Accord sur le Traitement des Données

OBJECTIF ET ORDRE DE PRIORITÉ

Le présent Accord sur le Traitement des Données, ainsi que ses annexes et tout document faisant expressément l'objet d'un renvoi (le « **DPA »**), est réputé faire partie de l'Accord de services conclu entre Iron Mountain et le Client («l'**Accord»**). Les conditions générales de l'Accord s'appliquent et régissent les droits et obligations des parties dans le cadre du présent DPA.

En cas de conflit entre les conditions générales contenues dans le présent DPA et les conditions générales énoncées dans l'Accord, les conditions générales énoncées dans le présent DPA seront réputées être les conditions générales dominantes en ce qui concerne l'objet du présent DPA. Le présent DPA annule et remplace tout Accord antérieur relatif au traitement des données ou toute clause relative à la protection des données ou de la vie privée entre les parties en ce qui concerne les Services fournis dans le cadre de l'Accord .

CONDITIONS GÉNÉRALES

1. DÉFINITIONS

Sauf définition spécifique dans le présent document, tous les termes commençant par une majuscule ont la même signification que celle qui leur est donnée dans l'Accord.

« Contrôleur » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données Personnelles ;

« Données Personnelles du Client » désigne les Données Personnelles appartenant au Client ou à ses affiliés ou collectées par eux, Traitées dans le cadre des Services ;

« Faille de Sécurité » désigne tout dommage, destruction, perte, altération, divulgation non autorisée ou accès non autorisé aux Données Personnelles du Client qu'Iron Mountain, son personnel ou ses sous-traitants traitent dans le cadre de la fourniture des Services ;

« Législation de Protection des Données » désigne toutes les lois et réglementations applicables relatives au Traitement des Données Personnelles qui peuvent exister dans les juridictions concernées, y compris, mais sans s'y limiter, le GDPR de l'UE (Règlement (UE) 2016/679), le GDPR du Royaume-Uni (le GDPR tel qu'applicable dans le cadre du droit interne du Royaume-Uni en vertu de l'article 3 de la loi de 2018 sur l'Union européenne (Retrait) et tel qu'amendé par la Protection des Données , de la Vie Privée et des Communications Electroniques (Modifications etc.) (Sortie de l'UE) Regulation 2019 (tel que modifié)), la loi sur la Protection des Données de 2018, le FADP (la loi Fédérale Suisse sur la Protection des Données), Les Lois sur la Protection de la Vie Privée des États américains, la LGPD (Loi Générale Brésilienne sur la Protection des Données), la PIPL (Loi sur la Protection des Informations Personnelles de la République de Chine) et toute législation et/ou réglementation qui les met en œuvre ou en découle, ou qui modifie, remplace, réédicte ou consolide l'une d'entre elles, y compris, le cas échéant, les orientations et les codes de pratique publiés par les autorités de contrôle ;
« Lois de l'État Américain sur la Protection de la Vie Privée » désigne toutes les lois de l'État Américain sur la protection de la vie privée et des données qui sont applicables au Traitement des Données Personnelles en vertu de l'Accord, y compris, sans s'y limiter, et telles qu'elles peuvent être modifiées, supplantées ou remplacées de temps à autre : (1) la Loi Californienne sur la Protection de la Vie Privée des Consommateurs, telle que modifiée par la Loi Californienne

« **Personne Concernée »** désigne une personne physique identifiée ou identifiable ;

« Services » désigne tous les Services fournis par Iron Mountain ou ses filiales au Client ou à ses affiliés dans le cadre de l'Accord ;

« Sous-traitant » désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des Données Personnelles pour le compte du Contrôleur ;

« Traitement » désigne toute opération ou ensemble d'opérations effectuées sur des Données Personnelles, que ce soit ou non par des moyens automatiques, comme la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre mise à disposition, le rapprochement ou la combinaison, le blocage, l'effacement ou la destruction ;

« Données Personnelles » désigne toute information relative à une Personne Concernée ;

Loi sur les Droits à la Vie Privée, et tout règlement d'application y afférent (ensemble, la « **CCPA** ») ; (2) la Loi sur la Protection de la Vie Privée du Colorado (« **CPA** »), (3) la Loi sur la Protection des Données des Consommateurs de Virginie (« **CDPA** ») ; (4) la Loi sur la Protection de la Vie Privée des Consommateurs de l'Utah (« **UCPA** ») ; et (5) la Loi sur la Protection des Données du Connecticut (« **CTDPA** »).

2. CHAMP D'APPLICATION ET DÉTAILS DU TRAITEMENT DES DONNÉES

2.1 Cet DPA s'applique aux Données Personnelles du Client Traitées par Iron Mountain en tant que Sous-traitant dans le cadre de la fourniture des Services conformément à l'Accord au nom du Client .

2.2 Iron Mountain peut collecter et traiter les Données Personnelles du Client et des employés de ses affiliés en tant que Contrôleur à des fins commerciales légitimes, telles que la gestion des contrats et des relations avec les Clients, et conformément à la Législation sur la Protection des Données et à l'avis de confidentialité d'Iron Mountain disponible sur les sites Web d'Iron Mountain et à d'autres politiques de confidentialité applicables. Les obligations d'Iron Mountain énoncées dans le présent DPA ne s'appliquent pas au traitement de telles Données Personnelles.

2.3 L'objet du Traitement des Données Personnelles est la prestation des Services. Les droits et obligations du Client et d'Iron Mountain sont définis dans le présent DPA. L'Annexe 1 du présent DPA définit la nature, la durée et la finalité du Traitement, les types de Données Personnelles du Client qu'Iron Mountain traite et les catégories de Personnes Concernées dont les Données Personnelles sont Traitées.

2.4 Lorsque Iron Mountain traite les Données Personnelles du Client dans le cadre de la fourniture des Services, Iron Mountain s'engage à :

2.4.1 Traiter les Données Personnelles du Client uniquement en conformité avec les instructions documentées du Client. Si Iron Mountain est tenue de Traiter les Données Personnelles du Client à d'autres fins en vertu de la législation à laquelle Iron Mountain est soumise, Iron Mountain informera d'abord le Client de cette obligation, à moins que cette ou ces lois ne l'interdisent pour des raisons importantes d'intérêt public ; et

2.4.2 Respecter à tout moment la Législation applicable en matière de Protection des Données et informer immédiatement le Client si, de l'avis d'Iron Mountain, une instruction de Traitement des Données Personnelles du Client donnée par ce dernier enfreint la Législation applicable en matière de Protection des Données.

2.5 Les instructions du Client seront contraignantes pour Iron Mountain, à moins que l'exécution des instructions ne nécessite la fourniture d'un service dans le cadre de l'Accord et que le Client n'accepte pas de payer les frais de service pour ces services.

2.6 Iron Mountain doit s'assurer que le personnel appelé à accéder aux Données Personnelles du Client est soumis à un devoir contraignant de confidentialité à l'égard de ces Données Personnelles du Client et prendre des mesures raisonnables pour garantir la fiabilité et la compétence du personnel d'Iron Mountain ayant accès aux Données Personnelles du Client.

3. FOURNIR UNE ASSISTANCE AUX CLIENTS

3.1 Iron Mountain doit fournir une assistance au Client, en tenant toujours compte de la nature du Traitement :

3.1.1 par des mesures techniques et organisationnelles appropriées et, dans la mesure du possible, en remplissant les obligations du Client de répondre aux demandes des Personnes Concernées exerçant leurs droits ;

3.1.2 en garantissant le respect des obligations du Client (telles que la Sécurité du Traitement, la notification d'une violation de Données Personnelles à l'autorité de contrôle, la communication d'une violation de Données Personnelles à la Personne Concernée, l'évaluation de l'impact sur la Protection des Données et la consultation préalable des autorités de contrôle lorsque le traitement entraînerait un risque élevé en l'absence de mesures prises par le Contrôleur pour atténuer le risque), en tenant compte des informations dont dispose Iron Mountain ; et

3.1.3 en mettant à la disposition du Client toutes les informations qu'il demande raisonnablement pour permettre au Client de démontrer que ses obligations en matière de sélection et de désignation d'Iron Mountain ont été respectées.

4. MESURES DE SÉCURITÉ

4.1 En tenant compte des procédures opérationnelles habituelles, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement, Iron Mountain mettra en œuvre des mesures techniques et organisationnelles appropriées et raisonnables conçues pour protéger la confidentialité, l'intégrité et la disponibilité des Données Personnelles du Client et pour protéger les Données Personnelles du Client contre un Traitement non autorisé ou illégal et contre la perte, la destruction, l'endommagement, l'altération ou la divulgation accidentels. Les normes de Sécurité d'Iron Mountain sont énoncées à l'Annexe 2 du présent DPA.

4.2 Il est de la seule responsabilité du Client d'évaluer si ces mesures techniques et organisationnelles répondent à ses besoins.

5. CONFORMITÉ AVEC LES LOIS

Le Client et ses affiliés doivent : (i) Traiter les Données Personnelles du Client conformément à la Législation sur la Protection des Données ; (ii) être autorisés à donner des instructions écrites à Iron Mountain sur le Traitement des Données Personnelles du Client dans le cadre des Services (y compris au nom de toute entité tierce qui est un Contrôleur des Données Personnelles du Client) ; et (iii) conserver à tout moment le contrôle et l'autorité sur les Données Personnelles du Client en ce qui concerne le Traitement.

6. SOUS-TRAITEMENT

6.1 Le Client reconnaît et accepte qu'Iron Mountain puisse engager sa société mère, ses filiales et d'autres sous-traitants tiers (y compris des sous-traitants tiers engagés par les filiales ou la société mère d'Iron Mountain) dans le but de traiter les Données Personnelles du Client en vertu de ce DPA, sous réserve de la clause 6.2 ci-dessous.

6.2 Une liste des sous-traitants agréés par le Client à la date du présent DPA est disponible ici[1]. Iron Mountain peut à tout moment remplacer ou nommer un nouveau sous-traitant, à condition que le Client en soit informé par écrit quinze (15) jours à l'avance et que le Client ne s'oppose pas à ces changements pour des raisons démontrables liées à la protection des Données dans ce délai. Afin de recevoir ces notifications par courriel, le Client doit s'inscrire et gérer tout abonnement existant au service de notification d'Iron Mountain via cette page Web[2].

