Avenant 1 relatif au traitement des données

Le présent Avenant sur le Traitement des données (ci-après, l'« Avenant ») est établi à la Date d'entrée en vigueur, par et entre :

Client tel que défini par l'EDT

– ci-après dénommé le « **Responsable du traitement** » –

et

L'entité Datasite telle que définie par le SOW

– ci-après dénommé le « **Sous-traitant** » –

Ci-après, chacun d'entre eux est également désigné individuellement comme étant la « **Partie** » et collectivement comme les « **Parties** »

Préambule :

(A) Les Parties ont conclu un Accord qui décrit les Services à fournir (définitions fournies à la Section 1 ci-dessous). Dans le cadre de la fourniture de Services par le Sous-traitant, des Données à caractère personnel peuvent être transférées par le Responsable du traitement au Sous-traitant.

(B) En cas de conflit entre les dispositions du présent Avenant et celles de l'Accord, les dispositions du présent Avenant prévaudront. Les termes en majuscules qui ne sont pas définis dans le présent Avenant sont définis dans l'Accord.

(C) Afin d'assurer le respect par les Parties des obligations de traitement conformément aux Règles de protection des données, telles que modifiées de temps à autre, les Parties conviennent de ce qui suit :

1. Définitions

1.1. Le terme « **Annexe** » désigne l'annexe jointe au présent Avenant et faisant partie intégrante de celui-ci.

1.2. Le « **Pays de protection des données** » ou les « Pays de protection des données » désignent un ou plusieurs pays où des lois sur la vie privée, la protection des données ou la sécurité des informations sont en vigueur et régissent les renseignements personnels ou privés ou les Données à caractère personnel, notamment l'Espace économique européen, le Brésil, Hong Kong, l'Australie, Singapour, le Canada, le Royaume-Uni et la Suisse.

1.3. Les « **Règles de protection des données** » désignent les lois nationales pertinentes qui s'appliquent au Traitement des Données à caractère personnel dans les Pays de protection des données, y compris, mais sans s'y limiter, les lois et règlements applicables en matière de confidentialité et de sécurité des informations qui s'appliquent de temps à autre.

1.4. Une « **Personne concernée** » désigne une personne physique identifiée ou identifiable dont les Données à caractère personnel font l'objet d'un Traitement ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, par référence à un identifiant tel qu'un nom, un numéro d'identification, une donnée de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques d'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale.

1.5. Un « **Incident lié à la sécurité des informations** » désigne tout transfert, accès et divulgation à des tiers, ou tout Traitement en violation du présent Avenant ou des Règles de protection des données ou tout événement affectant directement ou indirectement la confidentialité, l'intégrité ou l'authenticité des Données à caractère personnel.

1.6. Le « **Bouclier de protection des données** » désigne le Bouclier de protection des données UE-États-Unis, qui est entré en vigueur le 1er août 2016, et le Bouclier de protection des données Suisse-États-Unis, qui est entré en vigueur le 12 avril 2017.

1.7. L'« Accord » désigne l'Énoncé des travaux (EDT) et les Conditions générales conclus entre le Responsable du traitement et le Sous-traitant.

1.8. Les « **Données à caractère personnel** » désignent toute information relative à une Personne concernée et figurant dans le Contenu.

1.9. Les termes « **Traiter** », « **Traitement** » ou « **Traité** » désignent toute opération ou ensemble d'opérations effectuées ou non par des moyens automatisés sur des Données à caractère personnel, telles que la collecte,

l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou autre mise à disposition, l'alignement ou la combinaison, le verrouillage, la suppression ou la destruction.

1.10 Les « **Services** » désignent la prestation des services tels que décrits dans l'Accord et le présent Avenant.

1.11 Les « **Catégories particulières de données** » désignent les Données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques identifiant de manière unique une personne physique, ainsi que les Données à caractère personnel concernant la santé, la vie sexuelle ou l'orientation sexuelle.

2. Activités de traitement

Le Responsable du traitement est seul responsable de l'exactitude, de la qualité et de la légalité du Traitement des Données à caractère personnel, et doit se conformer aux règles applicables en matière de protection des données. Il est en outre responsable du respect de ces règles par les Utilisateurs invités. Le Sous-traitant accepte de traiter les Données à caractère personnel afin de fournir des Services conformément au présent Avenant et à l'Accord, conformément aux instructions écrites du Responsable du traitement énoncées à l'Annexe 1 du présent Avenant et que le Responsable du traitement peut communiquer de temps à autre. Si le Sous-traitant estime qu'une instruction enfreint les Règles de protection des données applicables, il en informe immédiatement le Responsable du traitement. Le Sous-traitant s'engage à traiter les Données à caractère personnel conformément aux Règles de protection des données en vigueur.

