A

ALGOZ GROUP

Cybersecurity & Data Protection

Our commitment to discretion, privacy and security in a digital era

CONFIDENTIAL CLIENT & PARTNER BRIEFING

Algoz FZ-LLC · RAKEZ, United Arab Emirates · algozgroup.com

INTRODUCTION

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. A travel itinerary, a residence, a movement pattern or a single contact detail — in the wrong hands — is no longer a data point. It is exposure.

We therefore treat every record we hold as if a principal's wellbeing could depend on it, because it can. This document sets out, in plain terms, how we protect the information entrusted to us across our platform and our operations — and the principles that govern everyone who works under the Algoz name.

"Discretion is our trade. Protecting the information behind it is our duty."

OUR APPROACH

Five 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 treated as an ongoing practice, not a fixed state.

PLATFORM SECURITY

How we protect your data

Our member, partner and administrative platforms are built on enterprise-grade cloud infrastructure and engineered 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.

Domain	What we do
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 to our systems 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 to limit 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 that recovery never becomes a route to exposure.
Activity logging	Sensitive administrative actions are logged, supporting accountability and the detection of unusual activity.

OPERATIONAL SECURITY

The human factor — where most breaches truly begin

Technology is only as secure as the people who use it. The majority of real-world breaches begin not with a technical flaw but with a person. Because of who our clients are, our teams are deliberately 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 on a strict 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 sensitised to 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.

PRIVACY & GOVERNANCE

Your data, under your control

- **Purpose limitation** — 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.
- **Aligned with recognised principles** — Our handling of personal data is guided by the principles of established frameworks, including the GDPR and international information-security good practice.
- **Client rights & control** — Clients may ask what we hold, request corrections, and request deletion where no legal or operational obligation requires retention.
- **Retention discipline** — Records are kept only as long as a legitimate purpose requires and are then securely retired.

VIGILANCE & READINESS

Prepared, monitored, and continuously improved

Robust prevention is paired with readiness. We monitor for unusual activity across our administrative systems, maintain procedures for responding quickly should an incident ever occur, and review our safeguards on an ongoing basis as the threat landscape changes. 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.

IN SUMMARY

A commitment, not a claim

Algoz Group exists to give discerning clients the freedom to move, host and operate in the world without surrendering their privacy. Our investment in cybersecurity and data protection is a direct extension of that promise. We hold ourselves to it not because a regulation requires it, but because our clients' trust — and sometimes their safety — depends on it.

Speak with us in confidence

For a detailed discussion of how we protect your information, contact your Algoz relationship manager or reach us directly.

privacy@algozgroup.com · algozgroup.com