ADDENDA SUR LE TRAITEMENT DES DONNÉES

Le présent Addenda relatif au traitement des données (« **ATD** ») fait partie intégrante du Contrat conclu entre la Société et vous (le « **Client** ») (collectivement les « Parties » et individuellement la « **Partie** ») lors de la création de votre compte. En cas de conflit entre le présent ATD et le Contrat, le présent ATD prévaudra exclusivement en ce qui concerne le traitement des Données Personnelles. Le présent ATD entrera en vigueur à la date d'entrée en vigueur du Contrat et restera en vigueur jusqu'à la résiliation du Contrat ou jusqu'à la suppression ou la restitution de toutes les Données Personnelles, selon les instructions de l'une ou l'autre des Parties en vertu du présent ATD, selon la dernière éventualité.

1. DÉFINITIONS.
Les termes commençant par une majuscule et non définis dans les présentes auront le sens qui leur est attribué dans le Contrat. Si une loi sur la protection des données existe dans une juridiction, les définitions qui y sont énoncées prévaudront sur celles des présentes lorsque cette loi prévoit cette terminologie.

1.1 « **Contrat** » désigne tout accord entre la Société et le Client relatif aux Services. Un tel contrat peut porter différents intitulés, tels que « Bon de commande », « Conditions de service », « Contrat de service » ou des intitulés similaires.

1.2 « **Coordonnées d'affaires**» désigne les coordonnées liées à l'activité professionnelle (adresse e-mail, numéro de téléphone, nom, fonction, adresse professionnelle).

1.3 « **Client** » désigne le client de la Société, soit par le biais d'un Contrat avec un client de la Société, soit par le biais d'un Contrat avec une personne physique.

1.4 « **Compte Client et Données d'Utilisation** » désigne les informations concernant le Client que celui-ci fournit à la Société dans le cadre de la création et de la gestion d'un compte, telles que le prénom et le nom, le nom d'utilisateur, l'adresse e-mail et les informations de facturation et de paiement des personnes associées à un compte. Afin d'éviter toute ambiguïté, les données statistiques, les données analytiques, les données de session individuelles et les données anonymisées ne sont pas incluses dans cette définition.

1.5 « **Société** » désigne Certn Holdings Inc. et ses filiales et sociétés affiliées en propriété exclusive, notamment Certn (Canada) Inc., Certn (USA) Inc., Certn (UK) Ltd., InterCheck Global Pty. Ltd. et Trustmatic. sro , et toutes les sociétés affiliées identifiées dans la liste des Sous-traitants disponible dans le centre de confiance de la société, (https://trust.certn.co/).

1.6 « **Responsable du traitement** » désigne une personne morale, une autorité publique, une agence ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données personnelles et donne des instructions concernant les activités de traitement.

1.7 « **Clients Corporatifs** » désigne les Clients de la Société qui sont une entité commerciale enregistrée.

1.8 « **Demande de la personne concernée** » désigne toute demande d'une personne physique (la « personne concernée ») visant à accéder, mettre à jour, réviser, corriger, supprimer, s'opposer au traitement de ses

Données Personnelles, ou toute demande similaire, formulée conformément à la législation applicable en matière de protection des données.

1.9 « **Législation sur la protection des données** » désigne toutes les lois, règles ou réglementations applicables au Contrat, aux Services, à la Société ou au Client, ainsi que les normes industrielles applicables concernant la confidentialité, la protection des données, la confidentialité, la sécurité des informations, la disponibilité et l'intégrité, ou la gestion ou le Traitement (y compris la conservation et la divulgation) des Données personnelles, telles qu'elles peuvent être modifiées, reformulées ou remplacées de temps à autre.

1.10 « **Données Personnelles** » ou « **Informations Personnelles** » désigne toutes les informations obtenues par la Société auprès ou au nom du Client ou des Sous-traitants de la Société, sous quelque forme ou format que ce soit, qui identifient, concernent, décrivent, sont raisonnablement susceptibles d'être associées ou pourraient raisonnablement être liées, directement ou indirectement, à une personne physique identifiée ou identifiable.

1.11 « **Traitement(s)** », « **Traitement** » ou « **Traité(s**) » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés sur des Données Personnelles, y compris, mais sans s'y limiter, la collecte, l'enregistrement, l'organisation, le stockage, l'accès, l'adaptation, la modification, la récupération, la consultation, l'utilisation, la divulgation, la diffusion, la mise à disposition, l'alignement, la combinaison, le blocage, la suppression, l'effacement ou la destruction.

1.12 « **Sous-traitant** » ou "**Processeur"** désigne la Partie au présent Contrat, ou en vertu d'un contrat comportant sensiblement les mêmes exigences que le présent ATD, qui traite les Données Personnelles sous réserve des directives du Responsable du traitement et de la législation applicable en matière de protection des données.

1.13 « **Vendre** » signifie vendre, louer, libérer, divulguer, diffuser, mettre à disposition, transférer ou communiquer de toute autre manière, oralement, par écrit ou par des moyens électroniques ou autres, des Données personnelles à un tiers pour une contrepartie monétaire ou autre.

1.14 « **Services** » désigne les services que la Société exécute conformément au Contrat.

1.15 « **Clauses contractuelles types** » ou « **CCT** » désigne (a) lorsque le RGPD s'applique, les clauses contractuelles types annexées à la décision d'exécution 2021/914 de la Commission européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil (« CCT de l'UE ») ; (b) lorsque le RGPD du Royaume-Uni s'applique, l'addendum sur le transfert international de données aux clauses contractuelles types de la Commission européenne publié par le commissaire à l'information du Royaume-Uni, version B1.0, en vigueur le 21 mars 2022 (« CCT du Royaume-Uni ») ; et (c) lorsque la LPD suisse s'applique, les clauses types de protection des données applicables publiées, approuvées ou reconnues par le Commissaire fédéral suisse à la protection des données et à la transparence (les « CCT suisses »), chacune pouvant être mise à jour de temps à autre.

