Annexe sur le Traitement des Données (ATD)

Les termes de la présente annexe sur le traitement des données (l'« **Annexe** ») font partie intégrante du contrat principal (le « **Contrat Principal** »), qui comprend les conditions générales de Validato SA (y compris toute société qui, de temps à autre, est une filiale de Validato SA, ci-après collectivement dénommée « **Validato** »), telles que publiées sur son site web de temps à autre, ou tout accord spécifique entre les parties.

Le Contrat Principal est conclu entre le client (le « **Responsable du Traitement** ») et Validato (le « **Sous-traitant** » ; ensemble, les « **Parties** ») et s'applique lorsque le Sous-traitant traite des données personnelles pour le compte du Responsable du Traitement conformément à la Loi suisse sur la protection des données, au Règlement général sur la protection des données de l'UE, au Règlement général sur la protection des données du Royaume-Uni ou à toute autre disposition équivalente des lois applicables sur la protection des données, sauf si les Parties ont conclu un accord spécifique de traitement des données.

1. Objet

La présente Annexe définit les exigences auxquelles le Sous-traitant doit se conformer lorsqu'il traite des Données Personnelles pour le compte du Responsable du Traitement.

Dans le cadre de leur relation contractuelle, les deux Parties s'engagent à respecter à tout moment les Règles Applicables en matière de Protection des Données.

Le Sous-traitant ne traitera les Données Personnelles que sur instructions documentées du Responsable du Traitement, sauf si la loi applicable exige le contraire. Dans ce cas, le Sous-traitant doit (dans la mesure permise par la loi) informer le Responsable du Traitement de cette exigence légale avant le traitement.

2. Définitions

Dans la présente Annexe, les termes suivants ont la signification indiquée ci-dessous :

« **Règles Applicables en matière de Protection des Données** » désignent (selon le cas) le Règlement général sur la protection des données de l'UE 2016/679 (« **RGPD** »), la Loi fédérale suisse sur la protection des données (« **LPD Suisse** »), le Règlement général sur la protection des données du Royaume-Uni (« **UK GDPR** ») et toute autre loi sur la protection des données expressément mentionnée dans le Contrat Principal ;

« **Personne Concernée** » désigne l'individu dont les Données Personnelles sont traitées conformément à la présente Annexe ;

« **Instructions** » désigne les instructions documentées du Responsable du Traitement (y compris par e-mail et via l'outil du Sous-traitant) adressées au Sous-traitant concernant le traitement des Données Personnelles ;

« **Données Personnelles** » désigne toute information concernant une personne physique identifiée ou identifiable traitée dans le cadre de la présente Annexe ; et

« **Sous-traitant secondaire** » désigne tout tiers engagé par le Sous-traitant pour traiter des Données Personnelles pour le compte du Responsable du Traitement.

3. Description des Activités de Traitement

Le Sous-traitant traite les Données Personnelles uniquement pour le compte du Responsable du Traitement et conformément à ses instructions, aux fins de fourniture des services définis dans le Contrat Principal (les « **Services** »). Les Services incluent la vérification des antécédents d'une Personne concernée conformément aux instructions du Responsable du Traitement.

Pour éviter tout doute, la présente Annexe régit l'ensemble du traitement des Données Personnelles par le Sous-traitant dans le cadre des Services, y compris toute activité de collecte, de vérification, d'analyse et de rapport effectuée dans le cadre de la vérification des antécédents.

Le Sous-traitant ne détermine pas les finalités ni les moyens essentiels du traitement des Données Personnelles au titre de la présente Annexe ; le Responsable du Traitement reste le seul Responsable du Traitement de ces Données Personnelles.

Les types de Données Personnelles pouvant être traitées dans le cadre de la présente Annexe sont énumérés à l'Annexe A.

Les Personnes Concernées comprennent (i) les employés, représentants et utilisateurs autorisés du Responsable du Traitement dont les Données Personnelles sont traitées pour l'administration des comptes et le support ; et (ii) les individus concernés par la vérification des antécédents (par ex. candidats, sous-traitants, clients ou autres personnes dont les Données Personnelles sont traitées dans le cadre de la fourniture des Services).

