ABA Manual for Compliance with LGPD

Data Governance and Best Practices - for Advertisers

This guide is provided by the LGPD Marketing WG, led by the ABA Legal Committee and comprised of the Entity Consumer Experience and Media Committees. It was prepared in partnership with Pinheiro Neto Advogados.

SUPPORT

National Council for Advertising Self-Regulation

Table of contents

Introduction

In August 2018, the General Data Protection Act - LGPD was sanctioned in Brazil. Therefore, the 24-month period started running for the new rules to come into force, and advertisers have to bring their activities into compliance with said law by August 2020.

The **ABA Manual for Compliance with LGPD - Data Governance Best Practices** - for Advertisers was prepared in this very context by the Brazilian Association of Advertisers - ABA, through its **LGPD Working Group in Marketing** alongside Pinheiro Neto Advogados. In view of the importance of the theme "data protection" and the imminent effectiveness of the new rules, the **LGPD Working Group in Marketing** was formed by ABA members, led by **ABA Legal Committee**, chaired by **Vanessa Vilar**, General Counsel Marketing LatAm, Corporate & Transactions Brazil at Unilever, also composed of **ABA Consumer Experience Committee** and **Media Committee**, chaired respectively by **Betania Gattai, Latam Consumer engage Centers Manager at Unilever, and Marco Frade, Head of Digital, Media & PR at LG**.

> *"It is essential that companies be structured to choose the most appropriate technologies and processes, according to their respective business models, with a view to complying with the rules and ensuring that information be processed with secrecy and transparency, while preserving brands, respecting persons and the privacy of consumers."*
>
> **Nelcina Tropardi**, President of ABA and Vice President of Sustainability and Corporate Affairs at HEINEKEN

In **partnership with Pinheiro Neto Advogados**, which contributed to the project from start to finish with its expertise on the new law and relying on the **support of the National Self-Regulating Advertising Council - CONAR**, of which ABA is a co-founder, the LGPD Working Group in Marketing assumed in 2019 the responsibility for the Collaborative Protagonism that is part of the ABA 2020 Strategic Plan. The LGPD Working Group in Marketing has delivered an effective contribution to the market via this manual, which disseminates and clarifies the LGPD new rules, while encouraging advertisers to align their Marketing & Communication practices, especially with regard to the direct relation with consumers and their personal data.

“The rules on use, protection and transfer of data in sync with corporate compliance and governance policies will write a new chapter in the history of consumer relations. Companies will have to conform to such rules and pursue innovations in respect of marketing strategies, while consumers will feel more protected and valued and, consequently, will look for products and services that respect such relation.”

Vanessa Vilar, General Counsel Marketing LatAm, Corporate & Transactions Brazil at Unilever

The LGPD applies to all activities involving the processing of consumer personal data in the Brazilian territory. Marketing activities are among the areas most affected by the new regulation, especially the digital marketing environment, as they often involve analyzing and working with data based on consumer habits and behaviors, resulting from the processing of personal data.

“Best practices in corporate governance and compliance are the cornerstone of our business credibility. We need to do our homework, always acting with ethics, integrity and transparency. By doing so, we protect the most important asset of the organization, that is, we safeguard the reputation of brands and gain the trust of our customers.”

Marco Frade, Head of Digital, Media & PR at LG, and Chair of ABA Media Committee

“Complying with LGPD new rules is an important step for organizations in their commitment to integrity and maturity in the relations between brands and consumers, respecting the privacy of customers and valuing their social role in the market.”

Betania Gattai, Latam Consumer engage Centers Manager at Unilever and Chair of the Consumer Experience Committee

ABA Manual for Compliance with LGPD – Data Governance Best Practices - for Advertisers provides, in a practical and didactic way, the terms and concepts that are relevant to understand the law, the bases for data processing established by the new guidelines, and the steps to be followed during the organization’s compliance process.

“In addition to administrative/judicial sanctions and hefty fines, non-compliance with LGPD may result in substantial damage to the image and reputation of organizations. Therefore, the adoption of policies on best practices and corporate governance set forth in this manual is essential not only to comply with the obligations established by LGPD, but also to demonstrate efforts in this respect, while strengthening the relations between advertisers and the market.”

Marcel Leonardi, Counsel at Pinheiro Neto Advogados, ABA’s pro bono partner in drafting this guide

“Complying with the new rules of the Brazilian General Data Protection Act, which will come into force in 2020, means abiding by CONAR’s core values, the freedom of expression and ethics in advertising. We continuously strive to have advertising play a constructive role in favor of consumers.”