1.16 « **Sous-traitant ultérieur** » ou « **Prestataire de services** » désigne un tiers engagé et supervisé par une Partie au présent Contrat, qui accepte de recevoir et de traiter des Données personnelles conformément aux termes du présent ATD, ou d'un accord comportant les mêmes exigences que le présent ATD, uniquement aux fins de traitement ou de fourniture des Données personnelles nécessaires à l'exécution du présent Contrat. La liste des Sous-traitants ultérieurs de la Société est disponible dans le Centre de documentation de la Société (https://trust.certn.co/).

1.17 « **Système** » désigne tout système, réseau, plateforme, base de données, ordinateur ou système de

télécommunications ou d'information détenu, contrôlé ou exploité par ou au nom de l'une des Parties ou de l'une de ses sociétés affiliées aux fins du traitement des Données Personnelles conformément à l'accord.

2. RÔLES DES PARTIES

2.1 Dans la mesure où les Données Personnelles du Client sont traitées par la Société, les Parties conviennent que le Client est le Responsable du traitement et la Société est le Sous-traitant.

2.2 Dans la mesure où les Données Personnelles de la Société sont traitées par le Client, les Parties conviennent que la Société est le Responsable du traitement et le Client est le Sous-traitant.

2.3 Nonobstant ce qui précède, chaque Partie convient qu'elle est le Responsable du traitement des Coordonnées d'affaires de l'autre Partie qu'elle traite dans le cadre du contrat.

3. TRAITEMENT DES DONNÉES PERSONNELLES

La Société s'engage à :

3.1. Traiter les Données Personnelles uniquement dans la mesure nécessaire pour fournir les Services au Client, et conformément à la Législation sur la protection des données, au Contrat, au présent ATD, y compris les annexes I et II, et à toute instruction écrite supplémentaire fournie par le Client ;

3.2. S'abstenir de (i) vendre ou partager des Données Personnelles (ii) conserver, utiliser ou divulguer les Données Personnelles à des fins autres que celles spécifiées dans le Contrat, (iii) conserver, utiliser ou divulguer les Données Personnelles en dehors de la relation directe entre la Société et le Client, et (iv) combiner des Données Personnelles provenant de différentes sources, sauf si cela est nécessaire à la fourniture de Services en vertu du présent Contrat.

3.3. Maintenir la confidentialité de toutes les Données Personnelles et s'assurer que son personnel, y compris les employés, les stagiaires, les travailleurs temporaires et les travailleurs intérimaires, ont signé des accords de confidentialité qui les empêchent de traiter sans autorisation les Données Personnelles pendant la durée de leur engagement avec le Client.

3.4. Ne pas divulguer de Données Personnelles à des tiers, y compris des agences gouvernementales, sauf si la loi l'exige, et à des Sous-traitants, sauf pour la fourniture de Services en vertu du présent accord.

3.5. Lorsque la Législation sur la protection des données l'exige, informer rapidement (par courrier électronique) le Client de :

3.5.1 Toute demande, requête, plainte, avis ou communication reçue d'un tiers, y compris une personne concernée ou une autorité de contrôle, concernant des Données Personnelles, et se conformer aux instructions du Client pour y répondre. Le Client s'engage à répondre à la notification de la Société dans un délai de dix (10) jours ouvrables. Le Client accepte qu'en l'absence de réponse, la Société puisse, selon son jugement raisonnable, déterminer la suite à donner à la demande de la personne concernée ou de l'autorité de contrôle ;

3.5.2. Toute demande de communication de Données Personnelles à un organisme, une autorité ou un tribunal gouvernemental, que ce soit par des moyens légaux ou autres, y compris des détails spécifiques sur les données fournies, sauf si la loi ou un ordre juridique l'interdit ;

3.5.3. Toute instruction du Client que la Société estime être en violation de la Législation sur la protection des données avant de procéder au traitement concerné ; et

3.5.4. Tout changement substantiel apporté aux avis, politiques ou procédures de la Société qui entraverait la capacité de la Société à respecter les termes du présent ATD concernant la protection des Données Personnelles.

3.6. Conformément à la Législation sur la protection des données et pour les Clients Corporatifs, soumettre, sur demande écrite, les bases de données, outils, bureaux (le cas échéant) et autres environnements ou lieux similaires, cloud ou locaux, utilisés par la Société pour traiter les Données Personnelles à un audit, conformément aux dispositions d'audit prévues par le Contrat et à *la section 9 « Demandes d'informations »* ci-dessous. Pour éviter toute ambiguïté, les droits d'audit dont dispose le Client sont limités aux Services qui lui sont directement fournis en vertu du présent Contrat.

3.7. Conserver des registres qui démontrent sa conformité à ses obligations en vertu du présent ATD et les mettre raisonnablement à la disposition du Client sur demande et/ou dans le cadre de tout audit mentionné à la section 3.6 ci-dessus et à la section 9. Demandes d'informations ci-dessous.

3.8. Aider et coopérer raisonnablement avec le Client, notamment en fournissant les informations demandées par le Client, pour permettre au Client de se conformer à ses obligations en vertu de la Législation sur la protection des données, y compris la certification de l'achèvement par la Société des évaluations d'impact sur le transfert, des évaluations d'impact sur la vie privée et des évaluations d'impact sur la protection des données ; et

3.9. Conserver les Données Personnelles conformément à la section 6. Conservation des données de l'accord et *à la section 8. Suppression ou restitution des Données Personnelles* du présent ATD, mais en aucun cas plus longtemps que nécessaire pour exécuter les Services.

