Accord de traitement des données

Conformément à l'article 28 du Règlement (UE) 2016/679 (RGPD). Version du 21 septembre 2026.

Entre

[Raison sociale du client], dont le siège social est situé [adresse], N° de TVA [●], représentée par [●] (le « **Responsable du traitement** »),

et

GREM S.R.L., dont le siège social est situé Via Matteo La Fragola 4, 84135 Salerno (SA), Italie, N° de TVA IT06136730659, représentée par son Administrateur unique, Mattia Guariglia (le « **Sous-traitant** »),

ensemble les « **Parties** ».

Préambule

A. Le Responsable du traitement est soumis aux obligations de vigilance à l'égard de la clientèle prévues par le décret législatif italien 231/2007 et, à compter du 10 juillet 2027, par le Règlement (UE) 2024/1624.

B. Le Sous-traitant fournit le service KYCJet (le « **Service** ») : vérification d'identité à distance au moyen de photographies du document, de la lecture de la puce, d'un contrôle du vivant du visage, du criblage des listes antiblanchiment et d'une décision sur le résultat prise par une personne qui, selon l'offre du Responsable du traitement, agit pour le compte de celui-ci ou est un opérateur du Sous-traitant (clause 3.6), avec approbation automatique facultative, sur instruction du Responsable du traitement, des seuls Dossiers au vert sur tous les contrôles, en vertu du contrat de service conclu entre les Parties (le « **Contrat** »).

C. Dans le cadre de la fourniture du Service, le Sous-traitant traite des données à caractère personnel pour le compte du Responsable du traitement. Le présent accord fixe les conditions de ce traitement et prévaut sur le Contrat pour toutes les questions relatives à la protection des données.

1. Définitions

Les termes commençant par une majuscule qui ne sont pas définis dans le présent accord ont le sens qui leur est donné par le RGPD. Les « **Personnes concernées** » sont les personnes dont l'identité est vérifiée. Le « **Dossier** » est une vérification individuelle ouverte par le Responsable du traitement. Les « **Données** » sont les données à caractère personnel traitées par le Sous-traitant pour le compte du Responsable du traitement, décrites à l'annexe A.

2. Objet et durée

2.1 Le Sous-traitant traite les Données uniquement pour fournir le Service, pour la nature, les finalités et les catégories décrites à l'annexe A.

2.2 Le présent accord s'applique pendant toute la durée du Contrat et, au-delà, aussi longtemps que le Sous-traitant conserve des Données en application de la clause 10.

3. Instructions du Responsable du traitement

3.1 Le Sous-traitant ne traite les Données que sur instruction documentée du Responsable du traitement, y compris en ce qui concerne les transferts vers des pays tiers, à moins qu'il ne soit tenu d'agir autrement en vertu du droit de l'Union ou du droit d'un État membre ; dans ce cas, il en informe préalablement le Responsable du traitement, sauf si la loi le lui interdit.

3.2 Constituent des instructions documentées : le Contrat et le présent accord ; les paramètres choisis par le Responsable du traitement dans le tableau de bord (en particulier les durées de conservation des données d'identification, des photographies et des Dossiers non terminés, ainsi que l'adresse de sa propre notice d'information) ; et les appels du Responsable du traitement aux interfaces du Service, en particulier la notification de la fin d'une relation d'affaires, l'effacement d'un Dossier et l'exportation des Données. Le Sous-traitant enregistre qui a donné ces trois dernières instructions, quand et d'où, et conserve cet enregistrement même après l'effacement des Données auxquelles il se rapporte.

3.3 L'activation de l'approbation automatique, désactivée par défaut, constitue également une instruction documentée : le Responsable du traitement l'active depuis le tableau de bord, quelle que soit son offre, en acceptant un texte versionné et en choisissant des seuils dédiés, et à partir de ce moment les Dossiers qui remplissent toutes les conditions de l'annexe B sont approuvés sans examen par une personne. La règle ne peut qu'approuver, jamais refuser. Le Responsable du traitement apprécie, dans le cadre de sa propre approche fondée sur les risques, s'il accepte de telles approbations, informe les Personnes concernées (article 13, paragraphe 2, point f), et article 22 du RGPD) et répond à leurs demandes d'intervention humaine : avec l'offre Standard, il procède lui-même au réexamen ; avec l'offre Institutionnelle, à sa demande, le Sous-traitant fait réexaminer le Dossier par un opérateur. Le Sous-traitant enregistre qui a activé ou désactivé l'approbation automatique, quand, avec quel texte et quels seuils, et chaque approbation automatique porte la référence de cette instruction.