João Luiz Faria Netto, President of the National Self-Regulating Advertising Council - CONAR

Aware of the importance of an ethical and responsible relationship with consumers, ABA is committed to pioneering the best practices in Marketing & Communication activities in Brazil. **ABA Manual for Compliance with LGPD - Data Governance Best Practices - for Advertisers** endorses ABA’s position toward Engaging the Marketing Area to Transform Business and Society, and is part of the calendar of actions for commemoration of the Association's 60 years. The creation of this document, along with the birth of LGPD, constitutes a joint achievement for advertisers, consumers and our partners alike.

Yours faithfully,

Sandra Martinelli
Executive President at ABA

About this guide

This guide was prepared by the Brazilian Association of Advertisers (ABA), in partnership with Pinheiro Neto Advogados, emphasizing attention points and relevant aspects of the Brazilian General Data Protection Act to marketing professionals. This guide is for information purposes only.

It neither replaces nor is construed as a legal advice.

LGPD Overview

Law 13,709/2018, known as General Data Protection Act ("LGPD"), will come into force in 2020. It introduces deep changes in the conditions for processing personal data, which includes activities such as collection, storage, use, sharing and erasure of information concerning identified or identifiable individuals.

The long period between the LGPD publication date (August 2018) and its effective date (August 2020) results from the complex actions to be taken for companies to become compliant with the new legal standards.

At the end of 2018, the National Data Protection Authority ("ANPD") was created through Provisional Measure 869/2018.

ANPD's role will be threefold:

(i) Monitoring - it may issue rules and procedures, resolve on the interpretation of the LGPD, and request information related to the processing of personal data;

(ii) Sanction – it will have powers to initiate administrative proceedings in case of LGPD breach, and exclusive jurisdiction to impose the sanctions contemplated by the LGPD; and

(iii) Awareness – it will raise awareness about the LGPD and security measures, providing guidelines for interpretation of the LGPD, setting standards for services and products that facilitate the control of personal data by data subjects, and preparing studies on national and international best practices for protection of personal data, among others.

Important terms and concepts for understanding this Guide

Data subject: means an individual to whom the personal data belongs.

Personal data: means any information concerning an identified or identifiable individual. Identity Card (ID), Individual Taxpayers' Register (CPF), address and birth date are some obvious examples of personal data; however, information such as consumption habits, geographical location, behavioral profile, preferences, purchase history, and other similar information, when related to an identified or identifiable individual, are also considered "personal data." Likewise, information about internet browsing, such as IP address and cookies, among others, are generally deemed personal data whenever the person related to that information can be identified.

Sensitive personal data: means personal data revealing racial or ethnic origin, religious beliefs, political opinions, membership to a trade union or religious, philosophical or political organizations, data on health or sexual life, genetic or biometric data, when related to an individual. The LGPD brings additional requirements and imposes some restrictions on the processing of sensitive data.

Anonymized data and identifiable person: anonymized data is the opposite of personal data, i.e. data that cannot be associated to an individual. It is important to note that although certain data are not directly and explicitly associated to an identified person, they can be deemed personal data (rather than anonymous data) whenever it is possible to associate them to an individual by using the technical means then available.

Reasonable technical means available: The LGPD does not establish specifically the standards, technical means or processes that should be applied for data to be considered sufficiently anonymized. The interpretation of what constitutes "reasonable technical means" in each scenario will be up to the National Data Protection Authority, while the LGPD only indicates that the authority should take into account objective factors such as necessary cost and time, considering available technologies and exclusive use of own means.

Data processing: means any activity which is performed on personal data – from collection to disposal, including mere storage. The LGPD expressly mentions many other examples: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, erasure, assessment or control of information, modification, communication, transfer, dissemination or retrieval.

General principles and best practices

The LGPD establishes some principles that apply to all data processing activities. They are general tenets that guide the understanding, interpretation and application of the LGPD rules, and should always be observed when an activity involves processing of personal data.

Among the most important principles for marketing professionals are:

Principles of Purpose, Adequacy, Necessity

According to these principles, personal data should be collected and processed only for the specific and legitimate purposes informed to the data subject, and which are compatible with the context in which the personal data are provided. The processing activities must be limited to the minimum extent necessary for achieving of the purposes informed to the data subject.

This means that before collecting, storing or otherwise using personal data, it is important to confirm:

i. if the data subject was informed in a clear and specific manner about the means and purposes of the processing - the reason for the processing;

ii. if the processing is compatible with the context in which data have been collected, that is, with the expectations of the data subject when providing his or her data or making them available; and

iii. if the processing is actually necessary to achieve those purposes.

