pénalités imposées par le gouvernement; (vi) la mise sur pied et l'entretien du site Web d'information et du centre d'appel téléphonique décrits dans les clauses (ii) et (iii) au paragraphe 5(b) de cette pièce jointe; et (vii) la protection contre le vol d'identité procurée à tous les individus concernés, comme on le mentionne dans la clause (iv) au paragraphe 5(b) de cette pièce jointe.

e. Lorsque survient une violation de données, Waste Management doit être autorisée (à son choix et à sa discrétion exclusive) à suspendre le transfert des données de Waste Management, à exiger du fournisseur qu'il cesse d'utiliser les données pertinentes de Waste Management et/ou à mettre immédiatement fin à l'entente et, dans chacun des cas, sans encourir de responsabilité ou d'amende et sans devoir verser des frais de résiliation. L'exercice des droits énoncés ci-dessus par Waste Management ne doit pas être considéré comme une violation de l'entente par celle-ci.

6. Destruction et retour des données.

a. Le fournisseur devra (i) remettre rapidement à Waste Management dans un format structuré et conforme aux normes de l'industrie ou sur un support standard dans l'industrie, la totalité ou une partie quelconque des données de Waste Management en sa possession ou sous son contrôle; et (ii) à moins d'indication contraire spécifique par Waste Management, détruire la totalité ou une partie des données de Waste Management en sa possession ou sous son contrôle de la manière décrite au paragraphe (b) du présent article, dans chaque cas selon la première éventualité : (A) date de la demande de Waste Management concernant la totalité ou la partie prescrite des données de Waste Management (B) date où les données de Waste Management ne sont plus nécessaires aux fins de la fourniture des produits et des services en lien avec ces données de Waste Management; et (C) date effective d'expiration ou de résiliation de l'entente qui concerne toutes les données de Waste Management. Sur demande de Waste Management, le fournisseur devra certifier qu'il s'est conformé à l'instruction immédiatement précédente dans un avis signé par un de ses administrateurs. Le fournisseur ne devra pas retenir de données de Waste Management dans le but de résoudre quelque conflit que ce soit.

b. Si le fournisseur élimine des documents sur papier, en version électronique ou autre qui renferment des données de Waste Management (que ces données aient intégrées ou non aux propres renseignements ou documents du fournisseur), celui-ci devra le faire en prenant toutes les mesures raisonnables (compte tenu de la sensibilité des données de Waste Management) afin de détruire ces données : (i) en les déchiquetant; (ii) en les effaçant et les supprimant de manière permanente et sécuritaire; (iii) en démagnétisant les supports sur lesquels elles sont inscrites; ou (iv) en modifiant autrement les données de Waste Management que renferment ces documents de manière à les rendre illisibles, impossibles à reconstituer ou indéchiffrables. Toutes les données personnelles identifiables spéciales doivent être éliminées de la manière décrite dans les clauses (i) à (iii) du présent paragraphe immédiatement après la date où elles ne sont plus nécessaires pour s'acquitter de ses obligations en vertu de l'entente.

c. Waste Management peut présenter au fournisseur toute partie des données de Waste Management qui sont retenues en raison d'un litige ou que le fournisseur ne doit pas détruire pour une autre raison. Le fournisseur devra s'abstenir de détruire ces données de Waste Management et devra les conserver de la manière décrite dans les instructions de Waste Management.

7. Essai.

a. Le fournisseur devra essayer régulièrement (et reprendre ces essais, au besoin) et surveiller les procédures et les systèmes de sécurité du fournisseur. De plus, il devra procéder à des examens périodiques pour assurer la conformité aux exigences énoncées dans cette pièce jointe et mettre en place des plans d'action dans le but de corriger les lacunes qu'on aura constatées. Le fournisseur devra mettre les résultats de ces examens à la disposition de Waste Management sur demande de celle-ci.

b. Sans limiter les obligations du fournisseur en vertu du paragraphe (a) du présent article, le fournisseur devra :

i. revoir, essayer (et reprendre ces essais, au besoin) et, selon le cas, réviser les mesures de protection des données : (A) au moins une fois l'an ou lors de tout changement dans les systèmes informatiques ou les pratiques d'affaires du fournisseur qui pourrait nuire à la sécurité, la confidentialité ou l'intégrité des données de Waste Management; et (B) sur demande raisonnable de la part de Waste Management. Si le fournisseur modifie les mesures de protection des données

© 2020 WM Intellectual Property Holdings, LLC.

après un tel examen, il devra aviser rapidement Waste Management des modifications et lui présenter ces modifications par écrit sur demande de Waste Management.