4. MESURES DE SÉCURITÉ DE L'INFORMATION

La Société déclare et garantit qu'elle a établi, maintient et respecte :

4.1. Des mesures de protection administratives, techniques et physiques visant à garantir la sécurité, la confidentialité, la fiabilité et l'intégrité des Données Personnelles, ainsi que de tous les systèmes, installations ou logiciels auxquels la Société accède ou qu'elle prend en charge dans le cadre du Contrat. Ces mesures de protection sont:

4.1.1. proportionnées au type et au volume des Données Personnelles Traitées par la Société, compte tenu de l'état de l'art et des normes de l'industrie, et devraient, au minimum, protéger les Données Personnelles et les Systèmes contre les menaces ou dangers raisonnablement anticipés, y compris l'accès non autorisé, la perte, le vol, la destruction, l'utilisation, la modification, la collecte, l'attaque ou la divulgation ;

4.1.2. conformes aux normes de contrôle de sécurité reconnues mondialement telles que l'ISO ; et

4.1.3. conformes aux normes spécifiques applicables du secteur, telles qu'elles peuvent s'appliquer aux Données Personnelles traitées par la Société.

4.2. Un programme et des politiques de sécurité écrits qui respectent ou dépassent les exigences imposées par la Législation sur la protection des données et sont conformes aux pratiques établies du secteur. Ce programme et ces politiques de sécurité couvrent au minimum les points suivants :

4.2.1. identification des rôles organisationnels définis de manière appropriée en matière de sécurité de l'information ;

4.2.2. les contrôles relatifs à l'emploi et à l'accès aux Données Personnelles par les employés, agents et Sous-traitants de la Société, y compris les vérifications des antécédents, la formation concernant le traitement des Données Personnelles et, le cas échéant, les habilitations de sécurité qui attribuent des privilèges d'accès spécifiques aux individus ;

4.2.3. un programme de sécurité réseau approprié qui comprend, sans limitation, le chiffrement et le partitionnement du réseau et des applications ;

4.2.4. l'identification et l'authentification des accès ;

4.2.5. entretien et élimination des supports ;

4.2.6. audit et responsabilité;

4.2.7. protections physiques et environnementales ;

4.2.8. sécurité des systèmes et des communications ;

4.2.9. réponse aux incidents et planification; et

4.2.10. l'intégrité et la fiabilité des installations, des systèmes et des Services, y compris l'identification des actifs critiques, la configuration et la gestion des changements pour les systèmes logiciels, ainsi que la planification d'urgence/la redondance.

4.3. Si les Données Personnelles traitées comprennent des données sensibles ou biométriques permettant d'identifier une personne physique de manière unique, ou des données relatives à des condamnations pénales et à des infractions, la Société appliquera des restrictions spécifiques et/ou des garanties supplémentaires, conformément à la Législation sur la protection des données. Le Client accepte que la Société puisse mettre en œuvre ponctuellement des mesures de sécurité alternatives adéquates, à condition que le niveau de sécurité de ces mesures ne soit pas significativement réduit.

4.4. La Société limitera l'accès aux Données Personnelles aux personnes qui en ont besoin pour remplir ses obligations relatives à la prestation des Services au Client. La Société veillera à ce que ces personnes soient informées par écrit du caractère confidentiel ou sensible des Données Personnelles.

5. INCIDENT DE SÉCURITÉ DES DONNÉES

5.1. Incident de sécurité des données signifie (i) la perte ou l'utilisation non autorisée (par quelque moyen que ce soit) de Données Personnelles ; (ii) la divulgation, l'accès, la modification, la corruption, le transfert, la vente, la location, la destruction ou l'utilisation par inadvertance, non autorisé et/ou illégal de Données Personnelles ; ou (iii) tout autre acte ou omission qui compromet ou peut compromettre la sécurité, la confidentialité ou l'intégrité des Données Personnelles ou d'un Système.

5.2. Si la Société soupçonne ou prend connaissance d'un Incident de sécurité des données, elle devra :

5.2.1. Notifier le Client sans retard injustifié, et en tout état de cause dans les soixante-douze (72) heures, après avoir pris connaissance de tout Incident de sécurité des données confirmé ;

5.2.2. Entreprendre une enquête sur un tel Incident de sécurité des données et répondre aux demandes raisonnables du Client en matière d'informations relatives à l'Incident de sécurité des données, si nécessaire ;

5.2.3. Assister raisonnablement le Client, ses autorités de régulation et les forces de l'ordre dans le respect de leurs obligations de notification en vertu de la Législation applicable en matière de protection des données. Sauf disposition contraire prévue par la législation applicable, le Client est seul responsable du respect des exigences de notification de violation de données prévues par la Législation applicable en matière de protection des données et de l'exécution de toute obligation de notification de tiers relative à tout incident de sécurité des données ; et

5.2.4. Prendre toutes les mesures correctives raisonnables dans les meilleurs délais, aux frais de la Société, afin de remédier à un tel Incident de sécurité des données et d'empêcher qu'il ne se reproduise.

6. SOUS-TRAITANTS

6.1. Le Client accorde par la présente à la Société une autorisation écrite générale pour désigner des Sous-traitants pour effectuer des activités de Traitement spécifiques en son nom. La liste des Sous-traitants actuellement engagés par la Société dans le cadre des Services est disponible dans le Centre de Confidentialité de la Société (https://trust.certn.co/).
6.2. La Société informera de la nomination d'un nouveau Sous-traitant sur son site web via (https://trust.certn.co/). Le Client est invité à consulter régulièrement la Liste des Sous-traitants afin de se tenir informé de la liste des Sous-traitants de la Société.