3. Durée et résiliation du présent Avenant

3.1. Le présent Avenant prend effet à la Date d'entrée en vigueur et demeure en l'état pendant la durée de l'Accord. Le présent Avenant prendra fin automatiquement à la résiliation ou à l'expiration de tout EDT.

3.2. Nonobstant la résiliation du présent Avenant, le Sous-traitant et tout prestataire demeurent liés par leurs obligations de confidentialité.

4. Transferts internationaux

Le Sous-traitant est certifié selon les cadres du Bouclier de protection des données et s'engage à respecter ses principes. Le Responsable du traitement reconnaît que le Sous-traitant peut traiter des Données à caractère personnel en dehors de l'EEE, du Royaume-Uni et des États-Unis. Toutefois, les Données à caractère personnel continueront à être stockées dans un Pays de protection des données ou aux États-Unis. Le Sous-traitant ne transmettra les Données à caractère personnel qu'en conformité avec les Règles de protection des données et informera le Sous-traitant s'il ne peut plus assurer un niveau de protection adéquat comme l'exigent les Règles de protection des données.

5. Normes de confidentialité et de sécurité des informations

5.1. Le Sous-traitant garantit la stricte confidentialité des Données à caractère personnel. Le Responsable du traitement doit s'assurer que ses employés connaissent les exigences applicables en matière de protection des renseignements personnels et de sécurité des informations et qu'ils sont tenus par des obligations de confidentialité juridiquement contraignantes.

5.2. Le Sous-traitant mettra en œuvre les mesures opérationnelles, techniques et organisationnelles appropriées pour protéger les Données à caractère personnel contre la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée et l'accès non autorisé tels que décrits à l'Annexe 2.

5.3. Le Sous-traitant mettra à jour les mesures de sécurité techniques et organisationnelles en fonction des développements technologiques raisonnables déterminés par ses soins et fournira sur demande une documentation à jour au Responsable du traitement sous la forme de sa certification ISO 27001 en vigueur.

6. Obligations de coopération et de notification

6.1. Les Parties coopéreront entre elles pour traiter rapidement et efficacement les demandes de renseignements, les plaintes et les réclamations relatives au Traitement des Données à caractère personnel émanant de toute autorité gouvernementale ou de toute Personne concernée. Si une Personne concernée s'adresse directement au Sous-traitant pour exercer ses droits relatifs aux Données à caractère personnel, le Sous-traitant doit transmettre cette demande au Responsable du traitement sans retard injustifié. Le Sous-traitant informera immédiatement le Responsable du traitement si les Données à caractère personnel font l'objet d'un contrôle ou d'une enquête des autorités publiques et ne divulguera aucune Donnée à caractère personnelle sans le consentement préalable du Responsable du traitement. Le Sous-traitant

fournira aux autorités publiques, sur demande, des renseignements concernant le Traitement en vertu du présent Avenant et autorisera les inspections dans le cadre de la portée énoncée à la présente Section 7.

6.2. Le Sous-traitant informera sans délai le Responsable du traitement d'un incident lié à la sécurité des informations dont il est déterminé qu'il a une incidence sur les Données à caractère personnel du Responsable du traitement. Le Sous-traitant doit fournir au Responsable du traitement les informations nécessaires pour aider et assister raisonnablement le Responsable du traitement, conformément aux Règles de protection des données.

7. Droits d'audit et d'inspection du Responsable du traitement

À la demande du Responsable du traitement, le Sous-traitant met à sa disposition les informations nécessaires pour démontrer que le Responsable du traitement respecte les obligations énoncées dans l'Avenant et dans les Règles de protection des données et pour permettre et contribuer aux audits, y compris les inspections effectuées par le Responsable du traitement ou par un auditeur tiers indépendant mandaté par celui-ci afin de vérifier la conformité du Sous-traitant au présent Avenant, à condition que les personnes effectuant cet audit signent avec le Sous-traitant un accord de confidentialité. Toutes les inspections doivent être effectuées pendant les heures normales de travail et sans nuire au déroulement des activités du Sous-traitant.

