Deutsch-Brasilianische Industrie- und Handelskammer

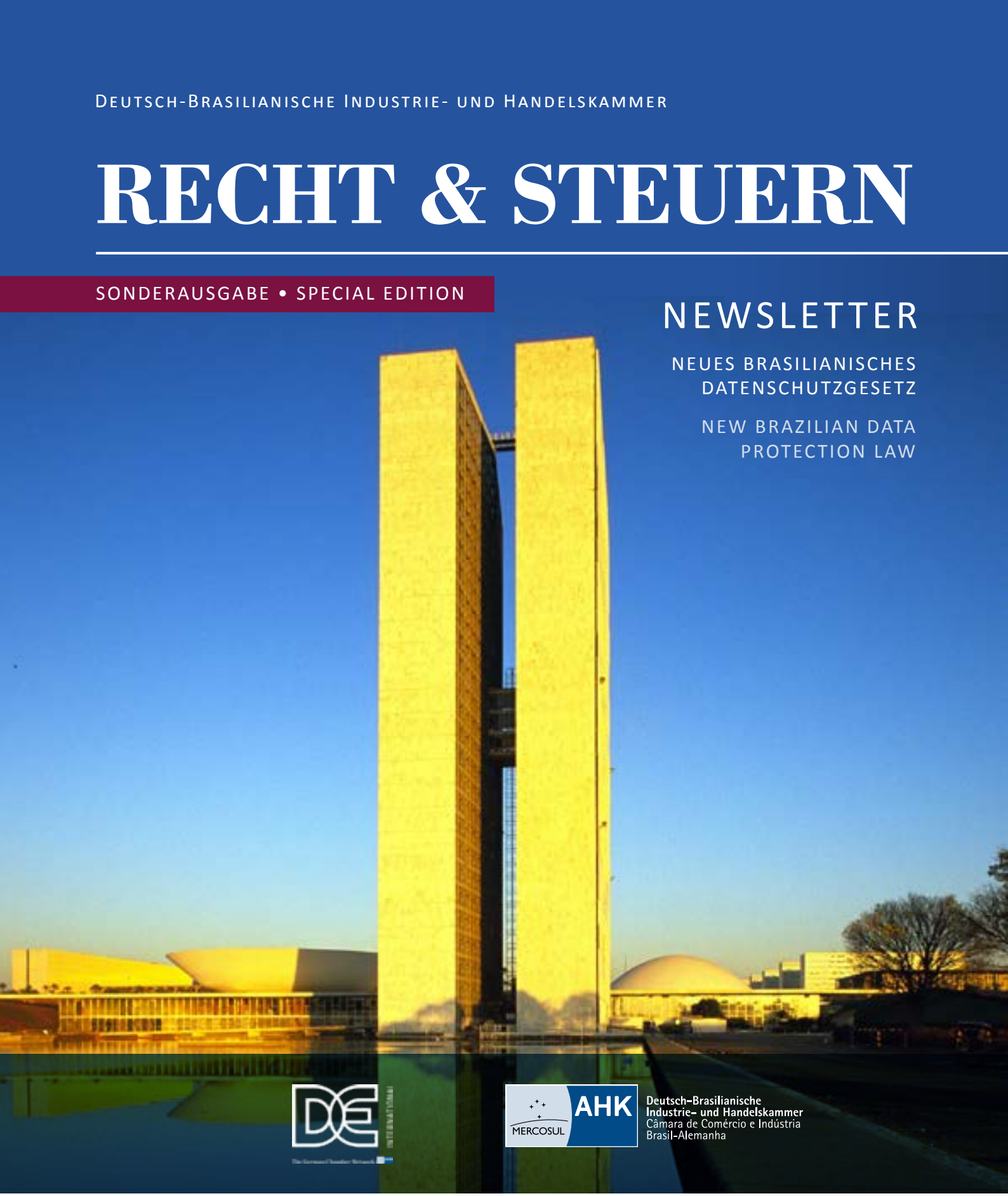
RECHT & STEUERN

SONDERAUSGABE • SPECIAL EDITION

NEWSLETTER

NEUES BRASILIANISCHES DATENSCHUTZGESETZ

NEW BRAZILIAN DATA PROTECTION LAW



Deutsch-Brasilianische Industrie- und Handelskammer
Câmara de Comércio e Indústria Brasil-Alemanha

Zilveti Advogados · Stüssi-Neves Advogados · Sperling Advogados · DEMAREST · LEFOSSE Advogados · Sonia Marques Döbler Advogados · DMKT Débora Motta & Karin Toscano advocacia criminal · Machado Associados

Inhalt • Index

Vorwort • Introduction

Das neue brasilianische Datenschutzgesetz

Am 14. August 2018 wurde das Gesetz 13.709/2018, das allgemeine Datenschutzgesetz (Lei Geral de Proteção de Dados - LGPD), in Brasilien verabschiedet.