4. Durée

La présente Annexe prend effet à la date d'entrée en vigueur du Contrat Principal et demeure en vigueur après la résiliation (pour quelque raison que ce soit) ou l'expiration du Contrat Principal.

5. Obligations du Sous-traitant (y compris indemnisation du Responsable du Traitement)

Le Sous-traitant s'engage envers le Responsable du Traitement à :

- traiter les Données Personnelles exclusivement pour les finalités définies aux sections 1 et 3 de la présente Annexe ;
- traiter les Données Personnelles exclusivement conformément aux instructions documentées du Responsable du Traitement (y compris par e-mail et via l'outil du Sous-traitant) ;
- garantir la confidentialité des Données personnelles conformément aux instructions et dans le cadre de la communication des Données personnelles à des tiers (par ex. anciens employeurs, autorités publiques, etc.) aux fins de la fourniture des Services ;
- veiller à ce que toute personne autorisée par le Sous-traitant à traiter des Données personnelles, y compris les employés, prestataires et autres membres du personnel agissant sous l'autorité du Sous-traitant, soit soumise à des obligations appropriées de confidentialité et reçoive une formation adaptée à son rôle et à ses droits d'accès ;
- informer immédiatement le Responsable du Traitement si le Sous-traitant n'est plus en mesure de se conformer aux termes de la présente Annexe ou aux Règles Applicables en matière de Protection des Données ; et
- fournir, sur demande, au Responsable du Traitement :
    - des preuves documentaires de la conformité continue du Sous-traitant à la présente Annexe et aux Règles Applicables en matière de Protection des Données ; et
    - tout autre document raisonnablement requis par le Responsable du Traitement pour établir la conformité du Sous-traitant à la présente Annexe (par ex. copie des audits

pertinents du Sous-traitant, rapports ISO (Organisation Internationale de Normalisation) ou rapports similaires et/ou confirmations écrites).

Sous réserve de la limitation de responsabilité prévue dans le Contrat Principal, le Sous-traitant indemnisera et tiendra indemne le Responsable du Traitement contre toutes réclamations, pertes, coûts (y compris frais d'avocat raisonnables), amendes et autres préjudices financiers subis par le Responsable du Traitement du fait de toute violation, par le Sous-traitant, de la présente Annexe ou des Règles Applicables en matière de Protection des Données. L'obligation d'indemnisation du Sous-traitant en vertu de la présente Annexe ne s'applique qu'aux dommages résultant d'une violation intentionnelle ou gravement négligente de la présente Annexe par le Sous-traitant. Le Sous-traitant ne sera pas tenu d'indemniser le Responsable du Traitement pour (i) les activités de traitement effectuées dans le cadre du rôle de responsable indépendant du Sous-traitant, (ii) les dommages causés par des données inexactes, incomplètes ou illégales fournies par le Responsable du Traitement, ses utilisateurs ou une Personne Concernée, ou (iii) les dommages résultant des instructions du Responsable du Traitement ou de son manquement à se conformer aux lois applicables en matière de protection des données.

Dans la mesure permise par le droit applicable, le Sous-traitant ne saurait être tenu responsable envers le Responsable du traitement des dommages, pertes, réclamations, coûts ou conséquences réglementaires résultant d'un manquement du Responsable du traitement à ses obligations en tant que responsable du traitement, y compris lorsque de tels dommages résultent de l'absence de base juridique valable, d'une transparence insuffisante à l'égard des personnes concernées, de données personnelles inexactes ou traitées de manière illicite fournies par le Responsable du traitement ou en son nom, ou d'instructions illégales données par le Responsable du traitement. Aucune disposition de la présente Annexe ne limite une responsabilité qui ne peut être limitée en vertu des Règles applicables en matière de protection des données, ni ne porte atteinte aux droits légaux des personnes concernées.

