Accord de Traitement des données

OBJET ET ORDRE DE PREVALENCE

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

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

CONDITIONS GÉNÉRALES

1. DÉFINITIONS

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

« **Données à Caractère Personnel** » désigne toute information relative à une Personne Concernée ;

« **Données à Caractère Personnel du Client** » désigne les Données à Caractère Personnel appartenant ou collectées par le Client ou ses affiliés et Traitées dans le cadre des Services ;

« Législation sur la Protection des Données » désigne toutes les lois et réglementations applicables relatives au Traitement des Données à Caractère Personnel qui peuvent exister dans les juridictions concernées, y compris, mais sans s'y limiter, le RGPD de l'UE (Règlement (UE) 2016/679), le *UK GDPR* (tel qu'applicable dans le cadre du droit interne du Royaume Uni en vertu de l'article 3 de *European Union (Withdrawal) Act 2018* et tel qu'amendé par le *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 20219* (tels qu'amendés)), le *Data Protection Act 2018*, le *FADP* (la loi fédérale suisse sur la protection des données), les *Lois Américaines sur la Protection des Données Personnelles* applicables aux Etats-Unis, le *LGBD* (la loi générale brésilienne sur la protection des données), la *PIPL* (loi sur la protection des informations personnelles de la République Populaire de Chine) et toute législation et/ou réglementation qui les met en œuvre ou en découle, ou qui modifie, remplace, adopte de nouveau 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 Américaines sur la Protection des Données Personnelles » désigne toutes les lois des états constitutifs des Etats-Unis d'Amérique sur la protection de la vie privée et des données qui sont applicables au Traitement des Données à Caractère Personnel en vertu du Contrat, y compris, sans s'y limiter, et telles qu'elles peuvent être modifiées, supplantées ou remplacées ponctuellement : (1) le *California Consumer Privacy Act*, telle que modifiée par le California Privacy Rights Act, et tout règlement d'application y afférent (ensemble, le « **CCPA** ») ; (2) le *Colorado Privacy Act* (le « **CPA** »), (3) le *Virginia Consumer Data Protection* Act (« **CDPA** ») ; (4) le *Utah Consumer Privacy Act* (« **UCPA** ») ; et (5) le *Connecticut Data Privacy Act* (« **CTDPA** ») ;

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

« Responsable du Traitement » 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 à Caractère Personnel ;

« **Services** » désigne tous les Services fournis par IM ou ses affiliés au Client ou à ses affiliés dans le cadre du Contrat ;

« **Sous-Traitant** » désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui Traite des Données à Caractère Personnel pour le compte du Responsable du Traitement ;

« **Traitement** » (et le cas échéant, « **Traiter** ») désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à Caractère Personnel ou des ensembles de Données à Caractère Personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ; et

« Violation de Sécurité » désigne tout dommage, destruction, perte, altération, divulgation non autorisée ou accès non autorisé aux Données à Caractère Personnel du Client qu'IM, son personnel ou ses Sous-traitants Traitent dans le cadre de la fourniture des Services.

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

2.1 Cet ATD s'applique aux Données à Caractère Personnel du Client Traitées par IM en tant que Sous-Traitant dans le cadre de la fourniture des Services conformément au Contrat pour le compte du Client.

2.2 IM peut collecter et Traiter les Données à Caractère Personnel du Client et des employés de ses affiliés en tant que Responsable du Traitement 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 la déclaration de confidentialité d'IM disponible sur les sites Web d'IM et à d'autres politiques de confidentialité applicables. Les obligations d'IM énoncées dans le présent ATD ne s'appliquent pas au traitement de telles Données à Caractère Personnel.

2.3 L'objet du Traitement des Données à Caractère Personnel est la prestation des Services. Les droits et obligations du Client et d'IM sont définis dans le présent ATD. L'Annexe 1 du présent ATD définit la nature, la durée et la finalité du Traitement, les types de Données à Caractère Personnel du Client qu'IM Traite et les catégories de Personnes Concernées dont les Données à Caractère Personnel sont Traitées.

2.4 Lorsque IM Traite les Données à Caractère Personnel du Client dans le cadre de la fourniture des Services, IM s'engage à :

2.4.1 Traiter les Données à Caractère Personnel du Client uniquement en conformité avec les instructions documentées du Client. Si IM est tenu de traiter les Données à Caractère Personnel du Client à d'autres fins en vertu de la législation à laquelle IM est soumise, IM 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 sur la Protection des Données et informer immédiatement le Client si, de l'avis d'IM, une instruction de Traitement des Données à Caractère Personnel du Client donnée par ce dernier enfreint la Législation sur la Protection des Données.

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

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

3. FOURNIR UNE ASSISTANCE AUX CLIENTS

3.1

IM 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 à Caractère Personnel à l'autorité de contrôle, la communication d'une violation de Données à Caractère Personnel à la Personne Concernée, l'analyse d'impact relative à 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 Responsable du Traitement pour atténuer le risque), en tenant compte des informations dont dispose IM ; 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'IM 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, IM mettra en œuvre des mesures techniques et organisationnelles appropriées et raisonnables conçues pour protéger la confidentialité, l'intégrité et la disponibilité des Données à Caractère Personnel du Client et pour protéger les Données à Caractère Personnel 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'IM sont énoncées à l'Annexe 2 du présent ATD.

