Data Protection Policy

Policy year 2026-27 · Effective 1 April 2026 to 31 March 2027 · Version 1.0 · Approved by the Management Board

Contents

1. 1. Purpose

Our clients trust us with sensitive personal information - identity documents, financial details, contact data. This policy sets out how InterAtlas Estate collects, uses, protects and deletes personal data, consistent with the GDPR and equivalent laws in our markets.

2. 2. Principles

- Lawfulness and transparency: we collect data only for stated, legitimate purposes and explain those purposes at the point of collection.
- Minimisation: we collect only what we need - nothing more.
- Accuracy: clients can review and correct their profile data in the investor portal at any time.
- Storage limitation: data is retained only as long as needed for the purpose or as law requires (e.g. AML records five years), then securely deleted.
- Security: personal data and identity documents are encrypted at rest (AES-256); access is restricted to vetted staff on a need-to-know basis; all access is logged.

- No selling: we never sell personal data, and we share it only with processors under contract or where law requires.

3. 3. Data subject rights

Clients may request access, correction, deletion, restriction or portability of their personal data, and may object to processing, by writing to privacy@atlasestate.estate. We respond within one month.

4. 4. Breach response

Suspected personal-data breaches are escalated immediately, contained, assessed, and - where risk to individuals exists - notified to the supervisory authority within 72 hours and to affected individuals without undue delay.

5. What we process, why, and for how long

- Account data (name, email, phone): contract performance; retained while the account is active plus 24 months.
- KYC identity documents and face captures: legal obligation (AML); encrypted at rest; retained 5 years after the relationship ends, then securely destroyed.
- Transaction records: legal obligation and contract; retained 6 years minimum.
- Marketing preferences: consent; until withdrawn - every message includes an opt-out.
- Technical logs: legitimate interest (security); retained 12 months.

6. Data subject rights - how we handle requests

- Requests to privacy@atlasestate.estate are logged on receipt and identity-verified before disclosure.
- Response within one month; extendable by two months for complex requests, with the requester informed of the reason.
- Erasure requests are honoured except where retention is legally required (e.g. AML records) - in which case we explain exactly what is kept and why.

7. Breach response timeline

- Hour 0: contain and assess; incident logged.
- Within 24 hours: severity classification and Management Board notification for material breaches.
- Within 72 hours: notification to the supervisory authority where a risk to individuals exists.
- Without undue delay: notification to affected individuals where the risk is high, with concrete guidance on protective steps.

8. Governance and oversight

We operate three lines of defence. The first line is the business itself: every employee and manager owns the risks of their own activity and applies this policy in daily decisions. The second line is the compliance function, which designs the controls, advises the business, monitors adherence and reports independently. The third line is independent review - periodic

internal audit work and, where engaged, external examination - which tests that the first two lines actually work. The Management Board sits above all three: it approves this policy, receives quarterly reporting on incidents, exceptions and control performance, and is escalated to within 24 hours for material events.

9. Risk assessment

Risk in this domain is assessed formally at least annually, and whenever our products, markets or the external environment change materially. Each identified risk is scored for likelihood and impact, assigned an owner and a mitigation with a deadline, and entered in the risk register reviewed quarterly by the Management Board. The factors below weigh most heavily in this policy's domain:

- KYC records concentrate highly sensitive identity documents and biometric-style face captures.
- Cross-border processing across six markets engages divergent local privacy laws.
- Third-party processors (email, hosting, payments) extend the attack and compliance surface.
- Marketing databases risk consent drift as contacts age.
- Insider access is the dominant realistic threat to encrypted stores.

10. Procedures and controls

The operating procedures below are mandatory. Deviation requires prior written approval from the compliance function, recorded in the exceptions log with rationale and expiry.

- A record of processing activities maps every data category to purpose, lawful basis, storage location, processor and retention.
- KYC documents and face captures are encrypted at rest (AES-256) and decrypted only for authorised compliance review; every access is logged.
- Data subject requests are logged on receipt, identity-verified, and answered within one month; extensions are communicated with reasons.
- New processors pass a due-diligence check and sign processing terms before receiving any personal data; international transfers rely on recognised safeguards.
- A DPIA is performed before any new high-risk processing (new biometric-style capture, profiling, large-scale monitoring).
- Breach playbook: contain and log at hour 0; classify within 24 hours; notify the supervisory authority within 72 hours where risk exists; notify affected individuals without undue delay where risk is high.
- Marketing lists honour opt-outs immediately; consent records are retained as evidence.
- Annual access-rights recertification removes dormant permissions.

11. Application across our markets

Application across our markets: GDPR is our baseline everywhere; where local law (UAE, Turkey) adds requirements, the stricter rule applies. Locale-specific privacy notices are maintained in all six site languages.