Principles of Transparency and Free Access

It is important to ensure that data subjects have access to clear and easily accessible information about how, by whom and for what purposes data relating to them are being processed.

This can be done in several ways, depending on the nature of the processing. It is recommended that clear, plain, concise and specific language be used in privacy policies or other similar materials, and that data subjects have easy access to any such materials.

In addition, data subjects must be offered an accessible communication channel to clarify their doubts and request information.

Principles of Security and Prevention

When processing personal data, it is important to implement technical and administrative measures to protect them against unauthorized access, loss, destruction, alteration, or undue disclosure, and to prevent any breaches that may result in damage to data subjects. This may include, for example, access controls, encryption techniques, system architecture review, database separation, among others.

Principle of Non-discrimination

Personal data cannot be processed for discriminatory, unlawful or abusive purposes.

Best practices: some examples

Use audiovisual resources. To provide information more appealing and easy to understand, consider using videos, pictures and infographics to illustrate personal data processing operations and activities. Interactive resources may also be interesting.

Clear and plain information is essential. Always try to provide information in a simple and direct way, avoiding ambiguities and quite complex technical terms in your documents and policies.

Be flexible. Whenever possible, leave users free to agree or not to provide their personal data and to manage their privacy choices, preferably through dashboards or similar tools. Do not leave pre-ticked boxes. Do not collect excessive or unnecessary data.

Be available. Implement a communication channel for users to maintain contact in an easy and simple way to clear up doubts about the processing of personal data.

Why is the LGPD important for marketing professionals?

Marketing activities often involve processing and sharing of personal data. Marketing activities are among the areas most affected by the LGPD, especially in the digital marketing context, because (among others) (i) they are strongly based on consumer habits and behaviors, arising from processing of personal data; (ii) data sharing for prospecting and obtaining leads is a common practice; (iii) contact information is used to call the attention of consumers interested in the advertising message and to make communications, and such information can also be considered personal data.

LGPD has an extensive scope of application. The LGPD applies to any personal data processing operation performed in the Brazilian territory or related to individuals located in Brazil at the time data were collected, or intended to offer products or services in Brazil. In addition, it is important to note that LGPD is not restricted to the digital environment. For example, personal data collected through research forms, events, among others, are also subject to the LGPD.

Impacts on operational routines. The rights and obligations contemplated by the LGPD require that several operational routines of companies be reviewed and brought into conformity. For example, the LGPD provides that data subjects may request access to their personal data maintained by the respective companies, as well as review of their personal or consumption profiles created via automated processing of data (i.e. by means of algorithms). Mechanisms must be created to fulfill such requests. Routines must also be established for exclusion of data upon withdrawal of the data subject's consent and where data no longer serve the purpose for which they had been originally collected. The LGPD also determines that data subjects may request the portability of their data to another service or product supplier, which also calls for the implementation of specific operational procedures.

Non-compliance with LGPD is costly. In addition to administrative and judicial sanctions for non-compliance – the fine may come up to 2% of the company's revenues in Brazil, capped at R$ 50 million per infringement – breaching LGPD may result in significant damage to reputation, tarnishing the company's image and brands in the eyes of consumers and customers.

Furthermore, the market itself will demand LGPD compliance, which will translate into an important competitive advantage for choosing business partners, and for companies to establish and maintain business relations. In addition, liabilities arising from breach of obligations established in the LGPD will also be key factors within the context of funding and M&A transactions.

Consent requirements

Personal data may be processed only in ten events established by the LGPD, known as legal bases for processing.

One of the legal bases for processing is the data subject's consent, i.e. agreement to the processing of personal data relating to him or her for a specific purpose.

However, to be considered valid, the consent must be:

