

Privacy & Data Protection Policy

Algoz Group · Confidentiality, Privacy and Security

“Discretion is our trade. Protecting the information behind it is our duty.”

Algoz FZ-LLC (trading as Algoz / Algoz Group) · Trade Licence 5033995 · Registration 4071452 · TRN 105119056700001
VUNE0977, Compass Building, Al Hulaila, Al Hulaila Industrial Zone-FZ, Ras Al Khaimah, United Arab Emirates
algoz.group · privacy@algozgroup.com · Version 2.2 · Updated: October 2026

Security is not a feature. It is the service. Algoz Group serves a clientele for whom privacy is not a preference but a condition of life. For high-net-worth and ultra-high-net-worth individuals, executives and the people who act on their behalf, information is inseparable from safety: an itinerary, a residence, a movement pattern or a single contact detail, in the wrong hands, is not a data point but an exposure. We therefore treat every record we hold as if a principal's wellbeing could depend on it, because it can. This Policy sets out, in plain terms, how Algoz FZ-LLC (trading as Algoz and Algoz Group) protects the information entrusted to us across our platform and our operations, in compliance with UAE Federal Decree-Law No. 45/2021 on the Protection of Personal Data (PDPL), RAKEZ regulations and, where applicable, the UK and EU GDPR.

1. Scope and Relationship to the Terms & Conditions

This Privacy & Data Protection Policy is the privacy policy referenced in the Algoz General Terms & Conditions (clause 11.1) and is incorporated by reference into those Terms and into the Algoz Member, Early Member and B2B (Partner, Agent, Provider, Professional, Vendor and Place) agreements. It applies to all clients, members, VIPs, counterparties and visitors whose personal data Algoz processes. Capitalised terms used but not defined here have the meaning given in the applicable agreement. In the event of any conflict on a data-protection matter, this Policy governs; in all other respects the applicable agreement prevails. This Policy is governed by the same law and jurisdiction as the Terms & Conditions (clause 18 below).

2. Our Approach: Principles That Govern How We Handle Your Information

Confidentiality by default. Every engagement is treated as confidential from first contact. Information is shared only with those who must have it to deliver the service.

Need-to-know access. Personnel and systems are granted the minimum access required for their role, never blanket access for convenience.

Defence in depth. Protection is layered across network, application, access and human controls, so no single safeguard is a single point of failure.

Data minimisation. We collect only what a mandate genuinely requires, hold it only as long as needed, and retire it under disciplined retention rules.

Discretion as doctrine. Privacy is embedded in how our teams communicate, coordinate and operate, not added as an afterthought.

Continuous improvement. Our safeguards are reviewed and strengthened as threats evolve. Security is an ongoing practice, not a fixed state.

3. Information We Collect and Purpose Limitation

We collect only the information a mandate requires, which may include: identity and contact details; KYC and compliance information; payment or payout details; itinerary, location, scheduling and operational details necessary to coordinate a service; and platform usage data. We use your information solely to deliver and coordinate the services you have requested. We do not sell client data, and we do not repurpose it for unrelated ends or for marketing.

3A. Documents You Keep in the Algoz App

Members and clients can keep copies of their passports, visas, residence permits, identity cards and other travel documents in My documents in the Algoz app, and Algoz may attach travel documents such as tickets or vouchers to a trip. These documents are used only to prepare and deliver the services the client requests. Each file is encrypted before it is stored (AES-256, with keys protected by Google Cloud Key Management Service) and can be opened only by the client and by the authorised Algoz staff who handle their requests; every staff access is recorded. A document is shared with a partner, a hotel, an airline or an authority only on the client's instruction or where the law requires it. When the client deletes a document in the app, it is erased permanently from our servers together with its encryption key. Documents are also deleted when the app account is closed.

4. Lawful Basis, Consent and KYC

Lawful basis and consent. We process personal data on the bases permitted by the PDPL and, where applicable, the GDPR, principally the performance of your engagement, your consent, our legitimate interests in delivering and securing the service, and compliance with legal obligations. The Client and VIP expressly consent to Algoz collecting, processing and sharing their personal data with necessary third-party partners for the sole purpose of facilitating service delivery, including onboarding, coordination, access to tickets and venues, transportation and flights, and accommodation.

KYC and AML. In accordance with UAE regulations and anti-money-laundering requirements, Algoz conducts strict Know Your Customer checks, collecting and verifying full name, date of birth, nationality, residential address, contact details and government-issued identification. KYC data is stored securely, used solely for legal compliance, fraud prevention and operational integrity, and treated with the highest confidentiality. We may delay or refuse service if satisfactory KYC documentation is not provided.