6.3. Lorsque la Législation sur la protection des données l'exige, et uniquement pour les Clients Corporatifs, la Société informera par écrit (un courriel suffit) le nouveau Sous-traitant ultérieur. Le Client Corporatif a le droit de s'opposer raisonnablement au recours à un Sous-traitant ultérieur. Les instructions relatives à l'opposition du Sous-traitant ultérieur sont disponibles dans le Centre de gestion de la confidentialité de la Société (https://trust.certn.co/). Si, en tant que Client Corporatif, une objection est soulevée, la Société déploiera des efforts raisonnables pour trouver un autre Sous-traitant ultérieur pour effectuer les activités de traitement spécifiques. Si aucun Sous-traitant ultérieur approprié ou aucune autre solution ne peut être trouvée, le Client peut résilier la partie concernée du Contrat à laquelle les Services du Sous-traitant ultérieur se rapportent.

6.4. La Société garantit que tout Sous-traitant engagé par la Société pour traiter des Données Personnelles en vertu du présent Contrat a :

6.4.1. Fournit des garanties appropriées et maintient un niveau de protection adéquat en ce qui concerne le traitement et le transfert des Données Personnelles ;

6.4.2. A conclu un accord écrit avec la Société, qui comprend des conditions sensiblement similaires à celles du présent ATD, contenant notamment les mêmes obligations de protection des données que celles énoncées dans le présent ATD ; et

6.4.3. A établi les mécanismes appropriés pour garantir que toute personne concernée dispose de droits exécutoires et de recours juridiques efficaces.

6.5. La Société reconnaît qu'en tant que Sous-traitant, elle est responsable envers les Clients Corporatifs du respect par le Sous-traitant de la Société de ses obligations en matière de protection des données telles qu'elles s'appliquent au traitement des Données Personnelles Traitées en vertu du Contrat et du présent ATD.

7. TRANSFERTS INTERNATIONAUX DE DONNÉES

7.1. **Généralités** . Les Parties conviennent que, dans le cas où une juridiction ne dispose pas actuellement d'une Législation sur la protection des données prévoyant des transferts de données hors du pays, ces transferts seront soumis aux normes et attentes imposées par le Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD UE ») et, par conséquent, aux Clauses contractuelles types de l'UE (« CCT UE »), y compris les transferts entre la Société et ses Sous-traitants. En signant le présent ATD, le Client autorise la Société à conclure les CCT UE pour son compte (en tant qu'exportateurs) avec ses propres filiales et Sous-traitants, afin de garantir un niveau de protection adéquat des Données personnelles, conformément à la Législation sur la protection des données. En cas de conflit entre le présent ATD et les Clauses contractuelles types de l'UE, les Clauses contractuelles types de l'UE prévaudront dans la mesure nécessaire au respect de la Législation sur la protection des données.

7.2. **Traitement et transferts de données vers des juridictions sanctionnées.** Dans le cadre de l'exécution du présent ATD et du Contrat, le Client autorise la Société à traiter et transférer des Données Personnelles depuis sa juridiction, si nécessaire, vers toute juridiction où la Société ou ses Sous-traitants sont situés, à condition que ces juridictions ne soient pas actuellement sanctionnées par l'Office of Foreign Assets Control (OFAC) ou par des listes de sanctions similaires au Canada, au Royaume-Uni ou en Australie, et vers tout autre pays reconnu par la Commission européenne comme offrant un niveau adéquat de protection des Données personnelles.

7.3. **Transferts de données depuis l'Espace économique européen soumis aux clauses contractuelles types de l'UE.** Lorsque le transfert de Données Personnelles est soumis au RGPD de l'UE et donc aux clauses contractuelles types de l'UE, l'« importateur de données » est le Sous-traitant ou son Sous-traitant ultérieur, selon le cas et tel que déterminé par le Sous-traitant, et l'« exportateur de données » est le Responsable du traitement ou le Responsable du traitement-Sous-traitant de ces Données Personnelles. Le Sous-traitant veille à ce que le Sous-traitant ultérieur concerné respecte (le cas échéant) les obligations de l'importateur de données, et le Responsable du traitement respecte celles de l'exportateur de données, dans chaque cas en vertu des clauses contractuelles types applicables.

7.3.1. La Société sera un Sous-traitant des Données Personnelles ;

7.3.2. Le Client sera un Responsable du Traitement des Données Personnelles ;

7.3.3. Le Module 2 (Responsable du Traitement à Sous-traitant) s'appliquera ;

7.3.4. La Clause 7 (Clause d'arrimage) s'appliquera ;

7.3.5. Les Parties choisissent l'Option 2 de la Clause 9 ;

7.3.6. L'option de la Clause 11(a) (Recours) du Module 2 s'appliquera ;

7.3.7. Les Parties choisissent l'Option 1 de la Clause 17, le droit irlandais s'appliquera ; et

7.3.8. Aux fins des Clauses Contractuelles Types, les Annexes I et II seront incorporées et respecteront les normes énoncées dans le RGPD de l'UE.

7.4. **Transferts de données depuis et vers des pays offrant des niveaux adéquats de protection des données.** Les Informations Personnelles peuvent être transférées des États membres de l'UE et des pays membres de l'EEE (Norvège, Liechtenstein et Islande) (collectivement, « EEE ») vers des pays offrant un niveau adéquat de protection des données (y compris le Canada) en vertu des décisions d'adéquation publiées par les autorités compétentes en matière de protection des données de l'EEE ou de la Commission européenne (« Décisions d'adéquation »), selon le cas, sans qu'aucune autre garantie ne soit nécessaire.