6.3 Si le Client ne souscrit pas à ce service de notification, Iron Mountain ne sera pas responsable de l'absence de notification du sous-traitant et toutes ces nominations seront considérées comme autorisées par le Client . Si le Client s'oppose par écrit, pour des raisons démontrables liées à la protection des Données, à la nomination d'un remplaçant ou d'un nouveau sous-traitant dans les quinze (15) jours de préavis écrit, Iron Mountain fera des efforts raisonnables pour mettre à la disposition du Client une modification des Services ou recommander une modification de la configuration ou de l'utilisation des Services par le Client, dans chaque cas pour éviter le Traitement des Données Personnelles du Client par le sous-traitant qui s'y oppose, pour examen et approbation par le Client. Si le Client n'approuve pas les modifications proposées par Iron Mountain dans un délai de quinze (15) jours, Iron Mountain peut, en adressant une notification écrite au Client, mettre immédiatement fin au Service ou à la partie du Service qui ne peut être fournie par Iron Mountain sans l'utilisation du sous-Processeur faisant l'objet de l'objection. Cette résiliation s'effectue sans préjudice des droits et obligations des parties, étant entendu qu'aucune indemnité de résiliation, frais ou autre compensation ne sera payable par Iron Mountain ou les filiales d'Iron Mountain dans le cadre de cette résiliation et que le Client prendra rapidement possession des actifs qu'il a fournis à Iron Mountain dans le cadre des Services résiliés, sous réserve des conditions de l'Accord et aux frais et dépenses du Client.

6.4 Iron Mountain doit s'assurer que tout contrat conclu avec des sous-traitants dans le cadre de ce DPA contient des dispositions qui sont, à tous égards importants, identiques à celles de ce DPA et qui sont conformes à la Législation applicable en matière de Protection des Données. Lorsqu'un sous-traitant d'Iron Mountain fait en sorte qu'Iron Mountain ne respecte pas ses obligations en vertu du présent DPA ou de toute Législation applicable en matière de Protection des Données, Iron Mountain demeure entièrement responsable envers le Client de l'exécution des obligations d'Iron Mountain en vertu des présentes conditions.

7. FAILLES DE SÉCURITÉ

7.1 En cas de suspicion de Faille de Sécurité, Iron Mountain s'engage à :

7.1.1 prendre rapidement des mesures pour enquêter sur la Faille de Sécurité présumée et pour identifier, prévenir et atténuer les effets de la Faille de Sécurité présumée et y remédier ;

7.1.2 notifier le Client sans délai excessif dès qu'il a un degré raisonnable de certitude qu'une violation de la Sécurité s'est produite et fournir au Client une description détaillée de la Faille de Sécurité, y compris les informations raisonnablement nécessaires pour que le Client puisse remplir ses obligations de notification en vertu de la Législation sur la Protection des Données.

7.2 Le Client accepte qu'Iron Mountain fournisse les informations visées à la clause 7.1.2 par étapes. Dans les cas où Iron Mountain n'a pas accès ou ne peut pas fournir certaines informations énumérées dans la clause 7.1.2 ou ne peut les fournir au Client, Iron Mountain en informera le Client et Iron Mountain ne sera pas responsable de l'absence de fourniture de ces informations.

---

[1] https://www.ironmountain.com/-/media/files/Utility/Legal/GLOBAL-Personal-Data-Subprocessors-List.xlsx?la=en

[2] https://urldefense.proofpoint.com/v2/url?u=https-3A_reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjl-qYEq5GmWmZcbgd--hgvVuleEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YjbdZ3Yg_2F68&s=xNzeKlzw6XbGZ_IoyLbqEap2144HRDTflVtNiXKr6M4&e=

8. AUDITS

Iron Mountain autorisera le Client et ses auditeurs ou agents autorisés respectifs, moyennant un préavis d'au moins dix (10) jours ouvrables à Iron Mountain, à effectuer des audits ou des inspections pendant la durée du contrat, à condition qu'Iron Mountain ne soit pas tenue de fournir ou d'autoriser l'accès aux informations concernant : (i) d'autres Client d'Iron Mountain ; (ii) tout rapport externe non public d'Iron Mountain ; et (iii) tout rapport interne préparé par l'audit interne ou la fonction de conformité d'Iron Mountain. Les objectifs d'un audit ou d'une inspection en vertu de cette clause se limitent à vérifier qu'Iron Mountain traite les Données Personnelles du Client conformément aux obligations qui lui incombent en vertu du présent DPA. Sauf en cas de Faille de Sécurité, il n'est pas procédé à plus d'un audit de ce type au cours d'une période de douze (12) mois.

9. TRANSFERTS INTERNATIONAUX DE DONNÉES (TRANSFERTS RESTREINTS)

9.1 Dans la mesure où cela est applicable, le Client consent et autorise par la présente les transferts internationaux de ses Données Personnelles vers les entités visées à l'Article 6.2 et conformément à l'Annexe 3 pour la fourniture des Services, et le Client et Iron Mountain en conviennent :

9.1.1 de se conformer à la Législation applicable en matière de Protection des Données en ce qui concerne ces transferts ;

9.1.2 qu'ils ont, en tenant compte, sans limitation, i) des catégories de Données Personnelles du Client , ii) des pays dont les lois nationales peuvent ne pas fournir un niveau de protection des Données Personnelles comparable à celui de la Législation de l'UE/du Royaume-Uni (**« Pays Tiers »**), iii) des mesures techniques et organisationnelles pertinentes énoncées dans la Section 7 et iv) des parties concernées participant au traitement de ces Données Personnelles du Client, ont procédé à une évaluation de l'adéquation du mécanisme de transfert pertinent adopté en vertu des présentes lorsque la loi l'exige et ont déterminé que ce mécanisme de transfert est conçu de manière appropriée pour garantir que les Données Personnelles transférées conformément au présent DPA bénéficient d'un niveau de protection dans le pays de destination qui est essentiellement équivalent à celui garanti en vertu de la Législation sur la Protection des Données.

10. RESPONSABILITÉ ET INDEMNISATION

10.1 Nonobstant toute disposition contraire de l'Accord, en cas de Faille de Sécurité causée directement par un manquement d'Iron Mountain à ses obligations en vertu de ce DPA, Iron Mountain doit rembourser au Client, dans la mesure permise par la loi applicable, les coûts directs, vérifiables, nécessaires et raisonnablement encourus par le Client dans le cadre (a) de l'enquête sur cette Faille de Sécurité,
(b) de la préparation et de l'envoi d'avis aux Personnes Concernées et aux autorités réglementaires, comme l'exige la Législation sur la Protection des Données, (c) de la fourniture de services de surveillance du crédit à ces personnes, comme l'exige la loi, pour une période n'excédant pas douze (12) mois, et (d) du paiement de la partie des amendes, pénalités ou sanctions réglementaires imposées par une autorité de surveillance et pour lesquelles l'autorité de surveillance déclare qu'Iron Mountain est directement responsable.

10.2 Dans le cas où une Personne Concernée dépose une plainte contre l'une ou l'autre ou les deux parties pour violation présumée de la Législation sur la Protection des Données (**« Plaintes de la Personne Concernée »**) lorsque cela est autorisé, chaque partie contrôlera sa propre défense de cette plainte (ou sa partie de la défense) et restera seule responsable de ses propres coûts, dépenses et responsabilités y afférents, y compris les frais juridiques ou tout montant accordé contre elle par un tribunal ou versé par elle dans le cadre d'un Accord de règlement, à condition toutefois que, lorsque chaque partie est responsable d'une partie ou que l'une ou l'autre partie est responsable du montant total des dommages subis par une Personne Concernée pour le même incident ou la même série d'incidents et que la Personne Concernée a obtenu une indemnisation complète de la part d'une seule partie (la **« Partie qui Indemnise »**), la Partie qui Indemnise a le droit de réclamer à l'autre partie la partie de l'indemnisation correspondant au dommage causé par cette autre partie. La partie compensatrice ne peut faire valoir son droit envers l'autre partie que dans les 12 mois suivant l'incident, dans la mesure où la loi applicable le permet.

10.3 Dans toute la mesure permise par les lois applicables, les limitations de responsabilité et les exclusions de dommages énoncées dans l'Accord régissent la responsabilité globale pour toutes les réclamations du Client découlant de ou liées à ce DPA, et/ou à l'Accord contre Iron Mountain. Ces limitations de responsabilité et exclusions de dommages s'appliquent à toutes les réclamations, qu'elles découlent d'un contrat, d'un délit ou de toute autre théorie de responsabilité, et toute référence à la responsabilité d'Iron Mountain signifie la responsabilité globale d'Iron Mountain et de toutes les filiales d'Iron Mountain pour les réclamations du Client et de toutes les autres affiliés du Client. Dans la mesure où les lois applicables l'exigent, la présente section n'a pas pour objet (i) de modifier ou de limiter la responsabilité des parties pour les réclamations des personnes concernées formulées à l'encontre d'une partie en cas de responsabilité conjointe et solidaire, ou (ii) de limiter la responsabilité de l'une ou l'autre des parties de payer les pénalités imposées à cette partie par une autorité de régulation.

10.4 Les Clauses 10.1 à 10.3 constituent le seul et unique recours et la seule responsabilité de chaque partie pour toute perte, tout dommage, toute dépense ou toute responsabilité en rapport avec le présent DPA.

11. DEMANDES DES AUTORITÉS PUBLIQUES

11.1 Dans la mesure où la loi le permet et sous réserve des clauses 11.2 à 11.5 ci-dessous, Iron Mountain accepte d'informer le Client si elle :

11.1.1 reçoit une demande juridiquement contraignante d'une autorité publique, y compris les autorités judiciaires, en vertu des lois du pays de destination pour la divulgation des Données Personnelles du Client transférées en vertu de l'Accord ; ou

11.1.2 a connaissance d'un accès direct par les autorités publiques aux Données Personnelles du Client transférées en vertu de l'Accord, conformément aux lois du pays de destination.

11.2 Si la législation du pays de destination interdit à Iron Mountain d'informer le Client, Iron Mountain s'engage à faire tout son possible pour obtenir une dérogation à cette interdiction, en vue de communiquer le plus d'informations possible, dans les meilleurs délais.

