



After several postponements, the omnibus Brazilian privacy law, the *Lei Geral de Proteção de Dados* ("LGPD"), entered into application on <u>18 September 2020</u>¹. The LGPD is a new law, providing the rules for the processing of personal data in Brazil by both private sector and public sector actors. Immediately after the final vote deciding the entry date of the LGPD, the Brazilian government also published the <u>decree</u>² establishing the Brazilian data protection authority. Enforcement of the law, or at least to the extent that penalties can be imposed, is poised to start in August 2021, but will also be dependent on yet to be created guidance from the regulator.

The LGPD builds on earlier privacy laws in Brazil and aims to provide a harmonized approach to the processing of personal data in all sectors. The law is clearly inspired by the EU General Data Protection Regulation (GDPR), providing for a similar approach to compliance. Nevertheless, there are key differences that organizations will need to be aware of when complying with the law. Just complying with the GDPR is not sufficient for compliance with the Brazilian LGPD. And as with the GDPR, a tick-box exercise will not prove to be sufficient to comply.

https://g1.globo.com/politica/noticia/2020/09/18/bolsonaro-sanciona-a-lei-geral-de-protecao-de-dados.ghtml

² https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226

This white paper provides you with an overview of the main requirements the LGPD imposes on organizations. It is intended as a general overview and cannot be regarded as legal advice. The information is based on the versions of the law and the decree available in September 2020.

Key Definitions and Elements

Key Definitions

- **Personal Data:** Under the LGPD, personal data is simply "any information relating to an identified or identifiable natural person." Unlike the GDPR, there are no examples on the definition outlined by the law, leaving this open for future interpretation by the Brazilian National Data Protection Authority, the public agency responsible for supervising, implementing and monitoring the compliance with the LGPD.
- Sensitive Personal Data: Much like the GDPR, the definition of sensitive personal data is nearly identiticial in stating that "sensitive personal data pertains to racial or ethnic origin, religious belief, political opinion, affiliation with a trade union or a religious, philosophical or political organization, data concerning health or sex life, genetic or biometric data, when related to a natural person."
- Anonymized Data: Fully outlined under the LGPD, data are considered to be anonymous, when "reasonable and available technical means" at the time of the processing are used to remove the possibility of direct or indirect association with a natural person.
- **Data Subject:** Under the LGPD, a data subject is a "natural person to whom the processed personal data refer."
- **Controller:** Similar to the GDPR, a controller is a "natural person or legal entity, of public or private law, that has the competence to make decisions regarding the processing of personal data."
- **Processor:** Again, similar to the GDPR, a processor is a "natural person or legal entity, of public or private law, that processes personal data in the name of the controller."
- Consent: Similar to the GDPR, consent is a "free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose." Consent shall in principle be in writing, or in another way that demonstrates the data subject's manifestation, shall be distinguishable from other contractual clauses and needs to be properly documented. It may be revoked at any time.

Key Elements

Legal Bases

Article 7 et seq. of the LGPD contain the legal bases for data processing in Brazil. These include compliance with a legal obligation, the processing in a public interest, or to protect health, but also consent and legitimate interest. For the latter two, the burden of proof is on the data controller – this means an organization will have to properly document how and when consent was received, or how the company's interests are balanced against the rights of the individual. For sensitive data, as well as for children's and adolescent's data, additional requirements apply. Two further explicit legal bases included in the LGPD are the use of personal data for the protection of credit, or for research purposes, ideally only until the data can be anonymized.

Individual Rights



A large part of the LGPD is dedicated to the rights of individuals. According to Article 17, each "natural person is assured ownership of her/his personal data, with the fundamental rights of freedom, intimacy and privacy being guaranteed". Everyone therefore has the right to get confirmation that their data are being processed. In addition, the law foresees the rights of access, correction, deletion, and data portability, as well as the possibility to block the processing of contested data. Controllers and processors are furthermore obliged to provide transparent information on their data processing activities.

The deadlines for dealing with individual requests for access are short. A simplified response (which is not defined in the law, but could for example include the statement that no data is held on the individual) needs to be provided immediately. For a more detailed response "that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy" the law foresees 15 days.

Data Breaches

The LGPD includes a requirement to notify security incidents "that may create risk or relevant damage to the data subject" to the ANPD and the individuals themselves. The law does not include any further threshold for the breach notification. Based upon the notification, the requirements of which are included in Article 48 of the law, the DPA may decide on further actions, including mitigation measures.

International Transfers

The LGPD defines international data transfers as "the transfer of personal data to a foreign country or to an international entity of which the country is a member". The rules are further specified in chapter V of the law. As a main rule, transfers may take place to countries that have been declared as adequate by the Brazilian DPA. Adequacy shall be determined based on various criteria, including the applicable data protection regime and the nature of the data, but also alignment of security requirements with the LGPD, and "the existence of judicial and institutional guarantees for respecting the rights of personal data protection". Since the DPA has only just been established, it may take some time before we will see such adequacy decisions.

