



SANDJAR GROUP

ATLAS PLATFORM

DOCUMENT No. 5

GDPR Policy

of ATLAS Platform

Data Protection, Privacy Framework & Cross-Border Data Transfer Governance

Issued by:	Atlas Overseas FZE
Document Version:	v1.0 — May 2026
Primary Laws:	EU GDPR 2016/679 UAE PDPL (Federal Law No. 45 of 2021) UK GDPR
Data Protection Officer:	Designated DPO — Atlas Overseas FZE
Classification:	Confidential & Proprietary — Regulatory Document

I. SCOPE, APPLICABILITY & LEGAL BASIS

This Privacy and Data Protection Policy ('Policy') sets out how Atlas Overseas FZE ('ATLAS', 'we', 'us') collects, processes, stores, transfers, and protects personal data in connection with the ATLAS Platform. This Policy applies to all users, regardless of their country of residence, who interact with the Platform.

1.1 Applicable Legal Frameworks

Regulation	Jurisdiction	ATLAS Trigger
GDPR (EU) 2016/679	European Union / EEA	Applies to all EU/EEA residents using the Platform, regardless of where ATLAS is established
UAE Federal Law No. 45 of 2021 (PDPL)	United Arab Emirates	Applies to all data processing activities conducted in or from the UAE
UK GDPR (post-Brexit)	United Kingdom	Applies to all UK residents using the Platform
DIFC Data Protection Law (DIFC Law No. 5 of 2020)	DIFC — Dubai	Applies if Platform operates from DIFC registered entity
ADGM Data Protection Regulations 2021	ADGM — Abu Dhabi	Applies if any processing infrastructure is located in ADGM
CCPA (California Consumer Privacy Act)	California, USA	Applies to California residents — right to know, delete, and opt-out of data sale

1.2 Legal Bases for Processing (GDPR Article 6)

Contract Performance: Processing necessary to execute property transactions, IP-Share acquisitions, and platform services the user has requested.

Legal Obligation: Processing required to comply with AML/KYC obligations, tax reporting, DLD regulatory requirements, and court orders.

Legitimate Interests: Processing for platform security, fraud prevention, dispute resolution, and service improvement — balanced against user rights.

Consent: Processing for marketing communications, optional analytics, and non-essential cookies — consent obtained at onboarding and withdrawable at any time.

II. DATA COLLECTED — CATEGORIES & PURPOSES

Data Category	Specific Data Points	Processing Purpose
Identity Data	Full legal name, date of birth, nationality, government ID number, passport number	KYC verification, AML compliance, account authentication, DLD title registration
Biometric Data	Face ID scan, liveness detection data (GDPR Art. 9 sensitive category)	Platform authentication, e-signature authorisation, Face ID payment approval
Contact Data	Email address, mobile number, residential/business address	Account communication, transaction notifications, regulatory correspondence
Financial Data	Bank account details (masked), transaction amounts, payment method, ATL wallet balance, IP-Share holdings	Transaction processing, fee settlement, royalty distribution, financial reporting
Property Data	Property details, title deed information, ownership history, DLD transaction records	Due diligence, listing verification, DLD integration, market analytics
Technical Data	IP address, device ID, browser type, session logs, access timestamps	Platform security, fraud detection, system performance, audit trail
Communications Data	In-platform messages, offer exchanges, document exchanges, dispute correspondence	Transaction record, legal evidence, dispute resolution, compliance audit
Behavioural Data	Search history, property views, click patterns, feature usage	Service personalisation, platform improvement, fraud pattern detection
Third-Party Data	Data received from DLD, RERA, OFAC/UN sanctions lists, blockchain analytics providers	Regulatory compliance, KYC verification, AML screening, sanctions compliance

