Acme Corp — Security & Compliance

Investor Due Diligence | Information Security & Risk Management

Data Protection & Privacy

• General Data Protection Regulation (GDPR) compliance implemented across all products and internal processes.

• Data Processing Agreements (DPAs) executed with enterprise customers.

• A designated Data Protection Officer (DPO) oversees privacy governance and compliance.

Security Posture

• Primary data residency on AWS eu-west-1 (Ireland).

• Encryption standards: AES-256 for data at rest; TLS 1.2+ for data in transit.

• Role-based access control (RBAC) with Single Sign-On (SSO) via Google Workspace.

• Daily encrypted backups with a 30-day retention policy.

• Automated vulnerability scanning performed monthly.

• High-severity vulnerabilities patched within 7 days.

Certifications & Audits

• SOC 2 Type II audit currently in progress; external auditor engaged.

• SOC 2 Type II report expected by Q4 2025.

• ISO 27001 certification targeted for 2026.

Sub-processors

• Amazon Web Services (AWS) — infrastructure hosting (eu-west-1).

• Stripe — payment processing.

• Sentry — application monitoring and error tracking.

Incident Response & Business Continuity

• 24/7 on-call incident response rotation in place.

• Mean Time To Resolution (MTTR) target of 2 hours for critical incidents.

• Customers notified within 72 hours for material security incidents.

• Post-incident root cause analysis and remediation actions documented.