Es folgt zeitlich nach dem Inkrafttreten der EU-Datenschutz-Grundverodnung - DSGVO (oder GDPR General Data Protection Regulation), welche bereits einen signifikanten Impakt auf internationale Geschäfte brasilianischer Unternehmen hatte. Das neue brasilianische Datenschutzgesetz folgt in grossen Teilen der europäischen Regelung, weisc aber auch an einigen Stellen von dieser abweichende Regelungen auf. In jedem Fall wird es weitreichende Auswirkungen haben und umfangreiche Massnahmen der Unternehmen zur Implementierung und Compliance mit der neuen Regelung erfordern.

Das Gesetz sollte ursprünglich ab Februar 2020 in Kraft treten. Am 27. Dezember 2018 wurde jedoch die vorläufige Maßnahme MP 869/2018 verabschiedet, die nicht nur das Inkrafttreten auf August 2020 verschiebt, sondern auch das Organ der Nationalen Datenschutzbehörde begründet und regelt.

In Anbetracht der Relevanz des Themas für unsere Unternehmen haben wir diese LGPD-Sonderausgabe mit Artikeln unserer AHK-Partnerkanzleien und Beratungsunternehmen erstellt, um Ihnen die wichtigsten Punkten dieser neuen Gesetzgebung näher zu erläutern.

The new Brazilian Data Protection Law

On August 14 2018, the law 13.709/2018, known as the general data protection law, was passed in Brazil.

It follows the new EU General Data Protection Regulation, in force since May 2018, which already had a significant impact on international business activities of Brazilian companies. The new Brazilian data protection law follows in large part the European regulation, but, in some aspects, deviates from these regulations. In any case, the new regulation will have far-reaching implications and require extensive action by companies to implement and comply with the new rule.

The law was originally intended to enter into force in February 2020. However, on 27 December 2018, provisional measure MP 869/2018 was adopted, which not only postponed the entry into force to August 2020, but also establishes and regulates the body of the National Data Protection Authority.

Given the relevance of the topic to our companies, we have prepared this Special Edition of the Newsletter with articles from our AHK partner law firms and consulting firms to help you better understand the key points of this new legislation.

An Overview about the scope of Brazilian Data Protection Law

Raphael Matos Valentim
Head of Compliance at Zilveti Advogados
rvalentim@zilveti.com.br

Zilveti Advogados
Av. Angélica, 2447 – 18º andar
01227-200 - São Paulo - SP/Brasil
T (+55) 11 3254 5500
F (+55) 11 3254 5501
www.zilveti.com.br

On August 2018, Brazil issued its long-waited Data Protection Law (Law N 13,709/2018), known as LGPD ("Lei Geral de Proteção de Dados"). Besides the noticeable inspiration on the European General Data Protection Law, known as GDPR, the Brazilian law has some unique characteristics and scope, which we will bring light upon on the following paragraphs.

• What kind of "data" is under protection of this law?

By means of the LGPD there are two different types of data to be protected: personal data and sensible data. "Personal data" is defined as any information related to an already identified individual or that is capable of being identified. In its turn, "sensible data" is a kind of personal data with special protection, related to racial or ethnic origin, religious conviction, political ideology, union membership, health or sexual orientation, genetic or biometric data.

The collection and processing of personal data must be supported by a direct consent of the owner, in written or other way that demonstrates the manifestation of the owner. In case of sensible data, it can only be collected by a specific consent of the owner, expressly mentioning the information to be collected and the processing to be done with it. Besides, in case of collection of data of people under 18 years old, it must be authorized by their relatives or legal representatives.

Despite the high level of convergence between the LGPD and the GDPR there is some differences in the normatives, while in GDPR there is a difference from identified data to anonymous data and pseudonymous data, this last one related to the data anonymization process, in Brazil there are only two classes of data: identified and anonymous. The reverse process of anonymization means in the terms of this law as an identification process.

• Who shall be subjected to the LGPD?