ii. Se procurer, sans coûts ou dépenses additionnels pour Waste Management, les rapports du vérificateur concernant les contrôles de l'organisme de services (« COS ») 1 et COS 2 de type II d'une firme de vérification de niveau 1 ou 2 pour tous les systèmes et les activités de comptabilité ou de contrôle interne en lien avec la fourniture des produits et la prestation des services et pour chaque installation d'où proviennent les produits et les services (que ce soit par l'entremise d'un fournisseur ou d'un tiers qui prend en charge les produits et les services). Les rapports de COS 1 doivent être émis en vertu de la norme d'attestation n° 18 des énoncés sur les normes des engagements d'attestation. Les rapports de COS 2 doivent être émis en vertu de la norme d'attestation AT, article 101 et doivent couvrir les principes d'un service de confiance et les critères (incluant la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la protection des renseignements personnels). Chaque rapport COS 1 et COS 2 doit être produit pour la période de douze (12) mois précédant immédiatement le 30 septembre chaque année et chacun de ces rapports doit être remis à Waste Management au moins quinze (15) jours ouvrables après leur réception par le fournisseur (mais en aucun cas plus tard que le 15 novembre chaque année). Le fournisseur doit fournir rapidement, mais au plus tard le 15 janvier chaque année, une déclaration écrite le 15 janvier chaque année attestant que (A) les mesures de contrôle existant à la date des rapports COS 1 et COS 2 les plus récents restent en vigueur; et (B) aucune lacune importante ou faiblesse dans le matériel (tels que définis par le Public Company Accounting Oversight Board [PCAOB]) n'a été constatée au cours de la période depuis les rapports COS 1 et COS 2 les plus récents qui pourraient influencer ces mesures de contrôle.

iii. À la demande de Waste Management, remplir un questionnaire de sécurité de l'information de Waste Management, qui doit comprendre les réponses aux questions touchant les mesures de contrôle du fournisseur pour n'importe quelle partie des produits et des services réalisés par un tiers par le fournisseur ou en son nom.

iv. Désigner un représentant chevronné approprié de l'équipe de sécurité de l'information qui rencontrera l'équipe de sécurité de l'information de Waste Management pour aborder les questions ou les préoccupations que Waste Management pourrait avoir concernant les mesures de protection des données.

8. Dossiers et évaluations.

a. Le fournisseur devra établir et tenir des livres, des avis, ainsi que des registres comptables et administratifs complets nécessaires afin de confirmer la conformité à cette pièce jointe incluant, sans s'y limiter, des comptes de toutes les transactions impliquant les données de Waste Management et devra tenir ces registres de la manière décrite dans les politiques de Waste Management alors en vigueur sur la tenue des documents pendant la durée de l'entente et pendant au moins sept (7) années par la suite.

b. Moyennant un préavis d'au moins cinq (5) jours remis au fournisseur, ce dernier doit permettre à Waste Management, à ses vérificateurs, aux représentants désignés de la vérification et aux organismes de réglementation incluant, sans s'y limiter, les organismes de réglementation responsables de la protection des données, de vérifier et d'inspecter, aux frais exclusifs de Waste Management (à moins d'indication contraire aux présentes) et au plus une fois par année (à moins d'indication contraire par les organismes de réglementation de Waste Management ou dans la loi en vigueur, ou à moins qu'une vérification ou une inspection antérieure n'ait révélé des lacunes); (i) les installations du fournisseur et des tiers sous-traitants et fournisseurs de services du gouvernement où les données de Waste Management sont stockées ou tenues par ou au nom du fournisseur; (ii) tout système informatisé ou sur papier utilisé pour partager, diffuser ou traiter autrement les données de Waste Management; (iii) les pratiques et les procédures de sécurité, les installations, les ressources, les plans et les procédures du fournisseur; et (iv) tous les livres, les avis, ainsi que les documents comptables et administratifs que doit conserver le fournisseur en vertu des présentes. Ces droits de vérification et d'inspection doivent servir à tout le moins à vérifier la conformité du fournisseur au contenu de la présente pièce jointe, à toutes les exigences en vigueur en matière de protection des données, ainsi qu'aux normes de l'ICP. Si une vérification et une inspection réalisées en vertu de ce paragraphe témoignent de bonne foi d'un problème technique, d'un problème de sécurité ou d'une autre non-conformité à cette pièce jointe, à des exigences en vigueur en matière de protection des données et/ou aux normes de l'ICP, le fournisseur devra verser les coûts assumés par Waste Management pour réaliser une telle vérification ou inspection et, dans les trente (30) jours suivant la réalisation de cette vérification ou inspection, il devra proposer une réponse écrite appropriée incluant, sans s'y limiter, un plan de correction du problème à l'intérieur d'un délai raisonnable demandé par Waste Management. Au moment où Waste Management approuvera un tel plan, le fournisseur devra mettre en œuvre le plan approuvé de Waste Management

© 2020 WM Intellectual Property Holdings, LLC.