6. Obligations du Responsable du traitement

Le Responsable du traitement s'engage envers le Sous-traitant à :

- s'assurer qu'il dispose d'une base juridique valable pour l'ensemble des Données personnelles soumises ou mises à disposition du Sous-traitant dans le cadre des Services ;
- s'assurer que tout traitement de catégories particulières de Données personnelles, de données relatives aux infractions ou condamnations pénales, de données issues de vérifications des antécédents ou d'autres informations sensibles est licite, nécessaire, proportionné et autorisé en vertu des Règles applicables en matière de protection des données ainsi que de toute législation applicable en matière d'emploi, de droit du travail, de réglementation ou de réglementation sectorielle ;
- fournir aux Personnes concernées l'ensemble des informations et notices de confidentialité requises avant de donner instruction au Sous-traitant d'exécuter les Services, sauf exception prévue par le droit applicable ;
- fournir des instructions claires, licites et documentées au Sous-traitant et s'assurer que ces instructions restent conformes aux Règles applicables en matière de protection des données ;
- s'assurer que les Données personnelles fournies au Sous-traitant sont exactes, pertinentes, limitées à ce qui est nécessaire et collectées de manière licite ;
- informer sans délai le Sous-traitant de tout changement de la législation, des instructions, du périmètre, des exigences de conservation ou des demandes des Personnes concernées susceptible d'affecter le traitement des Données personnelles par le Sous-traitant ;

- s’assurer que ses utilisateurs autorisés utilisent la plateforme et les Services du Sous-traitant conformément aux Règles applicables en matière de protection des données ; et
- effectuer toute exportation, téléchargement ou sauvegarde nécessaire des Données client avant l’expiration ou la résiliation des Services, sauf accord écrit contraire.

7. Sous-traitants secondaires

Le Responsable du Traitement accepte que le Sous-traitant puisse engager des sous-traitants secondaires pour effectuer certaines activités de traitement pour le compte du Responsable du Traitement. Le Sous-traitant tient à jour une liste publique et accessible des sous-traitants secondaires approuvés à l'adresse validato.com/sub-processors (la « **Liste des sous-traitants secondaires** »), y compris toute entité détenue à 100 % par le Sous-traitant dans l'EEE ou en Suisse. Si la Liste des sous-traitants secondaires est temporairement indisponible en ligne, la liste en vigueur est fournie sur demande.

Avant d'engager tout nouveau sous-traitant secondaire qui ne figure pas déjà sur la Liste des sous-traitants secondaires, le Sous-traitant en informe le Responsable du Traitement par écrit, par e-mail, au moins 30 jours à l'avance. Le Responsable du Traitement a le droit de s'opposer à l'engagement de ce sous-traitant secondaire pendant ce délai. Aucune Donnée Personnelle ne sera transférée à ce sous-traitant secondaire avant l'expiration du délai de notification sans objection, ou avant qu'une objection soulevée n'ait été résolue.

Dans le cadre des Services du Sous-traitant relatifs aux vérifications et contrôles d'antécédents, le Sous-traitant tient une liste distincte des sous-traitants secondaires engagés pour des vérifications spécifiques (la « **Liste des sous-traitants secondaires pour le screening** »). Cette liste peut varier selon le moment et l'étendue de la commande du Responsable du Traitement.

Compte tenu de la nature commercialement sensible des relations d'approvisionnement du Sous-traitant, la Liste des sous-traitants secondaires pour le screening est traitée comme une information confidentielle et mise à la disposition du Responsable du Traitement sur demande, sous réserve d'obligations de confidentialité qui ne soient pas plus strictes que celles déjà applicables au titre du Contrat Principal.

Les sous-traitants secondaires figurant sur la Liste des sous-traitants secondaires pour le screening ne sont engagés que lorsque la source d'information pertinente n'est pas en mesure de fournir directement les données au Sous-traitant, ou lorsqu'aucune source directe n'existe. La pratique standard du Sous-traitant consiste à vérifier les informations directement à la source, notamment auprès des registres officiels, des autorités publiques et des institutions émettrices, dans la mesure où cela est techniquement et opérationnellement possible. Par conséquent, le recours à des sous-traitants secondaires à des fins de vérification constitue l'exception plutôt que le mode standard de fourniture des Services.