5. How We Use Information; Use of Artificial Intelligence

We use personal data to coordinate and deliver services, process payments, ensure quality and safety, comply with legal obligations and secure our platforms. All written content we publish is authored by human professionals; the use of AI is limited strictly to grammatical and orthographic proofreading and translation. Some imagery and video are AI-generated to depict our services precisely so as to protect our clients' privacy: real clients are never shown for marketing purposes. AI tools may support the quality and efficiency of mission preparation and execution, but every action, decision and operational task is executed by experienced, qualified professionals, and AI never makes decisions about a client.

6. Partners, Sharing and Third Parties

Partners and third-party coordination. Algoz coordinates, under its RAKEZ licence, the services its clients request. Security, transportation and other operational services are delivered through vetted, licensed third-party partners, while Algoz also provides direct assistance and support to clients. Client data is shared with such partners only on a need-to-know basis, with all parties bound by strict confidentiality obligations.

Minimal sharing and consent. Information is shared with third parties only when strictly necessary to execute a service, limited to the minimum required, and only with client consent unless required by law or for immediate safety reasons.

Authorised users and Personal Assistants. Where a Member authorises a Personal Assistant or representative to operate their account, that authorised user accesses and processes the Member's personal data on the Member's instructions and is bound by equivalent confidentiality obligations; Algoz also verifies and processes the authorised user's own identity and contact data for verification and account security.

Agent and mission privacy. We enforce strict protocols to protect the identities of our agents and personnel, and we do not disclose live locations, venue names or mission-specific details to any external party not directly involved in the service.

Communication protocols. All client communication is handled by our main concierge or designated Principal Protection Officers; when missions are delegated, clients are introduced to the assigned team through official, controlled channels.

Safety and legal disclosure. In rare circumstances where client safety or a legal obligation requires it (including court orders, subpoenas, good-faith protection of rights, property or safety, or investigation of suspected fraud), information may be disclosed to relevant authorities, with utmost discretion and full compliance with privacy law.

7. Data Subject Rights

Subject to applicable law, you may request to know what personal data we hold, request corrections, and request deletion or restriction where no legal or operational obligation requires retention; you may also object to or request portability of your data and withdraw consent. Clients located in the United Kingdom or European Union have the corresponding rights under UK or EU GDPR. To exercise any right, contact our Data Protection Officer at dpo@algozgroup.com or privacy@algozgroup.com. Mandatory rights under applicable law are not affected by this Policy.

8. Data Retention

Records are kept only as long as a legitimate purpose requires and are then securely retired. Unnecessary client data is promptly deleted following mission completion; essential information may be securely retained for future engagements, in accordance with data-retention regulations and client instructions.

Account deletion in the Algoz app. When a member or client deletes their account in the Algoz app (Profile > Security > Delete my account), or asks us to by email, the account is closed at once and kept for 15 days; signing in again during that time restores it. After 15 days the profile, chats, requests, documents and login are erased permanently. Invoices and the record of the terms the member accepted are kept, as the law requires.

9. International Transfers

As Algoz operates a global network, personal data may be transferred across borders to coordinate a service. Where it is, we apply appropriate safeguards, including standard contractual clauses for transfers of EU or UK personal data, so that protections travel with the data.

10. Platform Security: How We Protect Your Data

Our member, partner and administrative platforms are built on enterprise-grade cloud infrastructure with security as a first-class requirement. The measures below summarise our technical safeguards at a level appropriate for sharing; specific configurations are kept confidential by design.

Encryption in transit. All communication with our platforms is encrypted using industry-standard TLS, with strict transport security enforced so connections cannot be downgraded.

Enterprise cloud. Data is hosted on leading enterprise cloud infrastructure benefiting from physical, network and platform security maintained to international standards.

Encrypted application & messaging. Our member application and operational communications run over encrypted channels, with sensitive coordination conducted on secure, privacy-focused messaging platforms.

Strong authentication. Access requires verified credentials, with two-factor (authenticator-based) authentication available and encouraged for every privileged account.

Role-based access control. A granular permission model limits each user and administrator to precisely the functions their role requires, enforced at the system level.

Session protection. Administrative sessions are protected against hijacking and fixation and expire automatically after inactivity, limiting the lifetime of any compromised session.

Hardened web defences. Our applications apply modern browser protections, including anti-clickjacking, content-security and strict-transport controls, to reduce the surface for common web attacks.