8. Recours à des Prestataires

8.1 Par la présente, le Responsable du traitement reconnaît et accepte que le Sous-traitant puisse avoir recours à des Prestataires pour Traiter les Données à caractère personnel. Le Sous-traitant mettra à la disposition du Responsable du traitement sa liste actuelle de Prestataires sur demande. Tout Prestataire sera autorisé à traiter des Données à caractère personnel uniquement pour fournir les Services que le Sous-traitant a retenus et sera lié contractuellement par des obligations contractuelles non moins protectrices que le présent Avenant. Le Sous-traitant est responsable des actes et omissions de tout Prestataire comme si les actes ou omissions avaient été effectués par le Sous-traitant. Le Sous-traitant tiendra le Responsable du traitement au courant de toute modification apportée au Traitement sous-traité et lui fournira sur demande une copie du présent contrat de sous-traitance.

8.2 Si le Sous-traitant a l'intention de nommer ou de remplacer un Prestataire visé par le présent Avenant, il doit informer le Responsable du traitement de cette situation et lui donner la possibilité de s'opposer raisonnablement à ces changements. Le Fournisseur fournira au Responsable du traitement toutes les informations que le Responsable du traitement peut raisonnablement demander pour évaluer si la nomination du sous-traitant proposé est conforme aux obligations du Responsable du traitement en vertu du présent Avenant et des Règles de protection des données applicables.

9. Retour et suppression des données à caractère personnel

À la demande du Responsable du traitement ou à la résiliation du présent Avenant, le Sous-traitant retournera ou détruira toutes les Données à caractère personnel et leurs copies. À la demande du Responsable du traitement, le Sous-traitant certifiera que cela a bien été fait.

10. Responsabilité et indemnisation

10.1 La Responsabilité des Parties et la limitation de cette responsabilité doivent être conformes à l'Accord.

10.2 Le Responsable du traitement couvre le Sous-traitant contre toute réclamation d'un tiers concernant le traitement des Données à caractère personnel fournies au Sous-traitant si le traitement de ces données n'était pas autorisé par les Règles de protection des données.

Responsable du traitement:	**Sous-traitant:**
Par : _____	Par : _____
Nom/Titre : _____	Nom /Titre : _____
Date :_____	Date : _____

Annexe 1 : Données à caractère personnel et finalités du traitement

Les Données à caractère personnel sont transférées et traitées aux **fins suivantes** :

- Référentiel en ligne sécurisé et partage de données à des fins de vérification diligente de l'entreprise, de transactions connexes ou à des fins commerciales internes.

Portée du traitement :

- Tel que décrit dans l'Énoncé des travaux, le Sous-traitant fournit une salle de données virtuelle, un référentiel en ligne sécurisé pour stocker, gérer, collaborer et distribuer des données et des documents.

Catégories de Données à caractère personnel :

- Noms, adresse, adresse e-mail professionnelle, numéro de téléphone professionnel, numéros d'identification nationaux, rémunération et avantages sociaux, informations sur les congés et les retraites, titres et fonctions et éventuellement tout autre type de données à caractère personnel intégrées dans les informations commerciales chargées par l'Administrateur du Responsable du traitement dans la salle virtuelle de stockage des données.

Catégories spéciales de données (le cas échéant) :

Les Données à caractère personnel concernent les Catégories spéciales de données suivantes (veuillez préciser) :

- Aucune, sauf indication contraire du Responsable du traitement

Personnes concernées :

Les Données à caractère personnel concernent les catégories suivantes de Personnes concernées :

- Renseignements commerciaux qui peuvent comprendre des données sur les propriétaires, les employés, les clients, les entrepreneurs et les fournisseurs.

Annexe 2 : Mesures de sécurité des informations

Sommaire de l'Annexe 2 :

I. Plan général de sécurité des données

Le Sous-traitant s'engage à mettre en place et à maintenir les mesures de protection des données suivantes :

