Data Processing Agreement

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR). Version of 21 September 2026.

Between

[Customer's company name], with registered office at [address], VAT no. [●], represented by [●] (the **"Controller"**),

and

GREM S.R.L., with registered office at Via Matteo La Fragola 4, 84135 Salerno (SA), Italy, VAT no. IT06136730659, represented by its Sole Director Mattia Guariglia (the **"Processor"**),

together the **"Parties"**.

Recitals

A. The Controller is subject to the customer due diligence obligations of Italian Legislative Decree 231/2007 and, from 10 July 2027, of Regulation (EU) 2024/1624.

B. The Processor provides the KYCJet service (the **"Service"**): remote identity verification through document photographs, chip reading, a face liveness check, anti-money-laundering list screening and a decision on the outcome by a person who, depending on the Controller's plan, is someone acting for the Controller or an operator of the Processor (clause 3.6), with optional automatic approval, on the Controller's instruction, of only those Cases that are green on every check, under the service agreement between the Parties (the **"Agreement"**).

C. In providing the Service the Processor processes personal data on behalf of the Controller. This agreement sets out the terms of that processing and prevails over the Agreement on all data protection matters.

1. Definitions

Capitalised terms not defined here have the meaning given in the GDPR. **"Data Subjects"** are the persons whose identity is verified. **"Case"** is a single verification opened by the Controller. **"Data"** means the personal data processed by the Processor on behalf of the Controller, described in Annex A.

2. Subject matter and duration

2.1 The Processor processes the Data solely to provide the Service, for the nature, purposes and categories described in Annex A.

2.2 This agreement lasts as long as the Agreement and, thereafter, for as long as the Processor retains Data under clause 10.

3. Controller's instructions

3.1 The Processor processes the Data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required to do otherwise by Union or Member State law; in that case it informs the Controller beforehand, unless the law prohibits it.

3.2 Documented instructions are: the Agreement and this agreement; the settings chosen by the Controller in the dashboard (in particular the retention periods for identification data, photographs and uncompleted Cases, and the address of its own privacy notice); and the Controller's calls to the Service interfaces, in particular notice of the end of a business relationship, erasure of a Case and export of Data. The Processor records who gave these last three instructions, when and from where, and keeps that record even after the Data it refers to has been erased.

3.3 The activation of automatic approval, which is off by default, is also a documented instruction: the Controller switches it on from the dashboard, on either plan, by accepting a versioned text and choosing dedicated thresholds, and from that moment Cases that meet all the conditions in Annex B are approved without review by a person. The rule can only approve, never refuse. The Controller assesses, within its own risk-based approach, whether to accept such approvals, informs Data Subjects (Articles 13(2)(f) and 22 GDPR) and answers their requests for human intervention: on the Standard plan the Controller carries out the new review itself; on the Institutional plan, at the Controller's request, the Processor has the Case reviewed again by an operator. The Processor records who switched automatic approval on or off, when, with which text and which thresholds, and every automatic approval carries a reference to that instruction.

3.4 If it considers that an instruction infringes the GDPR or other data protection provisions, the Processor immediately informs the Controller and may suspend its execution until it is confirmed or amended.

3.5 The Processor does not use the Data for its own purposes, does not disclose or sell it, and does not use it, or allow it to be used, to train models.

3.6 **Plans.** Who decides the Cases that are not approved automatically depends on the Controller's plan, stated in the Agreement and set by the Processor; failing that, the plan is Standard.

a) **Standard**: the Controller decides them, through its own owners and administrators, from the dashboard. It examines photographs, scores, data read from the document and screening hits with the details of the listed person; it approves, declines or asks the Data Subject to redo the verification; it assesses each screening hit and may re-run the screening. The Processor's staff do not open, view or decide these Cases: the Service prevents it.

b) **Institutional**: an operator of the Processor decides them, opening the Case, assessing the screening hits, possibly correcting data that was misread (Annex B), and deciding. The review is a service the Processor performs on the Controller's documented instructions, and it is the only case in which the Processor's 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 the due diligence obligations remain its own, and the Processor's review on the Institutional plan does not transfer them. Every decision records who made it, when, the scores and the thresholds in force.

4. Confidentiality

The Processor authorises to process the Data only the persons who need to do so to provide the Service, bound by contractual or statutory confidentiality and trained on the processing of biometric and anti-money-

laundering data. The Processor's staff access the identification data and images of a Case for review only on the Institutional plan (clause 3.6); every access by them to a Case, its images and its decisions is logged as described in Annex B.

5. Security

The Processor implements the technical and organisational measures in Annex B, appropriate to the risk under Article 32 GDPR, and updates them as technology evolves without reducing their overall level.

