ManageEngine AD360

ManageEngine Log360

The IT admin's guide to LGPD compliance:

Navigating Brazil's data protection law

LGPD Compliance Explained:
What Organizations Processing Brazilian Data Must Know

This document outlines the proof of concept designed to evaluate the feasibility and effectiveness of implementing ManageEngine AD360 within the organization's identity infrastructure. The objective of this PoC is to validate how AD360 enhances identity life cycle automation, governance, risk visibility, and operational efficiency across on-premises, cloud, and hybrid environments.

The PoC demonstrates AD360's ability to streamline onboarding and offboarding processes, reconcile identity discrepancies, enforce access controls, support compliance programs, and integrate with third-party applications. A selected set of test users, systems, and applications will be used to validate real-world scenarios aligned with identity security and governance requirements.

Penalties for violating the LGPD can be severe, including:

- **Fines:** Up to 2% of a company's revenue in Brazil, capped at R$50 million per infraction.
- **Suspension or prohibition** of data processing activities.
- **Reputational damage:** Businesses may also face reputational harm, which can be just as costly in the long run.

The ANPD also has the authority to impose corrective actions, such as mandating a company to cease certain data processing activities or implement remedial measures. As enforcement grows stronger in 2024, companies must remain vigilant and proactive in their compliance efforts.

How ManageEngine's IAM & SIEM support LGPD compliance

- **Centralized identity governance:** ManageEngine IAM solutions centralize user identity and access management, ensuring controlled and accountable access to personal data in line with LGPD principles.
- **Least-privilege and role-based access:** Access to sensitive and personal data is restricted based on job roles, reducing unauthorized access and insider risk.

- **Strong authentication controls:** MFA and adaptive access policies help prevent credential misuse and unauthorized data exposure.
- **Continuous security monitoring:** SIEM capabilities provide real-time monitoring of user activities, system events, and data access across on-premises and cloud environments.
- **Early threat and breach detection:** Correlation of logs and behavioral analytics help identify anomalies, potential data breaches, and suspicious access patterns at an early stage.
- **Incident response and investigation support:** Security teams can quickly investigate incidents, assess impact on personal data, and take corrective action as required by LGPD.
- **Audit trails and compliance reporting:** Detailed logs and prebuilt reports support audit readiness and demonstrate compliance to regulators and supervisory authorities.
- **Alignment with 2024 ANPD Enforcement Expectations:** The combined IAM and SIEM approach supports stronger governance, accountability, and evidence-based compliance aligned with ANPD's enhanced enforcement focus.

How ManageEngine IAM & SIEM controls help align with Brazil's LGPD requirements

LGPD Article & Requirement	Relevant IAM Controls	Relevant SIEM Controls	How ManageEngine's IAM & SIEM Help
Article 6 – Principles of Data Processing			
Personal data must be processed lawfully, securely, transparently, and for legitimate purposes.	Role-based access control (RBAC), least-privilege access, identity life cycle management	User activity monitoring, access log analysis	**AD360:** **RBAC: AD360** ensures that users are granted access to personal data based on their defined roles, enforcing the **principle of least privilege.** **Identity Life Cycle Management: AD360** automates the management of user roles from onboarding to offboarding, ensuring only the right people have access to sensitive data.

			Log360: **Real-time monitoring: Log360** continuously monitors user activity and system logs, correlating access events to ensure data is processed lawfully and securely. **Access log correlation:** Provides full visibility into user access patterns, ensuring compliance with data processing principles.
Articles 17–22 – Data Subject Rights			
Data subjects have rights to access, correct, delete, restrict, and port their personal data.	Centralized identity records, access governance, access logs	Log correlation, historical access reports	**AD360:** **Access logs: AD360** maintains detailed access logs for all user activities, ensuring the organization can fulfill data subject rights requests such as **access, correction, or deletion** of data. **Access governance:** Ensures that personal data is only accessible by authorized individuals, helping fulfill rights to restrict or remove data. **Log360:** **Historical access reports: Log360** provides **correlated access logs** to track who accessed personal data and when, helping organizations respond to requests for data corrections or deletions. **Data subject requests:** Simplifies responding to data subject rights requests by generating detailed reports of data access history.