III. DATA RETENTION, TRANSFERS & SECURITY

3.1 Retention Schedule

Data Category	Retention Period	Legal Basis
KYC / Identity Documents	5 years post-relationship end	UAE AML Law (Federal Decree-Law No. 20 of 2018), CBUAE requirements
Transaction Records	5 years post-transaction date	UAE AML Law; UAE Commercial Transactions Law; DLD requirements
Biometric Data (Face ID)	Duration of active account + 90 days	Minimisation principle; deleted on account closure

Financial / Payment Data	5 years post-transaction	Tax law; AML/CFT requirements; dispute resolution
Communications / Messages	3 years post-transaction closure	Contract evidence; dispute resolution; UAE Evidence Law
Marketing & Consent Records	Until consent withdrawn + 3 years	Proof of consent; regulatory requirement
Security / Access Logs	12 months rolling	Platform security; fraud investigation
Blockchain Records	Permanent (immutable ledger)	Technical impossibility of deletion; audit trail requirement

3.2 Cross-Border Data Transfers

ATLAS transfers personal data internationally in connection with its banking partners, DLD integration, sanctions screening, and blockchain infrastructure. All transfers comply with GDPR Chapter V requirements:

- EU/EEA transfers: Standard Contractual Clauses (SCCs — European Commission Decision 2021/914) with all data processors outside the EEA.
- UAE PDPL: Cross-border transfer to countries providing adequate data protection or with contractual safeguards per UAEDPA guidance.
- Blockchain data: Any on-chain data is considered pseudonymous. No directly identifiable personal data is written to the public blockchain — only transaction hashes and wallet addresses.
- Banking partners: Data sharing with licensed bank partners governed by data processing agreements compliant with GDPR Article 28.
- Sanctions screening providers: Data minimisation applied — only name, date of birth, and nationality transmitted for screening (no financial data shared).

3.3 Security Measures

- AES-256 encryption for all data at rest; TLS 1.3 for all data in transit.
- Zero-knowledge architecture for biometric data — Face ID templates never stored in raw form; only encrypted mathematical representations retained.
- Role-based access control (RBAC) — platform staff access only data necessary for their specific function.
- Annual penetration testing by accredited external security firm.
- 72-hour breach notification to relevant supervisory authority (GDPR Article 33) and affected users where high risk.
- Data Protection Impact Assessment (DPIA) conducted for all new high-risk processing activities.

IV. USER RIGHTS & ENFORCEMENT

4.1 Data Subject Rights

Right	Scope	ATLAS Response Time
Right of Access (Art. 15)	Copy of all personal data held; processing purposes; recipients; retention periods	30 days (extendable to 60 days for complex requests)
Right to Rectification (Art. 16)	Correction of inaccurate or incomplete personal data	14 days from verified request
Right to Erasure (Art. 17)	Deletion of data where: consent withdrawn; no longer necessary; processing unlawful — subject to legal retention obligations	30 days — legal retention data excluded (AML/transaction records)
Right to Data Portability (Art. 20)	Machine-readable export of user-provided data (JSON/CSV format via platform dashboard)	30 days
Right to Object (Art. 21)	Object to processing based on legitimate interests or direct marketing — immediate effect for marketing	Immediate for marketing; 30 days for other objections
Right to Restrict Processing (Art. 18)	Restrict processing during: accuracy dispute; unlawful processing contested; legal claim establishment	Applied within 72 hours of verified request
Right to Withdraw Consent	Withdraw consent for any consent-based processing at any time — does not affect prior lawful processing	Immediate effect via platform settings

4.2 Contact & Complaints

Data Protection Officer: privacy@atlas.io | Atlas Overseas FZE, Dubai, UAE

EU Representative: Designated EU representative per GDPR Article 27 — contact via privacy@atlas.io

Supervisory Authority: EU users may lodge complaints with their local Data Protection Authority. UAE users may contact the UAE Data Protection Authority via the DIFC Commissioner of Data Protection.

Disclaimer: This Policy is reviewed annually and updated to reflect changes in applicable law, platform functionality, or processing activities. Users will be notified of material changes with 30 days' advance notice via the platform and registered email.