Privacy Rights under the
Brazilian LGPD vs. the GDPR

August 16, 2018

Disclaimer
No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.
# Table of Contents

*Introduction* ........................................................................................................................................... 3

*General* ............................................................................................................................................... 3
  - Background & Timeline ......................................................................................................................... 3
  - What information is covered? ............................................................................................................... 4
  - Who does it apply to? ............................................................................................................................. 4

*Legal Bases for Processing of Personal Data* ....................................................................................... 4

*Rights of Individuals* ............................................................................................................................... 5

*Obligations of Controllers* ..................................................................................................................... 7

*Summary* ............................................................................................................................................... 8
Introduction

Despite being around for several years in the legislative pipeline, the Bill of the first Brazilian General Data Protection Law (‘lei geral e única de proteção de dados pessoais’ - “LGPD”) has drawn immense international attention after passing through Brazil’s Senate. While it is much leaner than the GDPR (approx. 30 pages as compared to GDPR’s 80+ pages), the LGPD is very reminiscent of the EU regulation. Being based on principles of accountability, purpose limitation, data minimization as well as security and privacy by design – it feels familiar to regular GDPR readers’ eyes. However, it also retains some distinguishing national specifics that are discussed in greater detail in the following sections.

General

Background & Timeline

After more than 8 years of debates and preparations, the Brazilian president sanctioned the LGPD Law on August 14, 2018. Therefore, given the 18 months of vacatio legis, the LGPD will become effective in February 2020 - allowing the organizations some time to adapt to its requirements.

The LGPD however was not sanctioned as a whole, but the president vetoed its certain sections - these will therefore not be applicable. The main vetoed section concerns the establishment of a new regulatory body, the National Data Protection Authority (ANPD). Similarly to the EU Member State Data Protection Authorities, the ANPD was meant to provide complementary norms and regulatory oversight. Furthermore, the establishment of National Council for the Protection of Personal Data and Privacy (a Brazilian equivalent of the EU Data Protection Board, former Art. 29 Working Party) was vetoed from the law as well. The president justified his veto by reference to a formal legal obstacle allowing for establishment of new regulatory bodies only through executive power initiative (and not by means of parliament-approved law). There is still support for creation of these agencies, but they will have to be created via a provisional measure (MP), a separate bill or similar legal measure.

The president also vetoed some of the LGPD's foreseen sanctions, such as the suspension of the operation of databases or the treatment activity. The reasoning for his ban was that the sanctions would bring “legal insecurity”. The president also vetoed certain provisions dealing with sharing of data between public authorities and their use by the government – these provisions were mostly focused on requirements of greater transparency for such operations.

What information is covered?

| LGPD – Articles 5(1), (2) | GDPR – Articles 4(1), 9(1) |
**Personal Data**

The LGPD understands personal data as all data related to an identified or identifiable individual.

**Personal Data**

The GDPR defines “personal data” in the same manner. It is worth noting that both the GDPR and the LGPD cover personal data from any person so long as his or her personal data are processed in the respective territory (EU and Brazil).

**Sensitive Personal Data**

The Law introduces a concept of sensitive personal data and links to it restrictive provisions for processing of such data. Sensitive personal data contain all the GDPR’s special categories of data and in addition biometric a genetic data.

**Special Categories of Personal Data**

While the GDPR provides a different name for these categories of personal data, they include (as well as the LGPD’s definition) personal data revealing racial or ethnic origin, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data about natural person’s sex life or sexual orientation.

**Who does it apply to?**

**LGPD – Article 3**

The LGPD has a very broad scope as it will apply to public and private entities (much like the GDPR) in cases when the personal data is (i) processed in the Brazilian territory, or (ii) the purpose of the processing activity is the supply of goods or services to individuals located in the Brazilian territory, or (iii) the personal data relating to the processing operation have been collected in Brazil. Personal data will be deemed to have been collected in national territory if the data subject located therein at the moment of the collection.

**GDPR – Article 3**

The GDPR applies not only to companies located in the European Union, but also to any company that processes the data of data subjects located in the EU where the processing activities are related to (i) the offerings of goods or services to data subjects in the EU, or (ii) the monitoring of their behavior.

The GDPR therefore has a very similarly broad scope of application as compared to the LGPD.

**Legal Bases for Processing of Personal Data**

**LGPD – Article 13**

**GDPR – Article 21**
The LGPD provides in a sum **10 legal bases** for processing of personal data.

These include all of the GDPR legal bases for processing with fairly similar conditions for their use. E.g. the individual’s consent has to be unambiguous, specific and freely given while the controller must be able to prove the was given in accordance with the legal requirements.

The additional legal bases include conduct of research studies, medical procedures, protection of credit and judicial proceedings. Generally, the additional LGPD’s legal bases would fall either under the GDPR’s ‘public interest and official authority’ or ‘legitimate interest’ bases to legal processing.