11.3 Iron Mountain s'engage à examiner la légalité de la demande de divulgation, en particulier si elle reste dans le cadre des pouvoirs accordés à l'autorité publique requérante, et à contester la demande si elle conclut qu'il existe des motifs raisonnables de considérer que la demande est illégale en vertu des lois du pays de destination. Elle ne divulgue pas les Données Personnelles du Client demandées tant qu'elle n'est pas tenue de le faire en vertu des règles de procédure applicables.

11.4 Iron Mountain s'engage à fournir le minimum d'informations autorisées lorsqu'elle répond à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

11.5 Iron Mountain s'engage à conserver les informations visées par la présente clause pendant toute la durée de l'Accord et à les mettre à la disposition de l'autorité de contrôle compétente sur demande.

12. DIVERS

12.1 En fonction de la nature des Services fournis par Iron Mountain, à la résiliation/expiration de l'Accord, sur la base des instructions spécifiques du Client et sous réserve des conditions de l'Accord, Iron Mountain supprimera/détruira ou renverra au Client ou à un tiers désigné par le Client toutes les Données Personnelles du Client. Toutes les Données Personnelles du Client contenues dans les actifs du Client stockés par Iron Mountain au nom du Client seront restituées au Client conformément à un plan de sortie ou de transition convenu, et sous réserve des coûts convenus, comme stipulé dans l'Accord ou dans tout autre document contractuel applicable. Dans tous les autres cas, si l'Accord est muet sur la suppression/destruction ou la restitution des Données Personnelles du Client et que le Client ne donne pas d'instructions concernant la suppression/destruction ou la restitution des Données Personnelles du Client dans les quinze (15) jours suivant la résiliation/expiration de l'Accord, Iron Mountain enverra un avis écrit au Client demandant de recevoir dans les quinze (15) jours des instructions spécifiques concernant la suppression/destruction ou la restitution des Données Personnelles du Client et informant le Client de tous les frais de destruction sécurisée ou autres frais applicables payables par le Client. Dans le cas où le Client ne fournirait pas d'instructions écrites dans ce délai de quinze (15) jours et ne paierait pas les frais applicables dans ce même délai, le Client autorise par la présente Iron Mountain à poursuivre le Traitement, la suppression et la destruction de toutes les Données Personnelles du Client après la résiliation de l'Accord, à la discrétion d'Iron Mountain et aux frais du Client.

12.2 Nonobstant la Clause 12.1, Iron Mountain ne manquera pas à ses obligations en ce qui concerne la suppression des Données Personnelles du Client conservées sur des bandes de sauvegarde tant que ces bandes de sauvegarde sont écrasées (et donc les Données Personnelles du Client supprimées) dans le cours normal des affaires.

12.3 À l'exception des Clauses Contractuelles Standards (telles que définies à l'Annexe 3 du présent DPA), le présent DPA et tout litige, réclamation ou controverse découlant du présent DPA ou s'y rapportant, ou la violation, la résiliation ou la validité de celui-ci, sont régis par les dispositions de l'Accord relatives au choix de la loi applicable ; tout litige, controverse ou réclamation découlant du présent DPA ou s'y rapportant sera principalement résolu par le biais de toute procédure de résolution des litiges définie dans le cadre de l'Accord.

12.4 Chaque partie peut notifier à l'autre partie par écrit, de temps à autre, toute modification du présent DPA qu'elle juge raisonnablement nécessaire pour répondre aux exigences de la Législation sur la Protection des Données ou à toute décision d'une autorité de contrôle ou d'un tribunal compétent. Ces modifications ne prendront effet que si et dans la mesure où elles sont énoncées dans un amendement au présent DPA convenu d'un commun accord et signé par les deux parties, sauf si une partie informe l'autre partie d'une nouvelle exigence légale et lui envoie un amendement qui ne comprend que les changements nécessaires et qui peut être accepté sans être formellement approuvé, c'est-à-dire en ne soulevant aucune objection dans un certain délai, sont considérés comme des amendements au présent DPA convenus d'un commun accord.

ANNEXE 1

Détails du Traitement et du Transfert de Données (le cas échéant)

A. LISTE DES PARTIES :

Les parties à cet DPA et les Rôles de l'Exportateur et de l'Importateur de Données sont définis dans l'Accord et dans l'Annexe 3 (Transferts Internationaux de Données), le cas échéant.

B. DESCRIPTION DU TRAITEMENT//TRANSFERT (le cas échéant) :

Catégories de Personnes dont les Données Personnelles sont traitées/transférées :

En fonction de la nature des Services d'Iron Mountain et des activités du Client, ce dernier peut soumettre à Iron Mountain des Données Personnelles appartenant à diverses catégories de Personnes Concernées, dont l'étendue est déterminée et contrôlée par le Client à sa seule discrétion. À ce titre, les catégories de personnes concernées peuvent inclure : les employés actuels et passés, les contractants ou consultants actuels et passés, les contractants ou consultants fournis par une agence et les détachés externes, les demandeurs d'emploi et les candidats, les étudiants et les bénévoles, les personnes identifiées par les employés ou les retraités comme bénéficiaires, conjoints, partenaires domestiques/civils, personnes à charge et contacts d'urgence, les retraités, les administrateurs et dirigeants actuels et passés, les actionnaires, les détenteurs d'obligations, les titulaires de comptes, les utilisateurs finaux/consommateurs (adultes, enfants), les patients (adultes, enfants), les passants (caméras de vidéosurveillance) et les utilisateurs du site Web.

Catégories de Données Personnelles traitées/transférées :

En fonction de la nature des Services d'Iron Mountain et de l'activité du Client, ce dernier peut soumettre à Iron Mountain des Données Personnelles appartenant à diverses catégories de Données Personnelles, dont l'étendue est déterminée et contrôlée par le Client à sa seule discrétion. À ce titre, les catégories peuvent inclure des Données personnelles relatives au Client et/ou à ses propres Client, employés, etc.

Données sensibles transférées (le cas échéant) :

En fonction de la nature des services d'Iron Mountain et de l'activité du Client, ce dernier peut soumettre à Iron Mountain des Données sensibles, dont l'étendue est déterminée et contrôlée par le Client à sa seule discrétion.

Le cas échéant, la fréquence du transfert (par exemple, si les Données sont transférées de manière ponctuelle ou continue) :

Le transfert s'effectue de manière continue.

Nature du traitement :

Collecte, enregistrement, organisation, structuration, stockage, adaptation ou modification, extraction, consultation, utilisation, divulgation par transmission, diffusion ou toute autre forme de mise à disposition, alignement ou combinaison, restriction, effacement ou destruction.

L'objectif du traitement/transfert des Données (le cas échéant) et le Traitement ultérieur :

La fourniture des Services tels que définis dans l'Accord.

Rétention des Données :

Les Données personnelles seront retenues par Iron Mountain pendant toute la durée des Services offerts au Client et jusqu'à ce que les Données personnelles soient renvoyées ou détruites conformément à la clause 10.1 du présent DPA.

Le cas échéant, pour les transferts à des (sous-)traitants, préciser également l'objet, la nature et la durée du traitement :

Pendant la durée de l'Accord avec le Client, les sous-traitants fournissent, entre autres, des services de technologie de l'information (TI) et de conseil, y compris une assistance informatique globale, des rapports sur les événements et des services de gestion.

C. AUTORITÉ DE SURVEILLANCE COMPÉTENTE

Comme indiqué à l'Annexe 3 (Transferts Internationaux de Données), le cas échéant.

ANNEXE 2

LES MESURES TECHNIQUES ET ORGANISATIONNELLES («MESURES DE SÉCURITÉ»)

1. PROGRAMME ET POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Iron Mountain doit maintenir un programme de Sécurité de l'information comportant des contrôles physiques, techniques et administratifs appropriés, conçus pour répondre aux normes de l'industrie. Le programme de Sécurité de l'information comprend :

1.1 La documentation, la publication interne et la communication des politiques, normes et procédures d'Iron Mountain en matière de Sécurité de l'information ;

1.2. Attribution claire et documentée de la responsabilité et de l'autorité pour l'établissement et le maintien du programme de Sécurité de l'information ;

1.3 Test régulier des contrôles clés, des systèmes et des procédures du programme de Sécurité de l'information ;

1.4 Des mesures administratives, techniques et opérationnelles conçues pour protéger toutes les Données Personnelles du Client en utilisant les pratiques, procédures et processus décrits dans la présente Annexe sur la Sécurité, dans la mesure où ils sont pertinents et applicables au format dans lequel les Données Personnelles du Client sont conservées.

2. ÉVALUATION DES RISQUES

Iron Mountain maintient un programme d'évaluation des risques de Sécurité de l'information conçu pour identifier et évaluer les risques et vulnérabilités internes et externes raisonnablement prévisibles qui pourraient affecter la sécurité, la confidentialité et/ou l'intégrité des Données Personnelles du Client. Iron Mountain évaluera et mettra à jour, si nécessaire, raisonnable et approprié, l'efficacité du programme de Sécurité de l'information actuel pour limiter ces risques, sur une base annuelle, ou à chaque fois qu'il y a un changement important dans les risques ou les vulnérabilités des Données Personnelles du Client.

3. GESTION DES MOYENS DE TRAITEMENT DE L'INFORMATION ET DES SUPPORTS PHYSIQUES

3.1 Gestion des actifs de traitement de l'information. Iron Mountain a mis en place un programme de gestion de l'inventaire des actifs afin de gérer les contrôles physiques, techniques et administratifs des actifs de traitement de l'information d'Iron Mountain (ordinateurs, serveurs, dispositifs de stockage, réseaux de communication, ordinateurs personnels, ordinateurs portables et dispositifs périphériques).
Le programme de gestion de l'inventaire des actifs comprend les éléments suivants :

3.1.1 Attribution documentée de la propriété des actifs au personnel d'Iron Mountain afin de garantir la classification appropriée des informations, la détermination des restrictions d'accès et l'examen des contrôles d'accès.

3.1.2 Assainissement des biens avant leur élimination conformément à la norme NIST 800- 88.

3.1.3 Obligation d'obtenir l'autorisation de la direction avant de retirer des locaux d'Iron Mountain un équipement ou un logiciel qui n'est pas attribué à une personne spécifique.