In the interim, or generally in absence of an adequacy decision for a country or international organisation, data can be transferred on the basis of sufficient guarantees the data will be protected (which includes the use of standard contractual clauses or ad hoc agreements, but also "global corporate rules", which would likely include BCRs and CPBRs). Also transfers for a range of public interests, on the basis of consent or following approval by the DPA are allowed.

The Brazilian DPA will in due course adopt Standard Contractual Clauses that can be used for international transfers. Article 35 LGPD already includes the assessment criteria, which will also be used for ad hoc transfer contracts or intra-group arrangements. These include compliance with "the requirements, conditions and minimum guarantees for the transfer that obey the rights, guarantees and principles of this Law", as well as possible "supplementary information or due diligences performed for verification of the processing operations". The latter implies that also Brazil expects a case-by-case assessment of international data transfers when using a contractual legal basis for the transfer, to ensure compliance is not just a paper tiger.

Accountability

The LGPD stipulates in Article 6(X) that accountability is one of the key principles to which data processing operations by controllers and processors shall be subject. According to the provision, this requires the controller or the processor to be able to demonstrate "the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures". A similar requirement can be found in Chapter IV, Section II, for public authorities. Both requirements are rather similar to the accountability requirement that can be found in the EU GDPR, and also comes with an obligation in Article 37 to maintain a processing activities register. In addition, data controllers can be asked to prepare an impact report for data processing operations, which



should include descriptions of security measures and risk mitigation. When such assessments will be mandatory will be defined by the DPA, which will also determine when a Data Protection Officer will need to be appointed.

A notable section of the LGPD related to accountability can be found in Article 50(1)I, which suggests the elements that organizations can use when building a privacy governance program. These vary from demonstrating "the controller's commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices regarding the protection of personal data" to "establishing adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy". When doing so, organizations will need to take into account relevant risk factors, such as the structure, scale and volume of their operations, as well as the sensitivity of the data. Furthermore, the privacy governance program will need to be integrated in the general governance structure of the organization and be updated on a regular basis.

Oversight

The Brazilian Data Protection Authority, the National Authority for Data Protection or "ANPD", was established by a decree based on the LGPD. The ANPD will fall directly under the presidency of the Republic, and has as main objective "to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person". Furthermore, the ANPD will have technical and decision-making authority, which serves to provide the implementing guidelines under the LGPD, for example to further guide the rules related to international data transfers or to impact and risk assessments. The Board of Directors of the ANPD will consist of five persons, to be nominated and appointed by the President, following approval by the Senate. In addition, the ANPD will have a National Council, that will propose strategic guidelines and make other suggestions on actions to be taken by the regulator. The National Council consists, among others, of representatives of various ministries and political bodies, as well as from civil society, academia and industry.

Enforcement

Controllers and processors that do not meet the requirements of the LGPD may be confronted with serious fines, as of August 2021. Apart from possible warnings, the blocking of processing activities and the publication of the contravention, the law foresees fines of up to 2% of the company's revenue in Brazil in the previous year (either at company, group or conglomerate level), with a maximum of 50 million reais (~ USD 9 million). In more serious situations, that maximum would apply to a daily fine, which could likely be imposed until the contravention is ended. As an additional sanction, the DPA is allowed to publish the committed infraction of the law.

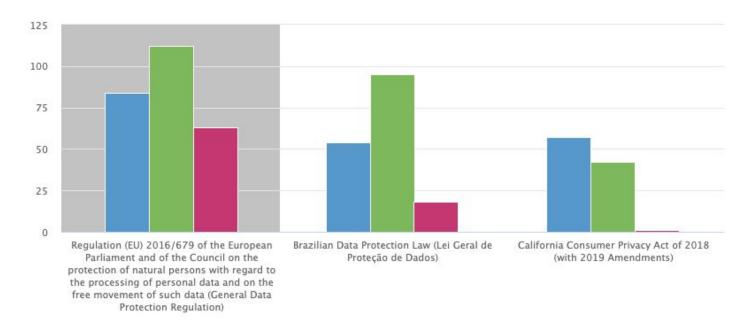
LGPD compared to GDPR and CCPA

As one of the newest data protection laws in the world, the LGPD has close links with other modern laws like the GDPR and the CCPA. Organizations that have already adapted their privacy programs to these laws, will have a clear advantage, even though the requirements are not identical. For none of these laws, compliance is a mere tick-box exercise. Organizations will need to implement appropriate policies and procedures and maintain proper documentation of their data processing practices.

LGPD and GDPR are both omnibus laws covering a wide spectrum of privacy concerns including data transfers, data security and data breaches. Both also have a wide range of legal bases for data processing, apply to the public and the private sector, and have explicit accountability provisions. The CCPA on the contrary has a more limited scope of application, focusing on individual rights in the private sector.

