

Accord de sous-traitance (DPA)

1. Objet et articulation avec le contrat de services

1.1. Objet

L'Accord définit les conditions dans lesquelles Junga traite, en qualité de sous-traitant, les données à caractère personnel dont le Cabinet est responsable de traitement, conformément à l'article 28 du règlement (UE) 2016/679 (ci-après le « RGPD ») et à la loi n° 78-17 du 6 janvier 1978 modifiée.

Il s'applique à l'ensemble des traitements réalisés par Junga pour le compte du Cabinet dans le cadre de la plateforme, quels que soient le module utilisé et le canal d'accès, y compris le portail client en marque blanche mis à la disposition des clients finaux du Cabinet.

1.2. Articulation avec le contrat de services

L'Accord complète le contrat de services conclu entre les Parties et en fait partie intégrante. Il ne s'y substitue pas : les stipulations relatives au prix, à la durée, aux niveaux de service et aux modalités d'exécution de la prestation demeurent régies par ce contrat.

L'acceptation du contrat de services emporte acceptation de l'Accord. Les cabinets qui exigent un exemplaire signé peuvent en faire la demande à dpo@junga.ai.

1.3. Ordre de priorité

En cas de contradiction entre l'Accord et le contrat de services sur une question relative au traitement de données à caractère personnel, l'Accord prévaut. Pour toute autre question, le contrat de services prévaut.

Aucune stipulation de l'Accord ne peut être interprétée comme dispensant l'une ou l'autre des Parties d'une obligation qui lui incombe directement au titre de la réglementation applicable à la protection des données.

2. Rôles des Parties et définitions

2.1. Définitions

Les termes « données à caractère personnel », « traitement », « responsable de traitement », « sous-traitant », « personne concernée », « violation de données à caractère personnel » et « autorité de contrôle » ont le sens que leur donne l'article 4 du RGPD. Les termes suivants sont propres à l'Accord.

- Clients finaux : les personnes physiques dont le Cabinet gère la relation patrimoniale et dont les données sont traitées dans la plateforme, ainsi que les bénéficiaires effectifs identifiés par le Cabinet.

- Utilisateurs du Cabinet : les collaborateurs du Cabinet disposant d'un compte sur le tableau de bord Junga.
- Plateforme : le tableau de bord destiné au Cabinet, le portail client en marque blanche et les interfaces applicatives associées.
- Sous-traitant ultérieur : tout tiers auquel Junga confie tout ou partie d'un traitement réalisé pour le compte du Cabinet.

2.2. Le Cabinet, responsable de traitement

Le Cabinet détermine les finalités et les moyens des traitements portant sur les données de ses clients finaux. Il lui appartient de s'assurer de l'existence d'une base légale pour chaque traitement, de la licéité des données qu'il transmet à Junga, de leur exactitude et de leur mise à jour, ainsi que du respect des obligations qui lui incombent au titre de la réglementation applicable à son activité.

2.3. Junga, sous-traitant

Junga traite les données des clients finaux uniquement pour le compte du Cabinet et sur ses instructions documentées, dans les conditions décrites par l'Accord.

Junga demeure responsable de traitement pour les données qu'elle traite pour son propre compte, notamment les comptes des utilisateurs du Cabinet, la facturation de l'abonnement et la sécurité de la plateforme. Ces traitements sont décrits dans la politique de confidentialité publiée sur www.junga.ai et ne relèvent pas de l'Accord.

2.4. Information des personnes concernées

Il appartient au Cabinet d'informer ses clients finaux du traitement de leurs données, conformément aux articles 13 et 14 du RGPD. Junga met à sa disposition un modèle de notice d'information destiné au portail client. Ce modèle est fourni à titre d'aide et ne constitue pas un conseil juridique : le Cabinet demeure responsable de l'information effectivement délivrée à ses clients finaux.

3. Description des traitements réalisés pour le compte du Cabinet

La présente section décrit, conformément à l'article 28, paragraphe 3, du RGPD, l'objet, la nature, la finalité et la durée des traitements réalisés pour le compte du Cabinet, ainsi que les catégories de données et de personnes concernées. Elle est reprise du registre des activités de traitement tenu par Junga au titre de l'article 30, paragraphe 2, du RGPD.

3.1. Nature et finalités des traitements

Junga réalise pour le compte du Cabinet les traitements suivants.

- Gestion des clients (KYC et onboarding) : constitution et gestion du dossier client réglementaire pour le compte du Cabinet.

