DORA Addendum to the KYCJet Service Agreement

Contractual provisions pursuant to Article 30 of Regulation (EU) 2022/2554 (DORA) and Commission Delegated Regulation (EU) 2025/532 on subcontracting. Version of 21 September 2026.

Between [Customer's company name] (the **"Financial Entity"**) **and** GREM S.R.L., Via Matteo La Fragola 4, 84135 Salerno (SA), Italy, VAT no. IT06136730659 (the **"Provider"**).

Recital

The Financial Entity is subject to Regulation (EU) 2022/2554. The Provider is an ICT third-party service provider. This addendum supplements the KYCJet service agreement (the **"Agreement"**) with the provisions required by Article 30 DORA and prevails over it in case of conflict.

The Parties acknowledge that the Service supports the customer due diligence function, which the Financial Entity [has / has not] classified as critical or important. Clauses 9 to 14 apply if it has, and the Financial Entity notifies the Provider of this in writing.

Provisions for all ICT services (Article 30(2))

1. Description of the Service (Article 30(2)(a))

The Provider makes available, as software as a service:

- creation of verification cases and their single-use links, from the dashboard and through an application programming interface;
- capture of the document photograph and its automated reading;
- reading and cryptographic verification of the chip of electronic documents (issuing State's signature, anti-cloning proof);
- the face liveness check and comparison with the document;
- screening against sanctions, politically exposed persons and criminal proceedings lists;
- the decision on cases not approved by the automatic approval rule, if the Financial Entity has switched it on, according to the plan stated in the Agreement: on the Standard plan, the tools with which the Financial Entity decides them from the dashboard; on the Institutional plan, review and decision by a Provider operator;
- notification of outcomes to the Financial Entity's systems;
- export of records, retention and erasure according to the Financial Entity's instructions.

The Service does not include customer risk assessment, the decision to enter into a business relationship, or the attestation under Article 27 of Legislative Decree 231/2007, which remain with the Financial Entity on either plan. The Provider may subcontract the parts listed in the *Sub-processors* document, under the conditions of clause 15.

2. Locations of service provision and data processing (Article 30(2)(b))

What	Country
Application and database	Germany (Hetzner Online GmbH)
Photographs, document reading, face comparison, liveness check	Ireland (Amazon Web Services, eu-west-1 region)
List screening	Switzerland (Dilisense)
Provider staff	Italy

The Provider gives written notice of any change to these locations at least [30 days] in advance. The Financial Entity may object and, if the Parties cannot find a solution, terminate under clause 7.

3. Availability, authenticity, integrity and confidentiality of data (Article 30(2)(c))

The Provider protects data with the measures in Annex B of the *Data Processing Agreement*, which forms part of this addendum, including for non-personal data.

4. Access, recovery and return of data (Article 30(2)(d))

At any time, and in the event of the Provider's insolvency, resolution or discontinuation of business, or of termination of the Agreement, the Financial Entity may:

- export from the dashboard all cases of a mode into an archive containing a CSV file and a JSON Lines file;
- export the record of a single case, with the document copies still retained, including through the application programming interface.

Methods and timing are set out in the *Exit Plan*.

5. Service levels (Article 30(2)(e))

Service levels are those in the *Service Level Agreement*, including updates agreed in writing.

6. Assistance in case of ICT incidents (Article 30(2)(f))

When an ICT incident related to the Service occurs, the Provider assists the Financial Entity **at no additional cost**, following the *Incident Management Procedure*: in particular it provides the information needed to classify the incident and, where major, to report it to the authority within the time limits of Article 19 DORA.

7. Cooperation with authorities and termination (Article 30(2)(g) and (h))

7.1 The Provider fully cooperates with the Financial Entity's competent and resolution authorities, including persons appointed by them.

7.2 The Financial Entity may terminate the Agreement, with [30 days'] notice and without penalty, in the cases set out in Article 28(7) DORA: significant breach by the Provider of applicable laws, regulations or contractual terms; circumstances identified through monitoring that may alter the performance of the functions provided, including material changes affecting the arrangement or the Provider's situation; the Provider's evidenced weaknesses in its overall ICT risk management, in particular in the security and integrity of data; the competent authority's inability to effectively supervise the Financial Entity as a result of the conditions of the Agreement. The ordinary termination right under the Agreement is unaffected.

8. Training and awareness (Article 30(2)(i))

Provider staff working on the Service take part, at the Financial Entity's request and on agreed terms, in the Financial Entity's ICT security awareness programmes and digital operational resilience training (Article 13(6) DORA).

Additional provisions for critical or important functions (Article 30(3))

9. Measurable service levels (Article 30(3)(a))

The *Service Level Agreement* sets precise quantitative and qualitative performance targets, measurement methods and remedies, so that the Financial Entity can monitor the Service and take corrective action without undue delay when they are not met.

10. Notice periods and reporting obligations (Article 30(3)(b))

The Provider notifies the Financial Entity in writing and without delay of:

- any development that may materially affect its ability to provide the Service at the agreed service levels;
- any change of sub-processors or processing locations, with [30 days'] notice;
- any change of control of the Provider.

11. Business contingency and security (Article 30(3)(c))

The Provider maintains and tests, at least [once a year], a business contingency plan for the Service, including backup and restore, and shares the results with the Financial Entity on request. It maintains the security measures of clause 3.

12. Threat-led penetration testing (Article 30(3)(d))

The Provider participates and fully cooperates in the Financial Entity's threat-led penetration testing (TLPT) under Articles 26 and 27 DORA, on agreed terms that do not compromise the security of other customers.

13. Access, inspection and audit (Article 30(3)(e))

The Financial Entity, a third party appointed by it and the competent authority have unrestricted rights of access, inspection and audit of the Provider in relation to the Service, including the right to take copies of relevant documentation. The Provider fully cooperates. Except in urgent cases or at the authority's request, audits by the Financial Entity are announced with [30 days'] notice and conducted in a way that protects the confidentiality and security of other customers; the Provider may propose certifications or pooled audits instead, which the Financial Entity is free to decline.

14. Exit strategy (Article 30(3)(f))

On termination for any reason, the Provider guarantees a transition period of [6 months], during which it continues to provide the Service on the terms in force and assists the Financial Entity in moving to another provider or insourcing, following the *Exit Plan*.

Subcontracting of critical or important functions

15. The Provider subcontracts parts of the Service only to the entities in the *Sub-processors* document. For each, it assesses the risks in advance, imposes by contract obligations equivalent to this addendum (including the audit rights of the Financial Entity and the authority and continuity obligations), monitors their performance, and remains responsible for the Service as a whole. Any material change of subcontracting is notified with [30 days'] notice; the Financial Entity may object and, if the change exceeds the risks it accepts, terminate under clause 7.

[Place, date]

The Financial Entity _____ The Provider _____