7.5. **Transferts de données depuis la Suisse** . La Société adhère à la Loi fédérale sur la protection des données révisée de la Suisse (LPD révisée). Dans la mesure où l'autorité de surveillance suisse considère que les CCT offrent des garanties appropriées aux fins du transfert d'Informations Personnelles et de données de personnes morales, les modifications suivantes s'appliquent aux transferts suisses : (i) les Parties adoptent la norme RGPD pour tous les transferts de données ; (ii) en ce qui concerne la clause 13a, l'autorité de surveillance de l'UE est compétente dans la mesure où le transfert de données est régi par le RGPD et l' autorité de surveillance suisse (PFPDT) exerce une surveillance parallèle, le cas échéant ; et (iii) en ce qui concerne la clause 18 c, le terme « État membre » doit être interprété de manière à permettre aux personnes concernées en Suisse de faire valoir leurs droits dans leur lieu de résidence habituelle (Suisse).

7.6. **Transferts de données depuis le Royaume-Uni** . Dans la mesure où l'autorité de contrôle britannique (le Commissaire à l'information) considère que les clauses contractuelles types offrent des garanties appropriées pour le transfert de Données Personnelles vers un pays tiers ou une organisation internationale, conformément à l'article 46 du RGPD britannique, et concernant les transferts de données des responsables du traitement vers les Sous-traitants et/ou des Sous-traitants vers les Sous-traitants, les modifications suivantes s'appliquent aux transferts depuis le Royaume-Uni :

7.6.1. Les détails du ou des transferts et en particulier les catégories d'Informations Personnelles transférées et la ou les finalités pour lesquelles elles sont transférées sont ceux spécifiés à l'annexe I, section B, lorsque les lois britanniques sur la protection des données s'appliquent au traitement des données par l'exportateur lors de ce transfert.

7.6.2. Les références au « Règlement (UE) 2016/679 » ou à « ce Règlement » sont remplacées par « Lois britanniques sur la protection des données » et les références à des articles spécifiques du « Règlement (UE) 2016/679 » sont remplacées par l'article ou la section équivalent(e) des lois britanniques sur la protection des données. En particulier :

7.6.2.1. Les références au règlement (UE) 2018/1725 sont supprimées ;

7.6.2.2. Les références à « Union », « UE » et « État membre de l'UE » sont toutes remplacées par « Royaume-Uni » ;

7.6.2.3. La clause 13(a) n'est pas utilisée et l'« autorité de contrôle compétente » est le Commissaire à l'information ;

7.6.2.4. La clause 17 est remplacée par « Les présentes CCT sont régies par le droit anglais et gallois » ;

7.6.2.5. La clause 18 est remplacée par « Tout litige découlant des présentes CCT sera tranché par les tribunaux anglais et gallois. Une personne concernée peut également intenter une action en justice contre l'exportateur et/ou l'importateur de données devant les tribunaux de tout pays du Royaume-Uni. Les Parties conviennent de se soumettre à la juridiction de ces tribunaux. » ; et

7.6.2.6. Les notes de bas de page des CCT ne s'appliquent pas aux transferts vers le Royaume-Uni.

7.6.2.7. La Société sera un Sous-traitant de Données Personnelles ;

7.6.2.8. Le Client sera Responsable du traitement des Données Personnelles ;

7.6.2.9. Le module 2 (du Responsable du traitement au Sous-traitant) s'applique ;

7.6.2. 10. La clause 7 (clause d'arrimage) s'applique ;

7.6.2.11. Les Parties choisissent l'option 2 de la clause 9.

7.6.2.12. L'option de la clause 11(a) (Recours) modèle 2 s'applique ;

7.6.2.13 . Les Parties choisissent l'option 1 de la clause 17, le droit anglais et gallois s'applique ; et

7.6.2.14 . Aux fins de l'addendum britannique, les annexes I et II suffisent et satisfont aux exigences requises par la législation britannique sur la protection des données.

7.7. **Transfert de données depuis l'EEE, le Royaume-Uni ou la Suisse vers les États-Unis**. Le transfert de données depuis l'EEE, le Royaume-Uni ou la Suisse peut être considéré comme adéquat s'il est effectué conformément au Cadre de protection des données UE-États-Unis ou Suisse-États-Unis. Ces cadres entre le Département du Commerce des États-Unis, la Commission européenne, le gouvernement britannique et l'administration fédérale suisse s'appliquent uniquement aux entités commerciales inscrites au Programme-cadre de protection des données du Département du Commerce des États-Unis, afin de permettre le transfert de Données Personnelles depuis l'Union européenne conformément à la décision d'adéquation de la Commission européenne.

7.8. **Transfert de données depuis la province canadienne du Québec.** Lorsque le transfert de Données Personnelles concernant un résident de la province canadienne du Québec est soumis à la Loi sur la protection des renseignements personnels dans le secteur privé (la « Loi sur le secteur privé »), la Société effectue une analyse d'impact du transfert conformément à la Loi sur le secteur privé afin de déterminer que ce transfert à son Sous-traitant ultérieur bénéficiera de niveaux de protection adéquats, proportionnels à la nature et au volume des Données Personnelles, y compris, mais sans s'y limiter, aux normes et attentes énoncées dans le présent Contrat.

