

Annexe A - Data processing agreement

Confidentialité : Public (C0)

Annexe A - Data processing agreement	1
SECTION I - DISPOSITIONS GÉNÉRALES	2
1. Objet et champ d'application	2
2. Invariabilité des clauses.....	2
SECTION II - OBLIGATIONS DES PARTIES	3
3. Instructions.....	3
4. Limitation de la finalité.....	3
5. Durée du traitement.....	3
6. Sécurité du traitement	3
7. Données sensibles	3
8. Documentation et conformité	4
9. Sous-traitants ultérieurs	4
10. Transferts internationaux	5
11. Assistance au Souscripteur	5
12. Notification de violations de données.....	5
SECTION III - DISPOSITIONS FINALES	6
13. Non-respect et résiliation	6
14. Sort des données au terme du Contrat	6
15. Droit applicable	6
APPENDICE I - Description des traitements.....	7
Catégories de personnes concernées.....	7
Catégories de données à caractère personnel.....	7
Finalités des traitements	7
Nature des traitements.....	8
Durée des traitements.....	8
APPENDICE II - Mesures techniques et organisationnelles	8
Chiffrement et protection des données.....	8
Continuité et résilience	9
Organisation interne.....	9

APPENDICE III - Notification de violations 9

Le présent accord de traitement de données (l'« **Addendum** ») définit les conditions dans lesquelles Legapass, en tant que sous-traitant, traite des données à caractère personnel sur instruction du Souscripteur. Dans le présent Addendum, Legapass se fonde sur les clauses contractuelles types entre responsables du traitement et sous-traitants adoptées par la Commission européenne dans sa Décision d'exécution (UE) 2021/915 du 4 juin 2021 au titre de l'article 28, paragraphes 7 et 8, du RGPD. La Décision d'exécution (UE) 2021/914 du 4 juin 2021, relative aux transferts vers des pays tiers, ne s'applique qu'en cas de transfert international dans les conditions de la Clause 10. Il complète le Contrat et y est incorporé. En cas de contradiction avec le Contrat, l'Addendum prévaut.

Legapass agissant en qualité de sous-traitant, le Souscripteur est présumé agir en qualité de Responsable de traitement pour tous les traitements autres que ceux réalisés par Legapass pour ses propres besoins, détaillés dans la Politique de Confidentialité de Legapass. Si le Souscripteur agit lui-même en tant que sous-traitant traitant des données sur instruction d'un tiers Responsable de traitement, il s'engage à :

- obtenir toutes les autorisations nécessaires à la conclusion du présent Addendum auprès du Responsable de traitement ;
- déclarer Legapass en tant que sous-traitant ultérieur auprès du Responsable de traitement ;
- avoir conclu un contrat avec le Responsable de traitement conforme à l'article 28 du RGPD et en adéquation avec le présent Addendum ;
- donner à Legapass des instructions conformes à celles reçues du Responsable de traitement, sans que Legapass ne reçoive d'instruction directement de celui-ci, sauf transfert de droits et obligations dûment établi ;
- mettre le présent Addendum à disposition du Responsable de traitement.

Le Souscripteur reste entièrement responsable envers Legapass de l'application du présent Addendum par le Responsable de traitement. Le Souscripteur garantit Legapass contre toute réclamation du Responsable de traitement résultant d'un manquement du Souscripteur à ses propres obligations, sans que cette garantie ne puisse être opposée aux personnes concernées au sens de l'article 82, paragraphe 4, du RGPD ni limiter la responsabilité propre de Legapass au titre des obligations qui lui incombent en qualité de sous-traitant ultérieur.

SECTION I - DISPOSITIONS GÉNÉRALES

1. Objet et champ d'application

1.1 Le présent Addendum a pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du Règlement (UE) 2016/679 (« **RGPD** ») et avec la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le présent Addendum s'applique au traitement des données à caractère personnel tel que décrit à l'Appendice I.

