

CONDITIONS DE TRAITEMENT DES DONNÉES

ENTRE :

Le Client (ci-après dénommé le « **Responsable du traitement des données** »),

ET

HCL America, Inc. (ci-après dénommé le « **Sous-traitant** »).

CONVIENNENT DE CE QUI SUIT :

1. **Objet des présentes Conditions de traitement des données**

- 1.1. Les présentes Conditions de traitement des données s'appliquent exclusivement au traitement des données à caractère personnel qui sont soumises à la Législation européenne en matière de protection des données [dans le cadre du contrat en vigueur au [date] entre les parties pour la [prestation de services] (« Services ») (ci-après dénommé le « Contrat ») et sont intégrées par référence au Contrat et régies par celui-ci.
- 1.2. L'expression « Législation européenne en matière de protection des données » désigne le règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

i Bien que soit considéré ici un modèle européen, d'autres lois applicables peuvent s'appliquer selon l'endroit où les Services sont fournis.

- 1.3. Les termes « Traitement », « Données à caractère personnel », « Responsable du traitement » et « Sous-traitant » ont le sens qui leur est donné dans la Législation européenne en matière de protection des données.
- 1.4. Dans la mesure où le Sous-traitant traitera des Données à caractère personnel soumises à la Législation européenne en matière de protection des données pour le compte du Responsable du traitement dans le cadre de l'exécution du Contrat avec le Responsable du traitement, les dispositions du présent Contrat de protection des données sont applicables. Un aperçu des catégories de Données à caractère personnel, des types de Personnes concernées et des finalités pour lesquelles les Données à caractère personnel sont traitées figure à l'Annexe 2.

2. Le Responsable du traitement des données et le Sous-traitant

- 2.1. Le Responsable du traitement des données déterminera la portée, les finalités et la manière dont les Données à caractère personnel pourront être consultées ou traitées par le Sous-traitant. Le Sous-traitant traitera les Données à caractère personnel uniquement conformément aux instructions écrites du Responsable du traitement.
- 2.2. Le Sous-traitant ne traitera les Données à caractère personnel que sur instructions documentées du Responsable du traitement d'une façon appropriée (et dans la mesure appropriée) pour la prestation des services, sauf si cela est nécessaire pour se conformer à une obligation légale à laquelle le Sous-traitant est soumis. Dans ce cas, le Sous-traitant informera le Responsable du traitement de cette obligation légale avant le traitement, à moins que cette loi n'interdise expressément la communication de ces informations au Responsable du traitement. Le Sous-traitant informera sans délai le Responsable du traitement si, selon lui, une instruction enfreint le présent Contrat.
- 2.3. Les parties ont conclu un Contrat afin de bénéficier de l'expertise du Sous-traitant en matière de sécurisation et de traitement des Données à caractère personnel aux fins énoncées à l'Annexe 2. Le Sous-traitant est autorisé à exercer ses propres directives quant au choix et à l'utilisation des moyens qu'il juge nécessaires à la poursuite de ces objectifs, sous réserve des exigences des présentes Conditions de traitement des données.

- 2.4. Le Responsable du traitement garantit qu’il dispose de tous les droits nécessaires pour fournir les Données à caractère personnel au Sous-traitant pour le traitement à effectuer dans le cadre des Services. Dans la mesure requise par la Législation applicable en matière de protection des données, il incombe au Responsable du traitement de s’assurer que toutes les personnes concernées consentent à ce Traitement et qu’un registre de ces consentements est tenu à jour. En cas de révocation d’un tel consentement par la personne concernée, il incombe au Responsable du traitement de communiquer cette révocation au Sous-traitant et celui-ci reste responsable de l’application de toute instruction du Responsable du traitement concernant le traitement ultérieur de ces Données à caractère personnel.

3. Confidentialité

- 3.1. Sans préjudice de tout accord contractuel existant entre les parties, le Sous-traitant traitera toutes les Données à caractère personnel comme strictement confidentielles et informera tous ses employés, agents et/ou sous-traitants ultérieurs agréés engagés dans le traitement des Données à caractère personnel de la nature confidentielle des Données à caractère personnel. Le Sous-traitant s’assurera que toutes ces personnes ou parties ont signé un accord de confidentialité approprié, qu’elles sont liées par un devoir de confidentialité ou qu’elles sont soumises à une obligation légale de confidentialité appropriée.