6. Sub-processors

6.1 The Controller grants general authorisation for the sub-processors listed in Annex D.

6.2 The Processor gives written notice of any addition or replacement at least [30 days] before it takes effect. The Controller may object on reasonable data protection grounds within [15 days]; if the Parties cannot find a solution, the Controller may terminate the affected part of the Agreement without penalty.

6.3 The Processor imposes on each sub-processor, by contract, data protection obligations no less protective than these, and remains fully liable to the Controller for their performance.

7. Transfers to third countries

7.1 The Data is processed in the European Union. The only exception is the Data Subject's first name and surname, sent for screening to Dilisense in Switzerland, a country covered by a European Commission adequacy decision (Article 45 GDPR).

7.2 No Data is transferred to countries without an adequacy decision.

7.3 No other transfer to a third country takes place without the Controller's written instruction.

8. Data Subjects' rights

8.1 The Processor forwards to the Controller, within [2 business days], any request received directly from a Data Subject, without answering it on the merits.

8.2 The Service provides the Controller with the tools to respond: viewing the Case, exporting the record in a structured format, erasing a single Case. For requests these tools do not cover, the Processor assists the Controller within [5 business days] of the request.

9. Breaches, impact assessments and prior consultation

9.1 The Processor notifies the Controller of any personal data breach affecting the Data without undue delay and in any event within [24 hours] of becoming aware of it, following the *Incident Management Procedure*, with the information under Article 33(3) GDPR available at that time, supplemented as soon as possible.

9.2 The Processor assists the Controller with its data protection impact assessment (Article 35) and any prior consultation (Article 36), in particular by providing the *DPIA Support Document* and answering reasonable

questions.

10. End of processing

10.1 During the Agreement, Data is erased automatically on the schedule in Annex C.

10.2 On termination of the Agreement the Controller may, within [30 days], export all Data from the dashboard in the formats described in the *Exit Plan*. After that period, or earlier at the Controller's written request, the Processor erases all Data, including copies, within [30 days] and confirms it in writing.

10.3 The Controller remains responsible for retaining the data that anti-money-laundering law requires it to keep beyond the Agreement: this is why the Service allows it to be exported.

10.4 The record of the Controller's instructions and of access by the Processor's staff (clause 3.2 and Annex B) survives erasure, without personal data of Data Subjects, because it demonstrates that processing and erasure took place as agreed.

11. Information and audits

11.1 The Processor makes available to the Controller the information necessary to demonstrate compliance with this agreement, in particular this documentation package and, where available, the ISO/IEC 27001 and 27017 certifications with their scope.

11.2 The Controller, or an auditor it appoints who is bound by confidentiality, may carry out audits, including inspections, with [30 days'] notice, during business hours and in a manner that does not compromise the security of other customers. The Controller's supervisory and data protection authorities may do so on the terms provided by law. Each Party bears its own costs, unless the audit reveals a material breach by the Processor.

12. Liability

Liability of the Parties towards Data Subjects is governed by Article 82 GDPR. Between the Parties, [the limitations of liability in the Agreement apply / specify].

13. Final provisions

13.1 In case of conflict between this agreement and the Agreement, this agreement prevails.

13.2 This agreement is governed by Italian law. The courts of [Salerno] have exclusive jurisdiction over any dispute.

[Place, date]

The Controller _____ The Processor _____

Annex A — Description of the processing

Categories of Data Subjects	Natural persons whose identity the Controller asks to verify (customers or prospective customers, beneficial owners, persons acting on their behalf)
Personal data	Surname, given names, date and place of birth, sex, nationality, document number, type and expiry date, tax code; verified fields and identification method; reference and declared name provided by the Controller; consent record (version, date, time, IP address); verification outcome, reason, check measurements and thresholds applied; corrections with the previous value
Special categories (Art. 9)	Face images processed for comparison with the document (liveness frame, chip portrait, document photograph): biometric data. The Service stores no biometric templates: the comparison only produces a numeric similarity score
Data relating to criminal convictions and offences (Art. 10)	Any screening hits on criminal proceedings lists, relating to the Data Subject or to third parties with the same name
Nature of the processing	Collection through a single-use link, automated document reading, chip signature verification, liveness check, face comparison, list screening, making the elements for its decision available to the Controller (Standard plan) or review and decision by an operator of the Processor (Institutional plan), and, where the Controller has switched it on, automatic approval of only those Cases that are green on every check, retention, export and erasure
Purpose	The Controller's customer due diligence (Legislative Decree 231/2007; Regulation (EU) 2024/1624)
Duration	For the term of the Agreement, on the schedule in Annex C

Annex B — Technical and organisational measures

Access and authorisation

- Dashboard access with personal credentials; passwords of at least 10 characters stored only as a hash.
- Controller roles: owner, administrator, member; members see no identification data, photographs or screening. Export and erasure require a specific permission. On the Standard plan only owners and administrators decide Cases.
- Separate roles for the Processor's staff: reviewer (sees the Cases of Controllers on the Institutional plan only) and administrator (manages customers and the system).
- On the Standard plan the Service prevents the Processor's staff from opening, viewing and deciding the Controller's Cases.
- Every access by the Processor's staff to a Case is logged (opening, viewing the document, viewing the face, decision, correction, screening assessment, erasure) in a log that no data erasure can reach.

