

Website Compliance for Anjouan Gaming Licensees

Issued by ANJ Management Ltd. (Anjouan Gaming) | Revised 13 October 2026

Purpose and application

This guide supports B2C licensees in implementing website, player-protection and operational obligations. Relevant B2B suppliers must support the controls applicable to their services. It must be read with applicable law, binding AOFA directions, licence conditions, the general Code of Conduct and the KYC and AML Code of Conduct, final edition dated 13 October 2026. AOFA means the Anjouan Offshore Financial Authority; Anjouan Gaming provides administrative services designated by AOFA.

New KYC/AML provisions apply from the date specified in the AOFA adoption notice. That notice must identify reporting recipients, secure channels and transitional arrangements. Existing obligations continue until replacement takes effect. This guide does not itself amend a licence condition or waive a stricter legal obligation. Escalate inconsistencies promptly to AOFA.

1. Licensing information and authorised websites

Display the operator's full legal name, company registration number, registered address and licence number site-wide in the footer. Provide accessible links to terms, privacy, responsible gaming, AML/KYC and withdrawal policies, complaints procedures and contact information.

Use only the official interactive validator code supplied by Anjouan Gaming, without modification. The validator must link to the correct live licence record for the authorised domain. Static licence images, copied validators, misleading seals and claims of sublicensing are prohibited. Only authorised brands, domains and URLs may operate under the licence.

An Anjouan licence does not authorise operations in every country or constitute endorsement of an individual product, payment service or commercial claim.

2. Eligibility, markets and registration

State that players must be at least 18, or the higher minimum applicable in their jurisdiction. Collect full legal name, date of birth, residential address and country, nationality, contact details and a unique player identifier before account activation. Obtain confirmation that the player acts for their own account.

Apply proportionate age, sanctions, geography and fraud controls at registration. Routine documentary identity verification before the first deposit or play is not required under the revised KYC/AML Code where no trigger applies. Earlier checks remain mandatory where required by applicable law, binding licence conditions, age concerns, identity doubts or suspicious activity. Do not permit minors to play.

Maintain an up-to-date prohibited-territories policy reflecting AOFA directions and applicable local law. The supplied September 2026 conditions include Australia, Austria, Comoros, France, Germany, the Netherlands, Spain, the United Kingdom and the United States, as well as specified sanctioned or FATF-blacklisted territories and other AOFA-designated jurisdictions. The list is non-exhaustive and must be checked against subsequent directions.

Use effective GEO-IP blocking and proportionate controls against circumvention. Investigate mismatches between declared residence, device location and payment information. Sanctions, prohibited markets, FATF high-risk jurisdictions and increased-monitoring jurisdictions require distinct assessments.

The excluded-territories list is non-exhaustive. Each operator is responsible for identifying and complying with applicable local laws in every jurisdiction in which it offers, markets or provides gaming services, including licensing, advertising and player-access restrictions. The absence of a jurisdiction from the excluded-territories list does not constitute permission to operate there. An Anjouan licence does not replace any local licence or authorisation required by law. Operators must assess their target markets, obtain qualified local legal advice where necessary and implement effective controls to prevent prohibited activity.

3. Identity verification and transaction thresholds

Complete identity, age and residence verification at the earliest of: aggregate lifetime deposits reaching EUR 3,000 or equivalent; the first withdrawal request, regardless of value; suspicious activity; a single qualifying financial transaction or identifiable linked series reaching EUR 3,000 or equivalent; or doubt about previously supplied identity information. A cancelled withdrawal request does not remove the trigger.

Verify before accepting the threshold-crossing deposit or executing another qualifying threshold-crossing financial transaction. Combine gross deposits across accounts and brands under the same licensee without deducting withdrawals, losses or refunds. Preserve historical EUR valuations. Internal wagers and recycling the same gaming balance do not themselves constitute new external funds movements.

If payment arrives before required verification, hold it in restricted suspense and do not make it available for play. Block further deposits, real-money wagers and payouts until required checks are completed or a lawful resolution is approved. Use reliable independent identity and residence evidence in accordance with licence conditions; the Code does not independently waive a stricter documentary condition.

Apply enhanced due diligence according to risk, including source of funds and, where appropriate, source of wealth. The EUR 3,000 trigger and a low-risk first withdrawal require verification, not automatic enhanced due diligence.

The separate CTR threshold is US\$10,000 or equivalent. It is not an identity-verification threshold. Follow Article 9.3 and Annex A of the revised KYC/AML Code for reportable movements, separate gross incoming/outgoing calculations, rolling 24-hour aggregation, longer demonstrably linked series, valuations and filing.

Once the reporting provisions commence, the weekly CTR period runs Monday 00:00 UTC to the following Monday 00:00 UTC, with filing by 17:00 UTC on the following Tuesday, including nil returns. Suspicious activity reporting is independent: report promptly and no later than 24 hours after suspicion or reasonable grounds for suspicion arise, through designated channels and separately to competent statutory recipients where required. Protect reporting confidentiality.