8. SUPPRESSION OU RESTITUTION DES DONNÉES PERSONNELLES

8.1. À l'expiration ou à la résiliation anticipée du Contrat, et à la demande du Client, la Société supprimera ou restituera, au choix du Client, toutes les Données personnelles en possession ou sous le contrôle de la Société

et des Sous-traitants de la Société, à moins que la conservation continue de ces Données personnelles ne soit requise par la loi applicable.

8.2. Sans limiter la généralité de ce qui précède, et sur demande écrite, la Société et ses Sous-traitants doivent, dans les trente (30) jours suivant une demande écrite du Client, ou à la suite d'une suspension du transfert des Données Personnelles, fournir une copie des Données Personnelles dans un format portable et facilement utilisable.

9. DEMANDES D'INFORMATIONS

9.1. Conformément au Contrat, la Société s'engage à coopérer raisonnablement avec les Clients Corporatifs afin de leur fournir les informations raisonnablement nécessaires pour leur permettre de démontrer leur conformité aux obligations énoncées dans le présent ATD, et à permettre et contribuer aux audits, y compris les inspections, menés par le Client Corporatif ou un évaluateur tiers indépendant qualifié, acceptable par la Société et tenu par des obligations de confidentialité satisfaisantes pour la Société, dans la mesure où ces informations sont sous le contrôle de la Société et que la loi applicable, un devoir de confidentialité, un privilège ou une protection juridique, ou toute autre obligation envers un tiers, ne l'empêchent pas de les divulguer. Les audits et inspections seront sujet à un préavis écrit de 30 jours, effectués aux frais du Client et au maximum une fois tous les douze (12) mois, pendant la durée du Contrat, pendant les heures ouvrables habituelles.

9.2. La Société s'engage, compte tenu de la nature du traitement et des informations dont elle dispose, à aider raisonnablement les Clients Corporatifs à respecter ses obligations décrites par la Législation applicable en matière de protection des données afin de préserver la sécurité des Données Personnelles en maintenant des normes de sécurité raisonnables telles que définies dans le présent ATD ; à aider raisonnablement les Clients Corporatifs à notifier l'autorité de régulation ou de surveillance compétente, y compris le Information Commissioner's Office (« ICO »), des violations de Données Personnelles ; à aider raisonnablement à notifier les Personnes Concernées des violations de Données Personnelles ; à aider raisonnablement les Clients Corporatifs à réaliser des analyses d'impact sur la protection des données (AIPD) lorsque cela est nécessaire, et, aux frais du Client Corporatif, à consulter raisonnablement l'ICO lorsqu'une AIPD indique qu'il existe un risque élevé qui ne peut être atténué.

10. CESSION ET SUCCESSEURS

Le Client ne peut céder aucun de ses droits ou obligations au titre du présent ATD sans le consentement écrit préalable de la Société, lequel ne pourra être refusé sans motif valable. Sous réserve de ce qui précède, les droits et obligations découlant du présent Contrat sont garantis au Client et à ses cessionnaires, bénéficiaires et successeurs autorisés et les lient. Toute tentative de cession en violation de la présente clause est nulle. Nonobstant ce qui précède, la Société a le droit de céder tout droit ou obligation au titre du présent ATD.

11. AVIS DE L'ENTREPRISE COORDONNÉES

11.1. Les notifications relatives aux Incidents de sécurité des données doivent être envoyées aux personnes suivantes :

À : Security@certn.co

CC : Privacy@certn.co and Legal@certn.co

11.2. Les avis relatifs aux Demandes d'exercice des droits des personnes concernées et aux mises à jour des Sous-traitants doivent être envoyés aux adresses suivantes :

À : Privacy@certn.co

11.3. Avis relatifs aux demandes de divulgation d'organismes gouvernementaux ou de réglementation :

À : Legal@certn.co

CC : Privacy@certn.co

11.4. Toutes les autres notifications relatives au présent ATD doivent être adressées à l'adresse suivante :

À: Privacy@certn.co

CC: Legal@certn.co

ANNEXE I

Section A : Liste des Parties

L'exportateur de données	L'exportateur de données est identifié comme le Client ou le « Responsable du traitement » dans le ATD.
L'importateur de données	L'importateur de données est Certn, un fournisseur de services de vérification des données et de vérification des antécédents.

Section B : Description du traitement et du transfert

1. Catégories de personnes concernées dont les Données Personnelles sont transférées
Les personnes et les candidats soumis aux Services de vérification des antécédents à des fins d'emploi, de location ou à toute autre fin légale et autorisée selon les instructions du Responsable du traitement.

2. Catégories de Données Personnelles transférées
Coordonnées d'affaires : A la signification qui lui est donnée à la section 1.2 de la DPA.

Données personnelles de la personne concernée : Les Données Personnelles exactes de la personne concernée varieront en fonction du service de vérification des antécédents demandé, mais peuvent inclure les éléments suivants, selon les besoins : adresses e-mail, noms, coordonnées, intitulés de poste, adresse résidentielle ou professionnelle ; photographie ; numéros d'identification personnels ; titre et qualifications académiques ; parcours professionnel ; permis de conduire ; registres de présence ; intitulé de poste ; sexe ; numéro de téléphone professionnel (y compris le numéro de téléphone portable) et numéro de fax ; adresse e-mail personnelle ; numéro de téléphone personnel (y compris le numéro de téléphone portable) ; score ou limite de crédit, score de risque, d'échec et de délinquance ; informations de paiement ; antécédents criminels ; dossiers de réclamations et de

jugements associés ; dossiers publics tels que mandats d'administrateur, insolvabilités, faillites, situation financière, adresse IP ; données de cookie ; identifiants de connexion (nom d'utilisateur et mot de passe) ; données de trafic ; images et sons ; données biométriques.

