Data Storage and Compliance Policy - Peterson Solution Hub

1. Data Storage Duration/Retention

All data is stored in Google Cloud Platform (GCP) for a period of 5 years. Clients have the option to delete sensitive data or define how long data is kept in the database before it's automatically deleted or archived.

2. Security Features

Our platform leverages Google Cloud's robust security features, including:

Data Protection:

- **Encryption at Rest and In Transit**: Default encryption of all data using AES-256 algorithm[2]. Managed keys (Google-managed), customer-managed (CMEK) [1], or customer-supplied (CSEK).
- **VPC Service Controls:** Defining perimeters around services to mitigate data exfiltration risks.
- **Confidential Computing:** Using secure enclaves to protect sensitive data during processing (available via Confidential VMs).
- **Server-side encryption**: Data is encrypted after GCP receives it, but before it is written to disk[1].
- **Client-side encryption**: Data can be encrypted before it is sent to GCP, adding an extra layer of security[1].
- Threat detection tools to identify and mitigate potential security risks.

3. Compliance Certifications

Google Cloud services meet strict compliance standards, including:

- **GDPR** (General Data Protection Regulation) compliance; GCP commits to complying with the EU's GDPR, ensuring that all data processing activities adhere to the regulation's requirements.
- **LFPDPPP** (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) GCP supports compliance with Mexico's federal law that regulates how private entities collect, use, and protect personal data.
- **LDPG** (Lei Geral de Proteção de Dados) GCP complies with the Brazilian law by offering data protection features such as data residency options, encryption, audit logging, and strong access controls, while supporting customers in meeting their own legal obligations under the law.

- **CMMC 2.0** (Cybersecurity Maturity Model Certification) compliance, Google Workspace supports CMMC 2.0 compliance by providing advanced security features like data loss prevention, multi-factor authentication, and phishing protection.
- **ISO/IEC 27001** commitment to implementing a robust Information Security Management System (ISMS) that covers risk management, data protection, access control, and continuous security improvement.

4. Importance of Cloud Compliance

Cloud compliance is crucial for protecting sensitive information and mitigating security risks. Our platform ensures that all data handling practices align with industry standards and regulatory requirements.

5. Data Backup Policy

Google Cloud ensures proper backup of production data to safeguard against any issues. Backup policies define schedules for jobs, retention periods, and replication to ensure data integrity and availability[3].

References

[1] Data encryption options | Cloud Storage - Google Cloud

[2] Default encryption at rest | Documentation | Google Cloud

[3] Define backup policies | Backup and DR | Google Cloud