4. Sécurité^{ii,iii}

- 4.1. Compte tenu de l’état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le Responsable du traitement des données et le Sous-traitant mettront en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité du traitement des Données à caractère personnel adapté au risque, sans préjudice des autres normes de sécurité arrêtées par les Parties. Ces mesures comprennent, selon les besoins :

ii Article 32(3) du RGPD : L’application d’un code de conduite approuvé comme le prévoit l’article 40 ou d’un mécanisme de certification approuvé comme le prévoit l’article 42 peut servir d’élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

iii Le Sous-traitant peut démontrer le respect en partageant les certifications

- (a) des mesures visant à garantir que les Données à caractère personnel ne soient accessibles qu'au personnel autorisé aux fins énoncées à l'Annexe 2 des présentes Conditions de traitement des données ;
 - (b) Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier de tous les risques présentés par le traitement, par exemple en cas de destruction, de perte ou d'altération accidentelle ou illicite, de stockage, de traitement, d'accès ou de divulgation non autorisés ou illicites de Données à caractère personnel ;
 - (c) la pseudonymisation et le chiffrement des Données à caractère personnel ;
 - (d) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - (e) des moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - (f) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des Données à caractère personnel ;
 - (g) les mesures visant à identifier les vulnérabilités en ce qui concerne le traitement des Données à caractère personnel dans les systèmes utilisés pour fournir des services au Responsable du traitement ;
 - (h) les mesures convenues par les parties à l'Annexe 3.
- 4.2. Le Sous-traitant doit disposer à tout moment d'une politique de sécurité écrite appropriée en ce qui concerne le traitement des Données à caractère personnel, décrivant en tout état de cause les mesures énoncées à l'article 4.1.
- 4.3. Sur demande du Responsable du traitement, le Sous-traitant démontrera les mesures qu'il a prises conformément au présent article 4 pour permettre au Responsable du traitement de vérifier et de tester ces mesures. Le Sous-traitant a droit à un préavis d'au moins 14 jours de la part du Responsable du traitement des données pour effectuer ou faire effectuer par un tiers ayant conclu un accord de confidentialité avec le Sous-traitant, des audits des locaux et des opérations du Sous-traitant relatifs aux Données à caractère personnel. Le Client est tenu d'assumer tous les frais et dépenses engagés dans le cadre d'un audit. À l'exception des audits effectués par un organisme de réglementation, les audits ne peuvent avoir lieu plus d'une fois par année civile et un préavis écrit d'au moins 14 jours doit être donné avant la réalisation d'un audit. Le Sous-traitant coopérera aux audits effectués par le Responsable du traitement ou en son nom. Le Client a le droit d'effectuer un audit des systèmes du Fournisseur utilisés pour le traitement des Données à caractère personnel du Client afin de vérifier que le Fournisseur respecte ses obligations au titre du présent Contrat en ce qui

concerne ce traitement. Tout audit sera soumis aux conditions suivantes :

- i. tout tiers nommé pour effectuer l'audit ne peut être un concurrent du Sous-traitant ou de l'une de ses Sociétés affiliées ;
- ii. Le Sous-traitant n'est pas tenu d'accorder à un tiers l'accès à ses systèmes, installations ou locaux à moins que ce tiers n'ait conclu un accord de confidentialité raisonnablement satisfaisant pour lui ;
- iii. la portée de tout audit sera strictement limitée aux systèmes (ou aux parties des systèmes) du Sous-traitant qui sont utilisés pour le traitement des Données à caractère personnel ;
- iv. sans limiter la portée de l'alinéa (c), ni le Responsable du traitement ni aucun tiers n'a le droit d'accéder aux données ou informations relatives aux autres clients du Fournisseur ou aux coûts ou marges internes du Fournisseur.

5. Améliorations à la sécurité

- 5.1. Les parties reconnaissent que les exigences en matière de sécurité évoluent constamment et qu'une sécurité efficace exige des évaluations fréquentes et des améliorations régulières des mesures de sécurité désuètes. Le Sous-traitant évaluera donc en permanence les mesures mises en œuvre conformément à l'article 4 et renforcera, complétera et améliorera ces mesures afin de maintenir le respect des exigences énoncées à l'article 4. Les parties négocieront de bonne foi le coût, s'il y a lieu, de la mise en œuvre des modifications importantes requises par les exigences de sécurité spécifiques mises à jour énoncées dans la Législation applicable en matière de protection des données ou par les autorités compétentes en matière de protection des données.
- 5.2. Lorsqu'une modification du Contrat est nécessaire pour exécuter une instruction du Responsable du traitement adressée au Sous-traitant en vue d'améliorer les mesures de sécurité qui peuvent être requises par des modifications périodiques de la législation applicable en matière de protection des données, les parties négocient de bonne foi une modification du Contrat.