3 . **Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui prennent pleinement en compte la nature des données et les risques encourus, comme une limitation stricte de la finalité, des restrictions d'accès (y compris l'accès uniquement pour le personnel ayant suivi une formation spécialisée), la conservation d'un enregistrement de l'accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires.**
Le contenu des Données Personnelles est varié et sous le contrôle de l'Exportateur de Données, mais peut, selon les Services concernés, inclure des données sensibles telles que définies par la Législation sur la Protection des Données applicable. Les Données Personnelles Sensibles seront protégées conformément aux mesures énoncées dans l'ATD.

4. Fréquence des Transferts
Les Transferts seront traités de manière ponctuelle et pour la durée nécessaire à l'exécution des Services ; à toute autre finalité stipulée dans le Contrat ; et dans le respect des lois et réglementations applicables.

5. Nature du Traitement
La nature et la finalité du traitement désignent toute opération telle que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'extraction, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre forme de mise à disposition, la restriction, l'effacement ou la destruction de données (que ce soit par des moyens automatisés ou non).

6. Finalité(s) du Transfert de Données et Traitement ultérieur
Fournir les Services au Client tel qu'indiqué dans le Contrat ; exécuter le Contrat, le présent ATD et/ou d'autres contrats exécutés par les Parties ; fournir un support et une maintenance technique, si convenu dans le Contrat ; prévenir, atténuer et enquêter sur les risques d'Incidents de sécurité des données, de fraude, d'erreur ou de toute activité illégale ou interdite ; se conformer aux lois et réglementations applicables ; toutes les tâches liées à l'un des éléments ci-dessus.

7. La durée de conservation des Données Personnelles ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée

Les Parties conviennent d'effacer les Données Personnelles de tout ordinateur, périphérique de stockage et support de stockage dès que possible après qu'il ne soit plus nécessaire pour elles de les conserver en vertu de la législation applicable en matière de protection des données ou conformément au Contrat. Nonobstant ce qui précède, sauf accord contraire entre les Parties ou exigence contraire de la législation applicable en matière de protection des données, les Parties conviennent que les dossiers des Clients seront conservés par la Société conformément à sa Politique de Conservation, susceptible d'être mise à jour.

Les Données Personnelles collectées et traitées dans le cadre d'une vérification de type « Disclosure and Barring Service (« DBS ») sont conservées pour une période minimale de deux (2) ans en conformément aux lignes directrices applicables.

8. Pour les transferts à des Sous-traitants, veuillez également préciser l'objet, la nature et la durée du traitement.
Tous les Sous-traitants autorisés sont tenus de mettre en œuvre et de maintenir des mesures, responsabilités et obligations techniques et organisationnelles identiques ou sensiblement similaires à celles exigées du fournisseur en vertu du présent ATD.

Section C : Autorité de contrôle compétente

1. Lorsque l'exportateur de données est établi dans un État membre de l'UE : L'autorité de contrôle chargée de veiller au respect par l'exportateur de données du règlement (UE) 2016/679 en ce qui concerne le transfert de données agit en tant qu'autorité de contrôle compétente.

2. Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE mais relève du champ d'application territorial du règlement (UE) 2016/679 conformément à son article 3, paragraphe 2, et a désigné un représentant conformément à l'article 27, paragraphe 1, du règlement (UE) 2016/679 : L'autorité de contrôle de l'État membre dans lequel le représentant au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi agit en tant qu'autorité de contrôle compétente.

3. Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE mais relève du champ d'application territorial du règlement (UE) 2016/679 conformément à son article 3(2) sans toutefois avoir à désigner un représentant conformément à l'article 27(2) du règlement (UE) 2016/679 : la Commission de protection des données (DPC) – 21 Fitzwilliam Square, South Dublin 2, D02 RD28 Irlande agira en tant qu'autorité de contrôle compétente.

4. Lorsque l'exportateur de données est établi au Royaume-Uni ou relève du champ d'application territorial des lois et règlements britanniques sur la protection des données, le Bureau du Commissaire à l'information agira en tant qu'autorité de contrôle compétente.

5. Lorsque l'exportateur de données est établi en Suisse ou relève du champ d'application territorial des lois et règlements suisses sur la protection des données, le Préposé fédéral à la protection des données et à la transparence de la Suisse agira en tant qu'autorité de contrôle compétente dans la mesure où le transfert de données concerné est régi par les lois et règlements suisses sur la protection des données.

6. Lorsque l'exportateur de données est établi dans la province canadienne du Québec ou relève du champ d'application territorial des lois québécoises sur la protection des données, la Commission d'accès à l'information du Québec agira en tant qu'autorité de contrôle compétente.

ANNEXE II

Vous trouverez ci-dessous les mesures techniques, physiques et administratives utilisées par la Société pour assurer la sécurité des Données Personnelles.

1. **Programme.** La Société maintient un programme écrit de sécurité de l'information (« Programme de sécurité de l'information »), qui contient des mesures de protection administratives, techniques et organisationnelles raisonnablement appropriées et conformes à la présente Annexe II. La Société organise des formations internes en matière de sécurité pendant la phase d'intégration et chaque année par la suite.

2. **Certifications de sécurité.** La Société maintient en permanence les certifications ISO 27001, SOC2 et SOC3. Le rapport de conformité ISO 27001 et SOC2 est disponible sur demande. Le rapport de conformité SOC 3 est accessible au public. Visitez le Centre de documentation de la Société pour plus d'informations (https://trust.certn.co/).