3.4 S'il estime qu'une instruction constitue une violation du RGPD ou d'autres dispositions relatives à la protection des données, le Sous-traitant en informe immédiatement le Responsable du traitement et peut en suspendre l'exécution jusqu'à ce qu'elle soit confirmée ou modifiée.

3.5 Le Sous-traitant n'utilise pas les Données à ses propres fins, ne les communique pas, ne les vend pas et ne les utilise pas, ni ne permet qu'elles soient utilisées, pour entraîner des modèles.

3.6 **Offres.** La personne qui décide des Dossiers non approuvés automatiquement dépend de l'offre du Responsable du traitement, indiquée dans le Contrat et paramétrée par le Sous-traitant ; à défaut, l'offre est Standard.

a) **Standard** : le Responsable du traitement en décide, par l'intermédiaire de ses propres propriétaires et administrateurs, depuis le tableau de bord. Il examine les photographies, les scores, les données lues sur le document et les correspondances du criblage avec les données de la personne inscrite sur la liste ; il approuve, refuse ou demande à la Personne concernée de recommencer la vérification ; il évalue chaque correspondance du criblage et peut relancer celui-ci. Le personnel du Sous-traitant n'ouvre pas et ne consulte pas ces Dossiers, et ne statue pas sur eux : le Service l'en empêche.

b) **Institutionnelle** : un opérateur du Sous-traitant en décide ; il ouvre le Dossier, évalue les correspondances du criblage, peut corriger les données mal lues (annexe B) et décide. L'examen est un service que le Sous-traitant fournit sur instruction documentée du Responsable du traitement, et c'est le seul cas où le personnel du Sous-traitant accède aux données d'identification aux fins de l'examen.

Quelle que soit l'offre, le Responsable du traitement demeure responsable du traitement et entité assujettie au sens du décret législatif italien 231/2007 : la décision de nouer la relation, l'évaluation des risques et les

obligations de vigilance restent les siennes, et l'examen du Sous-traitant dans l'offre Institutionnelle ne les lui transfère pas. Chaque décision enregistre son auteur, sa date, les scores et les seuils en vigueur.

4. Confidentialité

Le Sous-traitant n'autorise à traiter les Données que les personnes qui en ont besoin pour fournir le Service, tenues à la confidentialité par contrat ou par la loi et formées au traitement des données biométriques et des données relatives à la lutte contre le blanchiment. Le personnel du Sous-traitant n'accède aux données d'identification et aux images d'un Dossier aux fins de l'examen qu'avec l'offre Institutionnelle (clause 3.6) ; chacun de ses accès à un Dossier, à ses images et à ses décisions est journalisé comme décrit à l'annexe B.

5. Sécurité

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles de l'annexe B, appropriées au risque conformément à l'article 32 du RGPD, et les met à jour en fonction de l'évolution technologique sans en réduire le niveau global.

6. Sous-traitants ultérieurs

6.1 Le Responsable du traitement donne une autorisation générale pour les sous-traitants ultérieurs énumérés à l'annexe D.

6.2 Le Sous-traitant notifie par écrit tout ajout ou remplacement au moins [30 jours] avant sa prise d'effet. Le Responsable du traitement peut s'y opposer pour des motifs raisonnables liés à la protection des données dans un délai de [15 jours] ; si les Parties ne parviennent pas à trouver une solution, le Responsable du traitement peut résilier la partie concernée du Contrat sans pénalité.

6.3 Le Sous-traitant impose contractuellement à chaque sous-traitant ultérieur des obligations en matière de protection des données offrant une protection au moins équivalente à celle du présent accord, et demeure pleinement responsable à l'égard du Responsable du traitement de leur exécution.

7. Transferts vers des pays tiers

7.1 Les Données sont traitées dans l'Union européenne. La seule exception concerne le prénom et le nom de la Personne concernée, envoyés pour le criblage à Dilisense en Suisse, pays faisant l'objet d'une décision d'adéquation de la Commission européenne (article 45 du RGPD).

