ManageEngine

Strengthening data protection, visibility,

and trust with

ManageEngine Log360 and AD360

What is the LGPD, and why does it matter?

The Lei Geral de Proteção de Dados (LGPD) is Brazil's comprehensive data protection law that regulates how organizations collect, process, store, and protect personal data. It matters because it holds organizations legally accountable for safeguarding personal information, gives individuals greater control over their data, and imposes significant penalties for non-compliance—making data privacy, security, and governance a business-critical requirement, not just a legal one.

LGPD Data Subject Rights: Right to Delete, Right to Confirm and Access, Right to Correct, Right to Portability, Right to Information, Right to Object, Right to Consent

Key LGPD mandates and challenges

Protect personal data across its life cycle:
Organizations must ensure the confidentiality, integrity, and availability of personal data—often across complex hybrid IT environments.

Ensure accountability and auditability:
The LGPD requires demonstrable controls, access governance, and continuous monitoring—creating challenges for IT and security teams managing siloed tools.

Detect and respond to security incidents:
Rapid identification, investigation, and response to data breaches is critical yet difficult without centralized visibility.

Penalties for non-compliance

Fines of up to 2% of an organization's Brazilian revenue, capped at BRL 50 million per violation

Public disclosure of violations, reputational damage, and potential operational restrictions

How ManageEngine helps with LGPD compliance

ManageEngine delivers a unified defense-in-depth approach to the LGPD through Log360 and AD360, solutions that help organizations protect personal data, enforce access controls, and prove compliance.

How ManageEngine AD360 and Log360 controls help align with Brazil's LGPD requirements

LGPD Requirement	How the Requirement Is Addressed	Product(s)
Protect personal data from unauthorized access (Article 46 – Security Measures)	Audit and monitor access to Active Directory, file servers, and sensitive data repositories to detect unauthorized access	Log360
Prevent data leakage and misuse (Article 6 – Security & Prevention)	Detect anomalous user behavior and risky file copy or access activities using behavior analytics and real-time alerts	Log360
Maintain integrity of personal data (Article 6 – Data Quality)	Leverage file integrity monitoring and receive real-time alerts on unauthorized modifications to critical data	Log360
Ensure availability and recoverability of identity data (Article 49 – Secure Systems)	Back up and rapidly restore Active Directory objects and configurations to maintain identity system resilience	AD360
Enforce least-privilege access (Article 6 – Necessity)	Apply role-based access control, delegated administration, and approval workflows to limit excessive permissions	AD360
Control and monitor privileged accounts (Articles 46 & 50 – Security and Governance)	Track administrative actions, privilege escalations, and changes across Active Directory environments	AD360, Log360

Strengthen authentication mechanisms (Article 6 – Security)	Enforce MFA-enabled self-service password reset and account unlock, along with strong and granular password policies	AD360
Ensure accountability and traceability (Article 6 – Accountability)	Audit user logons, identity changes, and administrative activities with end-to-end traceability	Log360
Detect and respond to security incidents (Article 48 – Incident Notification)	Correlate logs, trigger alerts, investigate incidents, and build incident timelines from a single console	Log360
Demonstrate compliance to regulators (Articles 37 & 50 – Records and Governance)	Generate audit-ready reports and compliance dashboards to support regulatory reviews and audits	AD360, Log360

ManageEngine
AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology andexperiences while giving enterprises full visibility and control over their identity infrastructure. It offersautomated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing,compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-boxintegrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems toenhance security and streamline identity operations. Trusted by leading enterprises across healthcare,finance, education, and government, AD360 simplifies identity management, fortifies security andensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/

⊙ **Personalized demo**   ⬇ **Download**

ManageEngine
Log360

ManageEngine Log360, a unified SIEM solution with integrated DLP and CASB capabilities, helps organizations thwart attacks, monitor security events, and comply with regulatory mandates. The solution comes bundled with a log management component that provides better visibility into network activity, an incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents, an ML-driven UEBA add-on that baselines normal user behaviors, and spots anomalous user activities, and a threat intelligence platform that leverages dynamic threat feeds for security monitoring and helps enterprises stay on top of attacks.

For more information about Log360, visit manageengine.com/log-management/

⊙ **Personalized demo**   ⬇ **Download**