1.2 Les Appendices I à III font partie intégrante du présent Addendum.

2. Invariabilité des clauses

2.1 Les parties s'engagent à ne pas modifier les clauses issues des clauses contractuelles types, sauf en ce qui concerne l'ajout ou la mise à jour d'informations dans les Appendices.

2.2 Les parties peuvent inclure le présent Addendum dans un contrat plus large ou y ajouter des garanties supplémentaires, à condition que celles-ci ne contredisent pas les clauses contractuelles types ni ne portent atteinte aux droits des personnes concernées.

SECTION II - OBLIGATIONS DES PARTIES

3. Instructions

3.1 Legapass ne traite les données à caractère personnel que sur instruction documentée du Souscripteur, à moins qu'elle ne soit tenue d'y procéder en vertu du droit de l'Union ou du droit français. Dans ce cas, Legapass informe le Souscripteur de cette obligation juridique avant le traitement, sauf si la loi le lui interdit.

3.2 Legapass informe immédiatement le Souscripteur si, selon elle, une instruction constitue une violation du RGPD ou d'autres dispositions applicables en matière de protection des données.

3.3 Le Contrat et le présent Addendum constituent l'ensemble des instructions du Souscripteur à Legapass. Tout traitement excédant ce périmètre nécessite un accord préalable écrit entre les parties.

4. Limitation de la finalité

Legapass traite les données à caractère personnel uniquement pour les finalités spécifiques définies à l'Appendice I, sauf instruction complémentaire documentée du Souscripteur.

5. Durée du traitement

Le traitement est effectué pendant la durée du Contrat, ou pour toute durée inférieure sous le contrôle exclusif du Souscripteur. Les durées de conservation spécifiques à certains Services sont précisées dans les Conditions Particulières applicables.

6. Sécurité du traitement

6.1 Legapass met en œuvre les mesures techniques et organisationnelles décrites à l'Appendice II pour assurer la sécurité des données, notamment leur protection contre toute violation entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé. Les parties tiennent compte 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.

6.2 Legapass n'accorde à son personnel l'accès aux données que dans la mesure strictement nécessaire à l'exécution du Service. Les personnes autorisées sont soumises à un engagement écrit de confidentialité.

7. Données sensibles

Lorsque le traitement porte sur des catégories particulières de données au sens de l'article 9 du RGPD (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, biométriques aux fins d'identification, de santé, relatives à la vie ou à l'orientation sexuelle) ou sur des données relatives à des condamnations pénales et infractions au sens de l'article 10 du RGPD, Legapass met en œuvre les garanties spécifiques suivantes : (a) chiffrement renforcé des données concernées au repos et en transit ; (b) restriction des accès aux seuls personnels habilités et formés à la sensibilité de ces catégories ; (c) journalisation détaillée des accès et des opérations effectuées sur ces données ; (d) clauses de confidentialité renforcée pour les sous-traitants ultérieurs susceptibles d'y accéder ; (e) durée de conservation strictement limitée à ce qui est nécessaire à la finalité poursuivie ou à la durée légale applicable au Souscripteur. Dans le cadre des analyses de vigilance LCB-FT, ces garanties s'appliquent en particulier aux données relatives aux personnes politiquement exposées, aux mesures de gels d'avoirs et aux alertes médiatiques susceptibles de révéler des données sensibles ou des infractions.

8. Documentation et conformité

Legapass met à disposition du Souscripteur les informations nécessaires pour démontrer le respect des obligations du présent Addendum, et permet la réalisation d'audits, y compris d'inspections, par le Souscripteur ou par un auditeur tiers indépendant mandaté par lui.

