AVIS Land
Anti Money Laundering and Financial Crime Prevention Statement

Version 1.0 | 25 November 2026

GENESIS prohibits the use of AVIS Land to launder criminal proceeds, finance terrorism, finance prohibited proliferation or evade applicable financial sanctions. This Statement establishes responsibilities for proportionate prevention, detection, escalation and reporting across the marketplace and its connected services. Controls must address the actual activity and legal obligation, protect legitimate users and preserve the separate identities, assets and responsibilities of platform participants.

1 Operators participants and scope

AVIS Land is operated by GENESIS Collateral House Company Limited, Irish company number 823931, registered at 51 Bracken Road, Dublin D18 CV48, Ireland, and GENESIS Collateral House Company, North Carolina entity number 3214399, registered at 4111-E Rose Lake Drive, Charlotte, North Carolina 28217, USA. GENESIS operates within the Monkeyrock group. The responsible operator and any separately regulated provider must be identified for the relevant relationship.

This Statement governs GENESIS personnel and activities conducted for GENESIS through authorised agents and service providers. Vendors, franchisees, subsidiaries, issuers, manufacturers, laboratories and educational institutions must comply with their own applicable duties and agreed platform requirements. A user's licence, fund, insurance arrangement or asset does not become a GENESIS permission or asset through onboarding. Each entity remains accountable for duties arising from its actual conduct, including where it performs a regulated service.

2 Legal obligations and proportionate marketplace controls

Before introducing or materially changing a service, GENESIS must determine the activities, jurisdictions, responsible entities and financial-crime obligations involved. Ordinary marketplace participation does not automatically make every participant an AML-regulated financial institution. Identity, fraud-prevention and sanctions controls may nevertheless apply. Banking, brokerage, money transmission, crypto-asset services, certain professional services and other covered activities require the obligations appropriate to the entity and activity.

For Irish designated persons, the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended, governs relevant duties. US obligations depend on the applicable Bank Secrecy Act category and implementing rules, including the distinct requirements for money services businesses and securities broker-dealers. Moroccan and Tunisian operations must meet local requirements within their actual scope. Corporate registration alone does not establish financial-services authorisation.

FATF standards inform the risk framework; applicable law determines enforceable requirements. EU transfer-information rules already apply within their scope. Regulation (EU) 2024/1624 generally applies from 10 July 2027; preparation for it must not replace compliance with current duties. Legal changes must be assessed and implemented by the relevant application date.

3 Governance and accountable reporting

Each responsible GENESIS board must oversee its financial-crime framework, approve the applicable risk appetite and provide adequate resources. Management must allocate documented responsibility for risk assessment, customer checks, sanctions, monitoring, reporting, records and remediation. Where required, the entity must appoint a suitably qualified money laundering reporting officer or equivalent compliance officer, with adequate authority, access to information, independence and deputy arrangements.

The reporting function must be able to escalate concerns to senior management and make required reports without commercial interference. Revenue targets, group relationships or a project's strategic importance cannot override a legal prohibition. Conflicts involving staff, owners, introducers or related entities must be declared and handled independently. Required appointments, decisions and approvals must be recorded; this Statement does not represent that a particular appointment, audit or regulatory approval has already occurred.

4 Business and relationship risk assessments

GENESIS must maintain a documented assessment of money-laundering, terrorist-financing, proliferation-financing and sanctions-evasion exposures relevant to its business. It must consider customers and beneficial owners; products and asset types; payment methods and transaction patterns; countries, shipping routes and counterparties; delivery channels; intermediaries; and the complexity of ownership and control. New technology, remote onboarding, automated agents and changes in business scale require assessment before deployment.

Assessments must use current national, supranational and sector findings and applicable official sanctions and FATF publications. No country list is fixed by this Statement. A higher-risk location, PEP status, non-profit purpose or use of a self-hosted wallet is not by itself proof of wrongdoing. Simplified measures require a documented lawful basis and cannot displace mandatory checks, suspicion-based action or sanctions. Risk assessments must be reviewed at least annually and after material changes, with customer reviews proportionate to their risk.

5 Customer identification and verification

Required customer due diligence must establish the customer's identity, legal existence where relevant, business purpose, expected activity and authority of representatives. Verification must use reliable, independent information appropriate to the risk, with additional checks for inconsistent documents, impersonation or remote-identity concerns. A virtual-company profile, wallet address or platform account is not a substitute for evidence of the relevant legal person or individual.