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 à Caractère Personnel du Client conformément à la Législation sur la Protection des Données ; (ii) être autorisés à donner des instructions écrites à IM sur le Traitement des Données à Caractère Personnel du Client dans le cadre des Services (y compris au nom de toute entité tierce qui est un Responsable du Traitement des Données à Caractère Personnel du Client) ; et (iii) conserver à tout moment le contrôle et l'autorité sur les Données à Caractère Personnel du Client en ce qui concerne le Traitement.

6. SOUS-TRAITEMENT

6.1 Le Client reconnaît et accepte qu'IM puisse engager sa société mère, ses affiliés et d'autres Sous-Traitants ultérieurs (y compris des Sous-Traitants ultérieurs engagés par les affiliés ou la société mère d'IM) dans le but de Traiter les Données à Caractère Personnel du Client en vertu de cet ATD, 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 ATD est disponible ici[1]. IM 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 justifiées liées à la protection des données dans ce délai. Afin de recevoir ces notifications par e-mail, le Client doit s'inscrire et gérer tout abonnement existant au service de notification d'IM via cette page Web[2].

[1] https://www.ironmountain.com/en-gb/utility/legal/privacy-and-data-protection/iron-mountain-subprocessors

[2] https://urldefense.proofpoint.com/v2/url?u=https-3A reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFlot0PGng&r=JTlzF2zjl-gYEq5GmWmZcbgd--hqyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

6.3 Si le Client ne souscrit pas à ce service de notification, IM 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, IM 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 à Caractère Personnel du Client par le Sous-Traitant auquel il s'oppose, pour examen et approbation par le Client. Si le Client n'approuve pas les modifications proposées par IM dans un délai de quinze (15) jours, IM 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 IM sans l'utilisation du Sous-Traitant faisant l'objet de l'opposition. 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 IM ou les affiliés d'IM dans le cadre de cette résiliation et que le Client prendra rapidement possession des actifs qu'il a fournis à IM dans le cadre des Services résiliés, sous réserve des conditions du Contrat et aux frais du Client.

6.4 IM doit s'assurer que tout contrat conclu avec des Sous-Traitants dans le cadre de cet ATD contient des dispositions qui sont, à tous égards importants, identiques à celles de cet ATD et qui sont conformes à la Législation sur la Protection des Données. Lorsqu'un Sous-Traitant d'IM fait en sorte qu'IM ne respecte pas ses obligations en vertu du présent ATD ou de toute Législation sur la Protection des Données, IM demeure entièrement responsable envers le Client de l'exécution des obligations d'IM en vertu des présentes conditions.

7. VIOLATION DE SÉCURITÉ

7.1 En cas de suspicion de Violation de Sécurité, IM s'engage à :

7.1.1 prendre rapidement des mesures pour enquêter sur la Violation de Sécurité présumée et pour identifier, prévenir et atténuer les effets de la Violation 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 Sécurité s'est produite et fournir au Client une description détaillée de la Violation 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'IM fournisse les informations visées à la clause 7.1.2 par étapes. Dans les cas où IM n'a pas accès ou ne peut pas fournir certaines informations énumérées dans la clause 7.1.2, IM en informera le Client et IM ne sera pas responsable de l'absence de fourniture de ces informations.

8. AUDITS

IM autorisera le Client et ses auditeurs ou agents autorisés respectifs, moyennant un préavis d'au moins dix (10) jours ouvrables à IM, à effectuer des audits ou des inspections pendant la durée du Contrat, à condition qu'IM ne soit pas tenu de fournir ou d'autoriser l'accès aux informations concernant : (i) d'autres clients d'IM ; (ii) tout rapport externe non public d'IM ; et (iii) tout rapport interne préparé par les services d'audit interne ou de conformité d'IM. Les objectifs d'un audit ou d'une inspection en vertu de cette clause se limitent à vérifier qu'IM effectue des Traitements sur les Données à Caractère Personnel du Client conformément aux obligations qui lui incombent en vertu du présent ATD. Sauf en cas de Violation 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 RÉGLEMENTÉS)

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

9.1.1 de se conformer à la Législation sur la 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 à Caractère Personnel du Client, (ii) des pays dont les lois nationales peuvent ne pas fournir un niveau de protection des Données à Caractère Personnel comparable à celui de la Législation de l'UE/du Royaume-Uni (« **Pays Tiers** ») dans ce domaine, (iii) des mesures techniques et organisationnelles appropriées énoncées dans la clause 7 et (iv) des parties concernées participant au Traitement de ces Données à Caractère Personnel du Client, procédé à une évaluation de l'adéquation du mécanisme de transfert 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 à Caractère Personnel transférées conformément au présent ATD bénéficient d'un niveau de protection dans le pays de destination qui est globalement équivalent à celui garanti en vertu de la Législation sur la Protection des Données.