3.2 Contrôles. Les contrôles d'Iron Mountain comprennent les éléments suivants :

3.2.1 Procédures opérationnelles et contrôles techniques conçus pour protéger les documents, les supports informatiques, les Données d'entrée/sortie/de sauvegarde et la documentation du système contre toute divulgation, modification ou destruction non autorisée.

3.2.2 Procédures d'élimination sécurisée des supports électroniques ou physiques contenant des Données Personnelles du Client.

3.2.3 Un processus établi pour suivre tous les supports physiques du Client depuis la garde initiale par Iron Mountain jusqu'au retrait permanent ou à la destruction.

4. MESURES DE SÉCURITÉ DU PERSONNEL

4.1 Confidentialité. Iron Mountain doit raisonnablement exiger que tous les employés d'Iron Mountain, y compris les employés temporaires et contractuels, acceptent de préserver la confidentialité des Données Personnelles du Client et de se conformer aux exigences internes d'Iron Mountain en matière de Sécurité de l'information et d'utilisation acceptable.

4.2 Politique d'enquête sur les antécédents. Iron Mountain a mis en place une politique d'enquête sur les antécédents et de dépistage des drogues (aux États-Unis uniquement) pour ses employés. Iron Mountain continuera à maintenir ces politiques pendant la durée de l'Accord. Les exigences de la politique comprennent, sans s'y limiter, le dépistage de drogues (uniquement aux États-Unis), la vérification de l'identité du personnel, la recherche de casiers judiciaires, la vérification de l'emploi, la recherche de listes de surveillance gouvernementales/terroristes, ainsi que la vérification de l'éducation de certains employés, le permis de conduire et l'historique des infractions pour les candidats conducteurs et les conducteurs existants. Lorsque des informations désobligeantes sont identifiées lors d'une vérification des antécédents, Iron Mountain procède à une évaluation individualisée, conformément à la législation du travail et aux meilleures pratiques en vigueur.

4.3 Travailler avec les sous-traitants. Iron Mountain exigera de tout sous-traitant fournissant des Services dans le cadre de l'Accord qu'il se conforme à des restrictions similaires à celles énoncées dans le présent Article en ce qui concerne le personnel du sous-traitant qui fournira des Services dans le cadre de l'Accord impliquant le Traitement des Données Personnelles du Client.

4.4 Formation de sensibilisation à la sécurité. Au moins une fois par an, Iron Mountain organise une formation générale de sensibilisation à la Sécurité et une formation spécifique à la Sécurité en fonction du rôle de chacun pour tous les employés d'Iron Mountain ayant accès aux Données Personnelles du Client. Iron Mountain tient des registres indiquant les noms de ces employés d'Iron Mountain

qui ont participé à la formation et la date de chaque formation de sensibilisation à la sécurité. Iron Mountain doit régulièrement revoir et mettre à jour son programme de formation à la sensibilisation à la sécurité.

4.5 Renvoi du personnel d'Iron Mountain. Iron Mountain applique une procédure disciplinaire à ses employés qui ne respectent pas les exigences de sécurité énoncées dans le présent document.

4.6 Cessation de l'Accès en cas de Licenciement/Réaffectation. En cas de licenciement ou de réaffectation à un rôle ne nécessitant pas l'accès aux Données Personnelles du Client, l'accès d'un employé d'Iron Mountain aux Données Personnelles du Client doit être révoqué dans les plus brefs délais.

5. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

5.1 Contrôles de Sécurité Physique. Les installations d'Iron Mountain utilisent des contrôles physiques qui limitent raisonnablement l'accès aux Données Personnelles du Client, y compris, si Iron Mountain le juge approprié, des protocoles de contrôle d'accès, des barrières physiques telles que des installations et des zones verrouillées, des badges d'accès pour les employés, des registres de visiteurs, des badges d'accès pour les visiteurs, des lecteurs de cartes, des caméras de vidéosurveillance et des alarmes de détection d'intrusion. Tous les visiteurs doivent s'inscrire et être accompagnés à tout moment.

5.2 Utilitaires de soutien. Iron Mountain doit prendre des mesures pour protéger ses installations contenant les Données Personnelles du Client et ses systèmes contre les pannes d'électricité, de télécommunications, d'approvisionnement en eau, d'égouts, de chauffage, de ventilation et de climatisation, le cas échéant.

5.3 Sécurité Du Système De Transmission. Iron Mountain doit prendre des mesures pour protéger la sécurité physique de son infrastructure de réseau et de ses systèmes de télécommunication contre l'interception et l'endommagement des transmissions.

5.4 Équipement Hors Site. Dans le cas où Iron Mountain sous-traite des fonctions nécessitant l'utilisation d'équipements hors site pour la fourniture de services, tout équipement hors site stockant les Données Personnelles du Client sera protégé par des mesures de Sécurité équivalentes à celles utilisées pour l'équipement sur site utilisé dans le même but.

5.5 Accès Physique aux Moyens de Traitement de l'Information. Iron Mountain doit conserver pendant un an les dossiers des employés d'Iron Mountain autorisés à avoir un accès physique aux environnements informatiques contrôlés par Iron Mountain et utilisés par Iron Mountain pour fournir des Services et, à la demande du Client en cas de Faille de Sécurité, et sous réserve des politiques de Sécurité d'Iron Mountain, permettre au Client de consulter les dossiers vérifiables de ces employés d'Iron Mountain.

5.6 Accès Physique Restreint. Iron Mountain doit limiter l'accès physique aux installations contrôlées par Iron Mountain qui Traitent les Données Personnelles du Client aux employés d'Iron Mountain et aux personnes autorisées qui ont besoin de cet accès pour des raisons professionnelles. Iron Mountain doit disposer d'une procédure d'approbation pour autoriser et suivre les demandes d'accès physique à ces installations.

5.7 Réparations et Modifications. Iron Mountain doit consigner toutes les réparations et modifications liées à la Sécurité apportées aux composants physiques, y compris le matériel, les murs, les portes et les serrures des zones sécurisées au sein des installations où sont stockées les Données Personnelles du Client.

5.8 Registre. Tenir un registre des mouvements du matériel et des supports électroniques et de toute personne responsable de ces mouvements.

6. GESTION DES OPÉRATIONS DE COMMUNICATION ET DE TRAITEMENT DE L'INFORMATION

6.1 Normes de Configuration des Dispositifs. Iron Mountain doit créer, mettre en œuvre et maintenir des procédures d'administration des systèmes qui répondent aux normes de l'industrie, y compris, mais sans s'y limiter, le durcissement des systèmes, l'application de correctifs aux systèmes et aux appareils (système d'exploitation et applications) et l'installation et la mise à jour adéquates de l'antivirus.

6.2 Contrôle des modifications dans les systèmes de traitement de l'information. Iron Mountain doit disposer d'une procédure formelle interne de demande de gestion des modifications pour les systèmes de traitement de l'information et les réseaux de communication, et les demandes de modification d'Iron Mountain doivent être documentées, testées et approuvées avant la mise en œuvre de toute nouvelle capacité de traitement de l'information ou de communication en réseau, de tout correctif de système ou de toute modification apportée aux systèmes existants.

6.3 Séparation des tâches. Iron Mountain doit séparer les tâches et les domaines de responsabilité de manière à ce qu'aucune personne ne soit seule à pouvoir modifier les systèmes de traitement de l'information qui accèdent aux Données Personnelles du Client.

6.4 Séparation des Environnements de Développement et de Production. Les environnements de développement, de test et de production des systèmes de traitement de l'information d'Iron Mountain doivent être séparés logiquement ou physiquement.

6.5 Gestion de l'Architecture Technique. Iron Mountain doit mettre en place un processus de gestion de la configuration pour définir, gérer et contrôler les composants du système de traitement de l'information utilisés pour fournir les Services et l'infrastructure technique de ces composants.

6.6 Détection des Intrusions. Iron Mountain doit surveiller en permanence les systèmes et processus informatiques pour détecter les tentatives d'intrusion ou de violation de la sécurité, qu'elles soient réelles ou non, et informer le Client de tout accès non autorisé aux Données Personnelles du Client.

6.7 Sécurité du Réseau. Iron Mountain doit garantir la mise en place des éléments suivants :

- 6.7.1 En ce qui concerne les environnements hébergés par Iron Mountain et utilisés pour fournir les services, les événements d'alerte des systèmes de détection d'intrusion (« IDS ») et des capteurs de prévention d'intrusion (« IPS ») sont enregistrés et font l'objet de rapports quotidiens (collectivement appelés « IDS/IPS ») ;
- 6.7.2 En ce qui concerne les environnements hébergés par Iron Mountain et utilisés pour fournir les services, les IDS/IPS sont mis à jour au moins une fois par semaine, mais dès que possible après la réception des mises à jour, et les dernières signatures de menaces ou règles sont exécutées rapidement ;
- 6.7.3 Les ports à haut risque des systèmes orientés vers l'extérieur ne sont pas accessibles depuis l'internet ;
- 6.7.4 Les connexions au réseau d'Iron Mountain sont enregistrées et consignées dans des fichiers journaux ;

6.7.5 Déploiement d'un ou de plusieurs pare-feu conçus pour protéger et inspecter l'ensemble du trafic entrant et sortant des services de réseau entre des points de réseau définis ;

6.7.6 Des politiques de renforcement pour définir les ports réseau entrants et sortants ou le trafic de service pour tous les systèmes appartenant à Iron Mountain ou gérés par Iron Mountain qui sont documentés et autorisés dans le cadre du programme de sécurité de l'information ;

6.7.7 Des ports de réseau et de diagnostic correctement sécurisés ; et

6.7.8 Des politiques, procédures et contrôles techniques conçus pour prévenir, détecter et supprimer les codes malveillants ou les attaques connues sur les systèmes d'information d'Iron Mountain.

6.8 Références d'Authentification Cryptées. Iron Mountain doit veiller à ce que les données d'authentification transmises sur les appareils du réseau d'Iron Mountain soient cryptées en cours de route.

6.9 Administration d'un Réseau Sécurisé. Les réseaux d'Iron Mountain doivent être gérés et contrôlés de manière raisonnable afin de les protéger contre les menaces connues et de maintenir la sécurité de toutes les applications et données gérées par Iron Mountain sur le réseau ou en transit sur le réseau. Des contrôles techniques et des protocoles de communication sécurisés doivent être mis en œuvre pour interdire les connexions non restreintes à des réseaux non fiables ou à des serveurs accessibles au public.

