DPIA Support Document

Information that GREM S.R.L. provides to the controller for its data protection impact assessment (Article 35 GDPR), under Article 28(3)(f). The assessment and its conclusions remain the controller's. Version of 21 September 2026.

1. Why the assessment is required

The processing involves biometric data used to uniquely identify a person (Article 9), on a large scale, with new technologies, and determines access to a service: it meets the criteria of Article 35(3) and the Italian Data Protection Authority's list of processing operations subject to an impact assessment (decision no. 467 of 11 October 2018).

2. Description of the processing

1. The controller opens a case and generates a single-use link, valid for 30 minutes.
2. The person reads the controller's notice and gives consent; the system records the text version, date, time and IP address.
3. The person photographs the document. The reading service extracts the data; the machine-readable zone and the tax code are validated with their check digits.
4. If the phone has NFC, the person reads the chip. The server verifies the issuing State's signature and the anti-cloning proof.
5. The person performs the liveness check: a short capture of the face. The server reads the outcome back from AWS and compares the face with that on the document or chip, obtaining a similarity score.
6. The name read is screened against sanctions, PEP and criminal proceedings lists.
7. A person examines measurements, images, data read and screening and decides: approved, declined or retry. Who that person is depends on the plan (see below). If the controller has switched on automatic approval, only cases green on every check (chip signed by the State, anti-cloning proof, document not expired, liveness check and face with scores at or above the dedicated thresholds chosen by the controller, from 90 to 100, screening with no matches) are approved without review by a person. No refusal is decided by the machine. Every decision records who made it, when, the scores and the thresholds in force.
8. The controller receives notification of the outcome and reads the record. Data is erased on the schedules set.

Plans. On the **Standard** plan, cases not approved automatically are decided by the controller's owners and administrators, from the dashboard: they also assess each screening hit, with the details of the listed person, and may re-run the screening. GREM S.R.L. staff do not open or view these cases: the software prevents it. On the **Institutional** plan they are decided by a GREM S.R.L. operator, on the controller's behalf and on its instructions: the operator opens the case, and every opening is logged; assesses the hits; may correct misread data. It is the only plan in which GREM staff access identification data for review. On either plan the controller remains the controller and the obliged entity under Legislative Decree 231/2007: the decision to enter into the relationship, the risk assessment and due diligence remain its own.

The data processed, recipients, locations and periods are in Annex A and Annex C of the *Data Processing Agreement* and in the *Sub-processors* list.

3. Necessity and proportionality

- **Specified purpose**: the customer due diligence required by Legislative Decree 231/2007; no other use, no model training.
- **Legal basis**: legal obligation for identification (Article 6(1)(c)); explicit consent for biometric processing (Article 9(2)(a)), with a non-biometric alternative offered by the controller through its own channels.
- **Minimisation**: no biometric template stored, only a numeric score; only the name is sent for screening; automated notifications contain no data about verified persons; the controller's "member" role sees no data or images.
- **Storage limitation**: photographs for at most 30 days unless the controller chooses otherwise; identification data for the statutory period from the end of the relationship; uncompleted cases erased after 12 months unless the controller chooses otherwise; automatic erasure every six hours.
- **Accuracy**: on the Institutional plan, corrections only during review by a GREM operator, with the previous value retained and the controller notified; on the Standard plan, if the data read is wrong, the controller asks the person to redo the verification.

4. Risks and measures

Risk to the person	Likelihood and severity before measures	Measures	Residual risk
Someone impersonates the person with a forged or someone else's document	Medium, severe	State signature on the chip, anti-cloning proof, liveness check, face comparison, human decision	Low
An automatic approval accepts a person who is not who they claim to be	Low, severe	Only if switched on by the controller with a recorded instruction; only with State-signed data and a chip that proves it is not a copy; thresholds not below 90; screening with no matches; never a refusal; every automatic approval is identifiable and can be reviewed again on request	Low
A fake capture (recorded video, mask, synthetic image) passes the liveness check	Medium, severe	AWS liveness check with outcome read by the server and bound to the case; confidence threshold; human decision	Low-medium
The person is rejected because of a machine error, including in a discriminatory way	Medium, medium	No automated refusal; whoever decides sees measurements and images; possibility to retry; non-biometric alternative	Low
Theft or disclosure of face and document images	Low, very severe	Images outside the database, encrypted, accessible only through 5-minute links; short retention; staff access logged	Low
Use of data for other purposes or to train models	Low, severe	Contractual prohibition for us and for sub-processors	Low

Risk to the person	Likelihood and severity before measures	Measures	Residual risk
Retention beyond what is necessary	Medium, medium	Automatic erasure; dates fixed and not recalculable; erasure of a single case	Low
A name match with a sanctioned person leads to an unfair rejection	Medium, severe	Every hit is assessed by a person before the decision (from the controller on the Standard plan, a GREM operator on the Institutional plan), comparing the details of the listed person; reason recorded	Low
Unauthorised access by a provider employee	Low, severe	On the Standard plan provider staff cannot open cases; on the Institutional plan separate roles, tamper-proof log of every access, confidentiality obligations	Low
Improper access by the controller's staff, who on the Standard plan see images and data in order to decide	Low, severe	Only owners and administrators decide; the "member" role sees no data or images; images only through 5-minute links; every decision records who made it; **every opening of a case from the dashboard is recorded** with person, date and address, and the log is included in the organization export (`registro.jsonl`); two-step verification available for the controller's staff	For the controller to assess, according to its own internal measures
Exclusion of people without a suitable smartphone	Medium, medium	Chip reading is optional; alternative offered by the controller	Low

5. What the controller must add

- Its own risk assessment, the classification of the function and the alternatives it offers.
- The opinion of its data protection officer, if appointed.
- Where appropriate, the views of data subjects or their representatives (Article 35(9)).
- The decision on prior consultation of the supervisory authority, if the residual risk remains high (Article 36).
- On the Standard plan: which of its staff decide cases, how they are trained to read scores and screening hits, and how their access is controlled.
- If it switches on automatic approval: the assessment of the residual risk of an approval without review by a person, the information given to data subjects and how it answers requests for human intervention (Article 22(3)).