When comparing the three laws based on their mapping to the TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks, it is clear the GDPR is still the law requiring the most from organizations, both when building out a privacy program, and also when implementing requirements and demonstrating compliance. For the LGPD, this is mainly due to the fact that a lot of the accountability requirements will be further defined by the ANPD in forthcoming guidance. This is similar to what happened for CCPA under the Regulations published by the California Attorney-General.

Controls Comparison across TrustArc Framework Pillars



The fact that LGPD has less requirements than the GDPR, does not automatically mean that implementing all GDPR requirements leads to LGPD compliance: Some activities that organizations will need to implement under the LGPD are absent from the GDPR (or CCPA) and vice versa. For example, because the LGPD has more extensive requirements related to the legal bases of processing personal and sensitive personal data, the implementation requirements to comply with the law are more demanding than for GDPR. In addition, the LGPD requires companies to complete a risk assessment at the level of their privacy program, whereas GDPR only asks for risk-assessment at the processing activity level. In turn, the CCPA for the time being has more extensive requirements related to individual rights than the LGPD, although this may change based on further DPA guidance.

The full mapping of the LGPD to the TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks will be published in the TrustArc LGPD Accountability Handbook.

Complying with the LGPD

Although a lot of compliance details remain to be settled by the ANPD and enforcement won't really start until August 2021, organizations would be wise to start the update of their privacy program to get ready for LGPD now that the law has entered into force. It all starts with a better understanding of the law and the various requirements. In June 2020, 53% of respondents indicated in a <u>TrustArc survey</u>³ they had hardly any knowledge about the LGPD.

The next step would be to create a quick inventory of all data processing operations that would be impacted by the LGPD, either because they are taking place in Brazil, or because the organization is offering goods or services to persons in Brazil, or collecting personal data from persons in Brazil. For all these processing operations, a register will need to be created. The template for the register will be determined at a later stage by the ANPD, but will most likely be based upon the Article 30 GDPR Register. Given Brazil's restrictions on international data transfers, it is recommended to in any case document any data transfers taking place, including their legal bases.

Some data processing operations will in due course be subject to mandatory impact assessments. Since the DPA guidelines on this point have yet to be created, these cannot yet be completed. However, organizations can make a first determination of the likely high risk processing operations, and document what risks they see and how these are mitigated. Once the DPA guidelines are available, it will take less time to complete the full risk and impact assessments.

An element of the privacy program that can already be implemented relates to the requirements on individual rights. As mentioned before, Brazil has short deadlines to respond to requests, which means organizations will need to have clear procedures in place to ensure requests are dealt with in a proper and timely manner. Also, they will need to have a good understanding of their data holdings and data flows, to ensure the deadlines can indeed be met.

Further steps in an LGPD compliance project can be made at a later stage, once the ANPD has issued further guidelines.

How TrustArc Can Help

Solutions to Support Compliance with the Brazilian Data Protection Law



Research & Alerts

Stay up to date on the latest developments, guidance and enforcement decisions related to the LGPD, and gain access to comparative maps and charts to prepare your LGPD compliance program.



Law Comparisons

Have full access to the English language version of the LGPD and compare the law with 900+ other data protection and privacy laws.



Privacy Profile

Quickly identify if the LGPD applies to your organization and generate an initial compliance plan.

³ https://info.trustarc.com/Web-Resource-2020-06-16-Global-Privacy-Survey_LP.html





Data Inventory Hub

Create a comprehensive data inventory and data flow maps of business processes to identify the flow of personal data internally and with external processors.



LGPD Assessment

Assess your privacy compliance against the core requirements of the LGPD and provide a prioritized, step-by-step implementation plan for efficiently managing LGPD compliance. This assessment will be regularly reviewed and updated based on the forthcoming ANPD guidance.



Risk Profile

Complete risk and impact assessments of your data processing operations based on standard templates or - once available - the requirements of the ANPD.



Attestor / Accountability Profile

Document the implementation of, and compliance with, organizational policies and procedures for your Brazilian operations.



Operational Templates

Download ready-to-use templates for all elements of your LGPD compliance program.



Individual Rights Manager

Manage data subject requests for request types covered in the LGPD within the brief 15 day window from the date of request submission. This includes the ability to verify consumer identity, collect and process requests, and communicate with data subjects.



Consulting

TrustArc offers a wide range of consulting services to help you build, implement and manage privacy programs to address the LGPD.

About TrustArc

TrustArc automates the creation of end-to-end privacy management programs for global organizations. As the leader in privacy compliance and data protection, TrustArc is the only company to deliver the depth of privacy intelligence that's essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk and build trust. In 2019, TrustArc acquired Nymity to accelerate the development of its next-generation technology-driven privacy platform. For additional information visit www.trustarc.com.