6.10 Protection Antivirus. Iron Mountain doit mettre en œuvre et maintenir un programme de gestion anti-virus, comprenant une protection contre les logiciels malveillants, des fichiers de signatures à jour ou une protection alternative contre les menaces émergentes, des correctifs et des définitions de virus, pour les serveurs et les postes de travail gérés par Iron Mountain et utilisés pour héberger ou accéder aux Données Personnelles du Client.

6.11 Site Web - Cryptage du client. Iron Mountain doit s'assurer que pour chacun de ses sites Web, le protocole SSL (Technologie de chiffrement de Données) est activé et contient un certificat SSL valide nécessitant des contrôles de confidentialité, d'authentification ou d'autorisation.

6.12 Sauvegarde de l'Information. Iron Mountain doit créer des copies de sauvegarde appropriées des fichiers du système. En outre, Iron Mountain doit élaborer et maintenir des procédures de reprise après sinistre, voir la section "Reprise après sinistre" ci-dessous pour plus de détails.

6.13 Informations Électroniques en Transit. Iron Mountain doit utiliser un algorithme de cryptage standard avec une longueur de clé de 128 bits minimum pour protéger les Données Personnelles du Client transmises sur des réseaux publics lorsqu'elles proviennent de l'infrastructure hébergée par Iron Mountain.

6.14 Contrôles Cryptographiques. Iron Mountain doit suivre une politique documentée sur l'utilisation des contrôles cryptographiques. Les contrôles cryptographiques d'Iron Mountain doivent :

6.14.1 Être conçus pour protéger raisonnablement la confidentialité et l'intégrité des Données Personnelles du Client traitées, transmises ou stockées par Iron Mountain dans tout environnement de réseau partagé, conformément aux termes de l'Accord ;

6.14.2 Être appliquées, dans le(s) environnement(s) hébergé(s) par Iron Mountain et utilisé(s) pour fournir des services, aux Données Personnelles du Client en transit sur ou vers des réseaux "non fiables" (c'est-à-dire des réseaux qu'Iron Mountain ne contrôle pas légalement), y compris ceux utilisés pour envoyer des Données au réseau d'entreprise du Client à partir du réseau d'Iron Mountain, sous réserve, dans chaque cas, de la coopération du Client dans la gestion des clés de cryptage nécessaires pour décrypter les transmissions reçues par le Client ; et

6.14.3 Inclure des pratiques documentées de gestion des clés de chiffrement afin d'assurer la sécurité des technologies cryptographiques.

6.14.4 Inclure le cryptage de toutes les Données Personnelles du Client sur les ordinateurs portables ou autres appareils portables.

6.15 Exigences d'Enregistrement. Iron Mountain veille à ce que les éléments suivants soient respectés :

6.15.1 Les événements importants liés à la Sécurité et aux systèmes sont consignés et examinés ;

6.15.2 Les journaux d'audit sont conservés pendant au moins un an pour les systèmes dans le\les environnement(s) hébergé(s) par Iron Mountain et utilisé(s) par Iron Mountain pour fournir des services ;

6.15.3 Les journaux d'audit du système sont examinés pour détecter les anomalies ; et

6.15.4 Les installations et les informations des systèmes d'enregistrement sont raisonnablement protégées contre la falsification et l'accès non autorisé.

6.16 Synchronisation du Temps en Réseau. Iron Mountain doit synchroniser les horloges de tous les systèmes de traitement de l'information à l'aide d'une source de temps commune faisant autorité.

6.17 Ségrégation sur les Réseaux. Iron Mountain doit séparer de manière appropriée les groupes de services d'information, d'utilisateurs et de systèmes d'information connexes sur les réseaux.

7. CONTRÔLE D'ACCÈS

7.1 Politique de Contrôle d'Accès. Iron Mountain maintient des politiques de contrôle d'accès concernant les actifs de traitement de l'information qu'Iron Mountain approuve, publie et met en œuvre de manière formelle.

7.2 Autorisation d'Accès Logique. Iron Mountain dispose d'une procédure d'approbation pour les demandes d'accès logique aux Données Personnelles du Client et les demandes d'accès aux systèmes d'Iron Mountain dédiés à l'utilisation des Services.

7.3 Contrôle d'Accès et Vérification de l'Accès. Iron Mountain n'accordera l'accès aux Données Personnelles du Client qu'aux employés actifs d'Iron Mountain, y compris les employés temporaires et contractuels, et aux comptes d'utilisateurs actifs qui ont besoin d'un tel accès pour exercer leurs fonctions. Tous les accès privilégiés doivent être examinés et confirmés pour être cohérents avec le rôle actuel du poste et documentés au moins une fois par trimestre.

7.4 Contrôle de l'Accès des Tiers. Avant d'accorder à des tiers l'accès aux systèmes d'information d'Iron Mountain ayant accès aux Données Personnelles du Client, Iron Mountain doit s'assurer que des contrôles appropriés sont en place.

7.5 Contrôle d'Accès aux Systèmes d'Exploitation. Iron Mountain doit contrôler l'accès aux systèmes d'exploitation (qu'ils soient logiciels ou matériels) en exigeant un processus de connexion sécurisé qui identifie de manière unique la personne qui accède au système d'exploitation.

7.6 Appareils Informatiques Mobiles. Iron Mountain disposera d'une politique ou d'une procédure visant à protéger les appareils informatiques mobiles d'Iron Mountain contre tout accès non autorisé. Ces politiques ou procédures portent sur la protection physique, le contrôle d'accès et les contrôles de sécurité tels que le cryptage, la protection contre les virus et la sauvegarde des appareils.

7.7 Isolation des Systèmes Client. Iron Mountain doit, dans son (ses) environnement(s) hébergé(s) utilisé(s) pour fournir les Services, séparer logiquement et isoler les Données Personnelles du Client de toute autre information.

7.8 Comptes. Iron Mountain doit prendre les mesures suivantes en ce qui concerne les comptes :

7.8.1 Exiger l'authentification de l'identité de chaque employé d'Iron Mountain qui souhaite accéder aux systèmes d'Iron Mountain qui traitent les Données Personnelles du Client et interdire l'utilisation de comptes d'utilisateurs partagés ou de comptes d'utilisateurs avec des identifiants génériques (c'est-à-dire des Identifiants) pour accéder aux Données Personnelles du Client ou aux systèmes.

7.8.2 Exiger que tous les identifiants de comptes d'utilisateurs, y compris les comptes privilégiés, soient directement liés à une personne (par opposition à un poste).

7.8.3 Si les comptes d'administration par défaut ne sont pas désactivés ou supprimés, exiger l'utilisation de mots de passe temporaires, d'identifiants d'extraction ou de contrôles similaires pour l'accès aux comptes d'administration par défaut.

7.8.4 Exiger que les comptes ordinaires inactifs soient verrouillés ou désactivés après 90 jours d'inactivité.

7.8.5 Interdire l'accès à un compte à la suite de multiples tentatives d'accès infructueuses.

7.8.6 Exiger des identifiants uniques et des mots de passe robustes comprenant, au minimum, les éléments suivants : un nombre minimal de 8 caractères, un changement tous les 90 jours et des exigences en matière de complexité.

7.8.7 Interdire aux employés de partager ou de noter leurs mots de passe.

7.9 Contrôles pour les systèmes sans surveillance. Iron Mountain doit utiliser un économiseur d'écran protégé par un mot de passe pour tous les systèmes laissés sans surveillance et qui n'ont connu aucune activité pendant 30 minutes.

8. ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DE SYSTÈMES D'INFORMATION

8.1 Sécurité du Développement des Systèmes. Iron Mountain doit veiller à ce que la sécurité fasse partie intégrante du développement et de l'exploitation de tous les systèmes d'information et doit publier et respecter des méthodes de codage sécurisées internes basées sur des normes de sécurité pour le développement d'applications.

8.2 Gestion de la Sécurité des Logiciels. Les systèmes d'information d'Iron Mountain (y compris les systèmes d'exploitation, l'infrastructure, les applications commerciales, les services et les applications développées par les utilisateurs) doivent être conçus de manière à respecter les normes de sécurité de l'information.

8.3 Diagrammes de Réseau. Iron Mountain doit élaborer, documenter et tenir à jour des diagrammes physiques et logiques des dispositifs de mise en réseau et du trafic.

8.4 Évaluation de la Vulnérabilité des Applications/Piratage Éthique. Iron Mountain doit, au moins une fois par an, évaluer la vulnérabilité des applications dans son ou ses environnements hébergés utilisés pour fournir des services qui traitent les Données Personnelles du Client. Les résultats détaillés sont des informations confidentielles et exclusives d'Iron Mountain et ne seront pas fournis.

8.5 Vérification et Examen des Modifications. Iron Mountain doit vérifier et tester les modifications apportées aux applications et aux systèmes d'exploitation avant leur déploiement afin de s'assurer qu'il n'y a pas d'effet négatif sur les Données Personnelles du Client ou sur les systèmes.

9. REPRISE APRÈS SINISTRE

Iron Mountain doit maintenir un plan de reprise après sinistre, y compris la réplication des systèmes et des Données électroniques utilisés pour soutenir les Services dans un centre de Données de secours. La réplication des systèmes et des données électroniques n'inclut pas les Données Personnelles du Client qui sont physiquement stockées dans une installation d'Iron Mountain. Iron Mountain maintiendra un plan de continuité des affaires pour restaurer les fonctions critiques de l'entreprise. Iron Mountain effectuera des tests de reprise après sinistre au moins une fois tous les douze (12) mois.

