OR PROCUREMENT · DDQ / RFP RESPONSE KIT

Ezelman — pre-filled DDQ / RFP pack

ndependence · conflicts of interest · PI cover · DORA third-party governance · GDPR · information security · business continuity · subcontractors · financial crime · ESG · commercial terms. Answered once, on the page, the same way every time.

AT A GLANCE

LEGAL ENTITY

Ezelman SAS

France · SIRET / VAT / Kbis on request

FOUNDED

2020

Paris · founder-owned

FOUNDER & MANAGING PARTNER

Hannan Mohammad

~20 years in European G-SIB / Big-4 risk

PRACTICE FOCUS

CRR3 · ECB OSI · stress testing · Pillar 2 defence

PROFESSIONAL INDEMNITY

Tier-1 European carrier

€5m / claim · €10m aggregate

DORA STATUS

Not an ICT TPP

EBA outsourcing framework accepted

AUDIT & ACCESS RIGHTS

Accepted

Client · statutory auditor · competent supervisor

audit&ac-cess-rights@ezelman.com · +33 · Paris, France

RESPONSE SLA

5 business days

Bespoke DDQ / RFP completion, no charge

Version 2026-04-21

Contents

Use of this pack. This pack answers the standard questions a European G-SIB procurement team will send a specialist advisory supplier at onboarding. Items marked *"on request"* are provided after counter-signature of the mutual NDA. Nothing in this document modifies the terms of an executed statement of work — those remain governing.

SECTION 01

Firm & legal identity

1.1 Legal form of the supplying entity

Ezelman SAS, a French *société par actions simplifiée*, registered in France. Trading name: **Ezelman**. Registered office in Paris. SIRET, VAT (TVA intracommunautaire) and Kbis extract on request with the counter-signed NDA. The firm is founder-owned with no outside investors.

1.2 Parent, subsidiaries or affiliated entities

None. Standalone entity. **No group structure**, no parent, no subsidiaries, no affiliated advisory entities. Simplifies third-party risk assessment relative to supplying from a multi-entity consulting group.

1.3 Ultimate beneficial ownership (UBO)

Hannan Mohammad, founder, is the sole UBO with >25% ownership. Registry-level UBO attestation on request. No PEP status; no sanctions-list exposure; KYC pack on counter-signed NDA.

1.4 Year founded and years of continuous operation

Founded in **2020**. Continuous operation since incorporation. Founder tenure in the regulatory-risk field precedes incorporation by approximately two decades, primarily inside European G-SIBs and a Big-4 regulatory risk practice.

1.5 Geographies of legal operation

France (primary). Mandates executed across the EU (FR, DE, IT, NL, ES, LU), UK, GCC (UAE, KSA, Qatar) and US. No activity in sanctioned jurisdictions.

SECTION 02

Independence & conflicts of interest

2.1 Auditor independence

Not an audit firm. No statutory-audit or assurance relationship with any client; entirely outside the EU Audit Regulation perimeter. Where a bank's statutory auditor has a non-audit-service conflict with consulting work, that conflict is structurally absent at Ezelman.

2.2 Conflicts policy & register

Written COI policy on every mandate. Live register records client entity, scope, named supervisor counterparties and any regulatory-counterparty conflict. Three-step screen before a new mandate:

- **Client-level** — active or recent work for a direct competitor in the same supervisory ring-fence.
- **Supervisor-level** — overlap with a JST or NCA team where one engagement could compromise another.
- **Personal** — founder's regulatory contacts, former employers (cooling-off), former direct reports.

Policy included in this pack.

2.3 Regulatory cooling-off

Self-imposed **12-month cooling-off** from any former employer before any supervisor-facing mandate involving that employer's direct supervisory dialogue. Current window historical; policy remains in force for future partners.