7.2 Aucune Donnée n'est transférée vers des pays ne bénéficiant pas d'une décision d'adéquation.

7.3 Aucun autre transfert vers un pays tiers n'a lieu sans instruction écrite du Responsable du traitement.

8. Droits des Personnes concernées

8.1 Le Sous-traitant transmet au Responsable du traitement, dans un délai de [2 jours ouvrés], toute demande reçue directement d'une Personne concernée, sans y répondre sur le fond.

8.2 Le Service met à la disposition du Responsable du traitement les outils lui permettant de répondre : consultation du Dossier, exportation du rapport de vérification dans un format structuré, effacement d'un Dossier individuel. Pour les demandes que ces outils ne couvrent pas, le Sous-traitant assiste le Responsable du traitement dans un délai de [5 jours ouvrés] à compter de la demande.

9. Violations, analyses d'impact et consultation préalable

9.1 Le Sous-traitant notifie au Responsable du traitement toute violation de données à caractère personnel affectant les Données dans les meilleurs délais et, en tout état de cause, dans un délai de [24 heures] après en avoir pris connaissance, conformément à la *Procédure de gestion des incidents*, avec les informations visées à l'article 33, paragraphe 3, du RGPD disponibles à ce moment-là, complétées dès que possible.

9.2 Le Sous-traitant assiste le Responsable du traitement dans son analyse d'impact relative à la protection des données (article 35) et dans toute consultation préalable (article 36), notamment en fournissant le *Document de support à l'AIPD* et en répondant aux questions raisonnables.

10. Fin du traitement

10.1 Pendant la durée du Contrat, les Données sont effacées automatiquement selon le calendrier de l'annexe C.

10.2 À la cessation du Contrat, le Responsable du traitement peut, dans un délai de [30 jours], exporter toutes les Données depuis le tableau de bord dans les formats décrits dans le *Plan de sortie*. À l'expiration de ce délai, ou plus tôt sur demande écrite du Responsable du traitement, le Sous-traitant efface toutes les Données, y compris les copies, dans un délai de [30 jours] et le confirme par écrit.

10.3 Le Responsable du traitement demeure responsable de la conservation des données que la législation antiblanchiment l'oblige à conserver au-delà du Contrat : c'est pourquoi le Service lui permet de les exporter.

10.4 L'enregistrement des instructions du Responsable du traitement et des accès du personnel du Sous-traitant (clause 3.2 et annexe B) survit à l'effacement, sans données à caractère personnel des Personnes concernées, car il démontre que le traitement et l'effacement ont eu lieu comme convenu.

11. Informations et audits

11.1 Le Sous-traitant met à la disposition du Responsable du traitement les informations nécessaires pour démontrer le respect du présent accord, notamment le présent ensemble documentaire et, lorsqu'elles sont disponibles, les certifications ISO/IEC 27001 et 27017 avec leur périmètre.

11.2 Le Responsable du traitement, ou un auditeur qu'il mandate et qui est tenu à la confidentialité, peut réaliser des audits, y compris des inspections, moyennant un préavis de [30 jours], pendant les heures ouvrables et d'une manière qui ne compromet pas la sécurité des autres clients. Les autorités de surveillance et de protection des données du Responsable du traitement peuvent le faire dans les conditions prévues par la loi. Chaque Partie supporte ses propres frais, sauf si l'audit révèle un manquement substantiel du Sous-traitant.

12. Responsabilité

La responsabilité des Parties à l'égard des Personnes concernées est régie par l'article 82 du RGPD. Entre les Parties, [les limitations de responsabilité prévues au Contrat s'appliquent / préciser].

13. Dispositions finales

13.1 En cas de conflit entre le présent accord et le Contrat, le présent accord prévaut.

13.2 Le présent accord est régi par le droit italien. Les tribunaux de [Salerno] ont compétence exclusive pour tout litige.