Les modalités suivantes s'appliquent : (i) un préavis écrit raisonnable d'au moins trente (30) jours est respecté, sauf urgence motivée ; (ii) l'audit se déroule pendant les heures ouvrables et de manière à perturber le moins possible l'activité de Legapass ; (iii) la fréquence est limitée à une fois par année civile, sauf demande d'une autorité de contrôle, sauf survenance d'une violation de données significative ou sauf motif sérieux et documenté ; (iv) l'auditeur tiers est soumis à un engagement de confidentialité préalable. Legapass peut fournir, en complément, ses certifications et rapports d'audit indépendants pertinents ; (v) le périmètre de l'audit ne peut porter que sur le service dont le Souscripteur qui le demande est effectivement client ; ces éléments peuvent compléter l'exercice du droit d'audit du Souscripteur sans s'y substituer lorsqu'une demande spécifique est formulée.

9. Sous-traitants ultérieurs

9.1 Legapass dispose de l'autorisation générale du Souscripteur pour recourir à des sous-traitants ultérieurs. La liste à jour des sous-traitants ultérieurs autorisés, précisant pour chacun leur identité, leur localisation et la nature des opérations confiées, est tenue par Legapass et accessible à dpo@legapass.com ou dans les conditions de services. Legapass informe le Souscripteur par écrit (notamment par email à l'Administrateur ou par notification au sein du Service) de tout ajout ou remplacement de sous-traitant ultérieur au moins trente (30) jours avant la prise d'effet. Legapass informe le Souscripteur par écrit de tout ajout ou remplacement de sous-traitant ultérieur au moins trente (30) jours à l'avance.

9.2 Si le Souscripteur s'oppose de manière raisonnable et pour des motifs liés à la protection des données, il peut demander à Legapass de transférer les données vers un autre sous-traitant ultérieur. Si aucune alternative n'est raisonnablement possible et que l'opposition est maintenue pour un motif légitime, chaque partie peut résilier le Contrat moyennant un préavis de trente (30) jours. En l'absence d'opposition dans les trente (30) jours suivant la notification, le Souscripteur est réputé avoir accepté le nouveau sous-traitant.

9.3 Legapass conclut avec chaque sous-traitant ultérieur un contrat écrit imposant des obligations équivalentes à celles du présent Addendum. Legapass demeure pleinement responsable envers le Souscripteur des actes et omissions de ses sous-traitants ultérieurs.

9.4 Le Souscripteur peut demander copie du contrat conclu avec un sous-traitant ultérieur. Legapass peut en expurger les éléments couverts par le secret des affaires.

10. Transferts internationaux

10.1 Tout transfert de données vers un pays tiers n'est effectué que sur instruction documentée du Souscripteur ou pour satisfaire une exigence légale, et conformément au chapitre V du RGPD.

10.2 Lorsqu'un transfert est nécessaire, il s'effectue :

- vers un pays bénéficiant d'une décision d'adéquation de la Commission européenne ;
- vers un destinataire adhérent à un mécanisme de certification reconnu ; ou
- dans le cadre des clauses contractuelles types. À cette fin, le Souscripteur mandate Legapass pour conclure lesdites clauses en son nom et pour son compte.

10.3 Préalablement à tout transfert vers un pays tiers ne bénéficiant pas d'une décision d'adéquation, Legapass procède à une analyse d'impact du transfert (« Transfer Impact Assessment ») conformément aux recommandations 01/2020 du Comité européen de la protection des données, et met en œuvre, lorsque nécessaire, des mesures supplémentaires techniques, contractuelles ou organisationnelles permettant de garantir un niveau de protection des données substantiellement équivalent à celui assuré au sein de l'Union européenne. Le résumé de cette analyse est tenu à disposition du Souscripteur sur demande adressée à dpo@legapass.com.

11. Assistance au Souscripteur

11.1 Legapass informe sans délai le Souscripteur de toute demande sérieuse reçue directement d'une personne concernée et n'y donne pas suite elle-même, sauf autorisation du Souscripteur.

11.2 Legapass assiste le Souscripteur, par des mesures techniques et organisationnelles appropriées, dans l'accomplissement de son obligation de répondre aux demandes d'exercice des droits des personnes concernées, dans des conditions permettant le respect du délai légal.