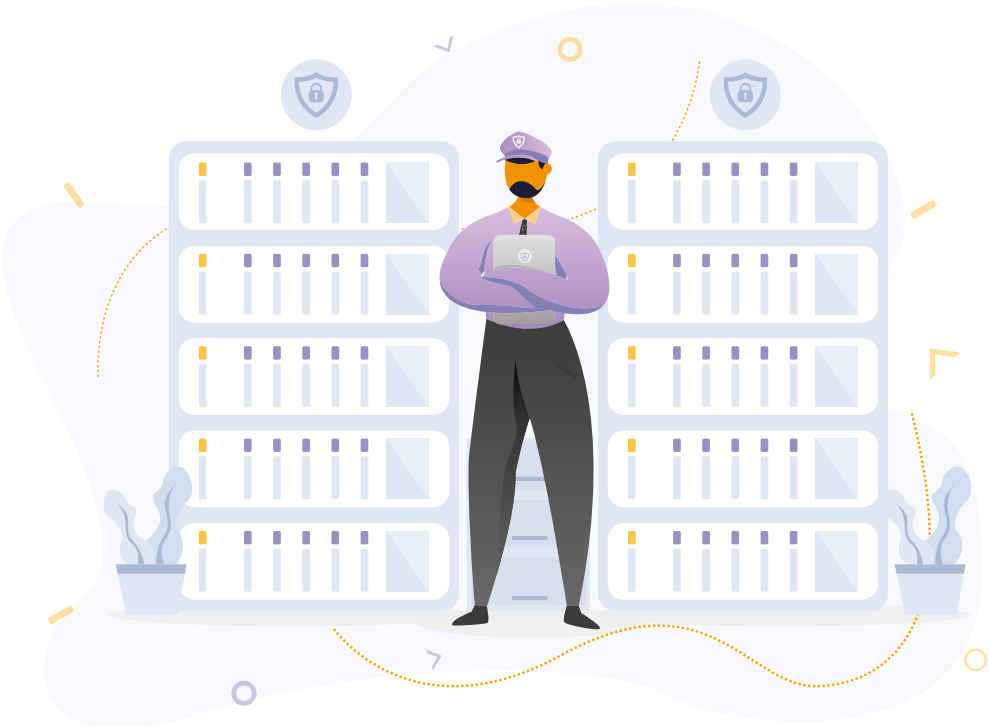
Free: consent must be freely given, i.e. the data subject cannot be compelled to consent to the processing of his or her data.

Informed: the data subject must receive clear, plain and sufficient information to make a conscious decision about the processing of his or her personal data for the purposes mentioned.

Unambiguous: there must be unambiguous demonstration of the consent. This can be done in writing or by other means indicating the data subject's wish, as long as it leaves no doubt (i.e. recording of a phone call). Implied consents, which have not been recorded, or which for any reason cast doubts about the data subject's wish, may be disregarded.

Related to a specific purpose: the data subject must authorize data processing for a specific purpose. Generic or unclear authorizations may be considered void.

In addition to the points outlined above, professionals must also bear in mind that consent may be withdrawn at any time by the data subject.



Can I process data without the consent of the data subject?

The LGPD establishes nine events in which personal data can be processed without the consent of the data subject. The most relevant events to marketing professionals are:

» **Fulfillment of a legal or regulatory obligation:** if a sector-specific regulation or law requires the performance of a certain data processing activity, no authorization must be requested from the data subject. This is the case, for example, of storage online application access logs to comply with record-keeping obligations under the Internet Civil Regulatory Framework, by which companies offering online functionalities must retain records concerning users' activities over the last six months.

» **Performance of a contract** or preliminary procedures relating to a contract executed with the data subject. For example, to deliver a product or service after completion of a purchase, the consumer's full name, address, and other contact information must be known. Such personal data are processed exactly to comply with the contract executed.

» **Regular exercise of rights in the course** of judicial, administrative or arbitral **proceedings**. In other words, storage or other type of processing of personal data for use in judicial proceedings is permitted, without the data subject's authorization. For example, retention of the purchase history and contact data of consumers may be needed in case of post-sale litigation.

» **Fulfillment of legitimate interests** of the company responsible for processing or of legitimate interests of third parties, as long as the data processing does not pose a significant risk to the fundamental rights and freedoms of the data subject. Such points are addressed in detail in the next section, which deals specifically with legitimate interest, but the LGPD requires an assessment of the impact on the data subject's privacy and the assessment-related documentation where legitimate interest is used.

The other events in the LGPD involve data processing for protection of the life or physical integrity of data subjects or of third parties, protection of credit or health, or specific situations of data processing by the public administration or a research body.

With regard to sensitive personal data, not all of the aforesaid legal bases are available - for example, the legitimate interest, the performance of a contract and the protection of credit do not authorize processing of sensitive personal data. In such cases, it is advisable to assess whether processing of sensitive data is actually worthwhile given the need to comply with LGPD additional requirements in such circumstances.

Legitimate interests

The processing of personal data based on legitimate interest is certainly the broadest and most flexible event dealt with in the LGPD. The LGPD does not establish in which situations there is or not a legitimate interest for processing personal data, only indicating that the relevant assessment is needed in specific situations.

A legitimate interest is more likely to exist in situations where data subjects reasonably expect that processing may take place, with small impact on their privacy, or where there is a relevant justification for the processing.

