Acceptable Use Policy

Version 2.2
Effective date: 20.11.2026

1. Purpose, scope and relationship to other terms

We are Arqen Finance ("Arqen", "we", "us" or "our"), a technology platform. The Contracting Entity for your Services is identified in the applicable service interface or commercial agreement before you enter into a binding agreement, as described in the Terms & Conditions (the "Terms"). Capitalised terms not otherwise defined in this AUP have the meaning given in the Terms.

This Acceptable Use Policy ("AUP") governs access to and use of the Arqen website, client portal, APIs, sandbox, card-related management tools and approved embedded or white-label integrations (the "Services"). It is incorporated into and forms an integral part of the Terms & Conditions. It applies to Clients, partners, Authorised Users, end users and cardholders to the extent incorporated into the agreement governing their access. Clients and partners must ensure that persons to whom they grant access are informed of and comply with applicable restrictions.

This AUP operates together with the Terms, applicable Order Forms and Programme Terms. It does not grant any right to issue cards, distribute financial services, receive funds or permit third parties to use a Programme. Financial and card services are governed by the applicable Programme Terms and legal requirements. Mandatory law prevails; the order of precedence is set out in Section 3 of the Terms. Stricter lawful programme restrictions apply to the relevant Programme. If a restriction is unclear, obtain written confirmation before proceeding.

2. Permitted use and eligibility

Use the Services only for lawful, disclosed and approved purposes, within the Programme, jurisdictions, user categories, spending controls and permissions agreed for your account. Depending on the approved programme, legitimate uses may include corporate expenditure, advertising and media buying, software subscriptions, business procurement, embedded spending tools, or other expressly permitted use cases.

- Users must meet the applicable minimum age (at least 18), legal capacity, eligibility and verification requirements. Representatives must be authorised to act for the relevant client or partner.
- Provide accurate, current and complete information about identity, ownership, business activities, authorised users, funding and intended use. Notify us promptly of material changes.
- Use only approved features, funding routes, permitted currencies and jurisdictions. Observe all applicable sanctions and geographic restrictions, provider limits and card network requirements.
- Obtain written approval before expanding an approved use case, distributing the Services to third parties or changing the underlying business model in a way that affects programme eligibility.

3. Prohibited activities

The following activities are prohibited whether carried out directly, indirectly, through another person, or through the API, a partner integration or any associated card programme:

3.1 Unlawful conduct and financial crime

- Money laundering, terrorist financing, sanctions violations, bribery, corruption, fraud, theft, tax evasion or any other unlawful activity; dealing in criminal proceeds or assisting another person in concealing the origin, ownership or destination of funds.
- Use of stolen, compromised, fabricated or unlawfully obtained identities, documents, cards, credentials or payment details; impersonation, nominee arrangements that conceal the true user or beneficial owner, or misrepresenting the intended recipient of services.

- Unlicensed or unauthorised financial activity, including receiving or transmitting funds for third parties, providing cash-out services, distributing payment instruments or exchanging assets where authorisation or programme permission is required and has not been obtained.
- Transactions or arrangements intended to evade verification, sanctions, screening, monitoring, reporting, geographic restrictions, spending limits or provider controls.

3.2 Misuse of cards and payments

- Using a card, account, funding instruction or token without valid authority; lending, selling, renting, sharing or transferring card access or credentials to a person who has not been approved under the relevant Programme.
- Card testing or enumeration, attempts to validate stolen payment details, fabricated purchases or refunds, collusive transactions, dishonest chargebacks, or transactions designed to create artificial turnover or extract funds without a legitimate underlying purpose.
- Using multiple cards, accounts or identities to circumvent platform, merchant, provider or network controls, enforcement decisions or restrictions. Multiple cards may be used for genuine operational purposes where permitted by the Programme.
- Improperly mixing third-party funds or using undisclosed or unapproved funding sources, including routing funds for persons who have not been verified where verification is required.
- Exceeding or manipulating merchant-category, merchant, transaction, geographic or velocity controls, or intentionally misdescribing a transaction or merchant to bypass them.

3.3 Harmful or unlawful business and content

- Illegal goods or services, illicit drugs, trafficking, exploitation, unlawful weapons transactions, counterfeit or stolen goods, intellectual property infringement, or other activities prohibited by applicable law.
- Fraudulent or deceptive advertising, phishing, malware distribution, scams, unlawful collection of personal data, or unlawful marketing practices.
- Activities that violate applicable card network rules, financial provider conditions or legally binding restrictions on the relevant Programme.

4. Restricted or programme-dependent activities

The following examples may be lawful in some circumstances but are subject to enhanced review, provider restrictions or express prior programme approval. Do not use the Services for these activities unless the relevant use case is permitted by the applicable provider and Arqen has confirmed eligibility in writing where required:

- Financial services, money transfers, payment facilitation, third-party funding, prepaid or stored-value products, currency exchange, and other cash-equivalent activity.
- Gambling, betting, gaming involving real-money prizes, regulated pharmaceuticals, tobacco, alcohol, adult-oriented businesses, weapons-related businesses and other regulated or high-risk sectors.
- High-risk merchant categories, unusual refund or chargeback exposure, high-volume card distribution, marketplace seller payouts, incentive or gifting programmes, or programmes involving end customers outside the approved client structure.
- Cross-border activity or participants in jurisdictions subject to enhanced programme restrictions.

This list is illustrative, not a definitive provider eligibility list or a promise of approval. Provider-specific country, sector and merchant-category restrictions apply as communicated for the relevant Programme. A lawful merchant category or business may still be unavailable under a particular programme. Approval of one activity or programme does not constitute approval of another.

