Document de support à l'AIPD

Informations que GREM S.R.L. fournit au responsable du traitement pour son analyse d'impact relative à la protection des données (AIPD) (article 35 du RGPD), conformément à l'article 28, paragraphe 3, point f). L'analyse et ses conclusions demeurent celles du responsable du traitement. Version du 21 septembre 2026.

1. Pourquoi l'analyse est requise

Le traitement porte sur des données biométriques utilisées pour identifier une personne de manière unique (article 9), à grande échelle, au moyen de nouvelles technologies, et conditionne l'accès à un service : il répond aux critères de l'article 35, paragraphe 3, et figure sur la liste des types d'opérations de traitement soumis à une analyse d'impact établie par l'autorité italienne de protection des données, le Garante per la protezione dei dati personali (décision n° 467 du 11 octobre 2018).

2. Description du traitement

1. Le responsable du traitement ouvre un dossier et génère un lien à usage unique, valable 30 minutes.
2. La personne lit la notice d'information du responsable du traitement et donne son consentement ; le système enregistre la version du texte, la date, l'heure et l'adresse IP.
3. La personne photographie le document. Le service de lecture extrait les données ; la zone de lecture automatique et le code fiscal sont validés au moyen de leurs chiffres de contrôle.
4. Si le téléphone dispose de la technologie NFC, la personne lit la puce. Le serveur vérifie la signature de l'État émetteur et la preuve anti-clonage.
5. La personne effectue le contrôle du vivant : une brève capture du visage. Le serveur relit le résultat auprès d'AWS et compare le visage avec celui figurant sur le document ou dans la puce, obtenant un score de similarité.
6. Le nom lu fait l'objet d'un criblage par rapport aux listes de sanctions, de PPE et de procédures pénales.
7. Une personne examine les mesures, les images, les données lues et le criblage et décide : approuvé, refusé ou à recommencer. Qui est cette personne dépend de l'offre (voir ci-dessous). Si le responsable du traitement a activé l'approbation automatique, seuls les dossiers au vert sur tous les contrôles (puce signée par l'État, preuve anti-clonage, document non expiré, contrôle du vivant et visage avec des scores égaux ou supérieurs aux seuils dédiés choisis par le responsable du traitement, de 90 à 100, criblage sans correspondance) sont approuvés sans examen par une personne. Aucun refus n'est décidé par la machine. Chaque décision enregistre son auteur, sa date, les scores et les seuils en vigueur.
8. Le responsable du traitement reçoit la notification du résultat et consulte le rapport de vérification. Les données sont effacées selon les échéances paramétrées.

Offres. Avec l'offre **Standard**, les dossiers non approuvés automatiquement sont décidés par les propriétaires et les administrateurs du responsable du traitement, depuis le tableau de bord : ils évaluent aussi chaque correspondance du criblage, avec les données de la personne inscrite sur la liste, et peuvent relancer le criblage. Le personnel de GREM S.R.L. n'ouvre pas et ne consulte pas ces dossiers : le logiciel l'en empêche. Avec l'offre **Institutionnelle**, ils sont décidés par un opérateur de GREM S.R.L., pour le compte du responsable du

traitement et sur ses instructions : l'opérateur ouvre le dossier, et chaque ouverture est journalisée ; il évalue les correspondances ; il peut corriger les données mal lues. C'est la seule offre dans laquelle le personnel de GREM 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 la vigilance restent les siennes.

Les données traitées, les destinataires, les lieux et les durées figurent aux annexes A et C de l'*Accord de traitement des données* et dans la liste des *Sous-traitants ultérieurs*.

3. Nécessité et proportionnalité

- **Finalité déterminée** : la vigilance à l'égard de la clientèle exigée par le décret législatif italien 231/2007 ; aucune autre utilisation, aucun entraînement de modèles.
- **Base juridique** : obligation légale pour l'identification (article 6, paragraphe 1, point c)) ; consentement explicite pour le traitement biométrique (article 9, paragraphe 2, point a)), avec une alternative non biométrique proposée par le responsable du traitement par ses propres canaux.
- **Minimisation** : aucun gabarit biométrique conservé, uniquement un score numérique ; seul le nom est envoyé pour le criblage ; les notifications automatiques ne contiennent aucune donnée relative aux personnes vérifiées ; le rôle « membre » du responsable du traitement ne voit ni données ni images.
- **Limitation de la conservation** : photographies pendant 30 jours au maximum, sauf choix contraire du responsable du traitement ; données d'identification pendant la durée légale à compter de la fin de la relation ; dossiers non terminés effacés après 12 mois, sauf choix contraire du responsable du traitement ; effacement automatique toutes les six heures.
- **Exactitude** : avec l'offre Institutionnelle, corrections uniquement pendant l'examen d'un opérateur de GREM, avec conservation de la valeur précédente et information du responsable du traitement ; avec l'offre Standard, si les données lues sont erronées, le responsable du traitement demande à la personne de recommencer la vérification.