2.4 Gifts, entertainment, anti-bribery

Zero-value threshold on gifts from regulated-entity clients in the 12 months either side of a live mandate. Entertainment logged. Anti-bribery policy consistent with the **French Sapin II law** and UK Bribery Act 2010 standard. No facilitation payments; no political contributions in the firm's name.

2.5 Independence from software vendors

We do not resell software. No commission, referral fee or revenue share from any technology provider discussed in a client deliverable. Vendor-selection work is fixed-fee with vendor-agnostic output expressly warranted.

SECTION 03

Insurance & financial standing

3.1 Professional indemnity & civil liability

PI placed with a tier-one European insurer. Standard limits: **€5m per claim · €10m aggregate** per policy year. Higher per-mandate limits available and placed on request. Annual certificate issued directly by the broker to procurement / TPRM within two business days of request.

3.2 Public & general liability

General liability (public, employer's, damage-to-premises) bundled in a standard French commercial package. Certificate on request.

3.3 Cyber liability

Standalone cyber-liability cover, first-party and third-party components (breach response, notification, BI, regulatory defence). Limits disclosed on counter-signed NDA.

3.4 Financial standing

Profitable, positive net equity, zero financial debt. French-GAAP statutory accounts available under NDA. No dependence on a bank line or invoice-discounting facility.

3.5 Revenue concentration

Operating policy: **no single client > 40% of trailing-twelve-month revenue**. Current concentration well inside the ceiling. Internal, not statutory; disclosed because TPRM teams ask.

SECTION 04

Regulatory & DORA outsourcing framework

4.1 DORA ICT third-party status

Services are **not ICT services** within Article 3(21) of Regulation (EU) 2022/2554 (DORA). Advisory professional services only — no ICT assets, ICT-related services or software provided to the in-scope entity. Where advisory work touches ICT concentration risk, we adopt ICT-service contractual clauses by analogy to simplify the bank's register.

4.2 EBA Guidelines on outsourcing (EBA/GL/2019/02)

Standard EBA framework accepted: activity description, SLAs, audit & access, sub-outsourcing notification, data protection, BCM, termination, supervisory access. On "critical-or-important" engagements we accept the tag, the governance obligations and the register entry.

4.3 Audit rights

Full audit & access rights for internal audit, the statutory auditor and the competent supervisor (ECB / NCA / ACPR, etc.): on-site access to working papers, IS walk-throughs, interviews with named mandate personnel. Rights survive termination for the applicable retention period.

4.4 Sub-outsourcing / chaining

No sub-outsourcing without prior written client consent (see s.08). Flow-down EBA/DORA clauses on any delivery partner consolidated under Ezelman; partner named in the client's outsourcing register.

4.5 Data residency

Default **EU-only**. Primary processing in France, DR in another EU member state. No export to non-adequate third countries. GCC/US mandates: in-region processing set up on a mandate basis with documented transfer mechanisms.

SECTION 05

Data protection · GDPR

5.1 Controller / processor classification

For client-instructed processing (typically limited — HR datasets, credit-file sampling), Ezelman acts as **processor** under GDPR Art. 28. Standard DPA executed on every mandate involving personal data.

5.2 Minimisation

De-identified samples wherever the analytical purpose permits. Client teams de-identify before transfer. Personal data requested only where regulatory purpose requires (e.g., credit-file review on an IRB inspection).

5.3 International transfers

EU-default. GCC/US dimensions supported by EU–US Data Privacy Framework (where applicable), SCCs or the equivalent GCC local-law mechanism. DPIA contribution on request.

5.4 Retention

Working papers: retained for the supervisor's access right (typically **10 years** from engagement close for ECB-relevant mandates; longer where an active supervisory dialogue is open). Personal data minimised before filing.

5.5 Data breach notification

Material incident affecting client data: **notification within 24h** to the client's Third-Party Risk contact; formal report within 5 business days. Incident playbook included.

