GenDiligence

SECURITY AND COMPLIANCE OVERVIEW

DATA ENCRYPTION AND PROTECTION

Q: How is sensitive user data encrypted both in transit and at rest?

- **In-Transit Encryption**: TLS 1.2/1.3 secures data across EC2 instances (servers), APIs, databases, and client connections.
- **At-Rest Encryption**: AES-256 encryption is applied across AWS S3 and exhaustively for all other storage solutions.
- **Key Management**: AWS Key Management Service (KMS) enforces strict key rotation and control.
- **Network Security**: HTTPS is enforced across the entire app using TLS 1.2/1.3 to encrypt data in transit, mitigating the risk of data interception and Man-in-the-Middle (MITM) attacks.

Q: What encryption protocols do you use?

- AES-256 encryption for all stored assets (S3, databases, logs).
- TLS 1.2/1.3 for all data in transit.
- HMAC signatures for secure API and webhook verification.

DATA ACCESS AND AUTHENTICATION

Q: Who has access to data, and how is access controlled?

- **App-Level Role-Based Access Control (RBAC)**: Access is restricted based on user roles to enforce least-privilege principles: Super Admin: Full access to system settings and data. Workspace Admin: Limited to specific workspaces. Standard User: Access to app features without admin privileges.
- **Multi-Factor Authentication (MFA)**: Enforced for all privileged users.
- **Zero-Trust Security Model**: Continuous authentication and access monitoring ensure no implicit trust is granted.
- **IAM Policies and AWS Security Groups**: Access control extends to AWS services using IAM roles and fine-grained permissions.

Q: What authentication mechanisms are in place?

- **For Clients:** 2FA, 3 step: password > email (one-time password) OTP > authenticator app (time-based one-time password) TOTP.
- **For Cloud Resources:** MFA using hardware tokens and software authenticators for AWS access.

DATA STORAGE AND COMPLIANCE

Q: Where is data stored, and how do you ensure compliance?

- **Data Residency:** Stored in AWS London (UK) data centres, compliant with GDPR and UK data protection regulations.
- **Regional Expansion:** Users will soon have the option to select preferred data residency locations for compliance needs.
- **Strict Data Sovereignty Policies:** No data is stored in regions with unfavourable privacy laws.

Q: What regulatory frameworks do you comply with?

- We closely align with GDPR, SOC 2, ISO 27001, DORA (Digital Operational Resilience Act) and AWS best cloud practices.
- Audits with the ICO (Information Commissioner's Office) are pending.
- Data Processing Agreements (DPA) available upon request.

CLIENT DATA HANDLING AND PRIVACY

Q: How is client data processed and protected?

- **Data Upload:** Personal Identifiable Information (PI) is automatically detected and redacted before processing.
- **Data Processing:** Operations (e.g., vectorization, metadata storage) use redacted data only.
- **Data Storage:** Encrypted storage ensures data is segregated by client.
- **Data Deletion**: Clients can trigger a full system purge of their data via the platform interface.
- Client data is not stored, retained, or used to train third-party models.
- All AI processing occurs in-memory, with no persistent storage outside our secure environment.

Q: How does the system ensure personal data is anonymized?

- RSe PI screening system redacts over 50 categories of personal data.
- No client data is ever exposed to third-party AI models.
- Users can request an audit of anonymization processes for transparency.

SECURITY THREAT PROTECTION

Q: How do you protect against cyber threats (DDoS, SQLi, XSS, bot attacks)?

- **AWS WAF (Web Application Firewall):** Blocks SQL injection, XSS, and bot attacks.
- **AWS Shield:** Prevents DDoS attacks by detecting and mitigating malicious traffic.
- **Rate Limiting:** Limits API calls to prevent brute force attacks.
- **Automatic Threat Detection:** AWS GuardDuty monitors network activity for anomalies.

Q: How do you detect and respond to security breaches?

- **Detection:** AWS GuardDuty, Inspector and Security Hub analyse real-time threats and classify risk level. Additionally, routine manual checks of cloud infrastructure activity and logs occur daily.
- **Alert:** If automated AWS managed services raised alarm, these alerts are sent to development team via AWS CloudWatch for immediate investigation.
- **Containment:** Affected systems are immediately isolated to prevent escalation.
- **Investigation:** AWS CloudTrail, VPC Flow and database logs track security incidents.
- **Mitigation:** Patches or configurations are applied securely.
- **Recovery:** System restoration adheres to strict Recovery Time Objectives (RTOs)
- **Breach Reporting:** in the event of a breach, clients are informed within 4 hours. Breach log is updated indicating scope of breach, date, compromised systems and affected resources, resolution, and root cause analysis.

Q: Do you use a SIEM system for monitoring?

- AWS GuardDuty, CloudTrail, and CloudWatch provide SIEM-like monitoring and real-time alerts.

BACKUP AND DISASTER RECOVERY

Q: How often is data backed up?

- Daily full backups with incremental backups throughout the day where possible.
- All backups are secured with industry standard encryption (AES-256).

Q: What is the disaster recovery plan?

- **RTO (Recovery Time Objective):** < 30 minutes in critical failure scenarios.
- **Failover Mechanisms:** Geo-redundant infrastructure ensures high availability.
- **Quarterly Penetration Testing:** Conducted by third-party security consultant.

SECURE SOFTWARE DEVELOPMENT AND COMPLIANCE

Q: How do you ensure secure software development?

- OWASP secure coding standards are enforced.
- Static and dynamic code analysis tools scan for vulnerabilities.
- CI/CD pipelines integrate automated security testing.
- Quarterly penetration testing with third-party ethical hackers.

Q: How do you evaluate third-party vendor security?

- All vendors must comply with ISO 27001, SOC 2, and GDPR.
- Monthly annual security audits and access reviews ensure compliance.
- Data encryption is enforced in transit and at rest when shared externally.

AI AND MODEL SECURITY

Q: How do you prevent AI model hallucinations?

- **Template Answering**: AI returns “Insufficient Information” instead of generating false responses.
- **Knowledge Base Grounding:** AI responses rely only on vetted, user-provided data.
- **Source References:** Every AI-generated answer includes citations for transparency.

Q: How do you protect AI models from adversarial attacks?

- Input validation filters out malicious queries.
- AI models are currently 3rd party (OpenAI)
- TLS 1.2/1.3 encrypts AI API communication.

API AND INTEGRATION SECURITY

Q: How do you secure API integrations?

- JWT (JSON Web Token), API keys, and IAM roles enforce authentication.
- TLS 1.2/1.3 encrypts all data in transit.
- Rate limiting and IP whitelisting prevent abuse.
- Webhooks secured with HMAC signatures prevent tampering.

INSIDER THREAT & EMPLOYEE ACCESS CONTROL

Q: How do you protect against insider threats?

- Least Privilege Access (Zero-Trust Model):
  - Admin actions are logged for full auditability.
- Privileged Access Review:
  - Quarterly audits of all admin accounts & IAM roles.
  - Temporary access granted on an as-needed basis and automatically revoked after 24 hours.
- Segregation of Duties (SoD):
  - Development, security, and operations teams have separate access levels to prevent misuse.

COMPLIANCE AND DATA PROTECTION GUARANTEES

Q: How do you ensure compliance with international regulations?

- We closely align with GDPR, SOC 2, ISO 27001, and DORA (Digital Operational Resilience Act) and are in the process of an ICO (Information Commissioner’s office) audit.
- Data Processing Agreements (DPA) available upon request.
- Legal review and ongoing security audits ensure compliance.

Q: Can clients conduct security audits?

- Yes, clients can request anonymization audits and data processing logs for verification.