- Vérification d'identité (documents KYC) : contrôle des pièces d'identité et détection de fraude documentaire.
- Questionnaire d'adéquation MIF2 : évaluation de l'adéquation produit (profil investisseur).
- Screening LCB-FT (gel des avoirs, personnes politiquement exposées, sanctions) : détection des personnes sous sanctions ou politiquement exposées.
- Gestion du patrimoine (actifs et valorisations) : suivi des actifs et de leurs valorisations pour le conseil patrimonial.
- Portail client en marque blanche : espace client aux couleurs du Cabinet (documents, signature, simulateurs).
- Emails transactionnels : notifications de service (invitations, relances documentaires, signatures).
- Signatures électroniques : signature des documents réglementaires (document d'entrée en relation, lettres de mission).

Les opérations réalisées sur ces données sont la collecte, l'enregistrement, l'organisation, la structuration, la conservation, la consultation, l'utilisation, le rapprochement, la mise à disposition du Cabinet et de ses clients finaux, la limitation et l'effacement.

3.2. Catégories de données à caractère personnel

- Gestion des clients (KYC et onboarding) : identité, coordonnées, situation familiale, données patrimoniales.
- Vérification d'identité : pièces d'identité et données issues du rapprochement facial.
- Questionnaire d'adéquation MIF2 : situation financière, objectifs, connaissances financières.
- Screening LCB-FT : identité, statut de personne politiquement exposée, données relatives à des condamnations pénales et à des infractions.
- Gestion du patrimoine : actifs financiers, comptes bancaires issus de l'agrégation, valorisations.
- Portail client en marque blanche : identité, données d'authentification, documents.
- Emails transactionnels : adresse électronique, nom, contenu des notifications.
- Signatures électroniques : identité, adresse électronique, preuves de signature.

3.3. Données relevant d'un régime particulier

Deux traitements sont susceptibles de porter sur des données soumises à un régime particulier.

- La vérification d'identité peut comporter un rapprochement facial, qui constitue un traitement de données biométriques aux fins d'identifier une personne physique de manière

unique, au sens de l'article 9 du RGPD. Ce traitement est mis en œuvre pour le compte du Cabinet, au titre de ses obligations de vérification de l'identité de ses clients. Le Cabinet, en sa qualité de responsable de traitement, s'assure qu'une condition de licéité prévue à l'article 9, paragraphe 2, est satisfaite ; Junga et son sous-traitant ultérieur de vérification d'identité lui apportent leur assistance à cette fin, notamment par le recueil du consentement explicite de la personne dans le parcours de vérification lorsque ce fondement est retenu.

- Le screening LCB-FT est susceptible de faire apparaître des données relatives à des condamnations pénales et à des infractions au sens de l'article 10 du RGPD. Ce traitement est mis en œuvre pour satisfaire aux obligations légales du Cabinet et l'accès à ces données est strictement limité.

3.4. Catégories de personnes concernées

- Les clients finaux du Cabinet.
- Les bénéficiaires effectifs identifiés dans le cadre du screening LCB-FT.
- Les utilisateurs du Cabinet, pour les emails transactionnels qui leur sont adressés.

3.5. Durée des traitements et durées de conservation

Les traitements sont réalisés pendant toute la durée du contrat de services. Les durées de conservation appliquées dans la plateforme, déterminées par les obligations légales qui s'imposent au Cabinet, sont les suivantes.

- Gestion des clients (KYC et onboarding) : cinq ans après la fin de la relation d'affaires (article L.561-12 du code monétaire et financier), suivis de cinq ans d'archivage.
- Vérification d'identité : cinq ans après la fin de la relation d'affaires.
- Questionnaire d'adéquation MIF2 : cinq ans, le questionnaire étant renouvelé tous les deux ans.
- Screening LCB-FT : cinq ans, dans un journal non modifiable.
- Gestion du patrimoine : durée de la relation, puis cinq ans ; les valorisations sont conservées sous forme d'historique non modifiable.
- Portail client en marque blanche : durée de la relation ; les sessions d'authentification sont conservées un an.
- Emails transactionnels : journaux conservés un an ; suppression des journaux chez le prestataire d'envoi sous trente jours.
- Signatures électroniques : dix ans (règlement eIDAS et article 1366 du code civil).

Les journaux d'audit de la plateforme sont conservés cinq ans et ne peuvent être ni modifiés ni supprimés, afin de garantir la traçabilité opposable lors d'un contrôle.