11.3 Legapass assiste en outre le Souscripteur dans le respect de ses obligations relatives à :

- la réalisation d'analyses d'impact relatives à la protection des données ;
- la consultation préalable de l'autorité de contrôle ;
- l'exactitude et la mise à jour des données ;
- la sécurité du traitement au sens de l'article 32 du RGPD.

12. Notification de violations de données

12.1 En cas de violation de données en rapport avec des données traitées par Legapass, celle-ci en informe le Souscripteur dans les meilleurs délais et au plus tard soixante-douze (72) heures après en avoir pris connaissance. Cette notification contient au minimum :

- une description de la nature de la violation, y compris les catégories et le nombre approximatif de personnes et d'enregistrements concernés ;
- les coordonnées du point de contact pour obtenir des informations complémentaires ;
- les conséquences probables de la violation ;
- les mesures prises ou proposées pour y remédier et en atténuer les effets.

12.2 Lorsque toutes les informations ne sont pas disponibles simultanément, elles sont communiquées de manière échelonnée dans les meilleurs délais.

12.3 Legapass coopère avec le Souscripteur et lui prête assistance pour la notification à l'autorité de contrôle et, le cas échéant, la communication aux personnes concernées.

SECTION III - DISPOSITIONS FINALES

13. Non-respect et résiliation

13.1 En cas de manquement de Legapass à ses obligations au titre du présent Addendum, le Souscripteur peut donner instruction de suspendre le traitement jusqu'à ce que Legapass se soit mise en conformité ou jusqu'à résiliation du Contrat.

13.2 Le Souscripteur peut résilier le Contrat si : (a) la suspension visée au 13.1 n'est pas levée dans un délai d'un mois ; (b) Legapass est en violation grave ou persistante du présent Addendum ; ou (c) Legapass ne se conforme pas à une décision contraignante d'une autorité de contrôle.

13.3 Legapass peut résilier le Contrat si, après avoir informé le Souscripteur que ses instructions enfreignent la loi applicable, celui-ci insiste pour qu'elles soient suivies.

14. Sort des données au terme du Contrat

14.1 À la résiliation du Contrat, le Souscripteur dispose d'un délai de quatre-vingt-dix (90) jours pour exprimer son choix entre (i) la restitution de l'ensemble des données personnelles sous une forme structurée, couramment utilisée et lisible par machine, ou (ii) leur suppression assortie d'une certification de suppression. À défaut d'instruction expresse dans ce délai, Legapass conserve les données pendant la durée minimale imposée au Souscripteur par sa réglementation sectorielle applicable, notamment au titre de l'article L.561-12 du Code monétaire et financier (cinq ans à compter de la clôture du dossier ou de la cessation de la relation d'affaires concernée), avant de procéder à leur suppression. Pendant cette période, Legapass garantit la confidentialité des données et limite leur accès aux seules personnes strictement nécessaires à leur conservation.

14.2 Legapass peut conserver les données dans la mesure exigée par la loi applicable, uniquement pour la durée et aux fins légalement prescrites, sous réserve d'en garantir la confidentialité.

15. Droit applicable

Le présent Addendum est soumis au droit français. Lorsque le Souscripteur agit dans le cadre et pour les besoins de son activité professionnelle, tout litige en découlant est soumis à la compétence exclusive du tribunal de commerce de Nice ou, à défaut, du tribunal judiciaire de Nice. Lorsque le Souscripteur n'agit pas pour les besoins de son activité professionnelle ou est qualifié de non-professionnel au sens du Code de la consommation, les règles de compétence territoriale de droit commun s'appliquent. Pour les clauses contractuelles types incorporées au présent Addendum, les parties conviennent de l'application du droit français et de la compétence des juridictions ci-dessus dans les mêmes conditions.