Likewise the European law, the LGPD is applicable to any entity regardless of the country it is headquartered or the place where the data are located.

The Brazilian law is mandatory to all private entities that process Brazilian or foreign citizens' personal data if the data is collected or processed in Brazil, or if the company processes its data for the purpose of offering or providing goods or services in Brazil.

For example, a services app hosted in Brazil that collects handful data from the users (Brazilian or foreigners) will be subjected to LGDP. The same situation applies to those who collects only foreigner data to be processes by Brazilian companies, like

Zilveti Advogados
Av. Angélica, 2447 – 18º andar
01227-200 - São Paulo - SP/Brasil
T (+55) 11 3254 5500
F (+55) 11 3254 5501
www.zilveti.com.br

hotels or resorts. In such case, it is important to point out that those companies may also be subject to GDPR, since the data collected is owned by a European citizen.

There are some cross border aspects to be pointed out. The Brazilian entities can only transfer the data to other jurisdiction on the following situations: in case the receiving jurisdiction provides data protection rules similar to the LGPD, in case there is a global corporate police allowing such transfer or in case of specific consent of the owner of the data.

The cross border aspect was one of the most discussed, since it can hamper the exchange of information between the headquarters and Brazilian subsidiary depending on which country the headquarters is located. However, German companies may have no problems, considering the GDPR covers all the data protection rules provided on the LGPD.

• What are the principles of this law?

Similarly to GDPR, the LGPD provides some principles that must be observed while data processing. Those principles focused in data protection, and are complemented by good faith. They are the following: (i) purpose: the purpose of the data processing must be explicit to the owner of the data; (ii) adequacy: the information required must be related to the purpose to be achieved; (iii) necessity: the processing should be limited to the minimum necessary to achieve the purpose explicit to the individual; (iv) free access: the entity must grant free access of the data collected to the owner of the data; (v) data quality: the data should be as correct and updated as its purpose requires; (vi) transparency: the entity should grant to the owner easy access to the information; (vii) security: the entity must grant technical and administrative measures to protect the data for unauthorized access or data leakage; (viii) prevention: the entity must adopt measures to prevent damages that might occur because of the data processing; (ix) non-discrimination: the data must not be used to discriminatory purposes; (x) accountability: the entity must demonstrate the adoption of effective measures to protect the data.

• What the entities must do?

The penalties may range from warnings to fines up to 2% of the company's gross revenue in Brazil in the previous year, limited to 50 million Brazilian Reais per violation. It is important to point out that the penalties are calculated upon Brazilian revenue only. Even foreigner companies may be subject to such penalties.

In order to avoid the risks of being punished by the Brazilian authorities, even if the company is already subject to the GDPR, it is mandatory to take some measures to adjust the internal procedures to attend the Brazilian law.

Among other things, the LGPD requires some activities of the entities related to both data protection and data processing. They are the following:

Zilveti Advogados
Av. Angélica, 2447 – 18º andar
01227-200 - São Paulo - SP/Brasil
T (+55) 11 3254 5500
F (+55) 11 3254 5501
www.zilveti.com.br

- Start a due diligence process in order to identify what kind of data is collected and processed in the company. In case of apps, it is also im portant to check if any information is collected while the user interacts with it;
- Analyze if the entity practices comply with LGPD, and in case they are not in compliance with it, develop measures to regularize it;
- Assign a Data Protection Officer (DPO) responsible for direct communication with the owners of the data also with the authorities. The DPO, together with the entity counsel, should implement data security measures;
- Observe the requirements of data collection, by obtaining the proper authorization to collect and process them accordingly to the principles mentioned;
- Grant data access to the owner, the right data to be corrected, anonymized or deleted upon prior request by the owner;
- Adopt technical and administrative data security measures to protect the data from unauthorized access, alterations or any other harmful acts;
- Develop a privacy policy to prevent data leakage;
- In case any data breach is detected, notifies immediately the authorities and the data owner.

In a few words, besides of each law particularities, they have some similarities that no need for adequacy and allow companies from Brazil and Germany exchange data since the data protection laws are observed.

Charles Wowk
charles.wowk@stussinevessp.com.br
T (+55) 11 3093-6650

Stüssi-Neves Advogados*
Rua Henrique Monteiro, 90 -
10º andar
05423-020 - São Paulo - SP/Brasil
T (+55) 11 3093 6600
F (+55) 11 3097 9130
www.stussi-neves.com

Stüssi-Neves Advogados

Data Processing – definition and situations of use

In modern society, we see that commercial relations give rise to the constant collection of personal data, from basic information regarding individuals, such as name, CPF, e-mail, address and occupation, to more advanced information relating to circle of friends, tastes and interests, physical characteristics, etc.