Three elements must be considered:

i. identify the purposes of the processing, and if such purposes are lawful and based on specific situations;

ii. assess whether the data processing is actually needed to achieve those purposes; and

iii. balance the legitimate interest identified against fundamental rights and freedoms of the data subjects affected by such processing.

The LGPD does not contain a pre-established list of what constitutes or not a legitimate interest because this determination will be made in accordance with each specific case. The LGPD mentions as examples the support and promotion of activities of the person responsible for processing the personal data.

In theory, this means that the processing of personal data for purposes related to marketing activities could be performed on the basis of legitimate interest, provided that the requirements and elements indicated above are observed. In practice, a detailed assessment of each marketing activity and of the means and purposes of processing will always be required to confirm whether legitimate interest can be used as a legal basis.

Upon confirmation of the possibility of processing personal data on the basis of legitimate interest, a data protection impact assessment (DPIA) report must be prepared. This report must describe the personal data processing activities that may pose risks to the freedoms and rights of the data subjects, as well as measures, safeguards and mechanisms adopted to mitigate risks. The National Data Protection Authority may request this report.

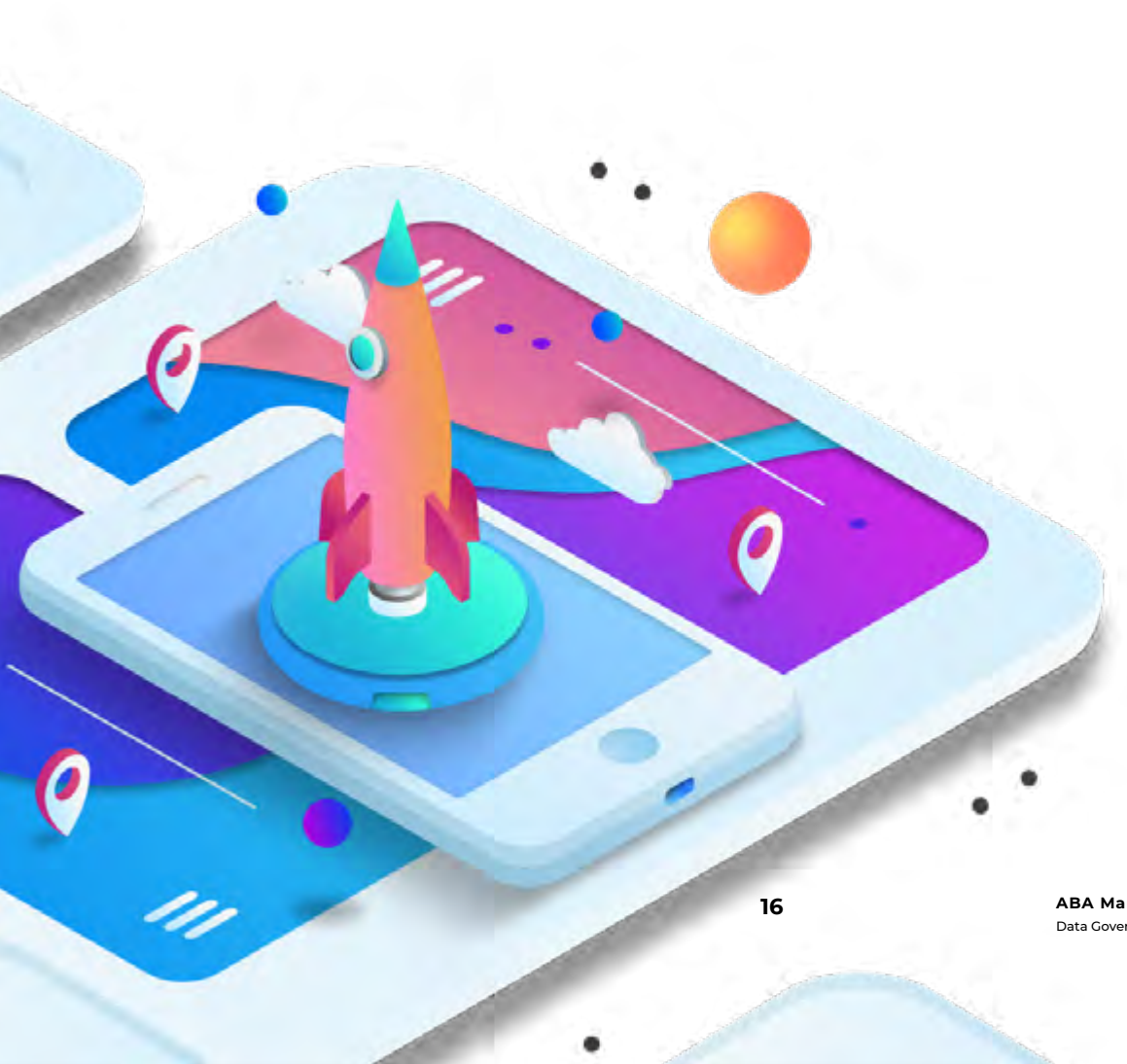
Data of children and teenagers

The personal data of children (under the age of 12) can only be processed with the specific and explicit consent given by one parent or legal guardian. The other events of data processing without consent, as indicated above, do not apply to the processing of children's data.

Conversely, the data of teenagers (between the ages of 12 and 18) can be processed in any of the ten events contemplated by the LGPD (including, for example, for performance of a contract to which the data subject is a party, for compliance with a legal obligation or for fulfillment of a legitimate interest of the person responsible for the processing). Where processing of the data of teenagers is based on consent, it is important to observe the rules dealing with civil capacity under Brazilian law: teenagers between the ages of 12 and 16 may only give consent if represented by one parent (or legal guardian), while teenagers between the ages of 16 and 18 must be assisted by one parent or (legal representative).

In any activity involving the processing of personal data of children or teenagers, information about the processing must be provided in simple, clear and accessible form, taking into account their physical-motor, perceptive, sensorial, intellectual and mental characteristics, with the use of audiovisual resources where appropriate.

Marketing activities should take into consideration whether the processing of personal data of children and teenagers is actually worthwhile given the need to comply with LGPD additional requirements under such circumstances.



Governance

To be aligned and fully compliant with the LGPD, it is strongly recommended that companies adopt privacy governance programs.

