Note on Regulation (EU) 2024/1689 (AI Act)

How the artificial intelligence systems used by KYCJet are classified. Version of 21 September 2026.

1. Which AI systems the Service uses

System	Provider	What it does	Who decides
Liveness check (Face Liveness)	Amazon Web Services	Estimates whether a real person is in front of the camera	A person who sees the score: the customer's team on the Standard plan, a Provider operator on the Institutional plan; or, if the customer has switched it on, the automatic approval rule (section 3)
Face comparison (CompareFaces)	Amazon Web Services	Measures how closely the captured face resembles the one on the document or chip	A person who sees the score and the images: the customer's team on the Standard plan, a Provider operator on the Institutional plan; or, if the customer has switched it on, the automatic approval rule (section 3)
Document reading (Textract)	Amazon Web Services	Extracts text from the photograph	Fields are validated with check digits; on the Institutional plan a Provider operator can correct them, on the Standard plan the customer can ask for the verification to be redone

The Service uses no language or generative models.

2. It is not a high-risk system

Annex III, point 1(a), classifies remote biometric **identification** systems as high-risk, but expressly excludes "AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be".

KYCJet does exactly that: a one-to-one comparison between the face of the person presenting themselves and the face on the document they present. It does not search for the person in a database of faces, does not categorise them by sensitive characteristics and does not recognise emotions. Nor does it fall within the prohibited practices of Article 5.

Text reading falls within no category of Annex III.

3. The obligations that remain

- **AI literacy (Article 4)**: the Provider's staff who review cases on the Institutional plan are trained to interpret the systems' scores, to know their limits and not to decide by automatism. The customer does the same for its own staff who use the outcomes and, on the Standard plan, decide cases.
- **Transparency towards the person**: not an Article 50 obligation, which covers other cases, but the controller's notice nevertheless explains that face and document are examined with automated tools, and

the verification page states whether the verification may conclude without review by a person.

- **Human oversight**: not required by law for these systems, it is applied by design. No case is declined by the machine, and every case that is not green on every check is decided by a person: the customer's team on the Standard plan, a Provider operator on the Institutional plan. On either plan the customer may switch on automatic approval of only those cases green on every check: chip data signed by the State, anti-cloning proof, document not expired, liveness check and face similarity not below the dedicated thresholds it chooses (from 90 to 100), screening with no matches. Under Article 22 GDPR the basis is necessity for the contract (Article 22(2)(a)), with the safeguards of Article 22(3) — information to the person and human intervention on request — resting with the controller, which provides the new review with its own staff on the Standard plan and which the Provider assists with a review by an operator on the Institutional plan.

4. The role of GREM S.R.L.

GREM S.R.L. is a **deployer** of the AWS systems within its Service, and the provider of a service that integrates them. It does not modify the models or train them with verification data.

5. When to revisit this note

Revisited on 21 September 2026 for optional automatic approval: the classification does not change, because it remains a one-to-one verification of the claimed identity, and the rule approves only with State-signed data, only at or above thresholds chosen by the customer, and never refuses. Revisited on the same day for the plans: human oversight is exercised by the customer's team on the Standard plan and by a Provider operator on the Institutional plan; the classification does not change.

If the Service introduced one-to-many comparison, any use of faces other than verifying the claimed identity, automatic approval without chip reading, or a model classifying photographs of documents, this classification must be redone before activating it.