The GDPR allows for **6 legal bases** on which the data subjects’ personal data processing can be based. These include: consent, contract performance, compliance with controller’s legal obligation, protection of data subject’s (or another individual’s) vital interest, performance of a task in the public interest or in the exercise of official authority, and the legitimate interests of the controller or a third party.

**Rights of Individuals**

<table>
<thead>
<tr>
<th>LGPD – Articles 8-12, 15</th>
<th>GDPR – Articles 14-21</th>
</tr>
</thead>
</table>
| The rights of the data subject (or in the Law’s terminology: the ‘data holder’) can be under the LGPD traced roughly to the same set of rights as stipulated by the GDPR. There are however some specifics. For example, the controller has to fulfill the holder’s right of access to the information within 15 days (half of the period provided by the GDPR). The holder also has a right to choose whether the requested information will be provided to him electronically or in paper form. Finally, the LGDP does not provide much clear guidance on the limitations to this right – as were well-outlined in the GDPR (excessive exploitation of the right, possibility to narrow-down the scope of requested information etc.). We may have to wait for further guidance on this – potentially from a Data Protection Authority, if established. | Data subjects have a wide palette of rights under the GDPR. These include:  
- right to be informed  
- right of access  
- right to rectification  
- right to erasure (‘right to be forgotten’)  
- right to data portability  
- right to object to processing  
- right not to be subject to automated decision-making, including profiling |

With regards to the right to data portability, the LGPD goes a step beyond the GDPR when stipulating that personal data have to be store in a format favoring the exercise of the holder’s right of access, and by extension...
enabling holder’s request for a full electronic copy of his personal data in a format allowing its further processing.
Obligations of Controllers

LGPD – Articles 37-39, 41, 48

**Breach Notification**

The LGPD proposes that in case of a security breach involving personal data, the controller should notify the Data Protection Authority within a reasonable time – in contrast to the GDPR, no specific deadline is set.

Furthermore, it is left up to the DPA determination, whether the holders (data subjects) involved will have to be notified as well.

**Appoint a DPO**

The obligation to appoint a DPO (‘information officer’) is present in the LGPD although it seems to be limited to controller only. It is associated brief outline of the officer’s duties (similar to the GDPR and WP29 overview) and a duty to publish his contact information. It is however currently not clear whether there will be *de minimis* condition for controllers not to appoint a DPO – as such, it is not present in the Law itself.

**Records of Data Processing and DPIAs**

Under the LGPD both the controller and the data processor (‘operator’) are obliged to maintain and keep up-to-date records of personal data that they process.

It is however not entirely clear from the legislation under which circumstances the controller also has to perform the DPIA. It is foreseen to be typically performed for processing of sensitive data, but we will still have to wait for further clarification of all the conditions for the mandatory DPIA performance.

GDPR – Articles 30, 33-35, 37-39

**Breach Notification**

The LGPD proposes that in case of a security breach involving personal data, the controller should notify the Data Protection Authority within a reasonable time – in contrast to the GDPR, no specific deadline is set.

Furthermore, it is left up to the DPA determination, whether the holders (data subjects) involved will have to be notified as well.

**Appoint a DPO**

The obligation to appoint a DPO under the GDPR applies to both controllers and processors that are public authorities, or regularly and systematically monitor data subjects on a large scale, or their core activities are processing of special categories of data/criminal convictions’ data on a large scale. The GDPR therefore clearly imposes this obligation only upon organizations with higher risks associated to their data processing and leaves major portion of controllers and processors out.

**Records of Data Processing and DPIAs**

The GDPR stipulates the obligation for both the controller and processor to record their data processing activities and includes a list of minimum information to be contained there. Also, the conditions for conducting a Data Protection Impact Assessment are very clearly outlined by the GDPR, as well as its necessary content. Furthermore, the WP29 (now EDPB) has further elaborated detailed guidelines to performing the DPIAs.
Summary

It is important to reiterate that while the LGPD is firmly set on its way to becoming effective, there are still uncertainties as to the fate of the data protection supervisory authorities. While the generous vacatio legis period provides for some time to sort out these issues and add more detailed guidance to some of the new obligations, the organizations should seize the opportunity to initiate their compliance preparations in time. After all, it is no wonder that the vacatio legis period is set so long, given the extent of new requirements that the LGPD brings to organizations both in and outside Brazil.

One thing is however clear already: the LGPD drew inspiration from the GDPR also when detailing the administrative sanctions. Non-compliance with the requirements of the LGPD could result in fines amounting to 2% of gross sales (of the company or a group of companies) or a maximum sum of R $ 50,000,000.00 (fifty million reais) per infringement, approximately USD 13 million. For all these reasons, it will pay off to make most of the time before its effective date to fully align the organization’s operations with the new legislative requirements.