ACHIEVE LGPD BRAZIL COMPLIANCE

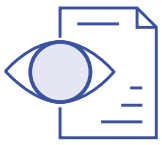
Brazil's Lei Geral de Proteção de Dados (LGPD; "General Data Protection Law"), went into effect in February 2020. The law unifies the many disparate attempts of the Brazilian government to protect personal data that exists both on and offline.

Similar to other internatioanl acts, LGPD applies to organizations that processes Brazilian citizens' personal data, regardless of where that business or organization is located. This means that any organization, including those outside of Brazil, with customers located in Brazil must ensure that their data infrastructure maintains LGPD Brazil compliance. Therefore, we see LGPD Brazil as a benchmark framework for data compliance across the South America continent.

The LGPD requires that data breaches are reported to national authorities

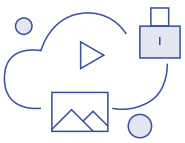
Non-compliance with LGPD may lead to penalties of up to 2 percent of Brazil-sourced revenue for the prior fiscal year. Fines are limited to a maximum of 50 million reals (approx. $9 million USD). Additionally, organizations are obligated to report any data security incidents or breaches to Brazilian national authorities.

HOW GROUND LABS CAN HELP ENSURE LGPD BRAZIL COMPLIANCE

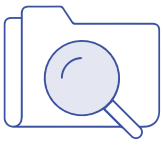


Identify over 300 different types of data and file formats, including data stored in servers, on desktops, email, and databases, on prem and in the cloud.

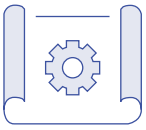
Demonstrate LGPD compliance with custom reporting and analytics available in the Enterprise Recon dashboard.



Search within both structured and unstructured data sources including servers, on desktops, email, and databases, on prem and in the cloud.

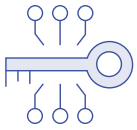


Search for PII across your entire digital infrastructure, with data discovery support for a wide array of platforms including Windows, macOS, Linux, Unix and more.

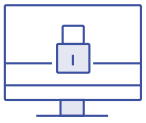


Create LGPD specific reports with an API that allows you to download match results and use them for bespoke reporting, remediation, risk scoring/mapping and custom integration requirements.

Reduce the overall investment required to reach and uphold LGPD compliance, even as regulations change over time.



Execute a proactive approach to data security - as opposed to a reactive approach that relies on damage control post-breach - to build a stronger foundation of trust within your organization.



Easily build custom data types and search platforms to locate and remediate unique data types to address your organization's unique LGPD needs.

Book a complimentary sample data analysis with Ground Labs at
https://go.groundlabs.com/book-a-demo

GROUND LABS

BRAZIL'S LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

What is LGPD?

Think of it as Brazilian GDPR. LGPD is intended to increase privacy and protect the data of Brazilian consumers. As with GDPR as an EU law, LGPD applies to any company that makes its website or services available to Brazilian citizens, including US companies.

LGDP grants Brazilian consumers the right to:

- Confirm the existence of data processing of their personal information
- Access the data that has been collected and correct incomplete, inaccurate, or out-of-date data
- Anonymize, block, or delete unnecessary or excessive data or data that is not being processed in compliance with LGPD
- Transfer data to another service or product provider, by means of an express request
- Delete personal data
- Request information about public and private entities with which the controller has shared data
- Request Information about the possibility of denying consent, the consequences of denial and the right to revoke consent

What does this mean for your company?

If your company is one that must comply with LGPD, you will need to implement policies, procedures, and protocols that:

- Enable Brazilian consumers to exercise their rights
- Ensure consumer requests are fulfilled completely, and timely. To do this effectively, you need to know what personal information you have, where it's located and how it's used in your organisation. This is where sensitive data discovery plays an instrumental role.
- Put safeguards in place to protect consumer personal data. A sensitive data discovery solution can not only help you find the data, but remediate it and report on it so it stays secure.
- Once you have these measures in place, you'll need to continuously monitor your systems to find and secure sensitive data in order to remain compliant and be audit-ready.

How is it similar to GDPR? Different?

At its core, the LGPD emulates GDPR. Just like with GDPR, LGPD applies in Brazil to organisations offering goods & services to persons in Brazil (no matter where the processing occurs). Similarly, consumers can request access and erasure of their personal information. LGPD also calls for appointing of a Data Protection Officer (DP0) to oversee the execution of LGPD regulatory requirements, and maintain ongoing compliance.

Keep in mind, there are a few key differences.

- LGPD grants Brazilian citizens the rights tp erase and access personal data. Compared to GDPR, LGPD imposes shorter deadlines for the controllers to comply with requests (15 days instead of GDPR-imposed 30 days). Data controllers must notify personal data breaches to the National Data Protection Authority and to the affected individuals.
- LGPD requires businesses and organisations to hire a DPO with one notable exception—LGPD does not provide any exceptions for small businesses or small-scale processing
- LGPD calls for stricter restrictions to the cross-border transfer of personal data. Such transfers are allowed to (i) countries deemed to provide an adequate level of data protection, or (2) where in force using standard contractual clauses or other mechanisms approved by the data protection

How Ground Labs can help?

If your organisation has implemented steps to be GDPR-compliant, you have the foundation for LGPD compliance. Ground Labs Enterprise Recon can help you to discover your sensitive data and secure it. The solution is designed to quickly and accurately search across your entire data estate to find more than 200 sensitive data types (i.e., credit cards, passport numbers, driver's licenses) so that you can discover, remediate, and report on sensitive data wherever it resides.

Since we expect more privacy laws in the coming months and years, taking the first step of sensitive data discovery is essential to adhering to what is becoming the new norm in data privacy legislation. As governments advocate for their citizens and residents, it's critical for organisations to increase data privacy and protect personal information for their constituents.