10. AUDITS ET ÉVALUATIONS EXTERNES

Les protocoles de sécurité d'Iron Mountain sont conçus pour être conformes aux normes industrielles. Iron Mountain fournira au Client tout rapport d'audit indépendant commandé par une tierce partie (par exemple, PCI, ISO27001, SOC2, etc.) concernant les Services dans la région où ces Services sont fournis (« Rapport d'audit »). Iron Mountain fournira tous les rapports de ce type commandés en vue d'être orientés vers le Client, quels que soient les résultats du rapport. Iron Mountain ne sera pas tenue de fournir les résultats de l'audit interne ou d'autres évaluations indépendantes qui ont été commandées dans l'intention de rester confidentielles pour Iron Mountain. Le Client et

ses auditeurs externes recevront, sur demande, des copies du Rapport d'Audit. Tout Rapport d'Audit ou autre résultat généré par les tests ou audits requis par cette section sera considéré comme une information confidentielle d'Iron Mountain. Le Client doit avoir le droit de fournir une copie de ce Rapport d'Audit à tous les client ou régulateurs concernés du Client, sous réserve de dispositions de confidentialité aussi restrictives que celles contenues dans le présent document. À la demande du Client, Iron Mountain doit confirmer par écrit qu'aucun changement n'a été apporté aux politiques, procédures et contrôles internes pertinents depuis l'achèvement d'un tel Rapport d'Audit, sans dépasser trois mois à compter de la fin de la période de déclaration du Rapport d'Audit.

ANNEXE 3

Transferts Internationaux de Données

1. DÉFINITIONS

« **Clauses Contractuelles Standard de l'UE 2021** » désigne les Clauses Contractuelles Standard pour le transfert de Données Personnelles vers des pays tiers conformément au GDPR, adoptées par la Commission Européenne en vertu de la décision d'exécution de la Commission (UE) 2021/914, disponible ici[3].

« **2022 Addendum du Royaume-Uni** » désigne le modèle d'Addendum B.1.0 publié par le Bureau du Commissaire à l'Information du Royaume-Uni et déposé devant le Parlement conformément à l'Article 119A de la Loi de 2018 sur la Protection des Données le 2 février 2022, tel qu'il peut être révisé en vertu de l'Article 18 de cette Loi, disponible ici[4].

« **Données Personnelles du Client de l'UE** » désigne le traitement des Données Personnelles du Client auquel les lois sur la protection des Données de l'Union Européenne, ou d'un État membre de l'Union Européenne ou de l'Espace Économique Européen, s'appliquaient avant leur traitement par Iron Mountain ;

« Zone protégée » désigne :

i. dans le cas des Données Personnelles du Client de l'UE, les États membres de l'Union Européenne et de l'Espace Économique Européen, ainsi que tout pays, territoire, secteur ou organisation internationale à l'égard desquels une décision d'adéquation est en vigueur en vertu de l'article 45 du RGPD ;

ii. dans le cas des Données Personnelles du Client du Royaume-Uni, le Royaume-Uni et tout pays, territoire, secteur ou organisation internationale à l'égard duquel une décision d'adéquation est en vigueur en vertu de la réglementation du Royaume-Uni en matière d'adéquation ;

iii. dans le cas de Données personnelles de Client Suisses, tout pays, territoire, secteur ou organisation internationale reconnu(e) comme adéquat(e) par le droit Suisse ;

iv. dans le cas de toute autre Donnée Personnelle du Client transférée hors d'une juridiction offrant des protections similaires à celles des Données Personnelles du Client de l'UE, du Royaume-Uni ou de la Suisse, tout pays, territoire, secteur ou organisation internationale reconnu(e) comme adéquat(e) par les lois de cette juridiction ;

« **Clauses contractuelles standard** » désigne collectivement les Clauses Contractuelles Standard de l'UE de 2021 et l'Addendum du Royaume-Uni de 2022.

« Données Personnelles du Client Suisses » désigne le traitement des Données Personnelles du Client auxquelles les lois Suisses sur la protection des Données étaient applicables avant leur traitement par Iron Mountain ;

« Données Personnelles du Client du Royaume-Uni » désigne le traitement des Données Personnelles du Client auxquelles les lois sur la protection des Données du Royaume-Uni s'appliquaient avant leur traitement par Iron Mountain ;

2. DIVERS

2.1 La présente Annexe 3 comprend les Parties suivantes : (i) Partie A - Transferts de Données Personnelles du Client de l'UE ; (ii) Partie B - Transferts de Données personnelles du Client Suisses ; (iii) Partie C - Transfert de Données personnelles du Client du Royaume-Uni, qui s'appliquent, le cas échéant, au transfert de Données Personnelles du Client par Iron Mountain dans le cadre de ses services.

2.2 Les Clauses Contractuelles Standard s'appliquent à Iron Mountain et à ses filiales en tant « qu'importateurs de données » et au Client et à ses affiliés en tant « qu'exportateurs de données. »

2.3 La signature et la date de l'Accord constituent toutes les signatures et dates nécessaires pour les Clauses Contractuelles Standard.

2.4 Si les parties transfèrent les Données Personnelles des Client de l'UE, du Royaume-Uni ou de la Suisse en dehors de la Zone protégée et qu'une décision pertinente de la Commission Européenne ou une autre méthode d'adéquation valide en vertu de la Législation sur la Protection des Données applicable sur laquelle Iron Mountain s'est appuyée pour le transfert de Données est jugée invalide, ou qu'une autorité de contrôle exige que les transferts de Données Personnelles effectués conformément à une telle décision soient suspendus, les parties coopéreront et faciliteront l'utilisation d'un mécanisme de transfert alternatif. Les parties conviennent également que les garanties appropriées utilisées pour faciliter les transferts internationaux dans la présente Annexe 3 ne sont pas exclusives et que les parties peuvent mettre en place des mécanismes de transfert supplémentaires, tels que l'Accord UE-États-Unis. Cadre de Confidentialité des Données.

PARTIE A - TRANSFERTS DE DONNÉES PERSONNELLES DU CLIENT DE L'UE

Si et dans la mesure où le Client ou ses Affiliés transfèrent à Iron Mountain ou à ses Filiales des Données Personnelles du Client de l'UE en dehors de la zone protégée dans le cadre des Services fournis par Iron Mountain en vertu de l'Accord, la présente Partie A de l'Annexe 3 s'applique, et les Parties conviennent de ce qui suit :

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

1. **Sélection de Clauses Contractuelles Standard.** Le texte du DEUXIÈME MODULE des Clauses Contractuelles Standard de l'UE 2021 s'applique lorsque le Client ou l'une de ses Affiliés est un Contrôleur et qu'Iron Mountain ou l'une de ses Filiales est un Processeur ; le texte du TROISIÈME MODULE des Clauses Contractuelles Standard de l'UE 2021 s'applique lorsque le Client ou l'un de ses Affiliés est un Processeur et qu'Iron Mountain ou l'une de ses Filiales est un sous-Processeur. Les dispositions pertinentes contenues dans les Clauses Contractuelles Standard de l'UE 2021 sont incorporées par référence dans le présent DPA et en font partie intégrante. Aucun autre module ni aucune clause marquée comme facultative dans les Clauses Contractuelles Standard de l'UE 2021 ne s'applique. Les informations nécessaires aux fins des appendices des Clauses Contractuelles Standard de l'UE 2021 figurent à l'Annexe 1 - Description du Traitement/Transfert, à l'Annexe 2 - Mesures Techniques et Organisationnelles, et à la Clause 6.2 du RGPD - Liste des sous-processeurs.

2. **Utilisation de Sous-Processeurs.** Aux fins de la clause 9 des Clauses Contractuelles Standard de l'UE 2021, option 2 (Autorisation Écrite Générale) relative à l'utilisation de sous-processeurs pour l'exécution des Services s'applique. Le Client reconnaît et accepte qu'Iron Mountain puisse engager de nouveaux sous-processeurs par le biais du mécanisme convenu dans la clause 6 de ce DPA et que le délai pour soumettre des demandes de changement de sous-processeurs soit de quinze (15) jours.

3. **Droit applicable et choix du forum.** Aux fins de la clause 17 des Clauses Contractuelles Standard de l'UE 2021 (Droit applicable), l'option 2 du droit applicable s'applique, et les présentes clauses sont régies par le droit de l'État Membre de l'UE dans lequel l'exportateur de Données est établi, dans la mesure où il autorise les droits des tiers bénéficiaires. Aux fins de la clause 18 des Clauses Contractuelles Standard de l'UE 2021 (élection de forum et de juridiction), il s'agit des tribunaux de l'État membre de l'UE dans lequel l'exportateur de Données est établi.

4. **Certification de la suppression.** Aux fins des clauses 8.5 et 16(d) des Clauses Contractuelles Standard de l'UE 2021, Iron Mountain ne fournira au Client un certificat de suppression des Données personnelles que sur demande écrite de ce dernier.

5. **Violations de données personnelles.** Aux fins de la clause 8.6(c) des Clauses Contractuelles Standard de l'UE 2021, les violations de données personnelles sont traitées conformément au mécanisme convenu dans la clause 7 du DPA.

6. **Audits.** Aux fins de la clause 8.9 des Clauses Contractuelles Standard de l'UE 2021, les audits de ces clauses sont effectués conformément au mécanisme d'audit convenu dans l'Accord .

7. **Réclamations.** Aux fins de la clause 11 des Clauses Contractuelles Standard de l'UE 2021, Iron Mountain informera le Client si elle reçoit une plainte d'une Personne Concernée relative aux Données Personnelles d'un Client de l'UE et communiquera la plainte au Client conformément au mécanisme convenu dans l'Accord.

8. **Autorité de surveillance.** Pour les Clauses Contractuelles Standard de l'UE 2022, l'autorité de surveillance compétente est déterminée conformément à la clause 13 des Clauses Contractuelles Standard de l'UE.

PARTIE B - TRANSFERTS DE DONNÉES PERSONNELLES DE CLIENT SUISSES

Si et dans la mesure où le Client ou ses Affiliés transfèrent des Données Personnelles du Client Suisse en dehors de la zone protégée à Iron Mountain ou à ses Filiales dans le cadre des Services fournis par Iron Mountain en vertu de l'Accord, la présente Partie B de l'Annexe 3 s'applique, et les Parties conviennent de ce qui suit :

1. **Sélection de Clauses Contractuelles Standard.** Les Clauses Contractuelles Standard de l'UE 2021 et les dispositions pertinentes de la Partie A s'appliquent lorsque le Client ou l'une de ses Affiliés est un contrôleur et qu'Iron Mountain ou l'une de ses Filiales est un Processeur, et/ou lorsque le Client ou l'une de ses Affiliés est un Processeur et qu'Iron Mountain ou l'une de ses Filiales est un sous-processeur, à l'exception de ce qui suit :

   a. l'autorité de surveillance compétente en vertu de la Clause 13 des Clauses Contractuelles Standard de l'UE 2021 est la Commission Fédérale Suisse de la Protection des Données et de l'Information ;

   b. le droit applicable aux réclamations contractuelles en vertu de la clause 17 des Clauses Contractuelles Standard de l'UE 2021 est le droit Suisse et le lieu de juridiction pour les actions entre les parties en vertu de la clause 18 (b) est les tribunaux Suisses.