Checks must be completed at the stage required by the applicable law and service. Any permitted delayed verification requires its legal conditions, documented justification and appropriate transaction controls. If mandatory due diligence cannot be completed, the responsible entity must not begin or continue the affected relationship or transaction where the law prohibits it, and must assess reporting obligations. Unrelated public browsing or ordinary services must not automatically be subjected to full financial-account onboarding. Customers must provide accurate information and notify material changes.

6 Beneficial ownership and effective control

For legal persons and arrangements, the responsible entity must understand the ownership and control structure and identify the natural persons required by the applicable regime. Checks must consider direct and indirect holdings, voting rights, agreements, nominees, trusts and control through other means. A single universal 25% test is insufficient. Applicable ownership thresholds, separate control-person requirements and trust-specific rules must be applied accurately.

Registers, customer declarations and corporate documents must be assessed together; material discrepancies require investigation and reporting where required. A senior-manager fallback may be used only where the governing conditions are met and the necessary steps and difficulties are recorded. US corporate beneficial-ownership filing exemptions do not themselves remove a covered financial institution's customer-due-diligence obligations. Existing information may be reused only as permitted, with updates when doubts, material changes, applicable rules or risk require them.

7 Enhanced checks and politically exposed persons

Enhanced due diligence must address relationships or transactions carrying higher risk or requiring enhanced measures by law. It may require additional identity and ownership evidence, examination of economic purpose, corroborated funding information, closer monitoring and senior approval. Unusual complexity, unexplained routing or credible adverse information must be investigated in context, with consideration of reliable explanations and the quality and age of the evidence.

Relevant politically exposed persons, their family members and known close associates must be identified using the governing definitions. Where required, senior management approval, source-of-wealth and source-of-funds enquiries and enhanced monitoring must precede or accompany the relationship. Former PEP status must be assessed under applicable minimum periods and continuing risk, rather than automatically cleared on leaving office. PEP classification is preventive and does not allege criminal conduct or require automatic rejection.

8 Source of funds and source of wealth

The source of funds concerns the origin of money or assets used in the particular transaction; source of wealth concerns how a person's overall wealth was acquired. The depth of enquiries must reflect the applicable rule and assessed risk. Evidence may include business income, employment, sale proceeds, financing agreements, inheritance records or other reliable information, with proportionate corroboration.

A payment from an established bank, a blockchain transaction history or a professional introducer's assurance does not by itself establish lawful origin. Material inconsistencies between funding, business activity, income, asset ownership and the stated purpose must be resolved or escalated. Employees must not coach a customer to manufacture a plausible explanation or divide activity to avoid checks.

9 Sanctions and proliferation financing controls

GENESIS must identify and apply the sanctions regimes governing the entity, persons, goods, service and transaction, including applicable UN-derived, EU, US OFAC and national measures. Screening must address relevant customers, beneficial owners, controllers, representatives, counterparties and payment details, and be refreshed when lists or relevant circumstances change. Potential matches require prompt assessment; mandatory freezing or prohibitions must not await discretionary commercial approval.

Name screening alone is insufficient. OFAC's 50 Percent Rule aggregates relevant blocked-person ownership; EU and other regimes have their own ownership, control and indirect-benefit tests. Licences, exemptions and derogations must cover the actual transaction and their conditions. Low assessed money-laundering risk does not permit a sanctions breach.

Proliferation controls must examine relevant end users, end uses, dual-use items, procurement intermediaries, transshipment and financing patterns. Industrial equipment, advanced materials, laboratory activity or research links require examination where the actual facts raise such issues. An ordinary commercial explanation does not replace required export permission or targeted-sanctions compliance. Evasion concerns and required blocked-property reports must be escalated to the appropriate authority separately from any AML reporting duty.

10 Trade manufacturing projects and franchise relationships

Risk-based commercial checks must connect the contracting parties, goods or services, invoices, delivery evidence and payment flows. Relevant indicators include unexplained over- or under-invoicing, duplicate invoices, phantom shipments, circular payments, mismatched quantities or quality, unexplained intermediaries and payments unrelated to the contract. Legitimate price differences, research uncertainty or complex supply chains require assessment rather than an automatic adverse conclusion.

Construction, waste-to-nanopowder, graphene, laboratory and manufacturing projects must retain evidence appropriate to their activity, including material origin, relevant permits, supplier identity and milestone payments. Franchise royalties, technology licences, university or research funding and project-development fees must have an identifiable recipient and credible contractual purpose. Mergers, acquisitions and tokenisation arrangements require proportionate checks on ownership, funding, proceeds, valuation rationale and introducer remuneration. A green label, patent, grant or institutional association does not replace financial-crime checks. Reviews must consider relevant proceeds-generating offences, including fraud, corruption, tax crime and illegal waste trafficking, where the facts indicate exposure.