3. **Contrôles d'accès.** Un système de contrôle d'accès applicable à tous les utilisateurs accédant au système informatique a été mis en œuvre. Le système permet à la Société de créer, d'approuver, de réviser et de supprimer des comptes d'utilisateurs.

a. La Société met en œuvre une authentification multi facteur pour tous les comptes ayant accès aux Données Personnelles. Lorsque les mécanismes d'authentification reposent sur des mots de passe, le Sous-traitant exige que le mot de passe comporte au moins huit caractères et soit conforme à des paramètres de contrôle très stricts, notamment en termes de longueur, de complexité des caractères et de non-répétabilité.

b. Autorisations basées sur les rôles, conformément à une politique de contrôle des autorisations établie. Lors de l'octroi d'accès ou de l'attribution de rôles d'utilisateur, le principe du « besoin de savoir » est respecté afin de limiter l'accès aux Informations Personnelles à ceux qui en ont besoin pour atteindre les finalités de traitement du Sous-traitant.

c. La Société maintient une politique de gestion des actifs qui définit les normes de configuration et toutes les variables applicables. Une politique de contrôle d'accès aux systèmes a été définie, documentée et mise en œuvre pour permettre l'évaluation des contrôles et de l'accès aux actifs de l'entreprise.

4. **Gestion des comptes.** La Société gère la création, l'utilisation et la suppression de tous les identifiants de compte utilisés pour accéder à son infrastructure clé, notamment en exigeant une authentification multifacteur dans tous les systèmes critiques. Les Informations Personnelles traitées sont limitées aux identifiants strictement nécessaires définis par les sources de données avec lesquelles nous opérons. Afin de garantir l'exactitude, la pertinence, l'exhaustivité et la mise à jour des Informations Personnelles, l'entreprise procède à des vérifications des données en temps réel, avec le consentement de la personne concernée et uniquement dans les limites de la finalité autorisée définie. Toute donnée potentiellement incomplète est reconfirmée auprès de la personne concernée et/ou de la source de données concernée.

5. **Gestion des vulnérabilités.** La Société assure la gestion des vulnérabilités, l'évaluation des risques, la gestion des actifs, les systèmes de détection et de prévention des intrusions (IDS) et de prévention des intrusions (IPS), la gestion des correctifs, la surveillance des terminaux et la gestion des fournisseurs d'outils SIEM. Le SIEM collecte les événements et les politiques, et des alertes sont créées à des fins d'analyse et d'enquête. Protection et surveillance des terminaux, détection et prévention des intrusions avec surveillance et évaluation.

6. **Segmentation de la sécurité.** La Société surveillera, détectera et restreindra le flux d'informations sur une base multicouche à l'aide d'outils tels que des pares-feux, des proxys et des systèmes de détection d'intrusion basés sur le réseau.
7. **Prévention des pertes de données.** La Société utilise des mesures de prévention des pertes pour identifier, surveiller et protéger les Données personnelles en cours d'utilisation, en transit et au repos. Ces processus et outils de prévention des pertes de données comprendront : (a) des outils automatisés conçus pour identifier les tentatives d'exfiltration de données ; et (b) l'utilisation d'une sécurité basée sur des certificats de chiffrement. Les procédures de sauvegarde et de restauration des données sont définies et documentées dans les politiques de la Société, disponibles sur demande dans le Centre de gestion de la confidentialité de la Société (https://trust.certn.co/). L'exécution des sauvegardes est surveillée pour garantir leur exhaustivité. La Société stocke les données sur le cloud AWS, qui dispose de sauvegardes automatiques configurées et chiffrées. De plus, plusieurs zones sont disponibles à des fins de redondance et de récupération.

8. **Chiffrement** . La Société chiffrera, à l'aide d'outils de chiffrement standard, toutes les Données personnelles que le Fournisseur transmet sur les réseaux publics. La Société déploie le chiffrement des données au repos et en transit à l'aide du chiffrement AES 256 et ≥ TLS v1.2.
9. **Pseudonymisation** . La Société, lorsque cela est possible et compatible avec les Services, utilise des techniques de pseudonymisation pour protéger les Données Personnelles.

10. **Garanties de développement de produits** . La Société applique une approche de confidentialité et de sécurité dès la conception et fait l'objet d'audits réguliers et indépendants afin de maintenir les normes les plus strictes du

secteur en matière de contrôles internes de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité.

11. **Garanties physiques.** La Société maintient des contrôles d'accès physiques pour sécuriser ses locaux physiques où se trouve l'environnement informatique pertinent de l'entreprise utilisé pour traiter les Données Personnelles, y compris un système de contrôle d'accès permettant à l'entreprise de contrôler l'accès physique à chaque installation de l'entreprise. La Société maintient une politique de sécurité physique qui couvre les dispositions relatives à l'accès physique aux bureaux avec des porte-clés, des alarmes de sécurité, une surveillance de sécurité et un accès limité aux visiteurs. Le périmètre physique de l'infrastructure du système informatique est inaccessible au personnel non autorisé. Des mesures techniques et organisationnelles appropriées sont mises en place pour protéger les zones de sécurité et leurs points d'accès contre l'entrée de personnes non autorisées. La Société stocke ses données sur le cloud AWS conformément aux meilleures pratiques et exigences. Les données sont segmentées, chiffrées et sauvegardées, avec une disponibilité multizone.

12. **Garanties administratives.** Avant de donner accès aux Données Personnelles du Client à l'un de ses employés, la Société prendra des mesures commercialement raisonnables pour : (a) vérifier la fiabilité de ce personnel ; et (b) dispenser une formation appropriée en matière de sécurité à ce personnel. La Société a établi une politique de conservation des données qui définit différents calendriers de purge pour chaque catégorie de données.