6. Transferts de données

- 6.1. Le Sous-traitant informera sans délai le Responsable du traitement de tout transfert (prévu) permanent ou temporaire de Données à caractère personnel vers un pays situé en dehors de l'Espace économique européen sans un niveau de protection adéquat et n'effectue un tel transfert (prévu) qu'après avoir obtenu l'autorisation du Responsable du traitement. L'Annexe 4 fournit une liste des transferts pour lesquels le Responsable du traitement donne son consentement lors de la conclusion du Contrat et des présentes Conditions de traitement des données.
- 6.2. Dans la mesure où le Responsable du traitement ou le Sous-traitant s'appuie sur un mécanisme légal spécifique pour normaliser les transferts internationaux de données qui est ensuite modifié, révoqué ou déclaré invalide par un tribunal compétent, le Responsable du traitement et le Sous-traitant conviennent de coopérer de bonne foi pour mettre fin rapidement au transfert ou pour

rechercher un autre mécanisme approprié qui puisse légalement soutenir le transfert.

7. Obligations d'information et gestion des incidents

- 7.1. Lorsque le Sous-traitant prend connaissance d'un incident ayant une incidence sur le Traitement des Données à caractère personnel faisant l'objet du Contrat de services, il doit informer sans délai le Responsable du traitement, coopérer à tout moment avec lui et suivre ses instructions en la matière, afin de lui permettre de mener une enquête approfondie sur l'incident, de formuler une réponse correcte et de prendre les mesures appropriées en cas d'incident.
- 7.2. Le terme « incident » utilisé à l'article 7.1 désigne en tout état de cause :
- (a) une réclamation ou une demande concernant l'exercice des droits d'une personne concernée en vertu de la Législation européenne en matière de protection des données ;
 - (b) une enquête ou une saisie des Données à caractère personnel par des fonctionnaires du gouvernement, ou une indication spécifique précisant qu'une telle enquête ou saisie est imminente ;
 - (c) tout accès non autorisé ou accidentel, tout traitement, toute suppression, toute perte ou toute forme de traitement illicite des Données à caractère personnel ;
 - (d) toute violation de la sécurité et/ou de la confidentialité telles que définies aux articles 3 et 4 des présentes Conditions de traitement des données entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux Données à caractère personnel, ou toute indication qu'une telle violation a eu lieu ou est sur le point de se produire ;
 - (e) lorsque, de l'avis du Sous-traitant, l'exécution d'une instruction reçue du Responsable du traitement violerait les lois applicables auxquelles le Responsable du traitement ou le Sous-traitant sont soumis.
- 7.3. Le Sous-traitant doit disposer à tout moment de procédures écrites lui permettant de répondre rapidement au Responsable du traitement en cas d'incident. Lorsque l'incident est raisonnablement susceptible de nécessiter une notification de violation de données par le Responsable du traitement en vertu de la Législation européenne applicable en matière de protection des données, le Sous-traitant mettra en œuvre ses procédures écrites de telle sorte qu'il soit en mesure d'informer le Responsable du traitement au plus tard 72 heures après avoir pris connaissance d'un tel incident.

- 7.4. Toute notification faite au Responsable du traitement en application du présent article 7 doit être adressée à l'employé du Responsable du traitement dont les coordonnées figurent à l'Annexe 1 des présentes Conditions de traitement des données, et doit contenir :
- (a) une description de la nature de l'incident, y compris, si possible, les catégories et le nombre approximatif de personnes concernées ainsi que les catégories et le nombre approximatif de dossiers de Données à caractère personnel concernés ;
 - (b) le nom et les coordonnées du délégué à la protection des données du Sous-traitant ou d'un autre point de contact où des informations complémentaires peuvent être obtenues ;
 - (c) une description des conséquences probables de l'incident ; et
 - (d) une description des mesures prises ou envisagées par le Sous-traitant pour faire face à l'incident, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs éventuels.

8. Contrats avec des Sous-traitants ultérieurs

[Le Responsable du traitement des données autorise le Sous-traitant à engager les sous-traitants ultérieurs dans les pays pour les activités liées au Service décrites à l'Annexe 2

- 8.1. Le Sous-traitant veillera à ce que le sous-traitant ultérieur soit lié par les mêmes obligations en matière de protection des données que le Sous-traitant en vertu des présentes Conditions de traitement des données.
- 8.2. Le Responsable du traitement des données peut demander que le Sous-traitant procède à l'audit d'un Sous-traitant ultérieur tiers ou confirme qu'un tel audit a eu lieu (ou, le cas échéant, obtenir ou aider le client à obtenir un rapport d'audit tiers concernant les opérations du Sous-traitant ultérieur tiers) pour s'assurer du respect de ses obligations imposées par le Sous-traitant conformément au présent Contrat.