APPENDICE I - Description des traitements

Catégories de personnes concernées

I.1 Les catégories de personnes concernées par les traitements réalisés par Legapass pour le compte du Souscripteur sont les suivantes :

- (a) les Souscripteurs, Administrateurs et Utilisateurs du Service ;
- (b) les Clients Enregistrés du Souscripteur, dont les informations sont renseignées dans le Service ;
- (c) les personnes physiques faisant l'objet d'analyses de vigilance LCB-FT, notamment les comparants, les bénéficiaires effectifs, les représentants légaux et les personnes politiquement exposées identifiées par le Service ;
- (d) les tiers dont les données sont transmises par le Souscripteur dans le cadre de l'exécution d'un mandat ou de l'utilisation du Service, notamment les héritiers, ayants droit, détenteurs d'actifs et tout interlocuteur sollicité dans le cadre du Service.

Catégories de données à caractère personnel

I.2 Les catégories de données traitées incluent :

- (a) données d'identification : nom, prénom, date et lieu de naissance, nationalité, sexe, situation familiale ;
- (b) données de contact : adresse postale, adresse email, numéro de téléphone ;
- (c) données d'identification professionnelle : profession, structure, numéro d'inscription à l'ordre ou auprès de l'organisme régulateur, numéro SIREN/SIRET ;
- (d) données d'identification formelle : pièce d'identité, justificatifs de domicile, justificatifs de nationalité transmis par le Souscripteur ;
- (e) données de connexion et de journalisation : adresse IP, User Agent, identifiants de session, horodatage des connexions, adresses des ressources accédées ;
- (f) données de vigilance LCB-FT : résultats de criblage PPE, listes de gels des avoirs et de sanctions nationales et internationales, alertes médiatiques défavorables, informations sur les bénéficiaires effectifs, niveau de vigilance déterminé ;
- (g) données financières : nature et montant des opérations, origine et destination des fonds, informations sur les flux financiers transmises par le Souscripteur ;

- (h) données relatives aux mandats : instructions du Souscripteur, correspondances avec les tiers, documents collectés dans le cadre de l'exécution du mandat ;
- (i) données générées par le Service : rapports d'analyse, résultats d'aide à la décision, pistes d'audit horodatées ;
- (j) toute autre donnée transmise par le Souscripteur dans le cadre de son utilisation du Service.

Les catégories détaillées par Service figurent dans la Politique de confidentialité de Legapass.

Finalités des traitements

I.3 Legapass traite les données à caractère personnel pour le compte du Souscripteur aux fins suivantes :

- (a) fourniture et fonctionnement du Service souscrit ;
- (b) exécution des analyses de vigilance LCB-FT pour le compte du Souscripteur ;
- (c) génération, conservation et mise à disposition des rapports de conformité et des pistes d'audit ;
- (d) exécution des mandats de recherche, de collecte et de récupération d'actifs ou d'informations confiés par le Souscripteur ;
- (e) assistance au Souscripteur dans le respect de ses obligations professionnelles, réglementaires et déontologiques ;
- (f) sécurisation du Service, gestion des erreurs et journalisation des accès.

Nature des traitements

I.4 Les opérations de traitement réalisées par Legapass incluent : la collecte, la réception, l'enregistrement, le classement, le stockage, la sécurisation, le chiffrement, la consultation, l'analyse, le criblage, le rapprochement, la transmission, la restitution et la suppression de données, ainsi que tout autre traitement nécessaire à la fourniture du Service.

Durée des traitements

I.5 Les traitements sont effectués pendant la durée du Contrat. À l'expiration du Contrat, Legapass conserve les données dans les conditions prévues à la Clause 14 du présent Addendum et, le cas échéant, pendant la durée minimale imposée par la réglementation applicable au Souscripteur, notamment l'article L.561-12 du Code monétaire et financier. Les durées de conservation spécifiques à certains Services sont précisées dans les Conditions Particulières applicables.