Confidentiality and integrity of data

- Encrypted communications in transit (TLS); notifications to the Controller's systems only to HTTPS addresses, signed with HMAC-SHA256 and free of data about verified persons (only case identifier, status, time and the Controller's reference).

- Single-use verification links, valid for 30 minutes, stored only as a SHA-256 hash; API keys stored only as a hash.
- Photographs never stored in the database: AWS S3 storage encrypted at rest, reachable only through signed links valid for 5 minutes.
- Separate test and live environments: a test key can neither see nor modify live data.
- Data corrections allowed only to an operator of the Processor, on the Institutional plan, during review, with the previous value retained and the Controller notified.

Reliability of the verification

- Chip signature verified on the server against the master list of issuing States' certificates; anti-cloning proof with a server-generated challenge.
- Liveness outcome read by the server from AWS and bound to the single Case; temporary AWS credentials scoped to the single session.
- No automated refusals: every refusal, and every Case that does not meet all the conditions for automatic approval, is decided by a person, from the Controller on the Standard plan and an operator of the Processor on the Institutional plan; every decision records who made it, when, the scores and the thresholds in force; a Case without complete screening cannot be approved.
- Automatic approval only on the Controller's instruction (clause 3.3), for only those Cases with chip data signed by the issuing State, proof that the chip is not a copy, an expiry date read from the chip that has not passed, liveness check and face similarity with the chip photo at or above the dedicated thresholds chosen by the Controller (from 90 to 100), and anti-money-laundering screening completed with no matches. Every automatic approval is identifiable as such in the Case, in the export and in the application programming interface.

Minimisation and retention

- Only the name is sent for screening; photographs and screening are not exposed to machine interfaces except through the logged export.
- Automatic erasure every six hours under Annex C, first from image storage and then from the database, with every erasure performed being logged.

Continuity and monitoring

- Automatic alerts on critical failures (certificate store, screening key, database migrations).
- [Daily encrypted database backups, retained for [30 days] in a separate location, with [quarterly] restore tests.]
- [Annual penetration test by a third party.]

Organisation

- ISO/IEC 27001:2022 certification with extension to ISO/IEC 27017:2015 (security controls for cloud services) of GREM S.R.L., Salerno site: no. QAIS-IS-ITA-GS-03.26.003, issued by QACS International Pvt. Ltd., a body accredited by International Accreditation Service (IAS, MSCB-150), a member of the International Accreditation Forum (IAF). Issued on 7 May 2026, expiring on 6 May 2029, with annual surveillance audits (6 May 2027 and 6 May 2028). Statement of Applicability GSRL/ED.01 of 13 January 2026. Scope: "Production and development of custom software, web-based applications, business management software, SaaS solutions, and CRM systems", which covers the Service as a SaaS solution developed and produced by GREM S.R.L. Verifiable on IAF CertSearch (www.iafcertsearch.org).

- ISO 9001:2015 certification of GREM S.R.L., quality management system, Salerno site: no. QACS-UAF-Q-ITA-GS-03.26.1260 (IAF sector 33), issued by QACS International Pvt. Ltd., a body accredited by United Accreditation Foundation (UAF), a member of the IAF. Issued on 7 May 2026, expiring on 6 May 2029, with annual surveillance audits; same scope.
- Staff bound by confidentiality and trained on biometric data, anti-money-laundering and the use of artificial intelligence systems (Article 4 of Regulation (EU) 2024/1689).

Measures in square brackets are commitments to be made effective before signature.

Annex C — Retention and erasure

Data	Period	Controller's choice
Verification link	30 minutes, single use	—
Photographs and face image	30 days from capture, or earlier when the Case is closed	May extend it, but not beyond the retention of the identification data
Identification data and anti-money-laundering record	From the end of the business relationship notified by the Controller, for the years set	1 to 10 years today; at most 5 for periods starting from 10 July 2027 (Regulation (EU) 2024/1624, Article 77)
Case never completed	Closed after 30 days of inactivity; data read is erased after the months set	1 to 24 months, default 12
Notifications to the Controller's systems and log of its API calls	30 days	—
Single Case on instruction	Immediately, with photographs, data, screening, decisions and notifications	Erasure from the dashboard or the interface

The erasure date of identification data is fixed once, when the period starts, and is not recalculated if the Controller changes its settings.

Annex D — Authorised sub-processors

The list in the *Sub-processors* document, version of 21 September 2026, which forms part of this agreement.