4. Instructions documentées

Junga ne traite les données du Cabinet que sur instruction documentée de celui-ci, y compris en ce qui concerne les transferts de données vers un pays tiers ou à une organisation internationale.

Constituent des instructions documentées du Cabinet : l'Accord et le contrat de services, l'utilisation de la plateforme par les utilisateurs du Cabinet, la configuration retenue par le Cabinet (paramétrage du KYC, du questionnaire MIF2, du dispositif LCB-FT, du portail client et des modèles de documents), ainsi que toute demande adressée par écrit par une personne habilitée du Cabinet.

Toute instruction complémentaire ou dérogatoire est formulée par écrit. Lorsque son exécution entraîne des développements ou des coûts supplémentaires, les Parties en conviennent préalablement.

Junga informe le Cabinet sans délai si elle estime qu'une instruction constitue une violation du RGPD ou d'une autre disposition du droit de l'Union ou du droit d'un État membre relative à la protection des données. Junga peut suspendre l'exécution de cette instruction jusqu'à ce que le Cabinet la confirme, la modifie ou la retire.

Lorsque Junga est tenue de traiter des données en vertu du droit de l'Union ou du droit français, elle en informe le Cabinet avant le traitement, sauf si ce droit interdit une telle information pour des motifs importants d'intérêt public.

5. Confidentialité des personnes autorisées

Junga veille à ce que les personnes autorisées à traiter les données du Cabinet s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

Cet engagement résulte du contrat de travail pour les salariés et d'un accord de confidentialité pour les prestataires. Il survit à la fin de la relation entre Junga et la personne concernée.

L'accès aux données du Cabinet est limité aux personnes qui en ont besoin pour l'exécution de la prestation, dans la limite de ce qui est nécessaire à leurs missions. Les accès sont nominatifs et journalisés.

6. Sécurité des traitements

Junga met en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD. Ces mesures sont les suivantes.

- Hébergement des données dans l'Union européenne, dans la région de Paris d'Amazon Web Services.
- Chiffrement des données en transit au moyen de TLS et au repos au moyen du service de gestion de clés d'Amazon Web Services.
- Cloisonnement des données entre cabinets : chaque cabinet n'accède qu'à ses propres données, ce cloisonnement étant vérifié en continu par des tests automatisés bloquants intégrés à la chaîne d'intégration.

- Séparation des espaces d'authentification du tableau de bord et du portail client, de sorte qu'une session ouverte sur le portail ne peut en aucun cas donner accès au tableau de bord.
- Contrôle d'accès authentifié et fondé sur les rôles, l'authentification à deux facteurs et les clés d'accès étant disponibles pour les comptes des utilisateurs du Cabinet.
- Journalisation des actions sensibles dans un journal d'audit qui ne peut être ni modifié ni supprimé, conservé cinq ans.
- Stockage des pièces justificatives et des documents dans un espace de stockage objet chiffré, sans exécution possible des fichiers déposés et avec conservation des versions.
- Supervision continue de la disponibilité et des erreurs applicatives, les données personnelles étant masquées avant leur transmission au service de supervision.
- Sauvegardes automatiques de la base de données permettant une restauration à un instant donné.
- Revue et évolution du dispositif en fonction de l'état de l'art, des risques identifiés et des évolutions de la plateforme.

7. Sous-traitants ultérieurs

7.1. Autorisation générale

Le Cabinet autorise de manière générale Junga à faire appel à des sous-traitants ultérieurs pour l'exécution de la prestation, dans les conditions prévues à l'article 28, paragraphes 2 et 4, du RGPD.

Junga impose par contrat à chaque sous-traitant ultérieur des obligations de protection des données équivalentes à celles de l'Accord. Junga demeure pleinement responsable devant le Cabinet de l'exécution par le sous-traitant ultérieur de ses obligations.

7.2. Liste des sous-traitants ultérieurs

La liste à jour des sous-traitants ultérieurs, précisant le service fourni, la localisation du traitement et le mécanisme d'encadrement des transferts applicable, est publiée sur www.junga.ai/sous-traitants. À la date de l'Accord, les sous-traitants ultérieurs intervenant dans les traitements réalisés pour le compte du Cabinet sont les suivants.

- Amazon Web Services : hébergement de la plateforme, Union européenne (Paris).
- Didit : vérification d'identité KYC, Espace économique européen (Espagne).
- Yousign : signature électronique, France.
- Brevo : envoi des emails transactionnels, France.
- Enable Banking : agrégation bancaire, Finlande.