Le Sous-traitant veille à ce que chaque Sous-traitant secondaire soit lié par des obligations en matière de protection des données offrant un niveau de protection au moins équivalent à celui prévu par la présente Annexe, dans la mesure applicable aux services fournis par ledit Sous-traitant ultérieur. Le Sous-traitant demeure responsable envers le Responsable du traitement de l’exécution des obligations en matière de protection des données de chaque Sous-traitant ultérieur.

8. Transfert transfrontalier

8.1. Transfert transfrontalier vers le Sous-traitant

Si le Sous-traitant est situé dans un pays pour lequel il n'existe pas de décision d'adéquation émise par le Commissaire suisse à la protection des données et à la transparence, ni de décision d'adéquation de l'UE, les Parties conviennent d'incorporer dans la présente Annexe les clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants établis dans des pays tiers (Décision d'exécution de la Commission (UE) 2021/914), dans la forme adoptée par la Commission européenne, telles que ces clauses peuvent être modifiées ou remplacées de temps à autre (les « **Clauses Types** »).

8.2. Transfert transfrontalier vers les sous-traitants secondaires

Le Sous-traitant peut, avec le consentement préalable écrit du Responsable du Traitement (y compris par e-mail et via l'outil du Sous-traitant) conformément à la section 6 ci-dessus, transférer des Données Personnelles à un sous-traitant secondaire situé dans un pays en dehors de l'Espace Économique Européen (« **EEE** »), du Royaume-Uni ou de la Suisse dans les situations suivantes :

- transfert vers un pays, territoire ou secteur bénéficiant d'une décision actuelle d'adéquation de la protection des données de la Communauté européenne et de la Suisse ;
- lorsqu'aucune décision d'adéquation n'existe, et dans la mesure nécessaire, le Responsable du Traitement autorise et instruit expressément le Sous-traitant à signer, avec le sous-traitant secondaire situé dans un pays hors EEE, Royaume-Uni ou Suisse, au nom et pour le compte du Responsable du Traitement, les Clauses Types, en tenant compte de toute exigence supplémentaire pouvant être imposée par une autorité de contrôle compétente et/ou un tribunal compétent (le Sous-traitant garantissant que tout transfert de Données Personnelles est effectué conformément aux Règles Applicables en matière de Protection des Données, telles qu'interprétées par les autorités de contrôle et les tribunaux compétents) ;
- mise en place par le Sous-traitant de moyens équivalents garantissant que le transfert de Données Personnelles est effectué en pleine conformité avec les Règles Applicables en matière de Protection des Données ; et
- si un tel transfert est requis de manière impérative par le droit de l'Union européenne, suisse, britannique ou national auquel le Sous-traitant est soumis. Dans ce cas, le Sous-traitant informe le Responsable du Traitement de cette exigence légale avant le transfert, sauf si la loi applicable interdit cette information pour des motifs importants d'intérêt public.

Si un mécanisme de transfert transfrontalier mentionné ci-dessus est jugé invalide par une autorité compétente et/ou conformément aux Règles Applicables en matière de Protection des Données, les Parties négocieront de bonne foi la mise en place d'une solution alternative pour permettre le transfert en conformité avec ces règles.

9. Fourniture d'informations aux Personnes Concernées

Le Responsable du Traitement fournira aux Personnes Concernées les informations requises conformément aux Règles Applicables en matière de Protection des Données.

Si une Personne Concernée contacte le Sous-traitant pour exercer un droit, le Sous-traitant transmet immédiatement la demande (et toutes informations pertinentes) au Responsable du Traitement. Sauf instruction écrite contraire du Responsable du Traitement, le Sous-traitant ne répondra pas directement à la demande. Le Sous-traitant assistera le Responsable du Traitement,

sur demande, dans le traitement des demandes des Personnes Concernées conformément aux Règles Applicables en matière de Protection des Données.

10. Notification d'une violation de Données Personnelles

Le Sous-traitant notifiera le Responsable du Traitement sans retard injustifié et en tout état de cause dans les 48 heures après avoir pris connaissance d'une violation de Données Personnelles.

La notification comprendra, dans la mesure des informations disponibles :

- une description de la nature de la violation (y compris les catégories et le nombre approximatif de personnes concernées et d'enregistrements, si possible) ;
- les conséquences probables de la violation ;
- les mesures prises ou proposées pour remédier à la violation et atténuer les effets négatifs possibles ; et
- les coordonnées du point de contact du Sous-traitant pour la gestion de l'incident.