Article 37 – Records of Processing Activities			
Controllers must maintain records of personal data processing activities.	Identity activity logs, access review and certification reports	Centralized log collection, retention, and compliance reporting	**AD360:** **Identity activity logs: AD360** automatically tracks and records identity activities (who accessed what and when), supporting the requirement for **processing activity records.** **Access review:** Ensures that access permissions are periodically reviewed and certified, maintaining an accurate record of data access and ensuring compliance. **Log360:** **Centralized log collection: Log360** aggregates and retains logs from all systems, ensuring centralized and auditable records of personal data processing activities. **Compliance reporting:** Provides automated reports that document data access and processing activities, supporting audits and compliance checks.
Article 41 – Data Protection Officer (DPO)			
Organizations must appoint a DPO responsible for overseeing LGPD compliance.	Role separation, delegated administrative access	Compliance dashboards, alerts, and reports	**AD360:** **Role separation: AD360** ensures data **protection officers (DPOs)** are assigned specific roles and responsibilities, with access tailored to their compliance and security duties. **Delegated administrative access:** Allows **DPOs** to delegate access and administrative duties while ensuring appropriate separation of duties.

			Log360: **Compliance dashboards: Log360** provides **real-time monitoring** of all user activities through customizable dashboards, giving the DPO visibility into compliance and security events. **Alerting and reporting:** The system generates **real-time alerts** for the DPO if a security breach or compliance issue is detected.
Article 46 – Security Measures			
Technical and administrative measures must be implemented to protect personal data.	MFA, privileged access controls, identity governance	Threat detection, behavioral analytics, alerting	**AD360:** **Multi-factor authentication (MFA): AD360** enforces **MFA** for users accessing sensitive data, enhancing security and ensuring only authorized access. **Privileged access management: AD360** helps enforce strict controls around privileged accounts, limiting high-level access to those who absolutely need it. **Log360:** **Behavioral analytics: Log360** detects **anomalous behavior,** such as unusual login attempts or unauthorized data access, helping identify potential security risks or breaches. **Real-time alerts:** Sends **instant alerts** for any detected suspicious activity, allowing for quick action to protect sensitive data.

Article 48 – Personal Data Breach Notification			
Security incidents involving personal data must be identified and reported.	Identity context for affected users and access paths	Incident detection, investigation workflows, real-time alerts	**AD360:** **Identity context: AD360** captures who accessed personal data and when, providing the context needed to assess the scope and impact of a breach. **Audit trail:** Tracks and maintains an **audit trail** of user activities, enabling a fast response to data breaches and ensuring compliance with breach notification requirements. **Log360:** **Incident detection: Log360** detects and reports **security incidents** in real-time, enabling rapid identification and response to potential data breaches. **Investigation workflows:** Correlates logs across systems to help investigate breaches and analyze the scope of the incident for accurate reporting and breach notifications.
Article 49 – Security Standards and Best Practices			
Organizations must adopt recognized security standards and good practices.	Policy enforcement, periodic access reviews	Continuous monitoring, compliance reporting	**AD360:** **Access control policies: AD360** enforces **security policies** that ensure personal data is only accessible to those with legitimate need, following security best practices. **Periodic access reviews:** Automates **access reviews,** ensuring continuous compliance with security standards.

			Log360: **Continuous monitoring: Log360** continuously monitors the environment, validating adherence to security standards by tracking all access and detecting deviations. **Compliance reporting:** Provides **compliance reports** to demonstrate adherence to recognized security standards and frameworks, helping ensure LGPD compliance.
Article 49 – Security Standards and Best Practices			
Organizations should implement governance frameworks and compliance programs.	Identity governance, access certifications, policy management	Compliance dashboards, audit-ready report	**AD360:** **Identity governance: AD360** centralizes and automates **identity governance,** ensuring that access rights align with organizational policies and compliance frameworks. **Access certifications: AD360** automates **access certification** processes, ensuring that users' access to personal data is continuously validated and complies with LGPD. **Log360:** **Real-time compliance dashboards: Log360** offers customizable dashboards that provide **real-time insights** into security events and compliance metrics, making it easier for organizations to track compliance with LGPD. **Audit-ready reporting: Log360** generates automated reports that are audit-ready, simplifying the documentation of governance and compliance efforts.

ManageEngine AD360

ManageEngine AD360 is a unified identity and access management (IAM) solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, access certification, risk assessment, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports of AD, Exchange Server and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for your IAM needs, including fostering a Zero Trust environment. For more information, please visit https://www.manageengine.com/active-directory-360/.

$ Get Quote Download

ManageEngine Log360

ManageEngine Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/

$ Get Quote Download