SECTION 06

Information & cyber security

6.1 Security control baseline

ISO/IEC 27001-aligned control baseline calibrated for a specialist boutique. Certification not held today; the certification decision is revisited in the 2027 roadmap. Independent penetration testing annually; findings closed before the next cycle.

6.2 Endpoint & device management

Managed fleet · full-disk encryption · MDM · no BYOD for client data · phishing-resistant MFA on every client-data system.

6.3 Client data segregation

Per-mandate data-room · least-privilege access · no cross-mandate reuse · immutable audit log for the full retention period.

6.4 Third-party tooling

Restricted, disclosed list of business applications. Each inventoried, risk-rated, due-diligenced. List available under NDA.

6.5 Incident response SLAs

Detection to client notification: **≤ 24h** for material incidents; ≤ 72h for contained incidents without client data exposure; written RCA within 10 business days of containment.

SECTION 07

Business continuity & key-person risk

7.1 Business continuity plan

Documented BCP covering founder unavailability, office unavailability, systems unavailability and extended force-majeure. Tested annually against a stated scenario (current: protracted founder unavailability for four consecutive weeks). BCP log under NDA.

7.2 Key-person risk — the honest answer

Ezelman is founder-owned. The firm is **structurally concentrated on one partner today**, with a roadmap to a second partner by end-2027 (see *stance*). Mitigants in place:

- **Continuity clause** in every mandate >12 weeks — partner named, minimum-hour commitment, unavailability escalation path.
- **Named external senior backstop** from a vetted senior-only network — pre-briefed, under NDA, named in the term sheet.
- **Mandate-level working-paper file** such that the backstop can pick up a supervisor-facing memo within five business days.
- **Published roster cap** — committed vs available founder capacity disclosed; new mandates declined below minimum time-per-mandate.
- **No sub-mandate chaining** — the question “is the partner actually working on our file this week?” has an auditable answer.

If a procurement team considers this mitigant set insufficient relative to mandate materiality, the correct conclusion is structural mismatch and a different supplier should be selected. We would rather lose a bid than hide this.

7.3 IT resilience · recovery

RTO/RPO for client working papers: **RTO 4h / RPO 1h**. Backups in a second EU member state. Restore-from-backup drill on a documented cadence; last-test date disclosed on request.

SECTION 08

Subcontractors & delivery partners

8.1 Subcontracting policy

Default: **no subcontracting**. Where specialist capacity is needed, a named delivery partner is proposed *before* the statement of work is signed, and contracted directly to the client where possible, or under Ezelman with flow-down EBA/DORA clauses.

8.2 Delivery-partner network

Small, vetted **senior-only delivery-partner network** supplements Ezelman on specific workstreams (FRTB quantitative modelling, GCC Arabic-language documentation, US Basel III Endgame, IFRS 9 model-risk review). Each partner is an independent senior practitioner or a specialist boutique, pre-vetted and contracted on a mandate basis.

8.3 Flow-down of obligations

Every contracted partner executes a mirror NDA, mirror conflicts warrant, and applicable data-protection / security obligations. Identity disclosed to the client before engagement; no silent subcontracting.

SECTION 09

Financial crime, AML & sanctions

9.1 AML / CFT policy

Written policy calibrated for a professional-services firm and consistent with the French AML regime applicable to consulting activity. KYC on the contracting entity at onboarding; PEP & sanctions screening on beneficial owners of both Ezelman and its clients.

9.2 Sanctions screening

EU, UK, US OFAC and UN sanctions lists screened at onboarding, re-screened on annual KYC refresh. No mandates from sanctioned entities or comprehensive-sanctions jurisdictions. We do not advise on **sanctions evasion** — explicit engagement-letter exclusion.

9.3 Anti-bribery / anti-corruption

Compliant with French Sapin II. UK Bribery Act 2010 standard for UK-facing mandates; US FCPA-equivalent discipline for US-facing mandates. Annual refresher training; hospitality log; facilitation payments forbidden.

