Policy on Preventing the Facilitation of Tax Evasion

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

Contents

1. 1. Purpose

It is a criminal offence in many jurisdictions for a business to fail to prevent persons associated with it from criminally facilitating tax evasion. InterAtlas Estate prohibits any such facilitation, anywhere, by anyone acting for it.

2. 2. Scope

This policy applies to InterAtlas Estate, its management, employees, contractors and anyone acting on its behalf, in every market where we operate. Third parties who act for us (agents, introducers, service providers) are expected to observe equivalent standards.

3. 3. Prohibited conduct

- Deliberately and dishonestly helping a client, supplier or partner evade tax - in any country.
- Structuring transactions, invoices or payment routes whose purpose is to conceal income or

assets from a tax authority.

- Turning a blind eye to red flags: requests for false invoices, payments to unrelated third parties or opaque jurisdictions without commercial rationale, or refusal to complete verification.

4. 4. Our controls

- KYC identity verification and source-of-funds checks on investors.
- Payments are accepted from and returned to verified account holders only.
- Staff training on red flags, with a clear duty to escalate rather than proceed.
- Risk-based due diligence on associated persons, with contractual anti-facilitation commitments.

5. 5. Reporting and breaches

Concerns can be raised with management or confidentially via compliance@atlasestate.estate, or anonymously under our Whistleblowing Policy. No one who raises a genuine concern in good faith will suffer retaliation of any kind.

Breaches of this policy are treated seriously. Employees who breach it face disciplinary action up to termination; engagements with third parties who breach it may be suspended or ended. Where conduct may be unlawful, we will notify the competent authorities and cooperate fully.

6. Practical scenarios

- A buyer asks for the invoice to be issued to a different company "for tax reasons" with no commercial substance: refuse and escalate.
- A seller requests part of the purchase price in cash or to an unrelated offshore account: refuse and escalate.
- A counterparty asks us to understate the property price in documents: refuse, escalate, and consider ending the relationship.
- An introducer offers to "handle the taxes" for a client in a way that seems too good to be true: pause the transaction and escalate before proceeding.

7. Risk assessment

We assess facilitation risk annually across our services, customer base, jurisdictions and intermediaries. Controls are proportionate to that risk: identity verification, source-of-funds checks, transaction documentation standards, and contractual anti-facilitation commitments from associated persons.

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:

- Buyers may request invoicing structures that disguise beneficial ownership or price.
- Introducers paid on commission have incentives to accommodate evasive requests.
- Cross-border settlements make destination-of-funds checks essential.
- Cash-adjacent instruments and crypto can be proposed to keep sums outside reporting.

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.

- Annual facilitation-risk assessment across services, customers, jurisdictions and intermediaries drives proportionate procedures.
- Invoices are issued only to the contracting counterparty; requests to re-paper to unrelated entities are refused and escalated.
- Purchase prices in documents must equal economic reality; any request to understate or split is refused, escalated and may end the relationship.
- Associated persons (introducers, agents) sign anti-facilitation commitments and acknowledge our right to audit.
- Payment destinations are checked against the counterparty's identity and country; unexplained third-country routing is held pending explanation.
- Staff-facing guidance lists refuse-and-escalate scenarios with the exact expected response.

11. Application across our markets

Application across our markets: the refuse-and-escalate standard applies identically in every jurisdiction; local legality of a structure does not exempt it where its purpose is evasive elsewhere.

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: a buyer asks for the invoice to name an unrelated company. Response: refused and escalated; re-papering to a party outside the transaction is a facilitation red flag.
- Situation: a request to split the purchase price into an inflated furniture package to reduce transfer tax. Response: refused, escalated, and the relationship reviewed.
- Situation: an introducer mentions a client prefers to avoid reporting under exchange-of-information rules. Response: treated as a red flag - enhanced diligence, and exit if the evasive purpose is confirmed.

13. Definitions

- Tax evasion facilitation — deliberately and dishonestly aiding another person's criminal tax evasion.
- Associated person — an employee, agent or other person performing services for or on behalf of InterAtlas Estate.
- Reasonable prevention procedures — the risk-based controls an organisation maintains to prevent facilitation by associated persons.

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:

- UK Criminal Finances Act 2017 corporate-offence principles applied group-wide
- Local criminal tax law of each operating market
- Exchange-of-information regimes (CRS) awareness in customer interactions

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.