

Data Processing Agreement (template)

Version 1.0 · September 2026 · Template for a Marqib pilot or licence. It is drafted to be compatible with UAE PDPL (Federal Decree-Law 45/2021), DIFC Data Protection Law 2020, ADGM Data Protection Regulations 2021, Türkiye KVKK (Law 6698) and EU GDPR Art. 28. **Not legal advice: have counsel review before signature.** Square brackets are to be completed.

Parties.

- **Controller:** [Customer legal name], [registered address], [licence number] (the "Customer").
- **Processor:** Nordera Works Teknoloji ve Danışmanlık A.Ş., [registered address], İstanbul, Türkiye ("Marqib").

1. Subject matter and duration

Marqib processes personal data only to provide the services in the [Pilot Agreement / Licence] dated [date]. This DPA runs for the term of that agreement and until all personal data has been returned or deleted.

2. Nature and purpose

Trade surveillance and transaction monitoring on the Customer's end-of-day data. This covers:

- preparing case files;
- drafting suspicious transaction reports for the Customer's review;
- keeping an audit trail.

Marqib makes no decisions about data subjects and files nothing with any authority.

3. Data subjects and categories

- **Data subjects:** the Customer's clients, their beneficial owners and counterparties, and the Customer's reviewers (as users).
- **Categories:**
 - identifiers (internal ids, names);
 - account and payment references;
 - transaction and trading records;
 - device ids and IP addresses;
 - country;
 - occupation and expected turnover;
 - user names and actions.
- **Special-category data:** none. Customer data is limited to what the Customer exports. Criminal-offence data may arise only in the form of the Customer's own suspicion assessments.

4. Processor obligations

Marqib will: (a) process only on the Customer's documented instructions, including this DPA; (b) ensure everyone authorised to process the data is bound by confidentiality; (c) implement the measures in Annex 1; (d) engage sub-processors only as set out in clause 5; (e) assist the Customer, taking into account the nature of the processing, with data-subject requests, security, breach notification, impact assessments and prior consultation; (f) at the Customer's choice, delete or return all personal data at the end of the services and certify deletion in writing, unless law requires storage; (g) make available the information needed to demonstrate compliance and allow audits by the Customer or its regulator on reasonable notice; (h) inform the Customer if an instruction appears to infringe applicable law; (i) not use Customer data to train or improve any model.

5. Sub-processors

The Customer authorises the sub-processors listed in Annex 2. Marqib gives at least 30 days' written notice of any addition or replacement. The Customer may object on reasonable grounds; if the parties cannot resolve the objection, the Customer may terminate the affected service without penalty. Marqib imposes data-protection obligations on each sub-processor that are no less protective than this DPA, and remains liable for their performance. **In a firm-hosted installation Marqib engages no sub-processors for Customer data.**

6. International transfers

Customer data is stored in the region the Customer selects ([region]). Any transfer outside that jurisdiction takes place only with the Customer's prior written approval and under a transfer mechanism recognised by the applicable law. Examples:

- adequacy;
- standard contractual clauses;
- KVKK Art. 9 undertakings;
- DIFC/ADGM-approved clauses.

7. Personal-data breach

Marqib notifies the Customer without undue delay, and in any case within [48] hours of becoming aware of a breach affecting Customer data. The notice gives the nature of the breach, the categories and approximate volume, likely consequences and measures taken. The Customer is responsible for any notification to authorities and data subjects.

8. Confidentiality of regulatory matters

Marqib treats case files, suspicion assessments and draft reports as confidential. It will not disclose the existence or content of any suspicion to any person except the Customer, or as required by law. This protects the Customer's tipping-off obligations.

9. Liability and precedence

Liability is governed by the main agreement. If this DPA conflicts with the main agreement on data protection, this DPA prevails.

10. Governing law

[To match the main agreement, e.g. laws of the DIFC / ADGM / UAE / Türkiye.]

Signed for the Customer: __ Name / title / date Signed for Nordera Works Teknoloji ve Danışmanlık A.Ş.: __ Authorised signatory / date

Annex 1 — Technical and organisational measures

- **Deployment:** firm-hosted in the Customer's environment, or a dedicated single-tenant instance in the Customer's region.
- **Encryption:** TLS 1.2+ in transit; AES-256 at rest (provider-managed, or the Customer's own).
- **Access:**
 - named users with roles and server-side maker-checker;
 - rate-limited sign-in;
 - signed sessions that expire after 12 h;
 - CSRF protection;
 - Marqib staff access only for supervised support, logged.
- **Integrity:** an append-only, hash-chained audit log written in the same transaction as each change; SHA-256 on every evidence pack.
- **Minimisation:** only the fields needed for the rules; no identity documents.
- **Model use (optional):** direct identifiers are tokenised before any call; evidence-cited output; endpoint chosen by the Customer; no training.
- **Deletion:** hosted pilot data is deleted at the end of the term, with written certificate.
- **Vulnerability handling:** security.txt; acknowledgement within 2 business days.

Annex 2 — Authorised sub-processors (hosted pilot only)

Vercel Inc. (hosting) · Neon Inc. (database) · Resend (transactional e-mail, user sign-in only) · model endpoint selected by the Customer, if drafting is enabled: [provider / region].