10. RESPONSABILITÉ ET INDEMNISATION

10.1 Nonobstant toute disposition contraire du Contrat, en cas de Violation de Sécurité causée directement par un manquement d'IM à ses obligations en vertu de cet ATD, IM 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 Violation de Sécurité, (b) de la préparation et de l'envoi de la notification aux Personnes Concernées et aux autorités réglementaires, comme l'exige la Législation sur la Protection des Données, (c) de la fourniture de services de suivi de la solvabilité 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 contrôle et pour lesquelles l'autorité de contrôle déclare qu'IM 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 (« **Plainte 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 part de l'indemnisation correspondant au dommage causé par cette autre partie. La Partie qui Indemnise ne peut faire valoir son droit envers l'autre partie que dans les 12 mois suivant l'incident, dans la mesure permise par la loi applicable.

10.3 Dans toute la mesure permise par les lois applicables, les limitations de responsabilité et les exclusions de dommages énoncées dans le Contrat régissent la responsabilité globale pour toutes les réclamations du Client découlant de ou liées à cet ATD, et/ou au Contrat contre IM. 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'IM signifie la responsabilité globale d'IM et de tous les affiliés d'IM pour les réclamations du Client et de tous 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 Plaintes 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 contrôle.

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 ATD.

11. DEMANDES DES AUTORITÉS PUBLIQUES

11.1 Dans la mesure permise par la loi et sous réserve des clauses 11.2 à 11.5 ci-dessous, IM accepte de notifier le Client si IM :

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 à Caractère Personnel du Client transférées en vertu du Contrat ; ou

11.1.2 a connaissance d'un accès direct par les autorités publiques aux Données à Caractère Personnel du Client transférées en vertu du Contrat, conformément aux lois du pays de destination.

11.2 Si la législation du pays de destination interdit à IM d'informer le Client, IM 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 IM 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 à Caractère Personnel du Client demandées tant qu'elle n'est pas tenue de le faire en vertu des règles de procédure applicables.

11.4 IM 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 IM s'engage à conserver les informations visées par la présente clause pendant toute la durée du Contrat 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 IM, à la résiliation/expiration du Contrat, sur la base des instructions spécifiques du Client et sous réserve des conditions du Contrat, IM supprimera/détruira ou renverra au Client ou à un tiers désigné par le Client toutes les Données à Caractère Personnel du Client. Toutes les Données à Caractère Personnel du Client contenues dans les actifs du Client stockés par IM 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 le Contrat ou dans tout autre document contractuel applicable. Dans tous les autres cas, si le Contrat est silencieux concernant la suppression/destruction ou la restitution des Données à Caractère Personnel du Client et que le Client ne donne pas d'instructions concernant la suppression/destruction ou la restitution des Données à Caractère Personnel du Client dans les quinze (15) jours suivant la résiliation/expiration du Contrat, IM enverra une notification écrite au Client demandant de recevoir dans les quinze (15) jours des instructions spécifiques concernant la suppression/destruction ou la restitution des Données à Caractère Personnel 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 IM à poursuivre le Traitement, la suppression et la destruction de toutes les Données à Caractère Personnel du Client après la résiliation du Contrat, à la discrétion d'IM et aux frais du Client.

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

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

12.4 Chaque partie peut notifier à l'autre partie par écrit, de manière ponctuelle, de toute modification du présent ATD que la partie 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 accord au présent ATD 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 accord 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, et qui est considéré comme un accord mutuel de modification du présent ATD.

ANNEXE 1

Détails du Traitement et du transfert de Données à Caractère Personnel (le cas échéant)

A. LISTE DES PARTIES :

Les parties à cet ATD et les rôles de l'exportateur et de l'importateur de Données sont définis dans le Contrat et dans l'Annexe 3 à l'ATD (Transferts internationaux de Données à Caractère Personnel), le cas échéant.

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

Catégories de Personnes Concernées dont les Données à Caractère Personnel sont Traitées/transférées :

En fonction de la nature des Services d'IM et des activités du Client, ce dernier peut soumettre à IM des Données à Caractère Personnel 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 prestataires ou consultants actuels et passés, les prestataires 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 familiaux/civils, personnes à charge et contacts d'urgence, les retraités, les administrateurs et dirigeants actuels et passés, les actionnaires, les détenteurs de titres boursiers, 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 à Caractère Personnel Traitées/transférées :

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

Données sensibles transférées (le cas échéant) :

En fonction de la nature des Services d'IM et de l'activité du Client, le Client peut soumettre à IM des Données à Caractère Personnel 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 à Caractère Personnel sont transférées de manière ponctuelle ou continue) :

Le transfert s'effectue de manière continue.

Nature du Traitement :

Collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, limitation, effacement ou destruction.

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

La fourniture des Services tels que définis dans le Contrat.

Conservation des Données à Caractère Personnel :

Les Données à Caractère Personnel seront conservées par IM pendant toute la durée des Services offerts au Client et jusqu'à ce que les Données à Caractère Personnel soient retournées ou détruites conformément à la clause 12.1 du présent ATD.