Secure, access-controlled backups. Backups are restricted to authorised personnel and handled under strict encryption discipline, so recovery never becomes a route to exposure.

Activity logging. Sensitive administrative actions are logged, supporting accountability and the detection of unusual activity.

11. Operational Security: The Human Factor

Technology is only as secure as the people who use it; most real-world breaches begin with a person, not a technical flaw. Because of who our clients are, our teams are treated as high-value and held to a correspondingly high standard.

Vetted personnel. Staff and operatives are vetted and bound by strict non-disclosure agreements; confidentiality obligations survive the end of any engagement.

Secure operative channels. Field coordination is conducted over encrypted, privacy-focused channels, with the most sensitive operations handled on dedicated secure messaging.

Compartmentalisation. Sensitive details (locations, schedules, identities) are shared strictly on a need-to-know basis, never broadcast across a team.

A single discreet point of contact. Clients interact through one trusted relationship manager, reducing how widely information must travel to deliver a result.

Awareness & phishing resilience. Our people are continuously trained against social-engineering and phishing tactics, the most common entry point for attackers targeting privileged access.

Clean separation of secrets. Credentials and keys are isolated from day-to-day systems and rotated under defined procedures, so a single exposure cannot cascade.

12. Confidentiality, NDAs and Audits

All Algoz personnel and third-party collaborators are bound by strict NDAs, ensuring continued confidentiality throughout and after the execution of services. We perform regular privacy audits and assessments to evaluate procedures, identify vulnerabilities and strengthen our practices, and our personnel undergo continuous training in data protection and cybersecurity awareness.

13. Vigilance, Monitoring and Incident Readiness

Robust prevention is paired with readiness. We monitor for unusual activity across our administrative systems, maintain procedures for responding quickly should an incident occur, and review our safeguards on an ongoing basis as the threat landscape changes. In the unlikely event of a data breach affecting your personal information, Algoz will notify affected clients as promptly as possible and in accordance with applicable data-protection regulations. Where a matter touches the physical safety of a principal, our security and operational teams coordinate as one: the same discipline that defines our protection work in the field is applied to the protection of information.

14. Children's Data

Algoz does not knowingly collect or process information relating to individuals under the age of 18 without verified consent from a parent or legal guardian.

15. Information Security and Client Responsibility

Client information is stored on secure servers and protected by industry-standard administrative, technical and physical safeguards. While we take all reasonable precautions, no data transmission over the internet or wireless networks can be fully guaranteed as secure. Clients and principals are expected to collaborate with our team in adhering to privacy and operational protocols; this mutual cooperation helps ensure the highest level of safety and confidentiality throughout the engagement.

16. Website, Imagery and External Links

Our website may contain links to external websites not operated by us; Algoz is not responsible for the privacy practices of third parties, and we encourage you to review their policies. All images and content used on algoz.group are royalty-free, sourced from our web builder's authorised libraries, created by our internal team, or AI-generated to depict services while protecting client privacy.

17. Purpose Limitation and Governance

We use your information solely to deliver and coordinate the services you have requested; we do not sell client data and do not repurpose it for unrelated ends. Our handling of personal data is guided by the

principles of established frameworks, including the GDPR and international information-security good practice, and is overseen by our Data Protection Officer.

18. Governing Law and Jurisdiction

This Policy is governed by and construed in accordance with the laws of the United Arab Emirates, consistent with the governing-law and jurisdiction provisions of the Algoz General Terms & Conditions (clauses 8 and 11.8). Any disputes are subject to the exclusive jurisdiction of the competent courts of Ras Al Khaimah / UAE, with arbitration under the RAKEZ Authority rules as provided in the Terms. Mandatory consumer-protection and data-protection rights of clients resident in the United Kingdom or European Union are unaffected.

19. Updates to This Policy

Algoz may update this Policy as our practices, technology or the law evolve. Updates are communicated via our website, email or invoice and take effect on publication. The version and date are shown in the header.

20. Contact

For any question regarding this Privacy & Data Protection Policy, or to exercise your data rights, contact our Data Protection Officer (DPO) and CEO & Owner, Mr Filipi Rodrigues Oliveira Silva, at dpo@algozgroup.com or privacy@algozgroup.com. Algoz FZ-LLC (trading as Algoz Group), Trade Licence 5033995 | Registration 4071452 | TRN 105119056700001, Compass Building, Al Hulaila, VUNE0977, Ras Al Khaimah, United Arab Emirates.

© 2026 Algoz FZ-LLC, RAKEZ, United Arab Emirates. All rights reserved.