4. Risques et mesures

Risque pour la personne	Probabilité et gravité avant mesures	Mesures	Risque résiduel
Quelqu'un usurpe l'identité de la personne avec un document falsifié ou appartenant à autrui	Moyenne, grave	Signature de l'État sur la puce, preuve anti-clonage, contrôle du vivant, comparaison faciale, décision humaine	Faible
Une approbation automatique accepte une personne qui n'est pas celle qu'elle prétend être	Faible, grave	Uniquement si elle est activée par le responsable du traitement au moyen d'une instruction enregistrée ; uniquement avec des données signées par l'État et une puce qui prouve qu'elle n'est pas une copie ; seuils non inférieurs à 90 ; criblage sans correspondance ; jamais un refus ; chaque approbation automatique est identifiable et peut être réexaminée sur demande	Faible

Risque pour la personne	Probabilité et gravité avant mesures	Mesures	Risque résiduel
Une fausse capture (vidéo enregistrée, masque, image de synthèse) passe le contrôle du vivant	Moyenne, grave	Contrôle du vivant d'AWS dont le résultat est lu par le serveur et lié au dossier ; seuil de confiance ; décision humaine	Faible à moyen
La personne est rejetée à cause d'une erreur de la machine, y compris de manière discriminatoire	Moyenne, moyenne	Aucun refus automatisé ; la personne qui décide voit les mesures et les images ; possibilité de recommencer ; alternative non biométrique	Faible
Vol ou divulgation des images du visage et du document	Faible, très grave	Images hors de la base de données, chiffrées, accessibles uniquement au moyen de liens valables 5 minutes ; conservation courte ; accès du personnel journalisés	Faible
Utilisation des données à d'autres fins ou pour entraîner des modèles	Faible, grave	Interdiction contractuelle pour nous et pour les sous-traitants ultérieurs	Faible
Conservation au-delà du nécessaire	Moyenne, moyenne	Effacement automatique ; dates fixées et non recalculables ; effacement d'un dossier individuel	Faible
Une homonymie avec une personne sanctionnée entraîne un rejet injustifié	Moyenne, grave	Chaque correspondance est évaluée par une personne avant la décision (du responsable du traitement avec l'offre Standard, un opérateur de GREM avec l'offre Institutionnelle), en comparant les données de la personne inscrite sur la liste ; motif enregistré	Faible
Accès non autorisé par un employé du prestataire	Faible, grave	Avec l'offre Standard, le personnel du prestataire ne peut pas ouvrir les dossiers ; avec l'offre Institutionnelle, rôles distincts, journal inaltérable de chaque accès, obligations de confidentialité	Faible
Accès inapproprié par le personnel du responsable du traitement, qui avec l'offre Standard voit les images et les données pour décider	Faible, grave	Seuls les propriétaires et les administrateurs décident ; le rôle « membre » ne voit ni données ni images ; images uniquement au moyen de liens valables 5 minutes ; chaque décision enregistre son auteur ; **chaque ouverture d'un dossier depuis le tableau de bord est enregistrée** avec la personne, la date et l'adresse, et le registre figure dans l'export de l'organisation (`registro.jsonl`) ; vérification en deux étapes disponible pour le personnel du responsable du traitement	À évaluer par le responsable du traitement, selon ses propres mesures internes
Exclusion des personnes ne disposant pas d'un smartphone adapté	Moyenne, moyenne	La lecture de la puce est facultative ; alternative proposée par le responsable du traitement	Faible

5. Ce que le responsable du traitement doit ajouter

- Sa propre évaluation des risques, la classification de la fonction et les alternatives qu'il propose.

- L'avis de son délégué à la protection des données (DPD), s'il en a désigné un.
- Le cas échéant, l'avis des personnes concernées ou de leurs représentants (article 35, paragraphe 9).
- La décision relative à la consultation préalable de l'autorité de contrôle, si le risque résiduel demeure élevé (article 36).
- Avec l'offre Standard : les membres de son personnel qui décident des dossiers, la manière dont ils sont formés à lire les scores et les correspondances du criblage, et la manière dont leurs accès sont contrôlés.
- S'il active l'approbation automatique : l'évaluation du risque résiduel d'une approbation sans examen par une personne, l'information des personnes concernées et la manière dont il répond aux demandes d'intervention humaine (article 22, paragraphe 3).