Le cas échéant, pour les transferts à des Sous-Traitants ultérieurs, préciser également l'objet, la nature et la durée du Traitement :

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

C. AUTORITÉ DE CONTROLE COMPÉTENTE

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

ANNEXE 2

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

1. PROGRAMME ET POLITIQUE DE SÉCURITÉ DE L'INFORMATION

IM doit gérer 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 de sécurité de l'information, normes et procédures d'IM ;

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 à Caractère Personnel 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 à Caractère Personnel du Client sont conservées.

2. ÉVALUATION DES RISQUES

IM gère 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 à Caractère Personnel du Client. IM évalue et met à jour, si nécessaire, raisonnablement et de manière 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 à Caractère Personnel du Client.

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

3.1 Gestion des moyens de traitement de l'information. IM a mis en place un programme de gestion de l'inventaire des actifs afin de gérer les contrôles physiques, techniques et administratifs des moyens de traitement de l'information d'IM (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'IM afin de garantir la classification appropriée des informations, la détermination des restrictions d'accès et l'examen des contrôles d'accès.

3.1.2 Nettoyage 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'IM un équipement ou un logiciel qui n'est pas attribué à une personne spécifique.

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

3.2.1 Procédures opérationnelles et contrôles techniques conçus pour protéger les documents, les supports informatiques, les données d'entrées/sorties/de sauvegardes 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 à Caractère Personnel du Client.

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

4. MESURES DE SÉCURITÉ DU PERSONNEL

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

4.2 Politique d'enquête sur les antécédents. IM a mis en place une politique d'enquête sur les antécédents et de dépistage des drogues (aux États-Unis uniquement) pour ses employés. IM continuera à maintenir ces politiques pendant la durée du Contrat. 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 la formation scolaire de certains employés, le permis de conduire et l'historique des infractions pour les candidats conducteurs et les conducteurs existants. Lorsque des informations défavorables sont identifiées lors d'une vérification des antécédents, IM procède à une évaluation individualisée, conformément à la législation du travail et aux bonnes pratiques en vigueur.

4.3 Travailler avec les Sous-Traitants. IM exigera de tout Sous-Traitant fournissant des Services dans le cadre du Contrat 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 du Contrat impliquant le Traitement des Données à Caractère Personnel du Client.

4.4 Formation de sensibilisation à la sécurité. Au moins une fois par an, IM 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'IM ayant accès aux Données à Caractère Personnel du Client. IM tient des registres indiquant les noms de ces employés d'IM qui ont participé à la formation et la date de chaque formation de sensibilisation à la sécurité. IM doit régulièrement revoir et mettre à jour son programme de formation à la sensibilisation à la sécurité.

4.5 Renvoi du personnel d'IM. IM 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 à Caractère Personnel du Client, l'accès d'un employé d'IM aux Données à Caractère Personnel du Client doit être révoqué dans les plus brefs délais.

5. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

5.1 Contrôles de sécurité physique. Les installations d'IM utilisent des contrôles physiques qui limitent raisonnablement l'accès aux Données à Caractère Personnel du Client, y compris, si IM 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 Services support. IM doit prendre des mesures pour protéger ses installations contenant les Données à Caractère Personnel 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. IM 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 IM sous-traite des fonctions nécessitant l'utilisation d'équipements hors site pour la fourniture de Services, tout équipement hors site stockant les Données à Caractère Personnel du Client sera protégé par des mesures de sécurités 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. IM doit conserver pendant un an les dossiers des employés d'IM autorisés à avoir un accès physique aux environnements informatiques contrôlés par IM et utilisés par IM pour fournir des Services et, à la demande du Client en cas de Violation de Sécurité, et sous réserve des politiques de sécurité d'IM, afin de permettre au Client de consulter les dossiers vérifiables de ces employés d'IM.

5.6 Accès physique restreint. IM doit limiter l'accès physique aux installations contrôlées par IM qui traitent les Données à Caractère Personnel du Client aux employés d'IM et aux personnes autorisées qui ont besoin de cet accès pour des raisons professionnelles. IM doit disposer d'une procédure d'approbation pour autoriser et suivre les demandes d'accès physique à ces installations.

5.7 Réparations et modifications. IM doit consigner toutes les réparations et modifications liées à la sécurité apportée 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 à Caractère Personnel 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. IM doit créer, mettre en œuvre et gérer 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. IM 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'IM 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. IM 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 à Caractère Personnel 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'IM doivent être séparés logiquement ou physiquement.

6.5 Gestion de l'architecture technique. IM 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. IM 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 à Caractère Personnel du Client.

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

6.7.1 En ce qui concerne les environnements hébergés par IM et utilisés pour fournir les Services, les événements d'alerte des systèmes de détection d'intrusion ou *Intrusion Detection Systems* (« **IDS** ») et des capteurs de prévention d'intrusion ou *Intrusion Prevention Sensors* (« **IPS** ») sont enregistrés et font l'objet de rapports quotidiens (collectivement dénommés « **IDS/IPS** ») ;

6.7.2 En ce qui concerne les environnements hébergés par IM 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 en contact avec l'extérieur ne sont pas accessibles depuis l'Internet ;

6.7.4 Les connexions au réseau d'IM sont enregistrées et consignées dans des historiques (*log files*) ;

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 IM ou gérés par IM 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'IM.