11 Cash payment instructions and third parties

Cash and equivalent instruments may be accepted only where the service permits them and applicable limits, aggregation, identification and reporting requirements are satisfied. Dividing connected transactions to evade a legal threshold is prohibited. The responsible entity must assess applicable currency-transaction or trade-and-business cash reporting separately from suspicious-activity reporting.

Payment instructions must be linked to an identified customer, contract and legitimate recipient. Third-party payments, overpayments followed by refund requests, changed bank details and rapid pass-through activity require proportionate verification. Refunds should follow the original lawful payment route unless a documented legitimate reason and required checks support another route. Neither a proposed refund nor account closure authorises release of blocked property. A hold must not be used to obtain unrelated fees or divert funds to another participant.

12 Crypto assets and transfer information

The entity performing a covered crypto-asset or money-transmission service must fulfil its own obligations. Required originator and beneficiary information must be obtained, verified where required, transmitted securely, screened and retained under the applicable travel-rule regime. The counterparty provider and its relevant status must be assessed. Missing information requires the lawful, risk-sensitive response, including requesting information, suspending, rejecting or returning a transfer and reporting repeated provider failures where required.

Under Regulation (EU) 2023/1113, covered crypto transfers require prescribed information; EUR 1,000 is not a general exemption. For transfers exceeding EUR 1,000 to or from a self-hosted address, the relevant provider must take adequate measures to assess whether the address is owned or controlled by its customer. Smaller transfers remain subject to applicable information, due-diligence and risk controls. Other jurisdictions have their own thresholds and rules.

Self-hosted addresses require the applicable identity, transaction-identification and risk assessment; they are not inherently unlawful. Blockchain analytics must be evaluated with other evidence and their attribution limitations. Travel-rule data must not be exposed on a public blockchain merely for convenience. GENESIS and its providers must never request a customer's private key or recovery seed for identity verification.

13 Ongoing monitoring and automated support

Monitoring must compare activity with the relationship's purpose, risk and expected pattern, including linked transactions, unusual velocity, geographic routing, sanctions exposure, dormant-account changes and unexplained transfers between participants. Terrorist financing can involve small sums and lawful sources; transaction value alone must not determine whether a concern is reviewed. Customer and ownership information must be refreshed when material changes or doubts arise.

Robotic and QUANTUM-connected systems may support screening, reconciliation and prioritisation within authorised instructions. Rules, data quality, thresholds, model changes and alert handling must be tested and reviewed, with accountable human investigation and escalation. An automated score is not proof of an offence, and closing an alert requires a recorded rationale. Commercial staff must not bypass an unresolved mandatory control; a technical fault in one service must be addressed within the affected risk and transaction scope.

14 Suspicion escalation and statutory reporting

Personnel must promptly escalate information giving rise to relevant knowledge, suspicion or reasonable grounds to the responsible reporting function, preserve supporting records and avoid unauthorised disclosure. The assessment must consider attempted, refused and completed transactions where the law requires. A suspicion does not require proof of the underlying crime. A flag alone is not a finding of guilt, and decisions to report or not report must record the relevant reasoning.

An Irish designated person must make a required suspicious-transaction report to both FIU Ireland and the Revenue Commissioners as soon as practicable under section 42 of the 2010 Act. In the United States, the covered entity must follow its applicable FinCEN SAR requirements and deadlines. Moroccan and Tunisian obliged entities must report through their applicable routes, including ANRF and CTAF respectively. Internal escalation or notifying another provider does not replace a person's statutory duty.

For an Irish designated person, section 42(7) requires the relevant suspicious or reported transaction or service not to proceed before the reports are sent to FIU Ireland and Revenue, unless stopping or delaying it is impracticable, or the person reasonably considers that not proceeding may alert the other person to a report or investigation. Any reliance on an exception must be documented and the reporting duty still fulfilled as soon as practicable. An exception does not override an effective direction or order under section 17 prohibiting the transaction or service.

Only lawful reliance or joint-reporting arrangements may alter which entity submits a report. Filing does not itself authorise a transaction or release funds. Reporting confidentiality and tipping-off restrictions must be observed, including restrictions on sharing a report or its existence within a group. Required contact with law enforcement, regulators or sanctions authorities must proceed through the authorised, legally applicable route.

15 Proportionate restrictions and lawful handling of assets

A restriction must have a lawful basis, be supported by the relevant obligation, contract or proportionate risk assessment, identify the affected entity, transaction, account or service, and be reviewed promptly. Confirmed sanctions restrictions, legal directions and mandatory due-diligence failures require the action prescribed by law. Where additional information can lawfully resolve a concern, it must be requested proportionately. Operational convenience is not a basis for indefinite or unrelated restrictions. Holding or blocking client assets requires the relevant legal or contractual authority; a risk score alone does not supply it.