Such programs should establish, for example, internal conditions, regimes and procedures for processing personal data, information security rules, technical standards, allocation of responsibilities and obligations between collaborators involved in the processing activities, awareness-raising actions, internal mechanisms for supervision and mitigation of risks, security incident response procedures, among others.

It is also very important that all processes, decisions, efforts and actions related to personal data governance in the company be documented and retained on file for submission to the ANPD, if necessary.

The adoption of policies on best practices and governance not only helps the company comply with the obligations set forth in the LGPD, but also demonstrates its efforts in this regard, in addition to constituting a mitigating circumstance on imposition of penalties for non-compliance with the LGPD.

From a practical viewpoint, a privacy governance program should:

a. demonstrate the company's commitment toward adopting internal procedures and policies to ensure full compliance with rules and best practices on protection of personal data;

b. apply to the whole set of personal data under the company's control, regardless of the way in which they were collected;

c. be consistent with the structure, scale and volume of operations of the company and with the sensitive nature of the processed data;

d. establish adequate policies and safeguards based on a systematic evaluation of impacts and risks to privacy;

e. aim to build a relation of trust with the data subject, through transparent acts where the data subject is assured of mechanisms enabling his or her participation;

f. be aligned with a general governance structure, also establishing and applying internal and external supervision mechanisms;

g. comprise incident response and remediation plans; and

h. be constantly updated on the basis of information obtained from continuous monitoring and periodic evaluations.

Cross-border aspects of the LGPD

The LGPD was strongly inspired by the General Data Protection Regulation – GDPR that came into force in Europe in May 2018. Similarly to GDPR, the LGPD imposes limitations on cross-border transfer of personal data to third countries that do not offer an adequate level of protection for personal data (equivalent to that ensured by the LGPD). Those limitations also apply to cross-border transfers resulting from cloud services and storage in data centers located in other countries.

This system is known as "adequacy" and is intended to prevent personal data protected by the LGPD from being transferred to countries that pose a risk to the privacy of data subjects, without the National Data Protection Authority having to intervene.

For this reason, the National Data Protection Authority should indicate which countries are considered to offer an adequate level of protection for personal data.

The LGPD provides for events in which personal data can be transferred to other countries not actually recognized as adequate by the National Data Protection Authority.

For example, companies making regular cross-border transfers should offer safeguards via contracts (which may be either standard clauses created by the National Data Protection Authority or global corporate rules created by the company and approved by the ANPD).

In other cases, companies may invoke the fulfillment of a legal or regulatory obligation, performance of a contract, or regular exercise of rights to make the cross-border transfer, or may rely on the specific and explicit consent given by the data subject for such transfer.