[Lieu, date]

Le Responsable du traitement _____ Le Sous-traitant _____

Annexe A — Description du traitement

Catégories de Personnes concernées	Personnes physiques dont le Responsable du traitement demande la vérification de l'identité (clients ou clients potentiels, bénéficiaires effectifs, personnes agissant pour leur compte)
Données à caractère personnel courantes	Nom, prénoms, date et lieu de naissance, sexe, nationalité, numéro, type et date d'expiration du document, code fiscal ; champs vérifiés et méthode d'identification ; référence et nom déclaré fournis par le Responsable du traitement ; enregistrement du consentement (version, date, heure, adresse IP) ; résultat de la vérification, motif, mesures des contrôles et seuils appliqués ; corrections avec la valeur précédente
Catégories particulières (art. 9)	Images du visage traitées pour la comparaison avec le document (image du contrôle du vivant, portrait de la puce, photographie du document) : données biométriques. Le Service ne conserve aucun gabarit biométrique : la comparaison produit uniquement un score numérique de similarité
Données relatives aux condamnations pénales et aux infractions (art. 10)	Éventuelles correspondances du criblage sur des listes de procédures pénales, concernant la Personne concernée ou des tiers homonymes
Nature du traitement	Collecte au moyen d'un lien à usage unique, lecture automatisée du document, vérification de la signature de la puce, contrôle du vivant, comparaison faciale, criblage des listes, mise à disposition du Responsable du traitement des éléments nécessaires à sa décision (offre Standard) ou examen et décision par un opérateur du Sous-traitant (offre Institutionnelle), et, si le Responsable du traitement l'a activée, approbation automatique des seuls Dossiers au vert sur tous les contrôles, conservation, exportation et effacement
Finalité	Vigilance à l'égard de la clientèle du Responsable du traitement (décret législatif 231/2007 ; Règlement (UE) 2024/1624)
Durée	Pendant la durée du Contrat, selon le calendrier de l'annexe C

Annexe B — Mesures techniques et organisationnelles

Accès et autorisations

- Accès au tableau de bord avec des identifiants personnels ; mots de passe d'au moins 10 caractères conservés uniquement sous forme hachée.
- Rôles du Responsable du traitement : propriétaire, administrateur, membre ; les membres ne voient ni les données d'identification, ni les photographies, ni le criblage. L'exportation et l'effacement requièrent une autorisation spécifique. Avec l'offre Standard, seuls les propriétaires et les administrateurs décident des Dossiers.
- Rôles distincts pour le personnel du Sous-traitant : examinateur (voit les Dossiers des seuls Responsables du traitement ayant l'offre Institutionnelle) et administrateur (gère les clients et le système).
- Avec l'offre Standard, le Service empêche le personnel du Sous-traitant d'ouvrir et de consulter les Dossiers du Responsable du traitement et de statuer sur eux.
- Chaque accès du personnel du Sous-traitant à un Dossier est journalisé (ouverture, consultation du document, consultation du visage, décision, correction, évaluation du criblage, effacement) dans un journal qu'aucun effacement de données ne peut atteindre.

Confidentialité et intégrité des données

- Communications chiffrées en transit (TLS) ; notifications aux systèmes du Responsable du traitement uniquement vers des adresses HTTPS, signées avec HMAC-SHA256 et exemptes de données relatives aux personnes vérifiées (uniquement l'identifiant du dossier, le statut, l'heure et la référence du Responsable du traitement).
- Liens de vérification à usage unique, valables 30 minutes, conservés uniquement sous forme d'empreinte SHA-256 ; clés API conservées uniquement sous forme hachée.
- Photographies jamais stockées dans la base de données : stockage AWS S3 chiffré au repos, accessible uniquement au moyen de liens signés valables 5 minutes.
- Environnements de test et réel séparés : une clé de test ne peut ni voir ni modifier les données réelles.
- Corrections des données autorisées uniquement à un opérateur du Sous-traitant, avec l'offre Institutionnelle, pendant l'examen, avec conservation de la valeur précédente et notification au Responsable du traitement.

Fiabilité de la vérification

- Signature de la puce vérifiée sur le serveur par rapport à la master list des certificats des États émetteurs ; preuve anti-clonage avec un défi généré par le serveur.
- Résultat du contrôle du vivant lu par le serveur auprès d'AWS et lié au seul Dossier concerné ; identifiants AWS temporaires limités à la seule session.
- Aucun refus automatisé : chaque refus, et chaque Dossier qui ne remplit pas toutes les conditions de l'approbation automatique, est décidé par une personne, du Responsable du traitement avec l'offre Standard et un opérateur du Sous-traitant avec l'offre Institutionnelle ; chaque décision enregistre son auteur, sa date, les scores et les seuils en vigueur ; un Dossier dont le criblage n'est pas complet ne peut pas être approuvé.
- Approbation automatique uniquement sur instruction du Responsable du traitement (clause 3.3), pour les seuls Dossiers dont les données de la puce sont signées par l'État émetteur, avec preuve que la puce n'est pas une copie, date d'expiration lue sur la puce non dépassée, contrôle du vivant et similarité du visage avec la photo de la puce égaux ou supérieurs aux seuils dédiés choisis par le Responsable du traitement (de 90 à 100), criblage antiblanchiment terminé sans correspondance. Chaque approbation automatique est identifiable comme telle dans le Dossier, dans l'exportation et dans l'interface de programmation d'applications.

