usercentrics

Checklist for the General Data Protection Law (LGPD) for Brazil

October 2021

LGPD Checklist

If your company has customers in Brazil – the largest country in both Latin and South America – or plans expansion there, and you collect or process personal data, you need to comply with the Lei Geral de Proteção de Dados (LGPD), or General Data Protection Law in English.

After presidential review, the LGPD became law on September 18, 2020. Its enforceability was backdated to August 16, 2020. The main goal of the Law was to unify 40 different Brazilian laws that regulate the processing of personal data.

The good news is: if you are already compliant with the GDPR or POPIA, then you have already done a great deal of the work necessary to comply with LGPD.

To help you achieve LGPD compliance, follow these steps:

Steps	Roadmap
1) Identify if your organization needs to comply	• Your business processes the **personal data of people in Brazil**, regardless of where your business is located.
2) Create a comprehensive Privacy Policy	• Ensure it is easy to **find, read and understand** for the average user. • **Inform** about who has access to personal data collected (e.g. from cookies). • **Implementation**: make the information and consent preferences about data processing available in a **Privacy Banner** when users visit your site. A **Consent Management Platform** ensures that you can include all necessary information and obtain required consents.
3) Inform users about their rights	• Inform users about the **nine fundamental rights** that data subjects have under Article 18 of the LGPD, e.g. right to **erasure**, right to **be informed**, and right to **object**.
4) Inform users that you use cookies or other tracking technologies	• Ensure that you **inform users of your intentions** at or before the point you start collecting data. • Particularly inform users about: 1. The specific purpose of the processing; 2. The type and duration of the processing; 3. The identity of the controller and their contact information;

Steps	Roadmap
	4. The shared use of data by the controller, and the purpose; 5. The responsibilities of the agents that will carry out the processing; 6. The data subject's rights, with explicit mention of the rights listed in Art. 18 of the LGPD. • Include this information in your **Privacy Policy**.
5) Explain in the first layer of the privacy banner what your cookies or other web technologies are doing and why	• Inform users about the **purpose of each cookie or web technology separately** to ensure you obtain specific and granular consent for each cookie objective. Users must have the option to **grant or withdraw consent for each purpose**. • It should be stated in the **first layer of the Privacy Banner.**
6) Obtain users' voluntary and informed consent to store cookies on their device(s) and enable refusal of consent or adjustment of preferences in the future	• Necessary where cookies involve the **collection and processing of personal data** from users (e.g. if the information can be linked to a particular individual's identity). • **Consent must be freely given**: Equal presentation and accessibility of "Accept" and "Reject" buttons. Refusing consent must be an equally accessible option. • **Consent must be easy to withdraw**: in the second layer users have to have the option to withdraw their consent. • **Documented**: You have the burden of proof of consent in the case of an audit.
7) Collect and process data only after obtaining valid consent	• Ensure that **no cookies are loaded until users have given consent**. • Once valid consent has been obtained, you can collect and process personal data for the purposes for which you informed users (i.e. using the web technologies to which they consented).
8) Document and store consent received from users	• Comply with documentation obligations to ensure you can verify users' consent in case of complaint or audit by Brazilian data protection authorities.

Steps	Roadmap
9) After opt out, ensure that no further data is collected or forwarded	• Ensure that from the **moment of the objection** on, no further data is collected or forwarded. This includes declined consent for new users or updated consent preferences for existing users.

LGPD Cookie Requirements

Cookies covered by LGPD

Identifiable data is protected by the LGPD. Thus, **cookies and other tracking web technologies** – that collect data that can be associated with a natural person – are subject to privacy compliance obligations under the law. E.g. the information is linked or linkable to a particular user, IP address, device or other specific identifier.

Brazilian Internet Act

The **Brazilian Internet Act** has provisions concerning the **storage, use, disclosure and other treatment of data collected on the Internet.** Also, the **established rights** of privacy, intimacy and consumer rights **apply equally to electronic media,** such as mobile devices and the Internet.

Violations can be subject to civil punishment under the National Data Protection Authority. Fines can be up to 2 percent of annual revenue for the preceding year, up to BRL 50 million, as well as full or partial suspension of data processing activities.

LGPD Checklist

Requirements for LGPD (Brazil)	Is Usercentrics compliant?
Freely given and informed consent is necessary	✓
The purpose has to be provided (first layer of the privacy banner)	✓
The recipient has to be named (second layer of the privacy banner)	✓
Withdrawal of consent has to be possible (second layer of the privacy banner)	✓
Options to grant or decline consent must be equal	✓
Proof that consent has been given must be stored	✓
The option to give or withdraw granular consent for each data processing purpose has to be provided	✓

DISCLAIMER

These statements do not constitute legal advice. They merely serve to support and inform you about the current legal situation. Please consult a qualified lawyer should you have any legal questions.

Would you like to learn more about Consent Management and how the Usercentrics Consent Management Platform helps with achieving **data privacy compliance?**

Get in touch with us