2. Les références au GDPR de l'UE dans les Clauses Contractuelles Standard de l'UE 2021 doivent être comprises comme des références au FADP.

3. Le terme « État membre » figurant dans les Clauses Contractuelles Standard de l'UE 2021 ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité de faire valoir leurs droits dans leur lieu de résidence habituelle (Suisse) conformément à la Clause 18 (c), des Clauses Contractuelles Standard de l'UE 2021.

PARTIE C - TRANSFERTS DE DONNÉES PERSONNEL CONCERNANT LES CLIENTS DU ROYAUME-UNI

Si et dans la mesure où le Client ou ses Affiliés transfèrent des Données personnelles du Royaume-Uni en dehors de la zone protégée à Iron Mountain ou à ses Filiales dans le cadre des Services fournis par Iron Mountain en vertu de l'Accord, la présente Partie C de l'Annexe 3 s'applique et les Parties conviennent de ce qui suit :

1. **Sélection de Clauses Contractuelles Standard.** Les Clauses Contractuelles Standard de l'UE 2021, les dispositions pertinentes de la Partie A et l'Addendum du Royaume-Uni 2022 s'appliquent lorsque le Client ou l'un de ses Affiliés est un Contrôleur et qu'Iron Mountain ou l'une de ses Filiales est un Processeur, et/ou lorsque le Client ou l'un de ses Affiliés est un Processeur et qu'Iron Mountain ou l'une de ses Filiales est un sous-processeur.

2. **Partie 1 : Tableau 1 - 3 de l'Addendum 2022 du Royaume-Uni :** Informations sur les Parties - Tableau 1 ; Sélection de SCC, de Modules et de Clauses Sélectionnées ; et informations sur les Appendices, y compris l'Annexe 1A : Liste des Parties, Annexe 1B : Description du transfert et Annexe 1C : Les mesures techniques et organisationnelles visant à assurer la sécurité des données - Tableau 3, sont considérées comme complétées par référence à la présente Annexe 3, y compris la Partie A, Tableau 4, de l'Addendum du Royaume-Uni : Le Client et Iron Mountain reconnaissent et acceptent que l'Addendum du Royaume-Uni peut être résilié par l'une des Parties.

3. **Partie 2 :** Clauses Obligatoires de l'Addendum du Royaume-Uni : Le Client et Iron Mountain reconnaissent et acceptent les Clauses Obligatoires de l'Addendum du Royaume-Uni.

4. **Autorité de surveillance.** Le Bureau du Commissaire à l'Information du Royaume-Uni agit en tant qu'autorité de supervision compétente.

PARTIE D - TRANSFERTS D'AUTRES DONNÉES PERSONNELLES DU CLIENT

Si et dans la mesure où le Client ou ses affiliés transfèrent à Iron Mountain ou à ses filiales des Données Personnelles du Client non couvertes par la PARTIE A-C dans le cadre des Services fournis par Iron Mountain en vertu de l'Accord, la Partie A de l'Annexe 3 s'appliquera dans la mesure où elle est pertinente et applicable en vertu de la Législation sur la Protection des Données en vigueur. Par ailleurs, dans la mesure où des garanties ou des mécanismes de transfert substitutifs ou additionnels appropriés en vertu de la Législation sur la protection des Données sont nécessaires pour transférer les Données Personnelles du Client vers un pays qui n'offre pas un niveau de protection adéquat des Données Personnelles du point de vue de l'exportateur de données, les parties conviennent de les mettre en œuvre dès que possible et de documenter ces exigences de mise en œuvre dans une pièce jointe au présent DPA.

ANNEXE 4

HIPAA - Accord de Partenariat (« BAA »)

Cet BAA complète et modifie tous les Accords actuels ou futurs conclus entre Iron Mountain et ses filiales et le Client et ses affiliés, en vertu desquels Iron Mountain ou filiales fournissent certains Services au Client ou à ses affiliés, lesquels Services exigent que le Partenaire commercial utilise et/ou divulgue des PHI au nom de l'Entité Couverte. Sauf dans la mesure où elles sont modifiées dans le présent BAA, toutes les conditions énoncées dans l'Accord doivent rester pleinement en vigueur et régir les Services fournis par Iron Mountain au Client.

Iron Mountain et le Client concluent ce BAA afin que les deux parties respectent leurs obligations respectives, qui deviennent effectives et contraignantes pour les parties en vertu des règles de confidentialité, de Sécurité et de notification des violations de l'HIPAA, ainsi que de tous les règlements d'application, y compris ceux mis en œuvre dans le cadre de la règle Omnibus (collectivement appelés les « Règles de l'HIPAA »), en vertu desquelles le Client et ses affiliés sont une « Entité Couverte » ou un « Partenaire commercial » et Iron Mountain et ses filiales sont un « Partenaire commercial » du Client. Aux fins du présent Accord, toute référence ci-après au Partenaire commercial sera considérée comme une référence à Iron Mountain ou à ses filiales concernées.

1. DÉFINITIONS

Les termes en majuscules utilisés sans autre définition dans le présent BAA ont la même signification que celle qui leur est attribuée dans les règles de l'HIPAA ou dans l'Accord, le cas échéant.

« HIPAA » désigne la loi de 1996 sur la transférabilité et la responsabilité en matière d'assurance maladie.

« Informations de Santé Protégées » ou **« PHI »** a la même signification que le terme "informations de santé protégées" énoncé dans 45 CFR §160.103 et se limite aux PHI créées par le Partenaire commercial au nom du Client ou reçues du ou au nom du Client conformément à l'Accord.

« La loi HITECH » désigne les dispositions applicables de la loi sur les technologies de l'information en matière de santé économique et clinique, telle qu'incorporée dans la loi américaine de 2009 sur le redressement et le réinvestissement, ainsi que tout règlement d'application.

« Partenaire Commercial » désigne l'entité du Partenaire commercial identifié ci-dessus dans la mesure où elle reçoit, conserve ou transmet des informations de santé protégées dans le cadre de la fourniture de Services aux Clients.

« Règle de Confidentialité » désigne les Normes relatives à la confidentialité des informations sur la santé identifiables individuellement énoncées dans le règlement 45 CFR §160 et §164, Sous-parties A et E.

« Règle de Notification des Failles » désigne la règle de notification des failles pour les informations de santé protégées non sécurisées (45 CFR §164 Subpart D).

« Règle de Sécurité » désigne les Normes de sécurité pour la protection des informations électroniques protégées sur la santé énoncées dans le règlement 45 CFR §160 et §164, sous-parties A et C.

2. OBLIGATIONS ET ACTIVITÉS DU PARTENAIRE COMMERCIAL

2.1. Le Partenaire commercial s'engage à ne pas utiliser ou divulguer les PHI en dehors de ce qui est autorisé ou exigé par le présent BAA ou par la loi.

2.2. Le Partenaire commercial accepte d'utiliser les garanties appropriées et de se conformer, le cas échéant, à la sous-Partie C de 45 CFR §164 en ce qui concerne les PHI Électroniques, afin d'empêcher les utilisations ou divulgations des PHI autres que celles prévues par le présent BAA ou l'Accord ; toutefois, les parties reconnaissent et acceptent qu'il incombe au Client, et non au Partenaire commercial, de se conformer aux exigences énoncées dans 45 CFR §164.312, en ce qui concerne les PHI électroniques
pour mettre en œuvre des mécanismes de cryptage ou de décryptage pour les PHI électroniques conservés sur des supports physiques (par exemple, des bandes) stockés par le Client auprès du Partenaire commercial.

2.3. Le Partenaire commercial s'engage à signaler rapidement au Client tout incident de sécurité, toute violation ou toute autre utilisation ou divulgation de PHI dont il a connaissance et qui n'est pas autorisée ou exigée par le présent BAA ou l'Accord. En cas de Faille, cette notification doit être effectuée conformément aux règles HIPAA et à ce qu'elles exigent d'un Partenaire commercial, y compris, mais sans s'y limiter, en vertu du règlement 45 CFR 164.410, mais en aucun cas plus de trois (3) jours ouvrables après que le Partenaire commercial a achevé son enquête interne et confirmé qu'une Faille s'est produite. Le Partenaire commercial fournira une assistance et une coopération raisonnables dans le cadre de l'enquête sur une telle Faille et documentera les dépôts spécifiques qui ont été compromis, l'identité de tout tiers non autorisé qui pourrait avoir accédé aux PHI ou les avoir reçus, si elle est connue, et toutes les mesures qui ont été prises par le Partenaire commercial pour atténuer les effets d'une telle Faille.

2.4. Conformément aux 45 CFR 164.502(e)(1)(ii) et 164.308(b)(2), selon le cas, le Partenaire commercial s'assure que tout partenaire commercial qui est un sous-traitant qui crée, reçoit, conserve ou transmet des PHI pour le compte du Partenaire commercial dans le but d'aider à fournir des Services conformément à l'Accord, accepte les mêmes restrictions, conditions et exigences qui s'appliquent au Partenaire commercial en ce qui concerne ces PHI dans le cadre du présent BAA.

2.5. Si le Partenaire commercial a la garde des PHI dans un ensemble de dossiers désignés concernant des individus, et si le Client en fait la demande, le Partenaire commercial accepte de fournir l'accès à ces PHI au Client en récupérant et en livrant ces PHI conformément aux conditions générales de l'Accord, afin que le Client puisse répondre à un individu pour satisfaire aux exigences du 45 CFR §164.524.

2.6. Le Partenaire commercial accepte que si une modification des PHI dans un ensemble de dossiers désignés sous la garde du Partenaire commercial est nécessaire, et si le Client demande au Partenaire commercial de récupérer ces PHI conformément à l'Accord, le Partenaire commercial doit effectuer ce service afin que le Client puisse apporter toute modification à ces PHI qui peut être requise par le Client ou un individu conformément au 45 CFR §164.526.