conformément à ses modalités. Waste Management ne devra être tenue d'assumer aucun coût ou aucuns frais additionnels en lien avec ce recours.

c. Waste Management peut procéder à des évaluations de sécurité périodiques de ses systèmes, ce qui peut comprendre, sans s'y limiter, une évaluation de certaines parties des systèmes informatiques et des réseaux du fournisseur. Le fournisseur accepte, si une telle évaluation devait révéler que la sécurité laisse à désirer chez le fournisseur, Waste Management, en plus des autres recours dont il peut se prévaloir, peut suspendre l'accès du fournisseur aux systèmes de Waste Management jusqu'à ce qu'il ait apporté les correctifs nécessaires au niveau de la sécurité. Une telle suspension ne sera pas considérée comme une violation de l'entente par Waste Management.

9. Indemnités. Le fournisseur devra indemniser et (au choix de Waste Management, à sa discrétion exclusive) défendre Waste Management, les entités de Waste Management, ainsi que leurs administrateurs, dirigeants, actionnaires, employés, agents, successeurs, ayant-droits et sous-traitants contre toute menace de réclamation, de perte, de responsabilités, de dommages, de règlements, de dépenses et de coûts découlant de, en lien avec ou reposant sur des allégations, en tout ou en partie, de ce qui suit : (a) un non-respect des exigences présentées dans cette pièce jointe ou des exigences de protection des données; (b) une violation de données ou une violation de données personnelles; (c) une négligence, une négligence grave ou une inconduite volontaire de la part du fournisseur, d'un membre du personnel du fournisseur, de sous-traitants ou de fournisseurs de services ou d'un tiers auquel le fournisseur donne accès aux données de Waste Management ou aux systèmes de Waste Management, en ce qui concerne la sécurité, la confidentialité ou l'intégrité des données de Waste Management et les systèmes de Waste Management; (d) toute mesure corrective prise par Waste Management en lien avec une violation de données; et (e) tous les autres coûts et dépenses encourus par Waste Management en lien avec l'exercice de ses droits en vertu de la présente pièce jointe. Sauf disposition expresse contraire dans cette pièce jointe, le fournisseur sera entièrement responsable et devra payer tous les coûts et dépenses encourus par lui ou par son personnel ou ses agents dans le cadre de ses obligations en vertu de la présente pièce jointe.

10. Collecte de données personnelles identifiables, envoi de messages électroniques commerciaux.

a. Dans les cas où le fournisseur recueille ou traite des données personnelles identifiables au nom de Waste Management, le fournisseur devra et verra à ce que ses employés et ses sous-traitants :

i. recueillent et traitent les données personnelles identifiables uniquement de la manière prévue de temps à autre dans les instructions de Waste Management;

ii. mentionnent aux individus concernés les raisons pour lesquelles il recueille et utilise des données personnelles identifiables dans le cadre de la prestation des services ou de la fourniture des produits et à ce qu'ils s'assurent que les buts mentionnés sont raisonnables;

iii. recueillent uniquement des données personnelles identifiables nécessaires aux fins de la prestation des services ou de la fourniture des produits;

iv. obtiennent tous les consentements nécessaires des individus pour les fins établies;

v. utilisent toute forme de consentement donné par Waste Management et confirment ce consentement en vertu de la politique sur la protection des renseignements personnels de Waste Management; et

vi. remettent à Waste Management un registre de ces consentements sur demande.

b. Dans les cas où un fournisseur envoie des messages électroniques commerciaux à Waste Management, le fournisseur devra :

i. s'assurer que chaque consentement relatif à l'envoi d'un message électronique commercial à un destinataire dans le cadre des services ou en lien avec ceux-ci :

(a) est obtenu en vertu d'un mécanisme de consentement facultatif;

(b) présente la forme prévue par Waste Management;

(c) informe la partie consentante qu'il pourrait se désabonner en tout temps des messages électroniques commerciaux; et

(d) contient toutes les coordonnées exigées dans les lois en vigueur.

© 2020 WM Intellectual Property Holdings, LLC.

ii. S’assurer que chaque message électronique commercial envoyé ou dont on a provoqué l’envoi dans le cadre des services ou en lien avec ceux-ci :

(a) est envoyé uniquement lorsque le fournisseur a déterminé qu’il a obtenu du destinataire en vertu des lois en vigueur les consentements nécessaires pour envoyer de tels messages ou qu’il est autrement autorisé à envoyer de tels messages en vertu des lois en vigueur;

(b) contient un mécanisme de désabonnement qui fonctionne;

(c) ne contient aucune affirmation fausse ou trompeuse dans les renseignements de l’expéditeur, dans le sujet, le releveur de coordonnées ou le corps du message;

(d) ne pas être acheminé à une adresse électronique obtenue au moyen d’un processus de collecte d’adresses; et