From a practical perspective, before making any cross-border transfer of personal data - even as a result of the use of cloud services - it is important to carefully examine whether the transfer is permitted and which legal mechanism will be used to justify it.

As the LGPD applies to any company, Brazilian or foreign, intending to process personal data of individuals located in the Brazilian territory, also in the context of the offering of products or services, marketing professionals must bear in mind that foreign business partners will also be subject to the LGPD if they process personal data of data subjects under such conditions.

Infringements and sanctions

LGPD infringements are subject to administrative sanctions, to be imposed by the National Data Protection Authority after an administrative proceeding, without prejudice to other civil or criminal sanctions or penalties.

The two main sanctions comprise:

i. a fine of up to two percent (2%) of the revenues earned by the economic group in Brazil in the preceding year, capped at fifty million Brazilian Reais (R$ 50,000,000.00) per infringement, and

ii. disclosure of the infringement, i.e. the National Data Protection Authority's determination that LGPD infringement be broadly disclosed in the media for public knowledge.

In other words, in addition to financial losses, LGPD infringement may result in significant damage to reputation, tarnishing the image and brands of the company as regards its consumers and customers.

Moreover, the National Data Protection Authority may impose a warning, indicating a deadline for adoption of corrective measures and, in more severe cases, determine temporary blocking or definitive erasure of the personal data to which the infringement refers.

Attention points and frequently asked questions

When does the LGPD not apply?

The LGPD is not applicable to the processing of data of legal entities and of anonymized data, as none of such data is deemed personal data.

By the same token, the LGPD is not applicable to the processing of personal data:

- by an individual solely for private and non-economic purposes;
- solely for journalistic, artistic or academic purposes;
- solely for purposes of public security, national defense, national security, or investigation and prevention of criminal offenses.

Are there personal data requiring more protection than others?

Yes, processing of some categories of personal data poses greater risks of damage to the respective data subjects and, therefore, such personal data are treated by the LGPD as "sensitive data."

The LGPD treats as sensitive data: personal data revealing racial or ethnic origin, religious beliefs, political opinions, membership to a trade union or religious, philosophical or political organizations, data on health or sexual life, genetic or biometric data. Note that the photo of the face of a person may be deemed biometric data.

In considerable part of the cases, marketing professionals must obtain specific consent of the data subjects to process sensitive data.

Can I reuse existing databases to develop new products/services?

Be careful. If the data are collected on the basis of consent for a specific use, without contemplating the development of such products or services, a new consent will probably have to be obtained from the data subjects.

Alternatively, it is necessary to evaluate whether the processing of personal data for development of such new products or services could be justified under one of the other nine hypothesis in which processing of personal data is permitted without consent, and whether such processing meets the LGPD precepts, notably the principles of transparency, purpose, adequacy, and necessity.

Can I use public data unrestrictedly?

Publicly available personal data – whether because they were made publicly available by the data subject, whether because they are on public databases – are still deemed personal data. In such cases, the LGPD authorizes the use of personal data without consent of the data subject, but it is nevertheless necessary to encompass such processing in one of the other available legal bases and to observe all rights of the data subjects and the principles set forth in the LGPD.

In other words, the processing of such publicly available data and the purposes of processing must be transparent, the processing activity must have a legal basis, and the data subject must have access to information regarding which personal data are being processed, how and why, among other applicable obligations.

And anonymous data?

Anonymous data are not deemed personal data and, in principle, are not subject to the LGPD. It is important, however, to confirm whether the data may be really deemed anonymous. Many times, apparently anonymous data may be easily re-identified.

For instance, there are situations in which personal data undergo procedures removing personal identifiers (such as name and individual taxpayers register – CPF), which are replaced with numbers, codes or hashes, thus creating a new database. However, if the owner of such database also has access to the original identified base (for example, when one same company creates different databases, with removal of personal information, so that different business areas can work with them), or may cross-check information from other databases to which it has access to identify the data subjects, then such supposedly anonymized database will be actually deemed only pseudonymized, thus being subject to the LGPD.

What to do in case of a security incident?

Security incidents that may result in risk or damage to the data subjects must be notified to the National Data Protection Authority and to the respective data subjects. The LGPD provides for the minimum information to be included in the notification.

In addition, upon identifying the severity of the incident, the National Data Protection Authority may determine further action, such as full disclosure of the fact in the media and measures to revert or mitigate the incident effects.

Every company must create and keep an incident response plan, defining how to act internally and externally in such situations.

What precautions should be taken about profiling?

First, the data subject has the right to request review of his or her profile (behavioral, consumption, and other profiles) created in an automated manner (for example, through algorithms).