9. Renvoi ou destruction de Données à caractère personnel

- 9.1. En cas de résiliation du Contrat et des présentes Conditions de traitement des données, sur demande écrite du Responsable du traitement des données, ou sur réalisation de toutes les finalités convenues dans le cadre des Services pour lesquelles aucun autre traitement n'est nécessaire, le Sous-traitant doit supprimer, détruire ou renvoyer toutes les Données à caractère personnel au Responsable du traitement et détruire ou renvoyer toute copie existante.
- 9.2. Le Sous-traitant informera tous les tiers qui soutiennent son propre traitement des Données à caractère personnel de la résiliation du Contrat et des présentes

Conditions de traitement des données et veillera à ce que ces tiers détruisent les Données à caractère personnel ou les renvoient au Responsable du traitement, à la discrétion de ce dernier.

10. Assistance au Responsable du traitement

- 10.1. Le Sous-traitant est tenu d'assister le Responsable du traitement en prenant les mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour l'accomplissement de son obligation de répondre aux demandes d'exercice des droits de la personne concernée dans le cadre du RGPD.
- 10.2. Le Sous-traitant aidera le Responsable du traitement à s'assurer du respect des obligations visées au point 4 (Sécurité) et des consultations préalables avec les autorités de contrôle prévues à l'article 36 du RGPD, compte tenu de la nature du traitement et des informations dont disposent les Données.
- 10.3. Le Sous-traitant doit mettre à la disposition du Responsable du traitement des données toutes les informations nécessaires pour démontrer le respect des obligations du Sous-traitant des données et permettre et contribuer aux audits, y compris les inspections, effectués par le Responsable du traitement des données ou un autre auditeur mandaté par celui-ci.

11. Durée et résiliation

- 11.1. Les présentes Conditions de traitement des données entrent en vigueur à la date d'entrée en vigueur du Contrat applicable qui régit l'assistance et l'entretien et/ou les services professionnels fournis par le Sous-traitant au Responsable du traitement des données.
- 11.2. La résiliation ou l'expiration du Contrat et des présentes Conditions de traitement des données ne libère pas le Sous-traitant de ses obligations de confidentialité découlant de l'article 3.
- 11.3. Le Sous-traitant traitera les Données à caractère personnel jusqu'à la date de résiliation du Contrat, sauf instruction contraire du Responsable du traitement, ou jusqu'à ce que ces données soient renvoyées ou détruites sur instruction du Responsable du traitement.

12. Divers

- 12.1. En cas de contradiction entre les dispositions des présentes Conditions de traitement des données et les dispositions du Contrat de service, les dispositions des présentes Conditions de traitement des données prévaudront.

- 12.2. Le Responsable du traitement des données ne doit pas refuser ou retarder de façon déraisonnable l'acceptation de toute modification corrélative au présent Addenda proposée par le Sous-traitant afin de protéger ce dernier contre les risques supplémentaires associés. Si le Responsable du traitement propose d'autres modifications au présent Addenda qu'il estime raisonnablement nécessaires pour satisfaire aux exigences de toute Législation en matière de protection des données, les parties discuteront rapidement des modifications proposées et négocieront de bonne foi en vue de convenir et de mettre en œuvre ces modifications ou d'autres modifications conçues pour répondre aux exigences identifiées dans la notification du Client dès que cela sera raisonnablement possible.
- 12.3. Le Sous-traitant doit aviser sans délai le Responsable du traitement des données s'il reçoit une demande d'une Personne concernée en vertu d'une Législation en matière de protection des données concernant les Données à caractère personnel de la Personne concernée ; et s'assurer que le Sous-traitant engagé ne fasse pas de demande sauf sur les instructions documentées du Client ou de la Société affiliée concernée du Client ou sauf si les lois applicables auxquelles le Sous-traitant engagé est soumis l'exigent, auquel cas, dans la mesure permise par les lois applicables, le Sous-traitant informera le Responsable du traitement des données de cette exigence légale avant de répondre à la demande.
- 12.4. Les présentes Conditions de traitement des données sont régies par les lois de l'État membre dans lequel les Données à caractère personnel sont traitées. Tout litige découlant des présentes Conditions de traitement des données ou lié à celles-ci sera porté exclusivement devant le tribunal compétent de l'État membre dans lequel les Données à caractère personnel sont traitées.
- 12.5. Les parties conviennent de signer l'addenda ci-dessous au besoin.

Annexe 1 :

Coordonnées du [délégué à la protection des données/responsable de la conformité] du Responsable du traitement des données.

[Coordonnées]

Coordonnées du [délégué à la protection des données/responsable de la conformité] du Sous-traitant.

[Coordonnées]

Annexe 2 :

Les Données à caractère personnel qui seront traitées dans le cadre du Contrat et les finalités pour lesquelles elles seront traitées

Annexe 3 :

Mesures de sécurité

Annexe 4 :

Transferts vers des pays en dehors de l'Esace économique européen sans un niveau de protection adéquat pour lesquels le Responsable du traitement des données a donné son autorisation :