2.7. Le Partenaire commercial accepte de documenter et de mettre à la disposition du Client les informations requises pour fournir un compte rendu des divulgations des PHI, à condition que le Client ait fourni au Partenaire commercial des informations suffisantes pour permettre au Partenaire commercial de déterminer quels enregistrements ou Données reçus du Client ou en son nom par le Partenaire commercial contiennent des PHI. La documentation des divulgations doit contenir les informations nécessaires pour que le Client puisse répondre à une demande d'un individu de comptabiliser les divulgations de PHI conformément au 45 CFR §164.528 ou à d'autres dispositions des règles de l'HIPAA.

2.8. Sauf convention contraire expresse dans l'Accord , le Partenaire commercial notifie rapidement au Client toute demande d'accès, de connaissance ou de correction de PHI émanant d'individus, sans répondre à ces demandes, et le Client est responsable de la réception et de la réponse à toute demande individuelle de ce type.

2.9. Dans la mesure où le Partenaire commercial doit exécuter une ou plusieurs obligations du Client en vertu de la sous-partie E de 45 CFR §164, le Partenaire commercial doit se conformer aux exigences de la sous-partie E qui s'appliquent au Client dans l'exécution de cette ou de ces obligations.

2.10. Le Partenaire commercial accepte de mettre ses pratiques internes, ses livres et ses registres à la disposition du secrétaire afin de déterminer la conformité avec les règles de l'HIPAA.

3. UTILISATIONS ET DIVULGATIONS AUTORISÉES PAR LE PARTENAIRE COMMERCIAL

3.1. Le Partenaire commercial peut utiliser ou divulguer des PHI dans la mesure nécessaire à l'exécution des services définis dans l'Accord.

3.2. Le Partenaire commercial peut utiliser ou divulguer des PHI si la loi l'exige.

3.3. Le Partenaire commercial s'engage à faire des efforts raisonnables pour limiter les PHI au minimum nécessaire pour atteindre l'objectif prévu de l'utilisation, de la divulgation ou de la demande.

3.4. Le Partenaire commercial ne peut pas utiliser ou divulguer des PHI d'une manière qui violerait la sous-partie E du 45 CFR §164 si le Client le faisait.

3.5. Le Partenaire commercial peut divulguer des PHI pour la gestion et l'administration appropriées du Partenaire commercial ou pour assumer les responsabilités légales du Partenaire commercial, à condition que les divulgations soient requises par la loi, ou que le Partenaire commercial obtienne des garanties raisonnables de la part de la personne à qui les informations sont divulguées que les informations resteront confidentielles et ne seront utilisées ou divulguées que comme requis par la loi ou aux fins pour lesquelles elles ont été divulguées à la personne, et que la personne notifie au Partenaire commercial tous les cas dont elle a connaissance dans lesquels la confidentialité des informations a été rompue.

4. OBLIGATIONS DU CLIENT

4.1. Le Client n'ordonnera pas au Partenaire commercial d'agir d'une manière qui ne serait pas conforme aux règles HIPAA.

4.2. Le Client doit notifier au Partenaire commercial toute(s) limitation(s) dans son avis sur les pratiques de confidentialité du Client conformément au 45 CFR §164.520, dans la mesure où cette limitation peut affecter l'utilisation ou la divulgation de PHI par le Partenaire commercial.

4.3. Le Client doit informer le Partenaire commercial de toute modification ou révocation de l'autorisation accordée à un individu d'utiliser ou de divulguer ses PHI, dans la mesure où ces modifications peuvent affecter l'utilisation ou la divulgation des PHI par Partenaire commercial.

4.4. Le Client doit informer par écrit le Partenaire commercial de toute restriction à l'utilisation ou à la divulgation des PHI qu'il a acceptée conformément au 45 CFR §164.522, dans la mesure où cette restriction peut affecter l'utilisation ou la divulgation des PHI par le Partenaire commercial.

5. DURÉE ET RÉSILIATION

5.1. Le présent BAA prend effet à la date d'entrée en vigueur et se termine automatiquement à la plus tardive des deux dates suivantes : (i) l'expiration de l'Accord ou (ii) la destruction ou la restitution au Client de toutes les PHI fournies par le Client au Partenaire commercial.

5.2. Dès qu'une partie prend connaissance d'une violation substantielle du BAA par l'autre partie, la partie qui n'a pas violé le BAA donne à la partie qui a violé le BAA la possibilité de remédier à la violation. Si la partie en violation ne remédie pas à la violation dans les trente (30) jours suivant la réception par la partie en violation d'une notification écrite de la partie non violente exposant les détails de cette violation substantielle, la partie non violente aura le droit de résilier le présent BAA et l'Accord conformément aux termes de l'Accord ou, si la résiliation n'est pas possible, de signaler le problème au secrétaire ou à toute autre autorité compétente.

5.3. Effet de la Résiliation:

5.3.1.1. Sauf dans les cas prévus au 5.3.2 ci-dessous, en cas de résiliation du présent BAA pour quelque raison que ce soit, le Partenaire commercial doit renvoyer ou détruire toutes les PHI reçues du Client conformément à l'Accord. Cette disposition s'applique aux PHI qui sont en possession de sous-traitants ou d'agents du Partenaire commercial. Le Partenaire commercial ne conserve aucune copie des PHI.

5.3.1.2. Dans le cas où le Partenaire commercial détermine que le retour ou la destruction des PHI n'est pas possible, le Partenaire commercial fournira au Client une notification des conditions qui rendent le retour ou la destruction impossible. Sur notification au Client, le Partenaire commercial doit étendre les protections du présent BAA à ces PHI et limiter les utilisations et divulgations ultérieures de ces PHI aux fins qui rendent le retour ou la destruction impossible, tant que l'associé commercial conserve ces PHI conformément aux conditions de l'Accord.

6. DIVERS

6.1. Indemnisation. Le Partenaire commercial accepte d'indemniser le Client de toutes les amendes ou pénalités imposées au Client à la suite d'une procédure de mise en application entamée par le secrétaire ou d'une action civile intentée par un procureur général d'État contre le Client, procédure ou action résultant directement et uniquement d'un acte ou d'une omission du Partenaire commercial qui constitue soit une violation des règles HIPAA, soit une violation substantielle du présent BAA (« Réclamation »). Le Partenaire commercial n'est pas tenu d'indemniser le Client pour toute partie de ces amendes ou pénalités résultant (i) de la violation par le Client des règles HIPAA ou du présent BAA, ou (ii) des actes ou omissions négligents ou intentionnels du Client. L'obligation d'indemnisation susmentionnée est expressément subordonnée à l'octroi par le Client au Partenaire commercial du droit, à sa convenance et à ses frais, et avec le conseil de son choix, de contrôler ou de participer à la défense d'une telle réclamation, à condition toutefois que, dans la mesure où une telle réclamation fait partie d'une procédure ou d'une action plus large, le droit du Partenaire commercial de contrôler ou de participer soit limité à la réclamation, et non à la procédure ou à l'action plus large. Dans le cas où le Partenaire commercial exerce son option de contrôle de la défense, (i) le Partenaire commercial ne doit pas régler une réclamation nécessitant une reconnaissance de faute de la part du Client sans son consentement écrit préalable, (ii) le Client a le droit de participer, à ses propres frais, à la réclamation ou au procès et (iii) le Client doit coopérer avec le Partenaire commercial dans la mesure où cela peut être raisonnablement exigé. Ce qui précède constitue le seul et unique recours du Client et la seule responsabilité du Partenaire commercial pour toute perte, tout dommage, toute dépense ou toute responsabilité du Client pour toute réclamation en rapport avec le présent BAA.

6.2. Mesures injonctives. Le Partenaire commercial reconnaît que toute utilisation ou divulgation non autorisée de PHI par le Partenaire commercial peut causer un préjudice irréparable au Client, pour lequel le Client aura le droit, s'il le souhaite, de demander une injonction ou toute autre mesure équitable.

6.3. Références réglementaires. Toute référence dans le présent BAA à une section des règles de l'HIPAA désigne cette section de l'HIPAA, la règle de confidentialité, la règle de sécurité, la LOI HITECH ou les règles Omnibus finales, telles que modifiées et en vigueur, et pour lesquelles la conformité est requise.

6.4. Modification. Les parties conviennent de négocier de bonne foi toute modification du présent BAA qui pourrait s'avérer nécessaire pour permettre au Client ou au Partenaire commercial de se conformer aux exigences des règles HIPAA. Si les parties ne parviennent pas à un accord mutuel sur les termes d'une telle modification dans les soixante (60) jours suivant la date de réception d'une telle demande écrite adressée par le Client au Partenaire commercial, l'une ou l'autre des parties a le droit de résilier le présent BAA et l'Accord moyennant un préavis écrit d'au moins trente (30) jours adressé à l'autre partie.

6.5. Pas de tiers bénéficiaires. Aucune disposition expresse ou implicite du présent BAA n'est destinée à conférer, ni ne doit conférer, à toute personne autre que le Client, le Partenaire commercial et leurs successeurs ou ayants droit respectifs, des droits, des recours, des obligations ou des responsabilités de quelque nature que ce soit.

6.6. Prestataires indépendants. Le Partenaire commercial, y compris ses directeurs, cadres, employés et agents, est un contractant indépendant et non un agent (tel que défini par le droit fédéral commun de l'agence) du Client ou un membre de sa main-d'œuvre. Sans limiter la généralité de ce qui précède, le Client n'a pas le droit de contrôler, de diriger ou d'influencer de quelque manière que ce soit la conduite du Partenaire commercial dans le cadre de l'exécution des services, autrement que par la mise en application du présent BAA ou de l'Accord, ou par la modification mutuelle de ceux-ci.

6.7. Préséance : Intégralité de l'Accord. Toute ambiguïté dans le présent BAA sera résolue afin de permettre aux parties de se conformer aux règles de l'HIPAA. Le présent BAA constitue l'intégralité de l'accord entre les parties en ce qui concerne l'objet du présent BAA et remplace toutes les communications, représentations, accords et ententes antérieurs relatifs aux règles HIPAA, y compris tous les accords de partenariat commercial antérieurs entre les parties.