Sanctions Compliance 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

InterAtlas Estate complies with all applicable economic and trade sanctions, including those of the United Nations, the European Union, the United Kingdom (OFSI) and the United States (OFAC), as relevant to our operations.

2. 2. Our commitments

- We do not provide services to, or deal with, individuals or entities designated on applicable sanctions lists, or entities owned or controlled by them.
- Customers and counterparties are screened at onboarding and periodically thereafter against applicable lists.
- We do not engage in transactions involving comprehensively sanctioned territories.
- Potential matches are escalated and resolved before any transaction proceeds; confirmed matches are rejected, funds are frozen where required, and reports are made to the competent authority.

3. 3. Red flags

- Reluctance to provide identity or ownership information.
- Payment routes involving third parties or jurisdictions unconnected to the client.
- Sudden changes of beneficiary or destination shortly before settlement.

4. 4. Breaches

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.

5. Screening process

- Lists in scope: UN Consolidated, EU Consolidated, UK OFSI, US OFAC SDN - as applicable to the transaction and parties.
- When: at onboarding, on beneficial-owner changes, on list updates, and before significant transactions.
- Matching: name and identifier screening including transliteration variants; potential matches are held - the transaction does not proceed while an alert is open.
- Alert handling: resolved within 2 business days where possible; confirmed matches are frozen, rejected and reported to the competent authority without tipping off.

6. Ownership and control assessment

For corporate counterparties we identify beneficial owners and assess whether any designated person owns 50% or more, or otherwise controls the entity. Where ownership is opaque and cannot be resolved, we decline the relationship.

7. 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.

8. 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:

- List volatility: designations change weekly across four regimes we track.
- Transliteration of names across Latin, Cyrillic, Greek, Arabic and Turkish alphabets complicates matching.

- Corporate customers can conceal designated ownership behind layered entities.
- Secondary-market token trades must be screened on both sides, not only at onboarding.

9. 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.

- Screening runs at onboarding, on every list update, before significant transactions and on both sides of secondary-market trades.
- Matching uses name, date of birth, identifiers and transliteration variants; potential matches place an automatic hold.
- Alerts are investigated and dispositioned within 2 business days; escalations go to compliance leadership same day.
- Beneficial ownership is identified for corporate counterparties; the 50% ownership and control test is applied and documented.
- Confirmed matches: freeze, reject, report to the competent authority without tipping off, and preserve the file.
- Licences or authorisations, where applicable, are obtained before any exempted dealing proceeds.

10. Application across our markets

Application across our markets: all four list regimes are screened for every customer regardless of market, because funds, customers and properties cross borders even when a transaction appears domestic.

11. 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: screening returns a hit matching name and date of birth. Response: automatic hold; investigation and disposition within 2 business days; freeze and report if confirmed.
- Situation: a corporate buyer's 50% shareholder traces to a designated entity. Response: the ownership and control test fails - the transaction is refused and reported without tipping off.
- Situation: a party to a secondary-market token trade is designated between order and settlement. Response: both-sides screening at execution halts the trade; the position is frozen pending authority guidance.

12. Definitions

- Sanctions — restrictive measures imposed by the UN, EU, UK, US or other authorities against countries, entities, persons or sectors.
- Designated person — an individual or entity named on an applicable sanctions list.
- Ownership and control — a designated person owning 50% or more of an entity, or otherwise directing it, extends sanctions to that entity.
- Screening — checking customers and counterparties against applicable sanctions lists at

onboarding and periodically.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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:

- UN Security Council consolidated list
- EU restrictive-measures regulations
- UK OFSI regime
- US OFAC SDN list where a US nexus could arise

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.

19. 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.