Minimisation et conservation

- Seul le nom est envoyé pour le criblage ; les photographies et le criblage ne sont pas exposés aux interfaces machine, sauf au moyen de l'exportation journalisée.
- Effacement automatique toutes les six heures conformément à l'annexe C, d'abord dans le stockage des images puis dans la base de données, chaque effacement effectué étant journalisé.

Continuité et surveillance

- Alertes automatiques en cas de défaillances critiques (magasin de certificats, clé de criblage, migrations de la base de données).
- [Sauvegardes quotidiennes chiffrées de la base de données, conservées pendant [30 jours] dans un lieu distinct, avec des tests de restauration [trimestriels].]
- [Test d'intrusion annuel réalisé par un tiers.]

Organisation

- Certification ISO/IEC 27001:2022 avec extension à l'ISO/IEC 27017:2015 (mesures de sécurité pour les services en nuage) de GREM S.R.L., site de Salerno : n° QAIS-IS-ITA-GS-03.26.003, délivrée par QACS International Pvt. Ltd., organisme accrédité par International Accreditation Service (IAS, MSCB-150), membre de l'International Accreditation Forum (IAF). Délivrée le 7 mai 2026, échéance le 6 mai 2029, avec des audits de surveillance annuels (6 mai 2027 et 6 mai 2028). Déclaration d'applicabilité GSRL/ED.01 du 13 janvier 2026. Périmètre : « Production and development of custom software, web-based applications, business management software, SaaS solutions, and CRM systems », qui couvre le Service en tant que solution SaaS développée et produite par GREM S.R.L. Vérifiable sur IAF CertSearch (www.iafcertsearch.org).
- Certification ISO 9001:2015 de GREM S.R.L., système de management de la qualité, site de Salerno : n° QACS-UAF-Q-ITA-GS-03.26.1260 (secteur IAF 33), délivrée par QACS International Pvt. Ltd., organisme accrédité par United Accreditation Foundation (UAF), membre de l'IAF. Délivrée le 7 mai 2026, échéance le 6 mai 2029, avec des audits de surveillance annuels ; même périmètre.
- Personnel tenu à la confidentialité et formé aux données biométriques, à la lutte contre le blanchiment et à l'utilisation des systèmes d'intelligence artificielle (article 4 du Règlement (UE) 2024/1689).

Les mesures entre crochets sont des engagements à rendre effectifs avant la signature.

Annexe C — Conservation et effacement

Données	Durée	Choix du Responsable du traitement
Lien de vérification	30 minutes, à usage unique	—
Photographies et image du visage	30 jours à compter de la capture, ou plus tôt à la clôture du Dossier	Peut la prolonger, mais pas au-delà de la durée de conservation des données d'identification
Données d'identification et rapport antiblanchiment	À compter de la fin de la relation d'affaires notifiée par le Responsable du traitement, pendant le nombre d'années paramétré	De 1 à 10 ans aujourd'hui ; au maximum 5 pour les délais commençant à courir à compter du 10 juillet 2027 (Règlement (UE) 2024/1624, article 77)
Dossier jamais terminé	Clôturé après 30 jours d'inactivité ; les données lues sont effacées après le	De 1 à 24 mois, 12 par défaut

Données	Durée	Choix du Responsable du traitement
	nombre de mois paramétré	
Notifications aux systèmes du Responsable du traitement et journal de ses appels API	30 jours	—
Dossier individuel sur instruction	Immédiatement, avec les photographies, les données, le criblage, les décisions et les notifications	Effacement depuis le tableau de bord ou l'interface

La date d'effacement des données d'identification est fixée une seule fois, au début de la période, et n'est pas recalculée si le Responsable du traitement modifie ses paramètres.

Annexe D — Sous-traitants ultérieurs autorisés

La liste figurant dans le document *Sous-traitants ultérieurs*, version du 21 septembre 2026, qui fait partie intégrante du présent accord.