APPENDICE II - Mesures techniques et organisationnelles

Legapass met en œuvre les mesures techniques et organisationnelles suivantes, conformément à l'article 32 du RGPD, pour garantir un niveau de sécurité adapté au risque. Ces mesures s'inscrivent dans le cadre d'un système de management de la sécurité de l'information conforme aux principes de la norme ISO/IEC 27001, complété, lorsqu'applicable, par les contrôles des normes ISO/IEC 27017 (sécurité dans le cloud) et ISO/IEC 27018 (protection des données dans le cloud). Legapass procède à des tests d'intrusion externes au moins une fois par an et met en œuvre des techniques de pseudonymisation lorsque celles-ci sont appropriées au traitement.

Chiffrement et protection des données

- (a) chiffrement des données au repos et en transit selon les standards de l'industrie ;
- (b) gestion des clés de chiffrement avec séparation des rôles.
- Sécurité de l'infrastructure
- (c) pare-feu, systèmes de détection et de prévention d'intrusion ;
- (d) gestion des vulnérabilités et application régulière des correctifs de sécurité ;
- (e) segmentation réseau et cloisonnement des environnements.
- Contrôle des accès
- (f) contrôle d'accès basé sur les rôles et le principe du moindre privilège ;
- (g) authentification renforcée des Utilisateurs, y compris authentification à deux facteurs lorsque le Service le prévoit ;
- (h) révocation des accès dans les meilleurs délais en cas de départ ou de changement de fonction d'un collaborateur.
- Traçabilité et surveillance
- (i) journalisation et surveillance des accès aux données et aux rapports d'analyse ;
- (j) conservation des journaux de connexion pendant douze (12) mois conformément aux obligations légales.

Continuité et résilience

- (k) sauvegardes régulières chiffrées sur des serveurs situés dans l'Espace Économique Européen ;
- (l) tests réguliers de restauration des sauvegardes ;
- (m) plan de continuité et de reprise d'activité.

Organisation interne

- (n) engagement écrit de confidentialité de l'ensemble du personnel ayant accès aux données ;
- (o) sensibilisation et formation régulières du personnel à la protection des données et aux enjeux LCB-FT ;
- (p) politiques et procédures documentées de gestion des incidents de sécurité ;
- (q) programme de Bug Bounty pour l'identification proactive des vulnérabilités ;
- (r) audit annuel de sécurité couvrant les mesures techniques et organisationnelles.

II.2 Les mesures sont revues et mises à jour périodiquement en fonction de l'évolution des risques et de l'état des connaissances. Le détail des mesures est accessible dans la politique de sécurité de Legapass à l'adresse legapass.com/securite/.

APPENDICE III - Notification de violations

III.1 En complément des informations prévues à la Clause 12, Legapass communique au Souscripteur, dès que disponibles :

- (a) l'identité et les coordonnées du DPO ou du point de contact dédié (dpo@legapass.com) ;
- (b) une chronologie détaillée de la violation, incluant la date et l'heure de sa découverte, sa nature probable et le vecteur d'attaque identifié le cas échéant ;

- (c) l'identification des catégories et du volume approximatif de données et de personnes concernées ;
- (d) une évaluation des conséquences probables de la violation pour les personnes concernées ;
- (e) les mesures de remédiation mises en œuvre et leur calendrier de déploiement ;
- (f) les recommandations à l'attention du Souscripteur pour minimiser les conséquences de la violation à l'égard de ses propres clients et des personnes analysées ;
- (g) toute information complémentaire nécessaire à la notification auprès de la CNIL conformément à l'article 33 du RGPD ou à la communication aux personnes concernées conformément à l'article 34 du RGPD.

III.2 Legapass tient un registre interne des violations de données. Le Souscripteur peut en demander communication, pour les violations le concernant, à dpo@legapass.com. Legapass répond à cette demande dans un délai maximal de trente (30) jours.