6.8 Identifiants d'authentification chiffrées. IM doit veiller à ce que les identifiants d'authentification transmis sur les appareils du réseau d'IM soient chiffrés durant leur transit.

6.9 Administration d'un réseau sécurisé. Les réseaux d'IM 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 IM 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. IM doit mettre en œuvre et entretenir 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 IM et utilisés pour héberger ou accéder aux Données à Caractère Personnel du Client.

6.11 Site Web - Chiffrement du Client. IM 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. IM doit créer des copies de sauvegarde appropriées des fichiers du système. En outre, IM doit élaborer et maintenir des procédures de reprise après sinistre, voir la clause « Reprise après sinistre » ci-dessous pour plus de détails.

6.13 Informations électroniques en transit. IM doit utiliser un algorithme de cryptage standard avec une longueur de clé de 128 bits minimum pour protéger les Données à Caractère Personnel du Client transmises sur des réseaux publics lorsqu'elles proviennent de l'infrastructure hébergée par IM.

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

6.14.1 Être conçus pour protéger raisonnablement la confidentialité et l'intégrité des Données à Caractère Personnel du Client traitées, transmises ou stockées par IM dans tout environnement de réseau partagé, conformément aux termes du Contrat ;

6.14.2 Être appliquées, dans le(s) environnement(s) hébergé(s) par IM et utilisé(s) pour fournir des Services, aux Données à Caractère Personnel du Client en transit sur ou vers des réseaux « non fiables » (c'est-à-dire des réseaux qu'IM ne contrôle pas légalement), y compris ceux utilisés pour envoyer des données au réseau d'entreprise du Client à partir du réseau d'IM, sous réserve, dans chaque cas, de la coopération du Client dans la gestion des clés de cryptage nécessaires pour déchiffrer 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 chiffrement de toutes les Données à Caractère Personnel du Client sur les ordinateurs portables ou autres appareils portables.

6.15 Exigences d'enregistrement. IM 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 vérifiés ;

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 IM et utilisé(s) par IM pour fournir des Services ;

6.15.3 Les journaux d'audit du système sont analysés 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 de l'heure du réseau. IM synchronise 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. IM sépare 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. IM maintient des politiques de contrôle d'accès concernant les moyens de traitement de l'information qu'IM approuve, publie et met en œuvre de manière formelle.

7.2 Autorisation d'accès logique. IM dispose d'une procédure d'approbation pour les demandes d'accès logique aux Données à Caractère Personnel du Client et les demandes d'accès aux systèmes d'IM dédiés à l'utilisation des Services.

7.3 Contrôle d'accès et vérification de l'accès. IM n'accordera l'accès aux Données à Caractère Personnel du Client qu'aux employés actifs d'IM, 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 sont 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'IM ayant accès aux Données à Caractère Personnel du Client, IM doit s'assurer que des contrôles appropriés sont en place.

7.5 Contrôle d'accès aux systèmes d'exploitation. IM contrôle 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. IM dispose d'une politique ou d'une procédure visant à protéger les appareils informatiques mobiles d'IM 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 chiffrement, la protection contre les virus et la sauvegarde des appareils.

7.7 Isolation des systèmes client. IM doit, dans son (ses) environnement(s) hébergé(s) utilisé(s) pour fournir les Services, séparer logiquement et isoler les Données à Caractère Personnel du Client de toute autre information.

7.8 Comptes. IM prend les mesures suivantes en ce qui concerne les comptes :

7.8.1 Exiger l'authentification de l'identité de chaque employé d'IM qui souhaite accéder aux systèmes d'IM qui traitent les Données à Caractère Personnel du Client et interdire l'utilisation de comptes d'utilisateurs partagés ou de comptes d'utilisateurs avec des identifiants génériques pour accéder aux Données à Caractère Personnel 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. IM utilise 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. IM veille à ce que la sécurité fasse partie intégrante du développement et de l'exploitation de tous les systèmes d'information et publie et respecte 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'IM (y compris les systèmes d'exploitation, l'infrastructure, les applications commerciales, les services et les applications développées par les utilisateurs) sont conçus de manière à respecter les normes de sécurité de l'information.

8.3 Diagrammes de réseau. IM élabore, documente et tient 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. IM 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 à Caractère Personnel du Client. Les résultats détaillés sont des informations confidentielles et exclusives d'IM et ne seront pas fournis.

8.5 Vérification et analyse des modifications. IM 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 à Caractère Personnel du Client ou sur les systèmes.