SECTION 10

ESG, diversity & conduct

10.1 Environmental

Scope-1/2 footprint reported at a boutique scale (largely travel). Hybrid delivery default where supervisor-facing defensibility is preserved. Carbon reporting on request, with the caveat that a firm of this size does not publish an annual sustainability report.

10.2 Social & diversity

Senior-only hiring means a very small N; meaningful statistics cannot be reported. Published hiring policy (see *careers*): no hiring below Director level, reference-driven evaluation, pay range disclosed up-front to every candidate.

10.3 Modern slavery / human rights

Low-risk supply chain (professional services, office, IT). Standard statement on request. Annual review of delivery-partner network for human-rights compliance under the French *loi de vigilance*, voluntarily where below threshold.

10.4 Code of conduct · whistleblowing

Written code of conduct for founder, any future partner and delivery-partner personnel in the firm’s name. External whistleblowing channel via an independent law firm (named on request) for clients and employees alike.

SECTION 11

Commercial terms & rate card

11.1 Engagement model

Default: **fixed-fee per statement of work**, scoped to a named supervisor-facing deliverable. Time-and-materials available for open-ended advisory; not preferred. Hybrid fixed-fee + capped T&M common on CRR3 programmes.

11.2 Typical mandate size

Single workstream: **€250k–€600k**. Multi-workstream / multi-quarter: **€600k–€1.5m**. Larger aggregates built as a sequence of scoped SoWs, not as open-ended frameworks.

11.3 Rate card

Founder / senior-partner day-rate disclosed in writing at proposal stage. **No hidden rate card**, no junior-substitution mechanism: the rate quoted is the rate delivered. No multi-tier pyramid hidden behind a blended rate.

11.4 Payment terms

30 days from invoice, monthly on milestone completion. EUR default; USD / AED available for US / GCC with FX locked at contract date.

11.5 Referral policy

A **5% mandate referral fee** to introducers on signed SoW. Disclosed to the client at proposal stage. Refused where the introducer is an employee of the client.

11.6 Walk-away / refund clause

Contractual **walk-away / refund clause**: if the seniority promised at proposal stage is not delivered during the mandate, the corresponding fee is refunded. Unusual and published on purpose. Details on the *about* and *stance* pages.

SECTION 12

Escalation, complaints & contacts

12.1 Primary procurement contact

procurement@ezelman.com — same-day response in EU business hours, next-day in GCC business hours. Direct founder line: **hmohammad@ezelman.com**.

12.2 Complaints escalation path

Level 1: founder in writing. Level 2: independent counsel of record (named on request). Level 3: external mediation via a Paris-based commercial mediation body where the client consents. No formal complaint has been escalated past Level 1; if that changes we will disclose it on request.

12.3 Litigation & regulatory action history

None. No open, pending or historical litigation as at the last review date. No regulatory action, no settlement, no client-initiated arbitration. Annual attestation refreshed on the DDQ cycle.

12.4 Bespoke questionnaires

Bank-proprietary DDQ / RFP templates completed within **5 business days** at no charge. Send to **procurement@ezelman.com** with a named TPRM point-of-contact on the bank side.

Firm-level attestation. The answers in this pack accurately describe Ezelman's policies and practice as at the version date on the cover. Any material change is reflected in the next published version of this document and, where relevant, in the equivalent page on ezelman.com/procurement.

SIGNATORY

Hannan Mohammad

CAPACITY

Founder & Managing Partner, Ezelman

DATE

2026-04-21

DOCUMENT ID

EZM-PROC-PACK-2026Q2

Sitewide figures policy: every number on ezelman.com is either (i) a public-source citation — bank Pillar 3 disclosures, ECB/SSM publications, EBA Basel III monitoring, ESRB or BCBS impact studies; (ii) an estimate with stated methodology derived from those sources; or (iii) an anonymised mandate outcome (specific client figures withheld). Items in this pack describe firm-level policies and are firm-level statements, not public-data figures.