

LGPD at DocuX

Last updated : November 1, 2021

In August 2018, Brazil approved Law No. 13.709 of 14 August 2018, Lei Geral de Proteção de Dados ('LGPD'), which was further amended by Law No. 13.853 of 8 July 2019. The LGPD came into effect from September 18, 2020. LGPD enforces data protection mechanisms for processing personal data of Brazilian subjects.

The LGPD is very similar to the GDPR. Therefore most, if not all of our existing GDPR practices to address compliance will be applicable.

Privacy is by design at DocuX. We do not need to, and we do not collect and process customers and individual's personal data beyond what is required for providing DocuX Services. DocuX adheres to global regulations and industry practices to maintain privacy and security of customer's data. Effective compliance addresses data privacy and security requirements no matter where your business is located or which industry you belong to. We enhance business value of our services by adhering to necessary standards and policies. Hence, our cloud ecosystem is capable of providing a robust and scalable structure for safe processing of your and your data. Our platform is LGPD ready to help you meet your compliance obligations. As a standard practice, we extend such capabilities and practices not only to our customers in the Brazil but also to all our customers worldwide.

1. KEY PRINCIPLES OF THE LGPD

Article 6 of the LGPD foresees that any activities of processing of personal data should be performed observing the following principles:

- a. **Good faith;**
- b. **Purpose:** processing for legitimate, specific, and explicit purposes informed to the data subject, without any possibility of further processing inconsistent with these purposes;
- c. **adequacy:** compatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing;
- d. **necessity:** limitation of the processing to the minimum necessary to achieve its purposes, covering data that is relevant, proportionate, and non-excessive in relation to the purposes of the data processing;
- e. **free access:** guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data;
- f. **data quality:** guarantee to the data subjects of the accuracy, clarity, relevancy, and updating of the data, in accordance with the need and for achieving the purpose of the processing;
- g. **transparency:** guarantee to the data subjects of clear, precise, and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy;
- h. **security:** use of technical and administrative measures able to protect personal data from unauthorised access and accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination;
- i. **prevention:** adoption of measures to prevent the occurrence of damage in view of the processing of personal data;
- j. **non-discrimination:** impossibility of processing data for discriminatory, unlawful, or abusive purposes; and
- k. **accountability:** proof, by the controller or processor, of adoption of effective measures able to prove observance of and compliance with the personal data protection rules, as well as of the effectiveness of these measures.

2. HOW WE ENSURE COMPLIANCE WITH LGPD?

We pay utmost attention to the data collection, processing, security, storage, and related practices at DocuX, both as data controller and processor. We ensure that all our practices and processes are designed to protect rights of individuals under LGPD. More particularly,

- a. We collect only such data from individuals as is necessary for the purpose for which it is collected. Refer our [Privacy Policy](#) for more information on what data is collected, stored, and processed. At individual's request and subject to our obligations to Customers under relevant [Terms of Service](#), or [Privacy Policy](#) or [DPA](#), we shall respond to the appropriate requests from individuals or customers.
- b. By design, our processes, products, services, programs, projects, are aligned to the privacy principles right the inception. This ensures the culture and practices of privacy and compliance are default principles. We have standard framework of policies and processes in relation to data protection. We have clearly defined responsibilities and defined metrics for monitoring and governing privacy practices.
- c. We conduct periodic audit of our own processes and maintain adequate records of the processing of customers data.
- d. We select and work with only those vendors and Subprocessors who are GDPR and LGPD compliant. We ensure we have related documentation and agreements in place before we engage with them. A list of such Subprocessors can be found [here](#).
- e. We keep updated with the changes in law and business practices and keep our employees well aware of the same by regular training and dissemination of relevant information across organization.
- f. We have appointed a Data Protection Officer.
- g. Our [Terms of Service](#), [Privacy Policy](#) and [DPA](#), are fully recognize and in compliant with the data processing requirements of LGPD.
- h. We ensure all data is encrypted in transit as well as at rest, based on the level of sensitivity and associated risks.
- i. We regularly cleanup our databases to ensure that we have only the relevant, the latest and most accurate information. This cleanup process includes removing terminated and dormant accounts.