9. REPRISE APRÈS SINISTRE

IM maintient 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 à Caractère Personnel du Client qui sont physiquement stockées dans une installation d'IM. IM maintient un plan de continuité des activités pour restaurer les fonctions critiques de l'entreprise. IM effectue 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'IM sont conçus pour être conformes aux normes industrielles. IM 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** »). IM fournira tous les rapports de ce type commandés en vue d'être orientés vers le Client, quels que soient les résultats du rapport. IM ne sera pas tenu de fournir les résultats de l'audit interne ou d'autres évaluations indépendantes qui ont été commandées dans l'intention de rester confidentielles pour IM. 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 clause sera considéré comme une information confidentielle d'IM. Le Client doit avoir le droit de fournir une copie de ce Rapport d'Audit à tous les clients 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, IM confirmera 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 à Caractère Personnel

1. DÉFINITIONS

« **2022 UK Addendum** » désigne le modèle d'Addendum B.1.0 publié par le *United Kingdom Information Commissioner's Office* et déposé devant le Parlement conformément à l'article 119A du *Data Protection Act 2018* le 2 février 2022, tel qu'il peut être révisé en vertu de l'article 18 de cet *Act*, disponible ici[33].

« **Clauses Contractuelles Standard** » désigne collectivement les Clauses Contractuelles Standard de l'UE 2021 et le 2022 UK Addendum.

« **Clauses Contractuelles Standard de l'UE 2021** » désigne les Clauses Contractuelles Standard pour le transfert de Données à Caractère Personnel vers des pays tiers conformément au RGPD, adoptées par la Commission Européenne en vertu de la décision d'exécution de la Commission (UE) 2021/914, disponible ici[44].

« **Données à Caractère Personnel du Client de l'UE** » désigne le Traitement des Données à Caractère Personnel 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, étaient applicables avant leur Traitement par IM.

« **Données à Caractère Personnel du Client du Royaume-Uni** » désigne le Traitement des Données à Caractère Personnel du Client auxquelles les lois sur la protection des Données du Royaume-Uni s'appliquaient avant leur Traitement par IM.

« **Données à Caractère Personnel du Client de la Suisse** » désigne le Traitement des Données à Caractère Personnel du Client auxquelles les lois suisses sur la protection des données étaient applicables avant leur Traitement par IM.

« **Zone Protégée** » désigne :

i. dans le cas des Données à Caractère Personnel 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 à Caractère Personnel 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 à Caractère Personnel du Client de la Suisse, tout pays, territoire, secteur ou organisation internationale reconnu(e) comme adéquat(e) par le droit suisse ;

iv. dans le cas de toute autre Donnée à Caractère Personnel du Client transférée hors d'une juridiction offrant des protections similaires à celles des Données à Caractère Personnel 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.

2. DIVERS

2.1 La présente Annexe 3 comprend les parties suivantes :

(i) Partie A - Transferts de Données à Caractère Personnel du Client de l'UE ;

(ii) Partie B - Transferts de Données à Caractère Personnel du Client de la Suisse ;

(iii) Partie C - Transfert de Données à Caractère Personnel du Client du Royaume-Uni, qui s'appliquent, le cas échéant, au transfert de Données à Caractère Personnel du Client par IM dans le cadre de ses Services.

2.2 Les Clauses Contractuelles Standard s'appliquent à IM et à ses affiliés en tant que « Importateurs de Données » et au Client et à ses affiliés en tant que « Exportateurs de Données ».

2.3 La signature et la date du Contrat constituent toutes les signatures et dates nécessaires pour les Clauses Contractuelles Standard.

[33] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

[44] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

2.4 Si les parties transfèrent les Données à Caractère Personnel des Client de l'UE, du Royaume-Uni ou de la Suisse en dehors de la Zone Protégée et qu'une décision d'adéquation de la Commission Européenne ou une autre méthode d'adéquation valide en vertu de la Législation sur la Protection des Données applicable sur laquelle IM s'est appuyée pour le transfert de données est jugée invalide, ou qu'une autorité de contrôle exige que les transferts de Données à Caractère Personnel 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 le *EU-U.S. Data Privacy Framework*.

PARTIE A - TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL DU CLIENT DE L'UE

Si et dans la mesure où le Client ou ses affiliés transfèrent à IM ou à ses affiliés des Données à Caractère Personnel du Client de l'UE en dehors de la Zone Protégée dans le cadre des Services fournis par IM en vertu du Contrat, la présente Partie A de l'Annexe 3 s'applique, et les parties conviennent de ce qui suit :

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'un de ses affiliés est un Responsable du Traitement et qu'IM ou l'un de ses affiliés est un Sous-Traitant ; le texte du TROISIÈME MODULE des Clauses Contractuelles Standard de l'UE 2021 s'applique lorsque le Client ou l'une de ses affiliés est un Sous-Traitant et qu'IM ou l'un de ses affiliés est un Sous-Traitant ultérieur. Les dispositions applicables contenues dans les Clauses Contractuelles Standard de l'UE 2021 sont incorporées par référence dans le présent ATD 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 – Détails du Traitement et Transfert de Données, à l'Annexe 2 – Les Mesures Techniques et Organisationnelles, et à la clause 6.2 du présent ATD - Liste des Sous-Traitants ultérieurs.

2 **Utilisation de Sous-Traitants ultérieurs.** 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-Traitants ultérieurs pour l'exécution des Services s'applique. Le Client reconnaît et accepte qu'IM puisse engager de nouveaux Sous-Traitants ultérieurs par le biais du mécanisme convenu dans la clause 6 du présent ATD et que le délai pour soumettre des demandes de changement de Sous-Traitants ultérieurs 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 en vigueur 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, IM ne fournira au Client un certificat de suppression des Données à Caractère Personnel que sur demande écrite de ce dernier.

