PMG Security Protocols for Encryption and Data Isolation

Data is secured in transit and at rest using strong encryption.

- Standards protocol:
  - Data at rest - AES 256-bit encryption
  - Data in transit - SSL/TLS1.2
- Physical protections managed through Amazon Web Services (AWS)
  - https://aws.amazon.com/compliance/data-center/controls/
- Infrastructure encryption through AWS Key Management Service (KMS)
  - Security modules validated under FIPS 140-2

Data at rest:

- Encryption standards include:
  - Disk volumes
  - Database data and logs
  - Data backups
- Disks and databases are dedicated to customer
- Enhanced security:
  - PMG application has an optional enhanced encryption layer for sensitive data elements such as personally identifiable information (PII)

Data in transit:

- Transport Layer Security (TLS) 1.2 over HTTPS for user-to-server communications
- Application-to-database communication over TLS 1.2
- PMG administration over IPsec VPN with multi-factor authentication

Data purging and archiving:

- Configurable workflows can be executed to purge selected data:
  - On a scheduled basis (e.g. after 2 years) or in alignment with corporate business practices
  - On demand to support privacy regulations such as EU's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA)

ABOUT PMG

PMG offers a low- and no-code software platform that empowers businesses to quickly build applications and automation solutions using drag-and-drop designers. Through PMG's workflow orchestration, automated tasks are connected to human activities for end-to-end business process automation. The PMG Platform also provides easily configurable portals and dashboards, as well as rich forms and API integration capabilities.