Le Sous-traitant tiendra le Responsable du Traitement informé des développements importants et coopérera de bonne foi afin de permettre au Responsable du Traitement de respecter ses obligations de notification et de communication.

Les notifications au titre de cette section doivent être envoyées à : gdpr@validato.com et info@validato.com.

11. Assistance du Sous-traitant au Responsable du Traitement

Le Sous-traitant s'engage à assister le Responsable du Traitement (i) pour les enquêtes initiées par, ou les consultations préalables auprès, des autorités de contrôle compétentes ; (ii) pour la notification d'une violation de données aux autorités de contrôle et la communication aux Personnes Concernées ; (iii) pour l'établissement d'une analyse d'impact relative à la protection des données.

Le Sous-traitant mettra à disposition du Responsable du Traitement toutes les informations et documents nécessaires pour démontrer la conformité du Responsable du Traitement aux Règles Applicables en matière de Protection des Données.

Le Sous-traitant permettra au Responsable du Traitement, ou à un tiers retenu par celui-ci, d'auditer et d'inspecter le Sous-traitant. Sauf en cas d'urgence (par ex. demande d'une autorité de contrôle compétente ou violation de Données Personnelles), un audit ne peut avoir lieu qu'aux heures normales de bureau et avec un préavis écrit d'au moins dix (10) jours. L'audit est limité aux sujets pertinents pour la présente Annexe. Les frais d'audit sont à la charge du Responsable du Traitement. Si un audit révèle une violation par le Sous-traitant de ses obligations, celui-ci remédiera rapidement à la violation à ses frais.

12. Retour / Destruction des Données Personnelles

À l'expiration du Contrat Principal, sauf obligation légale impérative applicable au Sous-traitant, ce dernier supprimera de manière sécurisée les Données Personnelles conformément aux Règles Applicables en matière de Protection des Données dans un délai de 120 jours.

Le Sous-traitant confirmera par écrit au Responsable du Traitement qu'aucune copie des Données Personnelles n'a été conservée, sauf si une obligation légale impérative impose la conservation d'une copie. Dans ce cas, le Sous-traitant s'engage à :

- garantir la confidentialité de ces Données Personnelles ; et

- ne traiter ces Données Personnelles que tant que nécessaire pour les finalités prévues par l'obligation légale imposant leur conservation.

13. Registre des activités de traitement

Le Sous-traitant tiendra un registre des activités de traitement effectuées pour le compte du Responsable du Traitement, conformément à l'article 30 (2) du RGPD et à l'article 12 de la LPD Suisse.

14. Mesures de sécurité à mettre en œuvre par le Sous-traitant

Le Sous-traitant s'engage à prendre toutes les mesures techniques et organisationnelles appropriées conformément à l'article 32 RGPD et à l'article 8 LPD Suisse (selon le cas), telles que définies à l'Annexe B (les « **Mesures de Sécurité** »), afin d'assurer un niveau de sécurité adapté aux risques, notamment :

- processus garantissant la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et Services de traitement ;
- processus de restauration de la disponibilité et de l'accès aux Données Personnelles en cas d'incident physique ou technique ;
- processus de test, d'évaluation et d'analyse réguliers de l'efficacité des mesures techniques et organisationnelles ;
- mesures garantissant que toute personne sous l'autorité du Sous-traitant ayant accès aux Données Personnelles les traite uniquement selon les instructions du Responsable du Traitement ;
- toute autre mesure définie dans la présente Annexe ou dans les instructions du Responsable du Traitement.

Le Sous-traitant maintiendra et révisera régulièrement les Mesures de Sécurité pour qu'elles restent à jour et efficaces.

Le Sous-traitant participe à un mécanisme de certification (tel que défini à l'article 13 de la LPD Suisse ou à l'article 42 RGPD, le cas échéant). Le mécanisme de certification utilisé par le Sous-traitant est ISO 27001.