5 **Violation de Données à Caractère Personnel.** Aux fins de la clause 8.6(c) des Clauses Contractuelles Standard de l'UE 2021, les violations de Données à Caractère Personnel sont traitées conformément au mécanisme convenu dans la clause 7 de l'ATD.

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 le présent ATD.

7 **Réclamations.** Aux fins de la clause 11 des Clauses Contractuelles Standard de l'UE 2021, IM informera le Client si elle reçoit une plainte d'une Personne Concernée relative aux Données à Caractère Personnel du Client de l'UE et communiquera la plainte au Client conformément au mécanisme convenu dans le le présent ATD.

8 **Autorité de contrôle.** Pour les Clauses Contractuelles Standard de l'UE 2021, l'autorité de contrôle compétente est déterminée conformément à la clause 13 des Clauses Contractuelles Standard de l'UE.

PARTIE B - TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL CONCERNANT LES CLIENTS SUISSES

Si et dans la mesure où le Client ou ses affiliés transfèrent des Données à Caractère Personnel du Client suisse en dehors de la Zone Protégée à IM ou à ses affiliés dans le cadre des Services fournis par IM en vertu du Contrat, 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'un de ses affiliés est un Responsable du Traitement et qu'IM ou l'un de ses affiliés est un Sous-Traitant, et/ou lorsque le Client ou l'un de ses affiliés est un Sous-Traitant et qu'IM ou l'une de ses affiliés est un Sous-Traitant ultérieur, à l'exception de ce qui suit :

   a. l'autorité de contrôle 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 RGPD 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 À CARACTÈRE PERSONNEL CONCERNANT LES CLIENTS BRITANNIQUES

Si et dans la mesure où le Client ou ses affiliés transfèrent des Données à Caractère Personnel du Royaume-Uni en dehors de la Zone Protégée à IM ou à ses affiliés dans le cadre des Services fournis par IM en vertu du Contrat, 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 appropriées de la Partie A et du 2022 UK Addendum s'appliquent lorsque le Client ou l'un de ses affiliés est un Responsable du Traitement et qu'IM ou l'un de ses affiliés est un Sous-Traitant, et/ou lorsque le Client ou l'une de ses affiliés est un Sous-Traitant et qu'IM ou l'un de ses affiliés est un Sous-Traitant ultérieur.

2. **Partie 1 : Tableau 1 - 3 du 2022 UK Addendum :** 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, du 2022 UK Addendum : le Client et IM reconnaissent et acceptent que le 2022 UK Addendum peut être résilié par l'une des parties.

3. **Partie 2 :** Clauses obligatoires du 2022 UK Addendum: Le Client et IM reconnaissent et acceptent les clauses obligatoires du 2022 UK Addendum.

4. **Autorité de contrôle.** Le *UK Information Commissioner's Officer* agit en tant qu'autorité de contrôle compétente.

PARTIE D - TRANSFERTS D'AUTRES DONNÉES À CARACTÈRE PERSONNELDU CLIENT

Si et dans la mesure où le Client ou ses affiliés transfèrent à IM ou à ses affiliés des Données à Caractère Personnel du Client non couvertes par les Parties A à C de l'Annexe 3 dans le cadre des Services fournis par IM en vertu du Contrat, la Partie A de l'Annexe 3 s'appliquera dans la mesure où elle est appropriée 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 à Caractère Personnel du Client vers un pays qui n'offre pas un niveau de protection adéquat des Données à Caractère Personnel 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 annexe au présent ATD.

ANNEXE 4

HIPAA - Accord de Partenariat (« AdP »)

Cet AdP complète et modifie tous les Contrats actuels ou futurs conclus entre IM et ses affiliés et le Client et ses affiliés, en vertu desquels IM ou ses affiliés fournissent certains Services au Client ou à ses affiliés, lesquels Services exigent que le Partenaire Commercial (tel que défini ci-après) utilise et/ou divulgue des PHI – (telles que définies ci-après) au nom de l'Entité Couverte (telle que définie ci-après). Sauf dans la mesure où elles sont modifiées dans le présent AdP, toutes les conditions énoncées dans le Contrat doivent rester pleinement en vigueur et régir les Services fournis par IM au Client.

IM et le Client concluent cet AdP 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 (tels que définis ci-après), 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 IM et ses affiliés sont un **« Partenaire Commercial** » du Client. Aux fins du présent AdP, toute référence ci-après au Partenaire Commercial sera considérée comme une référence à IM ou à ses affiliés concernés.

1. DÉFINITIONS

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

« **HIPAA** » désigne le *Health Insurance Portability and Accountability* Act de 1996.

« **Informations de Santé Protégées** » ou « **PHI** » a la même signification que le terme « informations de santé protégées » (*Protected Health Information*) énoncé dans le 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 au Contrat.

« **HITECH Act** » désigne les dispositions applicables du *Health Information for Economic and Clinical Health* Act, tel qu'incorporé dans le *American Recovery and Reinvestment Act* de 2009, 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 *Privacy of Individually Indentifiable Health Information* énoncées dans la législation *45 CFR §160 et §164, Subparts A et E*.