4. Responsible gaming and fair terms

Provide accessible self-exclusion, deposit, loss and time limits, reality checks and support information. Block self-excluded players within one working day, with immediate restriction where practicable. Do not send gambling promotions to self-excluded players. Monitor indicators of harm and document proportionate interventions.

Publish clear eligibility, game rules, payout structures, applicable odds or RTP, account rules, fees and deposit/withdrawal procedures. Prominent bonus terms must include wagering requirements, restrictions and expiry dates. Avoid retrospective or misleading changes and do not use AML checks or bonus rules to impose unjustified withdrawal barriers.

5. Payments and withdrawals

Use appropriately assessed payment providers and secure, traceable payment routes. Check payer ownership against registration information before a verification trigger and against verified identity afterwards. Escalate discrepancies and prohibit undisclosed third-party funding.

Publish realistic withdrawal timeframes and explain any lawful review delay to the extent permitted. Pay to an account or wallet controlled by the verified player, ordinarily through the original funding route where lawful and practicable. Document alternative routes. A CTR filing alone does not justify a withdrawal hold; incomplete checks or a SAR alone do not justify confiscation.

Where virtual assets are supported, assess assets, networks and providers, apply proportionate blockchain tracing and sanctions controls, and retain wallet addresses, transaction hashes and valuation evidence. Do not assume stablecoins always equal US\$1.

6. Game integrity and suppliers

Use games and RNG systems tested by independent laboratories approved by Anjouan Gaming, with certification appropriate to the product. Retain current certificates and evidence of scope; display testing badges only where their use is authorised and accurate.

Maintain anti-fraud, anti-collusion and manipulation controls. Assess platform and content suppliers for fitness and properness and required Anjouan B2B licensing or recognition. Address applicable technical standards, including GLI-19 for interactive gaming systems and GLI-33 for event wagering systems where required by the relevant approval.

7. Privacy, cybersecurity and resilience

Publish a clear privacy policy identifying lawful processing purposes, data categories, retention, sharing, international transfers and rights. Consent is one possible legal basis, not a universal requirement for regulatory processing. Apply GDPR and other data-protection law where applicable.

Use current TLS/HTTPS, secure coding, access controls, encryption, logging, vulnerability management and tested backups. Require multifactor authentication for privileged access and offer appropriate player-account safeguards. Assess vendors and protect identity documents and reports through secure transfer channels.

Maintain documented availability targets, outage procedures and recovery testing proportionate to risk. This guide does not impose a universal 99.9% uptime requirement or claim that every hosting location requires prior approval. Comply with any specific hosting or resilience conditions.

Notify the designated regulatory incident channel within 24 hours after discovery of a material cybersecurity incident affecting player data, funds, AML controls or reporting, in line with the revised Code. Meet shorter legal deadlines and other applicable licence-condition notifications, including the three-working-day serious-incident requirement where applicable.

8. Advertising, affiliates and accessibility

Avoid targeting minors or vulnerable people, misleading claims, guaranteed winnings or representations that gambling solves financial problems. Include responsible gaming messaging and oversee affiliate compliance. The licensee remains responsible for outsourced marketing.

Use clear navigation and accurate translations for the markets served. Provide proportionate accessibility measures with reference to current WCAG guidance. Support access to account information, policies, complaints and self-exclusion across devices.

9. Complaints and approved ADR

Acknowledge player complaints within 72 hours and make good-faith efforts to resolve them within 30 calendar days from receipt. If unresolved, explain access to the designated AOFA-approved ADR provider and provide its name and contact details in player-facing terms and complaints pages.

Participate in approved ADR in good faith, pay all applicable ADR costs and comply with binding outcomes under the applicable rules. Do not charge ADR fees to players. Anjouan Gaming oversees compliance; it does not adjudicate individual player disputes. AML reviews do not remove ADR obligations, although legal confidentiality and restrictions must be respected.

10. Governance, records and continuing review

Maintain a qualified Compliance Officer/MLRO, effective training, documented risk assessments, internal controls, independent review and management oversight. Keep CDD and relationship records for at least five years after closure and transaction records for at least five years after the transaction, subject to longer lawful retention requirements. Preserve reports, decisions and audit trails as required by the KYC/AML Code.

Maintain annual financial reporting, player-funds segregation and reconciliation, supplier records and regulatory returns as required. Cooperate with lawful audits and information requests. Review websites and policies at least annually and after material regulatory, product or operational changes.

Contact

ANJ Management Ltd. | info@anjouangaming.com | www.anjouangaming.com

Administrative correspondence address: Po Box 1212 Hamchako, Mutsamudu, Autonomous Island of Anjouan, ANJ901 Union of Comoros. Administrative offices are not public visitor facilities.