KYCJet Terms of Service

*Between GREM S.R.L., Via Matteo La Fragola 4, 84135 Salerno (SA), Italy, VAT no. IT06136730659 (the **"Provider"**) and the business activating the service (the **"Customer"**). Business-to-business agreement: consumer protection rules do not apply. Version of 21 September 2026.*

1. Subject matter

1.1 The Provider makes KYCJet (the **"Service"**) available to the Customer: a remote identity verification service described in clause 1 of the DORA addendum and in the application programming interface reference.

1.2 The Service gives the Customer the elements to identify its own customers. It does not replace the Customer in its obligations: risk assessment, the decision to enter into a relationship, retention of data required by law beyond the Agreement, and the attestation under Article 27 of Legislative Decree 231/2007 remain with the Customer.

1.3 The Customer may switch on automatic approval from the dashboard, on either plan: a rule that approves, without review by a person, cases green on every check, under the conditions and with the thresholds stated in the text it accepts. The activation is an instruction from the Customer, recorded with author, date, text and thresholds, and can be withdrawn at any time; the Customer adopts it within its own risk-based approach, is responsible for it and informs the persons verified about it. The rule never refuses: every refusal stays with a person, under clause 1.4.

1.4 **Plans.** Cases not approved by the rule are decided by a person, according to the plan stated in the Agreement and set by the Provider; failing that, the plan is Standard.

a) **Standard**: the Customer's owners and administrators decide them, from the dashboard, examining photographs, scores, data read and screening hits; they approve, decline or ask the person to redo the verification, assess the screening hits and may re-run the screening. The Provider's staff do not open or decide these cases.

b) **Institutional**: a Provider operator decides them, assessing the screening hits and possibly correcting data that was misread, with notice to the Customer. It is a service performed on the Customer's instructions; review times and price are set in the Agreement.

On either plan the obligations in clause 1.2 remain with the Customer, and every decision records who made it, when, the scores and the thresholds in force.

2. Contract documents

The contract (the **"Agreement"**) consists of, in order of precedence: the data processing agreement; the DORA addendum, if the Customer is a financial entity; the service level agreement; the exit plan; these terms; any commercial offer.

3. Activation and account

3.1 The Customer activates the Service by creating an organisation in the dashboard. The person creating it represents that they have authority to bind the Customer.

3.2 The Customer assigns its members the roles of owner, administrator or member, and is responsible for who has access and for the use of credentials and API keys, which it keeps secret.

3.3 Test mode is for integrating the Service: it must not be used with data of real persons.

4. Customer obligations

The Customer:

a) is the controller of the data of the persons verified and guarantees the legal basis for processing;

b) publishes its own privacy notice and sets its address in the dashboard before generating links (the Service does not generate them otherwise);

c) offers, through its own channels, an identification method alternative to the biometric one;

d) uses the Service only for due diligence on its own customers, in compliance with the law;

e) notifies the end of relationships through the Service in a timely manner, so that retention periods can start.

5. Provider obligations

The Provider supplies the Service with professional diligence, according to the service levels, and processes data as set out in the data processing agreement. On the Institutional plan it decides, through its operators, the cases not approved by the automatic approval rule; on the Standard plan it provides the Customer with the tools to decide them (clauses 1.3 and 1.4).

6. Fees

6.1 The Service is paid per use, from a prepaid balance in euro. Each completed verification is charged when the person completes the face check, for the modules performed, at the following prices, VAT excluded:

Module	Price
Verification: document, liveness check, face comparison	€0.33
NFC chip reading and verification, only if the chip was read	€0.15
Anti-money-laundering screening, on every completed verification	€0.20

A verification therefore costs at most €0.68. Nothing is charged for a verification that is not completed, for a rejected photo, for an interruption caused by the Provider's checks being unavailable, or for a failed liveness check. Erasing a case does not give rise to a refund.

6.2 The balance is topped up from the dashboard by payment card, through Stripe, with top-ups of €50, €200 or €1,000, VAT excluded; the balance does not expire. A verification link can be generated only if the balance

covers the maximum cost of a verification. There are no free verifications in live mode; in test mode the first 20 verifications of each month are free and the following ones cost the same as in live mode. Review on the Institutional plan is priced in the Agreement; any different terms are those in the commercial offer.

6.3 The Provider may change prices with [60 days'] notice; a Customer that does not accept them may terminate before they take effect.

7. Intellectual property

The Service, the software and the documentation remain the Provider's. The Customer receives a non-exclusive, non-transferable right of use for the term of the Agreement. The data of the Customer and of the persons verified remain the Customer's.

8. Confidentiality

Each Party treats as confidential the other's information it becomes aware of, for the term of the Agreement and for [5 years] thereafter, save for legal obligations or requests from authorities.

9. Liability

9.1 The Provider is liable without limit for damage caused by wilful misconduct or gross negligence. In all other cases its aggregate liability is limited to the fees paid by the Customer in the [12 months] preceding the event.

9.2 The Provider is not liable for the Customer's decisions on entering into relationships, for use of the outcomes other than as intended, or for approvals made by the automatic approval rule switched on by the Customer, where the Service has correctly verified the conditions the rule requires, or for decisions on cases made by the Customer on the Standard plan.

9.3 These limitations do not apply to liability towards data subjects under Article 82 GDPR, which is governed by the data processing agreement.

10. Suspension

The Provider may suspend the Customer's access, with immediate notice and only for as long as strictly necessary, solely in case of serious risk to the security of the Service or of data, or of manifestly unlawful use.

11. Term and termination

11.1 The Agreement lasts [12 months] and renews automatically from year to year.

11.2 The Customer may terminate at any time with [30 days'] written notice; the Provider with [6 months']. If the Customer is a financial entity, the termination rights of the DORA addendum also apply.

11.3 On termination the exit plan applies: the Customer may export all data, and the Provider erases it within the agreed periods. Any unused prepaid balance [is refunded / is not refunded], except on termination for the Provider's breach.

12. Changes

The Provider may change these terms with [30 days'] notice by email. Changes required by law or by authorities may take effect earlier. A Customer that does not accept them may terminate before they take effect.

13. Governing law and jurisdiction

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