LGPD Frequently Asked Questions

This document is an overview of Brazil’s general personal data protection law (commonly referred to as the LGPD). This document does not provide legal advice, and the information we present may not take into account future changes in the law and regulations. We encourage you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

Introduction

At Salesforce, Trust is always our #1 value and the protection of our customers’ data is paramount. We know that many organizations have questions about Brazil’s general personal data protection law, Lei Geral de Proteção de Dados Pessoais (“LGPD”), and their obligations under the law. To help address those questions about how the LGPD applies to customers’ use of Salesforce’s online services, below are answers to the most frequently asked questions.

What is the LGPD?

Brazil’s LGPD is a comprehensive data protection law that establishes rules for the collection, production, storage, use, transfer, sharing, and erasure of “personal data” (any information relating to an identified or identifiable natural person). The LGPD was modeled after the European Union’s General Data Protection Regulation (“GDPR”), granting certain rights to data subjects in Brazil and requiring organizations that process personal data to meet specific data protection obligations. It went into effect on September 18, 2020. Brazil’s national data protection authority, Autoridade Nacional de Proteção de Dados (“ANPD”), is scheduled to begin administrative enforcement on August 1, 2021.

Does the LGPD affect my organization and what are my main obligations?

The LGPD applies to any organization that processes the personal data of people in Brazil, regardless of where that organization is located. So, if you have customers or clients in Brazil, the LGPD will likely apply to you. Specifically, the LGPD governs:

• Personal data collected or processed in Brazil; and
The LGPD was modeled closely after the GDPR, so it contains similar terms, concepts, and data subject rights. You may have already updated your company’s internal processes and policies for compliance with the European Union’s GDPR. If so, your company’s privacy program is in a great spot, but it’s important to consider the differences between the GDPR and LGPD.

The specific requirements depend on whether your organization is a “controller” or a “processor.” For controllers, the obligations include:

- Processing personal data with a lawful basis, such as consent of the data subject, compliance with a legal or regulatory obligation of the controller, or when necessary to fulfill the legitimate interests of the controller.
- Providing a detailed privacy policy explaining personal data processing and sharing practices and describing data subjects’ rights.
- Providing data subjects with ways to submit requests to access, correct, or delete their personal data, confirm the existence of processing of personal data, revoke consent to process personal data, and bring data to another service provider.
- Providing reasonable security to protect personal data from unauthorized access or acquisition.
- Appointing a Data Protection Officer to receive and respond to privacy complaints, educate your organization about the LGPD’s requirements, and communicate with the ANPD.

For processors, the obligations include:

- Processing personal data only in accordance with the instructions of the controller.
- Deleting personal data about a data subject when instructed to do so by the controller.

We note that the ANPD is expected to issue guidance and regulations that address key areas of the law, such as international data transfers, security incident reporting, and data subject rights. As mentioned above, we encourage you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

How does Salesforce help its customers comply with their LGPD obligations when they use Salesforce’s services?

Compliance with privacy laws is a shared partnership between Salesforce and our customers in their use of our services, and Salesforce is dedicated to helping our customers on their LGPD compliance journey.
Salesforce has implemented procedures and controls designed to ensure that personal data submitted to Salesforce’s online services is processed only as instructed by the customer. Salesforce’s processing of data submitted to our services (“Customer Data”) is governed by our Data Processing Addendum (“DPA”) which is tailored to meet global data privacy law requirements, including those of the LGPD. Our DPA is accessible online and includes, among other things: (i) an obligation for Salesforce to access and use Customer Data only in accordance with our customers' instructions; (ii) a commitment to assist customers in responding to the exercise of rights by individuals whose personal data is processed by customers using Salesforce’s services; (iii) provisions requiring Salesforce personnel to keep information confidential; (iv) obligations regarding Salesforce’s use of sub-processors engaged in the processing of personal data; (v) information about Salesforce's security controls; (vi) security breach notification commitments; and (vii) details regarding Salesforce’s return and deletion of Customer Data.

Does Salesforce’s DPA take LGPD into account?

Yes. Salesforce’s current DPA is tailored to meet global data protection laws and regulations requirements, including those under the LGPD.

Do I need a new DPA in place for the LGPD?

Customers who signed earlier versions of our DPA, or who entered into a Master Subscription Agreement without a DPA, can sign our current DPA at any time. For existing customers with DPAs, the current DPA only adds to what a customer already has and does not replace any comparable or additional rights featured in their existing DPA (see Salesforce’s DPA FAQs for more information).

Salesforce customers’ existing DPAs may already contain the necessary provisions to accommodate the LGPD. However, customers should consult their own legal counsel to make this determination.

How does Salesforce help protect Brazilian Customer Data?

Salesforce has a privacy and security program focused on the processing, disclosure, and protection of Customer Data. Salesforce has implemented technical measures to help secure its services and offers customers configurable controls and tools to protect Customer Data. Salesforce also uses independent third parties to regularly audit, validate, and certify Salesforce’s information technology and privacy measures and controls to ensure we are appropriately protecting Customer Data.

For more details on Salesforce’s privacy and security program, please see the Security, Privacy, and Architecture Documentation for each service, available here.