Pendant la durée du Contrat Principal, le Sous-traitant s'engage à respecter continuellement les exigences de sa certification ISO 27001 et à la renouveler avant expiration. Sur demande, le Sous-traitant fournira au Responsable du Traitement une preuve de certification ISO 27001 valide. Le Sous-traitant informera immédiatement le Responsable du Traitement si la certification ISO 27001 n'est pas renouvelée, expire sans renouvellement, est suspendue ou retirée.

15. Rôles du Responsable du Traitement et du Sous-traitant

Pour toutes les Données Personnelles traitées dans le cadre de la présente Annexe et des Services (y compris vérifications/diligences préalables), le Responsable du Traitement est le responsable du traitement et le Sous-traitant est le sous-traitant.

Le Sous-traitant peut traiter certaines données de contact professionnelles des utilisateurs et représentants autorisés du Responsable du Traitement (nom, e-mail professionnel, téléphone, rôle, communications de facturation et de support) en tant que responsable indépendant pour l'administration des comptes, la facturation, la prévention de la fraude et la conformité. Ce traitement est régi par la politique de confidentialité du Sous-traitant et la législation applicable.

16. Juridiction et droit applicable

La clause relative au choix du forum prévue dans le Contrat Principal s'applique au présent avenant.

La clause relative au choix de la loi prévue dans le Contrat Principal s'applique au présent avenant.

ANNEXE A – Catégories de Données Personnelles

Données d'identification

- Prénom
- Nom
- Date et lieu de naissance
- Nationalités
- Domicile
- Tutelle légale
- État civil
- Prénom et nom des parents
- Carte d'identité
- Passeport
- Adresse e-mail
- Numéro de téléphone
- Âge
- Sexe
- Permis de travail
- Numéro d'identification national

Données KYC

- Activité professionnelle
- Fonctions publiques (PEP locaux et internationaux, organisations internationales et sportives, etc.)
- Extrait de casier judiciaire
- Registre de recouvrement / intégrité financière
- Notation de crédit personnelle

Données sur les habitudes et relations

- Activités de loisirs
- Comportement particulier ou contacts sociaux
- Famille et partenariat enregistré
- Adhésions à des associations (hors politique, religion, syndicat)

Données relatives à la carrière

- CV
- certificats de travail
- diplômes
- références
- mandats externes
- pouvoirs de représentation

Données sur les caractéristiques personnelles

- Opinions politiques

Données biométriques

- Un scan facial de la personne concernée (capture en direct sous plusieurs angles)

ANNEXE B – Mesures de Sécurité

1. Gouvernance & Politiques

- Politiques de sécurité de l'information, gestion des risques, révisions périodiques.
- Obligations de confidentialité du personnel et des prestataires.

2. Contrôle d'accès

- Contrôle d'accès basé sur les rôles (principe du moindre privilège), MFA pour accès administratifs.
- Politiques de mots de passe sécurisées, revues d'accès périodiques.

3. Chiffrement

- Chiffrement des données en transit (TLS) et chiffrement des données au repos pour les Données personnelles stockées, le cas échéant.
- Contrôles de gestion des clés et accès restreint aux clés.

4. Journalisation & surveillance

- Journalisation de sécurité.
- Surveillance/alertes pour activités suspectes.

5. Gestion des vulnérabilités et correctifs

- Analyses régulières des vulnérabilités et application en temps opportun des correctifs de sécurité.
- Configurations sécurisées.

6. Développement sécurisé et gestion des changements (le cas échéant)

- Contrôle des changements, revues par les pairs, séparation des environnements.
- Tests de sécurité proportionnés au risque.

7. Sauvegarde et restauration

- Sauvegardes régulières, le cas échéant, et tests de restauration.
- Mesures de reprise après sinistre et de continuité d'activité proportionnées aux risques.

8. Réponse aux incidents

- Processus documenté de réponse aux incidents ; procédures d'escalade en cas de violation.
- Revue post-incident et actions correctives.

9. Sécurité des sous-traitants secondaires

- Diligence raisonnable et obligations contractuelles en matière de sécurité ; surveillance de la conformité.

10. Minimisation des données & conservation

- Séparation logique des clients, contrôle de conservation conformément à la section 11.