12. Applying this policy: worked examples

The examples below illustrate how the requirements of this policy operate in practice. They are

illustrative, not exhaustive; where a real situation is not covered, the escalation duty applies.

- Situation: an investor emails asking for a copy of all data we hold on them. Response: request logged, identity verified, full response within one month.
- Situation: marketing proposes emailing a contact list collected in 2023. Response: consent records are checked first; contacts without valid consent are excluded.
- Situation: a device with admin panel access is lost. Response: hour-0 containment - sessions revoked, credentials rotated, incident classified within 24 hours, notification assessed against the 72-hour rule.
- Situation: a processor proposes moving storage to a new region. Response: transfer safeguards are re-verified and documented before approval.

13. Definitions

- Personal data — any information relating to an identified or identifiable natural person.
- Special category data — data revealing racial or ethnic origin, political opinions, religious beliefs, health, or biometric data used for identification.
- Processing — any operation performed on personal data: collection, storage, use, disclosure, erasure.
- Data subject — the individual to whom personal data relates.
- Personal data breach — a breach of security leading to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data.

14. Roles and responsibilities

- Management Board — owns this policy, approves it annually, sets the risk appetite and receives escalation of material issues within 24 hours of identification.
- Compliance function — maintains this policy, delivers training, performs monitoring, investigates concerns and reports quarterly to the Board on incidents, exceptions and control performance.
- Line managers — embed the policy in day-to-day operations, ensure their teams have completed training, and act as the first escalation point.
- All employees and associated persons — read and follow this policy, complete required training on joining and annually thereafter, and escalate concerns promptly rather than act on doubt.

15. Training and communication

Everyone in scope receives training on this policy at induction and at least annually, with targeted refreshers whenever the policy or the law changes materially. Completion is recorded. The current version of this policy is available to all staff and is published on the Governance page of atlasestate.estate; material changes are communicated directly.

- Induction: policy walkthrough within the first 10 working days, before unsupervised client contact.
- Annual refresher: scenario-based session covering the red flags and escalation routes in this document.
- Role-specific modules: deeper training for the functions most exposed to this policy's risks.

- Attestation: annual written confirmation of having read and understood the current version.

16. Records and retention

Records evidencing compliance with this policy - approvals, screenings, registers, training logs, investigation files - are kept accurately, stored securely with access restricted to those who need them, and retained for at least six years (or longer where law requires), after which they are securely destroyed.

17. Monitoring, audit and review

Compliance monitors adherence to this policy through periodic sample testing, exception reporting and review of escalations. Findings, together with any breaches and remediation actions, are reported to the Management Board quarterly. This policy is reviewed at least annually, and additionally whenever our operations, the law or regulatory guidance change materially.

- Quarterly: sample testing of controls and registers; exception-log review; Board reporting pack.
- Annually: full policy review against legal developments and incident learnings; training completion audit.
- Ad hoc: thematic reviews triggered by incidents, near misses or external findings.

18. Breaches and consequences

A breach of this policy is a serious matter. Confirmed breaches by employees are handled under our disciplinary process and may result in sanctions up to dismissal; breaches by suppliers, introducers or other associated persons may result in contract termination. Where conduct may amount to a criminal offence, we will cooperate fully with the competent authorities. Honest mistakes that are self-reported promptly are treated as learning opportunities, not misconduct - concealment, not error, is the aggravating factor.

19. Regulatory context and related documents

We design our controls by reference to internationally recognised frameworks and the local law of each market in which we operate. The frameworks most relevant to this policy include:

- EU General Data Protection Regulation (GDPR)
- UAE and Turkish data-protection statutes for local processing
- ePrivacy rules on electronic marketing
- Supervisory-authority guidance in each EU market

This policy forms part of the InterAtlas Estate governance framework and should be read together with the other policies published at atlasestate.estate/en/governance, including the Code of Conduct, the Whistleblowing Policy and the Data Protection Policy.

20. Version control

- Version 1.0 - 1 April 2026 - Initial adoption for policy year 2026-27 - Approved by the Management Board.
- Next scheduled review: March 2027 (or earlier upon material change in law or operations).
- Policy owner: Compliance function, compliance@atlasestate.estate.

Annex A - Contacts and escalation routes

- Compliance function: compliance@atlasestate.estate - policy questions, approvals, escalations and suspicion reports; acknowledgement within 1 business day.
- Whistleblowing routes: any route in the Whistleblowing Policy, including anonymous reporting; acknowledgement within 3 business days.
- Urgent matters (suspected live fraud, sanctions hit, data breach): escalate immediately by the fastest available channel, then confirm in writing the same day.
- External: nothing in this policy prevents any person from reporting directly to a competent authority at any time.