Quick Reference Guide:
Google Cloud & Lei Geral de Proteção de Dados (LGPD)

Brazil's Lei Geral de Proteção de Dados (LGPD) is a data privacy law that governs the processing of personal data by businesses and organizations who are established in Brazil, or who serve users in Brazil, among other cases. Brazil's LGPD includes principles such as accountability, purpose limitation, data minimization, and security and privacy by design -- all important principles that Google stands behind.

Complying with the LGPD may require changes across your business. Here are some key actions you should consider:

- ✓ Ensure your business is educated on LGPD compliance requirements.
- ✓ Evaluate current and planned processing of personal data and determine if the LGPD's requirements are applicable to them.
- ✓ For scenarios where LGPD is applicable - compare your current policies, controls, and processes for managing and protecting personal data with the LGPD's requirements. Identify gaps present and create plans to address them.
- ✓ Monitor development of the Brazilian Data Protection Authority (DPA) and the standards and expectations that the DPA may publish.
- ✓ Ensure your privacy policy, disclosures, and security and consent mechanisms are clear and documented in alignment with LGPD guidance.

We've worked diligently over the last decade to help our customers directly address these requirements, with regular updates to account for new privacy regulations and standards, such as the EU's General Data Protection Regulation (GDPR).

- ✓ We are working to ensure that Google Cloud customers can confidently use our services in alignment with the LGPD when it goes into effect.
- ✓ Google offers products and solutions that customers may utilize as part of their LGPD compliance strategy:
- ✓ Security and privacy features that help you to comply with LGPD and better protect and govern personal data.
- ✓ Services and infrastructure built to ensure the security of data processing and employing appropriate privacy practices.
- ✓ Continuous evolution of our products and capabilities as the regulatory landscape changes.
- ✓ Strong data processing, privacy, and security commitments in our terms for Google Workspace and GCP.

Certifications, audits, and legal commitments

Google Cloud's industry-leading security, third-party audits and certifications, documentation, and legal commitments help support LGPD compliance and meeting industry privacy standards.

ISO /IEC	AICPA SOC	
ISO 27001 **ISO 27017** **ISO 27018** **ISO 27701**	**SOC 2** **SOC 3**	**EU Model Contract Clauses**

LGPD at a glance

- Regulates how businesses and organizations can collect, use, and handle personal data.
- Supplements or replaces existing federal sectoral privacy laws to increase accountability.
- Authorizes fines on businesses and organizations that fail to meet its requirements.
- Allows for the creation of a Data Protection Authority (DPA).
- Imposes rules on the transfer of personal data collected within Brazil.

Google Cloud

For more information, visit **cloud.google.com/security/compliance/lgpd**

Relevant Products and Features

Google Cloud offers security, privacy, and data management products and features that can support LGPD compliance efforts. Customers can operate as data controllers or processors, and our products and features can be used to address needs for both scenarios. Examples of relevant products and features that can be leveraged to protect and manage data in alignment with the LGPD and other privacy regulations include the following:

There are certain products and features that both GCP and Google Workspace customers can leverage:

- Encryption in Transit and at Rest: Google employs several security measures to help ensure the authenticity, integrity, and privacy of our customers' data while it's in transit and at rest.
- Cloud Identity: Unified identity, access, app, and device management (IAM/EMM) platform helps IT and security teams protect data and improve end-user efficiency.
- Access Transparency: When Google Cloud Platform and Google Workspace administrators access your content, Access Transparency gives you near real-time logs of their actions.
- 2-Step Verification reduces the risk of unauthorized access by asking users for additional proof of identity when signing in.
- Data loss prevention rules for protects sensitive information within Google Workspace and Drive from unauthorized sharing; for GCP, Cloud Data Loss Prevention also provides classification and redaction for sensitive data elements like names, credit card numbers, and more.

Google Cloud Platform	
• Identity-Aware Proxy (Cloud IAP) controls access to cloud applications running on Google Cloud Platform. • Cloud Logging and Cloud Monitoring integrate logging, monitoring, alerting, and anomaly detection systems into Google Cloud Platform. • VPC Service Controls provides perimeter protection for services that store highly sensitive data to enable service-level data segmentation. • Access Approval requires Google administrators to seek explicit customer approval before Google can access data. • Organization Policy constraints can be applied at the organization, folder, or project level. The physical location of a new resource can be limited with the Organization Policy Service resource locations constraint.	• Cloud Key Management allows customers to manage encryption keys on Google Cloud., including the ability to apply hardware security modules (HSMs), use external KMS to protect data in Google Cloud and implement customer-managed encryption keys (CMEK). • Security Command Center allows customers to view and monitor an inventory of their cloud assets, scan storage systems for sensitive data, detect common web vulnerabilities, and review access rights from a single, centralized dashboard.

Google Workspace	
• Vault: Retain, search, and export your organization's data from select apps with Vault for Google Workspace Business and Enterprise editions. • Security Center - Google Workspace: Protect your organization with security analytics and best practice recommendations from Google. Included with Google Workspace Enterprise edition. • Data Export - Google Workspace: Easily export and download a copy of your data securely from our Google Workspace services. • Advanced phishing and malware protection protects against suspicious attachments and scripts from untrusted senders, as well as malicious links and images. • Information rights management in Drive allows you to disable downloading, printing, and copying of files from the advanced sharing menu, and to set expiration dates on file access.	• Context-aware access can enforce granular access controls on Google Workspace apps, based on a user's identity and context of the request. • App access control governs access to Google Workspace services using OAuth 2.0. Control which third-party and internal apps can access Google Workspace data, and find more details about any third-party apps already in use. • Data Regions lets you store your covered data in a specific geographic location by using a data region policy • Endpoint device management can make your organization's data more secure across your users' mobile devices, desktops, laptops, and other endpoints.