Another attention point about profiling is the difficulty in rendering profiles anonymous. Profiles composed of a great volume of information, though not attributed to a personal identifier (such as name, CPF or ID) sometimes allow for the identification of the person to which they refer by means of inferences. This is so because the greater the volume and the more specific the information concerning a person (though not identified), the smaller the universe of individuals to whom those data may be attributed.

For example, initially one could think that information on the transportation habits of unidentified persons is deemed anonymous information. However, if such habits are detailed to the point of identifying routes, specific routines and addresses, such person may become easily identifiable and his or her profile cannot be deemed anonymous.

Can I be held liable for third-party acts?

Yes. All professionals or companies that take decisions and are directly involved in personal data processing activities in violation of the law will be held jointly and severally liable for redressing damage caused to the data subjects, unless they can evidence that (i) they did not perform the data processing attributed thereto, or (ii) although they performed the personal data processing attributed thereto, the data protection law was not violated, or (iii) the damage was caused through the sole fault of the data subject or of third parties.

For such reasons, it is of paramount importance to work with business partners seeking to become LGPD compliant because any third-party non-compliance, depending on the circumstances, may result in joint and several liability.

The LGPD comes into force in 2020. What about the rules of the Internet Civil Regulatory Framework?

Under the Internet Civil Regulatory Framework (Law 12,965/2014), in effect since June 2014, the following rights are warranted to internet users:

i. non-disclosure of their personal data to third parties, including connection logs and internet application access logs, unless upon the free, prior and informed consent (opt-in), or in the events prescribed by law;

ii. clear and complete information on collection, use, storage, processing and protection of their personal data, which may only be used for purposes that: a) justify the collection of such personal data; b) are not prohibited by law; and c) are set out in the services agreements or terms of use for internet applications;

iii. express consent to collection, use, storage and processing of personal data, which must be given separately from the other contractual clauses, and

iv. definitive exclusion of the personal data provided to a given internet application, at the users' request, upon termination of the relationship between the parties concerned, except for the events of compulsory retention of logs.

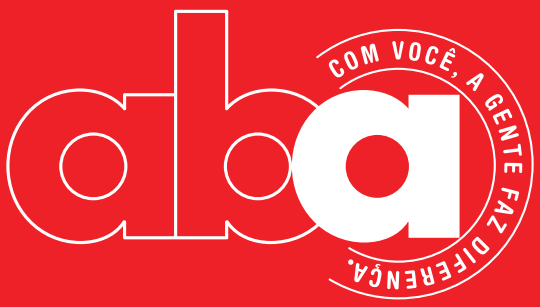
The LGPD, however, regulates all personal data processing activities, including through digital means.

This means that, until the LGPD becomes effective, the rules under the Internet Civil Regulatory Framework continue valid for online marketing activities. Later, the LGPD is expected to replace the rules of the Internet Civil Regulatory Framework so as to avoid conflicts between both laws.

Checklist

Marketing professionals and companies must bring their processes into compliance with the LGPD by August 2020. The first steps involved in this compliance project are described below:

- Map in general all activities involving personal data processing, including collection, storage and sharing processes, verifying as well whether processing of sensitive personal data is in place.
- Define the most appropriate legal bases for data processing, according to the specific purpose (consent, legitimate interest, performance of contract, fulfillment of a legal or regulatory obligation, and so forth).
- Analyze whether there are discrepancies between the legal obligations and the activities of the company, and define the compliance strategies to be adopted.
- Allocate internal responsibilities for implementation of the necessary actions.
- Implement tools that allow the data subjects to exercise their rights warranted by the LGPD.
- Prepare, review, adapt and amend contracts involving processing and/or sharing of personal data, in the relations with users and consumers, and with suppliers and business partners alike.
- Prepare data protection impact assessment reports in cases of processing on the basis of legitimate interest and in other situations in which this is recommendable.
- Prepare and review internal policies, incident response plans, and other documents on privacy and protection of personal data.
- Review and implement information security techniques and procedures, and privacy by design and by default programs.
- Implement a personal data protection governance program.



WFA World Federation of Advertisers

WFA Affiliate
World Federation of Advertisers

wfanet.org
info@wfanet.org
+32 2 502 57 40

twitter @wfamarketers
youtube.com/wfamarketers
linkedin.com/company/wfa

ABA
Brazilian Association of Advertisers

aba.com.br
contato@aba.com.br
+55 11 3283-4588

bit.ly/facebook-aba
twitter.com/abatransformar/
instagram.com/abatransformar/
bit.ly/linkedin-aba