« **Règle de Notification des Violations** » désigne la règle de notification des violations pour les Informations de Santé Protégées non sécurisées (*45 CFR §164 Subpart D*).

« **Règle de Sécurité** » désigne les *Sécurity Standards for the Protection of Electronic Protected Health Information* énoncées dans la législation *45 CFR §160 et §164, Subparts 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 AdP ou par la loi.

2.2. Le Partenaire Commercial accepte d'utiliser les garanties appropriées et de se conformer, le cas échéant, à *45 CFR §164 Subpart C* en ce qui concerne les PHI électroniques, afin d'empêcher les utilisations ou divulgations des PHI autres que celles prévues par le présent AdP ou au Contrat ; 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 chiffrement ou de déchiffrement des 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 fuite ou toute autre utilisation ou divulgation de PHI dont il a connaissance et qui n'est pas autorisée ou exigée par le présent AdP ou le Contrat. En cas de violation, cette notification doit être effectuée

conformément aux Règles de l'HIPAA et à ce qu'elles exigent d'un Partenaire Commercial, y compris, mais sans s'y limiter, en vertu de la législation *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 violation s'est produite. Le Partenaire Commercial fournira une assistance et une coopération raisonnables dans le cadre de l'enquête sur une telle violation 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 violation.

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 au Contrat, accepte les mêmes restrictions, conditions et exigences qui s'appliquent au Partenaire Commercial en ce qui concerne ces PHI dans le cadre du présent AdP.

2.5. Si le Partenaire Commercial a la garde des PHI dans un ensemble de registres 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 du Contrat, afin que le Client puisse répondre à un individu pour satisfaire aux exigences de *45 CFR §164.524*.

2.6. Le Partenaire Commercial accepte que si une modification des PHI dans un ensemble de registres désignés sous la garde du Partenaire Commercial est nécessaire, et si le Client demande au Partenaire Commercial de récupérer ces PHI conformément au Contrat, 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 à *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 documents 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 le Contrat, le Partenaire Commercial doit notifier 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 *45 CFR §164 Subpart E*, le Partenaire Commercial doit se conformer aux exigences de ladite *Subpart 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 Ministère 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 est susceptible d'utiliser ou de divulguer des PHI dans la mesure nécessaire à l'exécution des Services définis dans le Contrat.

3.2. Le Partenaire Commercial est susceptible d'utiliser ou de divulguer des PHI si la loi l'exige.

3.3. Le Partenaire Commercial s'engage à faire ce qui est raisonnablement nécessaire 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 contreviendrait à *45 CFR §164 Subpart E* si le Client le faisait.

3.5. Le Partenaire Commercial est susceptible de 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 de l'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 à *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 le 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 à *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 AdP prend effet à la date d'entrée en vigueur et se termine automatiquement à la plus tardive des deux dates suivantes : (i) l'expiration du Contrat 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 AdP par l'autre partie, la partie qui n'a pas contrevenu à l'AdP donne à la partie qui a contrevenu à l'AdP la possibilité de remédier à la violation. Si la partie en infraction ne remédie pas à la violation dans les trente (30) jours suivant la réception par la partie en infraction d'une notification écrite de la partie non fautive exposant les détails de cette violation substantielle, la partie non fautive aura le droit de résilier le présent AdP et le Contrat conformément aux termes du Contrat ou, si la résiliation n'est pas possible, de signaler le problème au ministère ou à toute autre autorité compétente.

5.3. Effet de la Résiliation :

5.3.1.1. Sauf dans les cas prévus au paragraphe 5.3.2 ci-dessous, en cas de résiliation du présent AdP pour quelque raison que ce soit, le Partenaire Commercial doit renvoyer ou détruire toutes les PHI reçues du Client conformément au Contrat. Cette disposition s'applique aux PHI qui sont en possession de Sous-Traitants ou d'agents du Partenaire Commercial. Le Partenaire Commercial ne doit conserver 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 AdP 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 le Partenaire Commercial conserve ces PHI conformément aux conditions du Contrat.

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 ministère 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 infraction aux Règles de l'HIPAA, soit une infraction substantielle au présent AdP (« **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 de l'HIPAA ou du présent AdP, 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

règlera aucune 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 AdP.

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 en équité.

6.3. Références réglementaires. Toute référence dans le présent AdP à une section des Règles de l'HIPAA désigne cette section de l'HIPAA, la Règle de Confidentialité, la Règle de Sécurité et de Notification des Violations, l'HITECH Act 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 AdP qui pourrait s'avérer nécessaire pour permettre au Client ou au Partenaire Commercial de se conformer aux exigences des Règles de l'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 AdP et le Contrat 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 AdP n'est destinée à conférer, ni ne doit conférer, à toute personne autre que le Client, le Partenaire Commercial et leurs successeurs ou ayants droits 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 mandataire (tel que défini par le droit fédéral commun sur le mandat) du Client ou un employé. 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 AdP ou du Contrat, ou par la modification mutuelle de ceux-ci.

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