- Sentry : supervision des erreurs applicatives, Union européenne (Allemagne).
- Langfuse : supervision technique des traitements d'intelligence artificielle, Union européenne.
- Anthropic : traitements d'intelligence artificielle (assistants et analyse de documents), États-Unis.
- Groq : traitements d'intelligence artificielle (analyse de texte et transcription), États-Unis.
- Hookdeck : acheminement des notifications techniques entrantes, Canada.

Stripe et PostHog, également mentionnés sur la page des sous-traitants, interviennent au titre des traitements dont Junga est responsable, respectivement la facturation de l'abonnement et la mesure d'usage du tableau de bord par les utilisateurs du Cabinet.

7.3. Changement de sous-traitant ultérieur

Junga informe le Cabinet de tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur, par la mise à jour de la page mentionnée ci-dessus et par une notification adressée au Cabinet, au moins trente jours avant que le nouveau sous-traitant ultérieur ne commence à traiter des données pour le compte du Cabinet.

Par exception, lorsque le remplacement est rendu nécessaire par un impératif de sécurité ou de continuité du service, notamment en cas d'incident affectant un sous-traitant ultérieur ou de cessation soudaine de son service, Junga peut y procéder sans préavis. Elle en informe alors le Cabinet sans délai indu, et au plus tard cinq jours ouvrés après la mise en service. Le Cabinet dispose dans ce cas d'un délai de quinze jours à compter de la notification pour exercer la faculté d'opposition prévue ci-dessous.

Le Cabinet peut s'opposer à ce changement pour un motif légitime tenant à la protection des données, en le notifiant par écrit avant l'expiration de ce délai. Les Parties recherchent alors une solution raisonnable. À défaut d'accord, le Cabinet peut résilier le contrat de services pour la partie de la prestation concernée, sans indemnité de part ni d'autre.

7.4. Transferts hors de l'Union européenne

Les données sont hébergées dans l'Union européenne. Certains sous-traitants ultérieurs sont établis en dehors de l'Espace économique européen, en particulier Anthropic et Groq aux États-Unis et Hookdeck au Canada.

Ces transferts sont encadrés par les clauses contractuelles types adoptées par la Commission européenne, complétées le cas échéant de mesures supplémentaires. Junga documente le mécanisme applicable à chaque fournisseur dans son registre des fournisseurs et communique au Cabinet, sur demande adressée à dpo@junga.ai, une copie des garanties applicables.

Junga ne transfère aucune donnée du Cabinet vers un pays tiers en dehors de ces cas sans instruction préalable du Cabinet.

8. Assistance au Cabinet

8.1. Droits des personnes concernées

Junga assiste le Cabinet, par des mesures techniques et organisationnelles appropriées et dans la mesure du possible, pour lui permettre de donner suite aux demandes d'exercice des droits prévus au chapitre III du RGPD : accès, rectification, effacement, limitation, portabilité et opposition.

Lorsqu'une demande d'exercice de droits est adressée directement à Junga par un client final du Cabinet, Junga n'y répond pas sur le fond. Elle la transmet au Cabinet sans délai indu et informe la personne concernée qu'elle doit s'adresser à son conseiller.

L'assistance est fournie au moyen des fonctionnalités de la plateforme et, à défaut, par une intervention ponctuelle des équipes de Junga.

8.2. Sécurité, analyses d'impact et consultation préalable

Compte tenu de la nature du traitement et des informations à sa disposition, Junga aide le Cabinet à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, notamment la sécurité du traitement, la notification des violations, la réalisation d'analyses d'impact relatives à la protection des données et la consultation préalable de l'autorité de contrôle.

Junga communique au Cabinet, sur demande, les informations nécessaires à ces travaux pour la part du traitement qu'elle opère.

8.3. Violations de données à caractère personnel

Junga notifie au Cabinet toute violation de données à caractère personnel affectant les données traitées pour son compte, sans délai indu et au plus tard 48 heures après en avoir pris connaissance.

La notification décrit, dans la mesure des informations disponibles au moment où elle est adressée : la nature de la violation, les catégories et le nombre approximatif de personnes concernées et d'enregistrements concernés, les conséquences probables, les mesures prises ou proposées pour y remédier et en atténuer les effets, ainsi que les coordonnées du point de contact. Les informations manquantes sont communiquées au fur et à mesure, sans nouveau délai indu.