	Exigence en matière de sécurité	Comment le Sous-traitant met-il en œuvre la mesure spécifique de sécurité des informations ?
	Veuillez décrire les mesures de contrôle d'accès (physiques) de votre entreprise pour empêcher les personnes non autorisées d'accéder aux systèmes de Traitement dans lesquels les Données à caractère personnel sont traitées ou utilisées (si votre entreprise a plusieurs filiales ou succursales, veuillez distinguer les différences entre les sites).	Tous les centres de données (datacentre) sont certifiés ISO 27001:2013 et SOC 2 Type 2. De plus, les centres de données sont certifiés selon les règles du Bouclier de protection des données. Un périmètre de contrôles de sécurité multiples est en place pour tous les centres de données qui incluent des méthodes d'authentification multiples pour y accéder.
2.	Veuillez décrire les mesures de contrôle d'accès prises dans votre entreprise pour empêcher l'utilisation des systèmes de traitement sans autorisation.	L'accès des utilisateurs est autorisé selon les besoins de l'activité et nécessite l'identification et l'approbation des rôles de gestion. Des fonctionnalités de délai d'attente, des exigences d'authentification strictes et des droits d'accès sont mis en œuvre et peuvent être suivis.
3.	Veuillez décrire les mesures de contrôle d'accès (virtuelles) prises dans votre entreprise pour garantir que les personnes autorisées à utiliser un système de Traitement n'ont accès qu'aux Données à caractère personnel auxquelles elles ont un droit d'accès et que ces données ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation lors de leur Traitement ou de leur utilisation et après stockage.	L'accès des utilisateurs autorisés est géré au moyen d'une procédure officielle d'enregistrement et de désinscription pour accorder et révoquer l'accès à tous les systèmes et services en fonction de leur rôle professionnel. Les rapports d'audit permettent une surveillance précise de l'activité des utilisateurs et des contrôles d'accès sont en place pour protéger l'intégrité et la confidentialité des données.
4.	Décrivez les mesures de contrôle de transmission prises dans votre entreprise pour garantir que les Données à caractère personnel ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant la transmission ou le transport électronique, et qu'il est possible de vérifier et d'établir à quels organes le transfert de ces données est envisagé à l'aide de moyens de transmission de données.	Le Sous-traitant dispose d'une politique sur les supports amovibles et des contrôles techniques appropriés pour protéger l'intégrité et la confidentialité des données et interdire le transfert non autorisé de Données à caractère personnel. L'accès à distance est contrôlé par authentification multifactorielle. Les données sont chiffrées au repos et en transit à l'aide de technologies de chiffrement approuvées par le gouvernement.

5.	Décrivez les mesures de contrôle de saisie pour s'assurer qu'il est possible de vérifier et d'établir si et par qui les Données à caractère personnel ont été ajoutées dans les systèmes de Traitement, modifiées ou supprimées.	Le Sous-traitant n'a aucune influence sur les données que le client choisit de charger. Toutes les actions de l'utilisateur en ce qui concerne l'intégrité et la confidentialité des données sont suivies et doivent faire l'objet d'un rapport. Le Responsable du traitement détermine seul quelles données sont fournies au Sous-traitant.
6.	Décrivez les mesures de contrôle de l'affectation dans votre entreprise pour vous assurer que, dans le cas d'un Traitement commandé, les Données à caractère personnel sont traitées en stricte conformité avec les instructions.	Des audits sont effectués chaque année dans le cadre de la certification ISO 27001 et du rapport SOC 2 de type 2 pour s'assurer que les exigences de conformité sont respectées. Les utilisateurs autorisés suivent la formation et reconnaissent chaque année le respect du code de déontologie et des politiques de l'entreprise. Tous les employés et les entrepreneurs doivent signer un
7.	Décrivez les mesures de contrôle de la disponibilité prises par votre entreprise pour garantir que les Données à caractère personnel sont protégées contre la destruction ou la perte accidentelle.	Le Sous-traitant dispose d'un mécanisme de redondance pour chaque plateforme et tient des registres de la disponibilité du système. De plus, la redondance permet des sauvegardes continues du système. Le Sous-traitant dispose de plans de reprise après sinistre et de continuité des opérations qui sont examinés, mis à
8.	Décrivez les mesures de contrôle de séparation que votre entreprise a prises pour s'assurer que les Données à caractère personnel recueillies à des fins différentes peuvent être traitées séparément.	La séparation logique est maintenue dans la même base de données mutualisée. Les utilisateurs autorisés sont limités au projet auquel ils sont authentifiés. Le Sous-traitant assure une séparation des données à 3 niveaux : développement, test et production.

II. Procédure/processus de sécurité des informations appliqué(e) par le Sous-traitant

Le Sous-traitant met en œuvre et suit les normes, processus et procédures suivants :

Datasite exploite un système de gestion de la sécurité des informations conforme aux exigences de la norme ISO/IEC 27001:2013 dans l'objectif suivant : la gestion de la sécurité des informations s'applique aux processus de protection des informations des clients concernant les services mondiaux de transactions financières et de rapports, de marketing et de communications pour les industries de réglementation, ainsi que le contenu des clients et les collaborations.