(e) contient toutes les coordonnées exigées dans les lois en vigueur.

iii. Le fournisseur devra immédiatement donner suite aux demandes de désabonnement qu’il reçoit en lien avec les services, conserver la preuve à l’effet qu’il a donné rapidement suite à ces demandes de désabonnement et remettre immédiatement chacune de ces demandes à Waste Management.

iv. Le fournisseur devra assurer seul la conformité des messages électroniques commerciaux qu’il envoie ou qu’il demande d’envoyer en vertu de la présente entente aux lois en vigueur incluant, sans s'y limiter, les exigences en matière de protection des données, la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, L.C. 2010, ch. 23 (« LCAP »). Waste Management devra apparaître comme étant l’expéditrice de ces messages électroniques commerciaux. Tout message électronique commercial nommant ou décrivant Waste Management ou sa propriété intellectuelle, ses produits ou ses services devra contenir une mention à l’effet qu’il est envoyé par Waste Management, faire état de l’adresse postale et d’au moins un numéro de téléphone, d'une adresse de courriel ou d'une adresse de site Web de Waste Management, alors que les coordonnées de Waste Management seront fournies par elle-même, incluant un mécanisme de désabonnement qu’elle peut prévoir et qui permet aux destinataires d’ajouter leur adresse de courriel à la liste des individus qui désirent voir leur nom retiré des activités de Waste Management. Avant d’envoyer de tels messages électroniques commerciaux, le fournisseur divulguera les adresses de destination de ces messages (« liste ») à son fournisseur de services de courriel désigné afin d’en retirer les noms des individus qui souhaitent se désabonner et/ou suivra ces autres processus ayant pour but de retirer les noms de ces individus comme Waste Management pourrait le demander. Le fournisseur de services ne devra envoyer aucun message électronique commercial faisant référence à Waste Management, à ses marques, ses produits ou inclure la divulgation de la LCAP de Waste Management à quelque adresse que ce soit qui apparaît sur la liste de désabonnement de Waste Management.

11. Généralités.

a. Le fournisseur devra désigner un membre de l’équipe de gestion comme principal gestionnaire du fournisseur en vertu de l’entente qui sera disponible pour aider Waste Management vingt-quatre (24) heures sur 24, sept (7) jours sur sept. La responsabilité du gestionnaire principal de la sécurité du fournisseur consistera à gérer et à coordonner le respect, par le fournisseur, de ses obligations en vertu de la présente pièce jointe.

b. Les parties acceptent, dans la mesure où cette entité ne participe pas à l’entente, que toutes les entités de Waste Management sont de tiers bénéficiaires des dispositions de la présente pièce jointe, ainsi que des dispositions sur la protection des renseignements personnels et la sécurité des données contenues dans l’entente, alors que des dispositions doivent s’appliquer au profit des entités de Waste Management. Sans limiter la phrase immédiatement précédente, les entités de Waste Management doivent être autorisées à appliquer les dispositions de la présente pièce jointe, ainsi que toutes les dispositions sur la protection des renseignements personnels et la sécurité des données contenues dans l’entente comme si chacune avait signé l’entente.

c. Le fournisseur reconnaît, en raison de la nature unique des données de Waste Management, que la

© 2020 WM Intellectual Property Holdings, LLC.

divulgation ou l'autorisation non autorisée des données de Waste Management peut causer des torts irréparables à Waste Management et que l'ampleur de ces torts sera difficile à évaluer, sans compter qu'il n'existe à ce niveau aucun recours judiciaire. Par conséquent, le fournisseur reconnaît que Waste Management, en plus de tous les autres recours disponibles, doit détenir le droit d'obtenir une injonction immédiate et tout autre redressement équitable empêchant toute violation ou menace de violation des dispositions de la présente entente sans devoir déposer un cautionnement ou toute autre garantie.

d. Sur demande de Waste Management, le fournisseur devra certifier par écrit et, sur demande, démontrer à Waste Management qu'il respecte les dispositions présentées dans la présente pièce jointe.

e. Advenant que le fournisseur échoue ou soit incapable de se conformer aux obligations qu'on retrouve énoncées dans cette pièce jointe, il devra aviser rapidement Waste Management qui sera alors autorisée (à son choix et à sa discrétion exclusive) de suspendre le transfert des données de Waste Management, d'exiger du fournisseur qu'il cesse d'utiliser les données en question de Waste Management et/ou de mettre immédiatement fin à l'entente et, dans chacun des cas, sans encourir de responsabilité ou de pénalité et sans être admissible à des frais de résiliation. L'exercice des droits énoncés ci-dessus par Waste Management ne doit pas être considéré comme une violation de l'entente par celle-ci.

© 2020 WM Intellectual Property Holdings, LLC.