Il appartient au Cabinet, en sa qualité de responsable de traitement, d'apprécier la violation et, le cas échéant, de la notifier à la Commission nationale de l'informatique et des libertés dans le délai de soixante-douze heures prévu à l'article 33 du RGPD et d'en informer les personnes concernées. Junga ne procède à ces notifications ni à la place du Cabinet ni en son nom, sauf instruction écrite de celui-ci.

Junga documente les violations dont elle a connaissance et coopère avec le Cabinet pour l'établissement de la documentation qui incombe à ce dernier.

9. Audit et démonstration de conformité

Junga met à la disposition du Cabinet toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD, conformément à son paragraphe 3, point h.

Le Cabinet peut faire réaliser un audit, y compris une inspection, par lui-même ou par un auditeur indépendant qu'il mandate et qui n'est pas un concurrent de Junga. L'audit se déroule sur préavis écrit raisonnable, pendant les heures ouvrées, sans perturbation excessive de l'activité de Junga et sous réserve d'un engagement de confidentialité de l'auditeur.

L'audit ne peut porter que sur les traitements réalisés pour le compte du Cabinet. Il ne donne accès ni aux données d'autres cabinets, ni aux données personnelles de tiers, ni aux éléments dont la divulgation compromettrait la sécurité de la plateforme ou les engagements de confidentialité de Junga envers ses autres clients.

Junga peut satisfaire à une demande d'audit en communiquant la documentation existante : description des mesures techniques et organisationnelles, résultats des contrôles internes, réponses à un questionnaire de sécurité et, lorsqu'ils existeront, rapports d'audit ou certificats délivrés par un tiers indépendant.

Sauf lorsque l'audit fait suite à une violation de données affectant le Cabinet ou révèle un manquement de Junga à l'Accord, les frais de l'audit sont à la charge du Cabinet, y compris le temps que Junga y consacre, facturé au tarif convenu entre les Parties. Sauf circonstance particulière, un audit sur site est limité à un par année civile.

10. Sort des données à l'issue de la prestation

À l'expiration ou à la résiliation du contrat de services, le Cabinet choisit entre la restitution des données traitées pour son compte et leur suppression. Il exprime ce choix par écrit.

En cas de restitution, Junga met à la disposition du Cabinet un export des données dans un format structuré et couramment utilisé, ainsi que les documents stockés dans la plateforme.

Junga supprime ensuite les données de ses systèmes actifs et fait supprimer les copies détenues par ses sous-traitants ultérieurs, dans un délai convenu entre les Parties. Les données présentes dans les sauvegardes sont supprimées à l'expiration du cycle de conservation de celles-ci.

Par exception, Junga conserve les données dont la conservation est imposée par le droit de l'Union ou par le droit français, notamment les enregistrements relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme (cinq ans après la fin de la relation d'affaires, article L.561-12 du code monétaire et financier), les documents signés électroniquement (dix ans) et les journaux d'audit (cinq ans). Le traitement de ces données est alors limité à leur conservation et à la finalité qui l'impose, jusqu'à l'expiration du délai applicable.

Junga confirme par écrit au Cabinet la réalisation des opérations de restitution et de suppression.

11. Durée, responsabilité et droit applicable

11.1. Durée

L'Accord entre en vigueur à la date d'effet du contrat de services et demeure applicable tant que Junga traite des données à caractère personnel pour le compte du Cabinet. Les stipulations qui, par leur nature, ont vocation à lui survivre, notamment celles relatives à la confidentialité et au sort des données, demeurent applicables après son terme.

11.2. Responsabilité

Chaque Partie répond des dommages causés par un traitement qui méconnaît le RGPD, dans les conditions prévues à son article 82. Junga n'est responsable du dommage causé par le traitement que si elle n'a pas respecté les obligations qui incombent spécifiquement aux sous-traitants ou si elle a agi en dehors des instructions licites du Cabinet ou contrairement à celles-ci.

Les limitations et plafonds de responsabilité stipulés au contrat de services s'appliquent à l'Accord, dans les limites permises par la loi.

11.3. Droit applicable et juridiction compétente

L'Accord est régi par le droit français. Tout litige relatif à sa validité, à son interprétation ou à son exécution relève de la juridiction désignée par le contrat de services.

11.4. Contact

Toute demande relative à l'Accord est adressée au délégué à la protection des données de Junga, Nicolas Molins, à dpo@junga.ai ou par courrier au siège social.

Junga