GENESIS must not treat a concern in one participant or service as an automatic prohibition on every unrelated user's activity. Broader restrictions require a substantiated connection or legal requirement. Users retain ownership of their assets; compliance review does not authorise appropriation, unrelated

use or application against another person's debt. Relevant records, contractual entitlements and lawful complaint routes must be preserved. Explanations and updates must be given to the extent permitted without tipping off, compromising an investigation or breaching another legal duty.

16 Records and retention periods

The responsible entity must retain retrievable records of required identity checks, beneficial ownership, risk assessments, material transaction evidence, investigations, decisions, reports and relevant approvals. Records must allow the activity and decision to be reconstructed and made available to competent authorities as required. Retention must follow a documented schedule by jurisdiction, record type and legal trigger.

Irish section 55 generally requires relevant records for at least five years, with different starting points for customer, relationship, transaction and service records. EU transfer-information records are generally retained for five years. US BSA retention requirements commonly prescribe five years, but the applicable rule and starting event must be identified. Current OFAC rules generally require covered transaction records for at least ten years, and blocked-property records throughout blocking and for at least ten years after unblocking. Lawful extensions, preservation directions and other applicable duties must be assessed; data must then be securely deleted or anonymised when no lawful retention basis remains.

17 Data protection providers and group cooperation

Financial-crime information must be processed for a lawful purpose, limited to what is necessary, kept accurate and protected by appropriate access, confidentiality and security measures. AML data must not be repurposed for unrelated advertising or unrestricted model training. Data-subject requests must be handled under applicable law, including lawful restrictions protecting reporting and investigations. Cross-border disclosure requires an appropriate legal basis and transfer safeguards where required.

Outsourcing technology or checks does not transfer an entity's legal accountability. Providers must be assessed for competence, controls, security and access to required evidence, with contractual oversight and lawful audit and regulator access. Reliance on another institution's due diligence is permitted only where the governing conditions are satisfied. A vendor's assertion that it has completed KYC is insufficient by itself.

Group information sharing must be necessary, legally permitted and protected; it must not expose another participant's confidential records without authority. Correspondent or comparable provider relationships require the applicable enhanced checks and clear allocation of responsibilities. Prohibited shell-bank relationships must not be established or facilitated. A shared gateway does not establish permission to pool client assets or exchange confidential reporting material without restriction.

18 Training assurance and remediation

Relevant personnel must receive role-appropriate induction and continuing training on current risks, customer checks, sanctions, reporting, confidentiality and escalation. Training must address the actual marketplace, payment, securities, crypto, industrial and research functions performed. Attendance, understanding and required refreshers must be recorded.

Controls must undergo independent testing or assurance appropriate to the entity, law and risk, with findings reported to accountable management. Reviews must consider effectiveness, false positives, missed concerns, data quality and timely reporting, rather than completion counts alone. Deficiencies require assigned owners, deadlines and verification of remediation. Management must review material incidents, legal changes and provider failures and revise the framework accordingly. Publication of this Statement is not certification that every control has already been tested.

19 Enquiries concerns and continuing application

All enquiries, corrections and concerns may be sent to legalcube@avis.land. Telephone and WhatsApp: +34 674 002 006. Principal operating and enquiries office: GENESIS, 17–25 Via Ingegno, 84087 Sarno (SA), Italy. Website: https://avis.land. Financial-crime concerns received through this contact must be routed promptly and confidentially to the responsible function. Request a suitable secure channel before transmitting sensitive identity or financial documents.

No person may retaliate against a good-faith report or require disclosure of a confidential statutory report as a condition of resolving a complaint. Applicable external reporting, regulator and court rights remain available. This Statement supplements the relevant service terms and internal procedures; it does not waive mandatory rights, create financial-services authorisation or expand contractual authority over user assets. Updates must reflect applicable law and material changes without retrospectively removing accrued rights.

Reference publications

FATF Recommendations as amended June 2026

Ireland Criminal Justice Act 2010 on money laundering and terrorist financing as revised

Central Bank of Ireland AML and CFT regulatory requirements and guidance

Regulation EU 2023/1113 on information accompanying funds and crypto asset transfers

FinCEN Customer Due Diligence Rule FAQs incorporating 2026 account opening relief

US Treasury OFAC reporting procedures and recordkeeping requirements under 31 CFR Part 501

Morocco Ministry of Economy and Finance ANRF information

Tunisian Financial Analysis Commission CTAF