5. Cards, funding and authorised users

Clients must identify and manage all persons authorised to access the Services or use cards in accordance with the relevant Programme. A card issued to a named individual may not be used by others unless that arrangement is explicitly permitted by the issuer and the applicable card terms. Where a Programme permits corporate, contractor or employee spending, maintain an accurate allocation of users and permissions and retain evidence of the legitimate business purpose or other approved use.

Personal expenditure, cash withdrawals, transfers, cash equivalents or other non-business spending are permitted only if expressly allowed under the relevant Programme and contractual arrangements and otherwise lawful. The client is responsible for appropriate accounting and documentation and must not disguise personal expenditure as business activity.

Use only the funding instructions, accounts, wallets or routes approved for the Programme, as described in Section 7 of the Terms. Third-party funding is not permitted unless disclosed, verified where required and approved by the relevant provider. Do not request refunds or withdrawals to an unauthorised recipient. Provide authentic transaction evidence and cooperate with legitimate reconciliation, refund and dispute processes.

Do not imply that a technical account or a balance shown in Arqen is a bank account, deposit or protected balance unless the actual provider terms establish that status. The applicable financial provider controls the regulated financial functions under its own terms.

6. API, sandbox and platform security

- Use API credentials only for the environment, application and permissions for which they were granted; protect keys, tokens, login credentials and webhook secrets against disclosure and unauthorised access.
- Respect documented rate limits, retry and idempotency requirements, fair-use controls and technical restrictions. Do not intentionally overload, disrupt or interfere with the Services.
- Do not access or attempt to access another tenant, user, system or dataset without authority; do not probe, exploit or scan systems without express permission, or introduce malicious code or interfere with monitoring or audit logs.
- Use sandbox environments solely for authorised testing. Do not submit live card credentials or real personal data to a sandbox unless specifically authorised and protected under the applicable data arrangements.
- Comply with applicable payment-data security requirements, including PCI DSS to the extent applicable to your activities and scope. Do not retain or transmit sensitive authentication data contrary to applicable rules.
- Promptly revoke or rotate compromised credentials, secure affected accounts and report suspected misuse, incidents or vulnerabilities to compliance@arqen.finance. Coordinate responsible disclosure where appropriate; nothing prevents lawful reporting to competent authorities.

7. Partner, reseller and white-label use

Resale, sublicensing, card distribution and white-label use require an express written agreement and any necessary Programme or provider approval under Section 10 of the Terms. Partners must operate only within granted rights and must not represent themselves or Arqen as a bank, issuer, licensed financial provider or authorised agent unless that status and representation are accurate and expressly authorised.

- Ensure the appropriate client and cardholder terms, privacy notices, fees and programme disclosures are supplied and accepted before access is provided.
- Perform the onboarding, user verification, support, monitoring, complaint handling and escalation functions allocated to you in the written responsibility matrix. The responsible provider or other

authorised party retains its own regulatory decisions and duties. Do not assume that verification by another party discharges your own obligations.

- Keep accurate records of approved end users, permissions, use cases and relevant verification and transaction evidence, subject to applicable data protection requirements.
- Apply this AUP and applicable provider restrictions to downstream users through enforceable terms, and promptly notify Arqen of suspected material breaches, security incidents or unauthorised use.
- Do not offer unsupported services, make misleading claims about funds or protection, promise guaranteed approvals or refunds inconsistent with the applicable terms, or obscure the identity of the actual financial provider where disclosure is required.

8. Monitoring and cooperation

To protect the Services and enforce applicable obligations, Arqen may review relevant platform activity, technical logs and programme information lawfully available to it. Arqen or the relevant provider may request additional information, including identity, ownership, business purpose, authorised-user details, source of funds or transaction evidence, where necessary and appropriate. Clients and partners must cooperate promptly, submit accurate and authentic records and take reasonable steps to prevent further misuse.

We will process and share personal data only in accordance with applicable law, our Privacy Policy and relevant data processing arrangements. Providers remain responsible for their own regulatory decisions and monitoring obligations.

9. Enforcement, review and treatment of funds

A violation of this AUP may constitute a breach of the Terms. Where there are reasonable grounds to believe that this AUP or an applicable Programme restriction has been breached, or action is necessary to protect the Services, comply with law or respond to a valid provider requirement, we may take proportionate action within our contractual authority under Sections 14 and 15 of the Terms. Measures may include requesting clarification, requiring remedial action, restricting access or features, disabling credentials, suspension, termination or referral to the responsible provider or competent authority.

Where reasonably practicable and lawful, we will communicate the reason for a restriction, relevant next steps and the available review procedure. Immediate action may be necessary where there is a material security, fraud, legal or compliance risk, or where required by law. For correctable issues, the applicable remediation and termination rules in Sections 14 and 15 of the Terms apply. Affected Clients may contact compliance@arqen.finance to request review and provide supporting information. Arqen cannot override a lawful provider or authority decision.

Restrictions on Arqen access do not, by themselves, transfer ownership of or extinguish a lawful entitlement to funds. Card suspension, transaction blocking, reserves, settlement, chargebacks and the return of available balances are determined by the responsible party under applicable Programme Terms and law. The funding, refund and closure provisions in Sections 7, 8 and 15 of the Terms apply. This AUP creates no right to automatic forfeiture or confiscation. Platform fees are governed separately by the Terms and applicable commercial agreement.

10. Updates and reporting

We may update this AUP to reflect applicable law, provider rules, security requirements or changes to the Services. The current version will be published at https://arqen.finance/. Notice, effective dates and acceptance of material changes are governed by Section 18 of the Terms; urgent legal or security measures may take effect earlier where permitted. Report suspected misuse, prohibited activities or security incidents to compliance@arqen.finance. Do not include full card details, authentication secrets or unnecessary personal data in ordinary email.