This enormous quantity of information is stored in various data banks, which are very valuable economically, enabling businessmen and politicians to direct their operational strategies, and determining market, political, behavioral and religious tendencies, among others.

In view of the unbridled use of this information, it was considered necessary to regulate this activity in order to avoid abuse leading to violation of the fundamental rights of individuals, including privacy and intimacy.

In this context, in the wake of international legislation, especially the General Data Protection Regulation of the European Union (known as GDPR), Law 13.709/2018 (LGPD) has been enacted in Brazil, the object of which is to regulate the manner in which companies, government agencies and even individuals process personal data.

For the purposes of the LGPD, processing is any operation relating to personal data, such as those involving the collection, production, reception, classification, utilization, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transference, diffusion or extraction. Personal data is any information relating to an identified or identifiable natural person.

Thus, in short, one can say that personal data processing is any conduct that involves information relating to natural persons.

Data processing is allowed in various situations described in article 7 of the LGPD, as follows:

I - with the consent of the data subject – this is the general rule and is based on the principle that someone can only deal with your personal data with your permission. The consent must be a free, informed and unequivocal statement, whereby the data subject agrees to the processing of his/her personal data for a given purpose, bearing in mind that such consent may be revoked at any moment by a further statement by the data subject. Consent is not required for data manifestly made public by the data subject, but the obligation to respect his/her rights continues.

Stüssi-Neves Advogados*
Rua Henrique Monteiro, 90 -
10º andar
05423-020 - São Paulo - SP/Brasil
T (+55) 11 3093 6600
F (+55) 11 3097 9130
www.stussi-neves.com

Stüssi-Neves Advogados

II - for compliance with a statutory or regulatory obligation by the controller - the controller is defined as the natural person or legal entity responsible for the decisions relating to the processing.

III - by the public authorities, for the processing and shared use of data necessary for the execution of public policies.

IV - for carrying out studies by a research body, on the guarantee, whenever possible, of anonymization of the personal data – anonymization of personal data means, as the very name implies, ensuring that the data subject remains anonymous, in other words, to make it impossible to link that information to that specific individual.

V - when necessary for execution of a contract or preliminary procedures relating to a contract to which the data subject is a party, at the latter's request;

VI - for the regular exercise of rights in judicial, administrative or arbitration proceedings;

VII - for protection of the life or physical safety of the data subject or of a third party;

VIII - for the protection of health, in a procedure carried out by health professionals or sanitary entities;

IX - when necessary to meet the legitimate interests of the controller or of a third party, except in the event of prevalence of fundamental rights and liberties of the data subject which require protection of the personal data; or

X - for the protection of credit.

It should also be observed that, even in cases of processing of personal data to which the public have access, the purpose, good faith and public interest justifying the disclosure must be taken into consideration.

Apart from the general rules relating to the processing of personal data, the LGPD established rules for when the processing refers to sensitive personal data, the latter being defined as any personal data regarding racial or ethnic origin, religious belief, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person.

Sensitive personal data can only be processed in the following events:

I - whenever the data subjects or their legal representative specifically and emphatically consent to such processing, for specific purposes;

II - without the data subjects' consent, whenever they are essential for:

a) compliance with a statutory or regulatory obligation by the controller;

Stüssi-Neves Advogados*
Rua Henrique Monteiro, 90 -
10º andar
05423-020 - São Paulo - SP/Brasil
T (+55) 11 3093 6600
F (+55) 11 3097 9130
www.stussi-neves.com

Stüssi-Neves
Advogados

b) shared processing of data required for the enforcement by the public authorities of public policies set forth in the laws or regulations;

c) carrying out studies by a research body, on the guarantee, whenever possible, of anonymization of the sensitive personal data;

d) the regular exercise of rights in judicial, administrative or arbitration proceedings;

e) protection of the life or of the physical safety of the data subjects or of third parties;

f) protection of health, in a procedure carried out by health professionals or by sanitary entities; or

g) guarantee of the prevention of fraud and of the security of the data subjects, in the processes of identification and certification of records in electronic systems, observing the rights mentioned in article 9 of this Law and except in the event of prevalence of fundamental rights and liberties of the data subjects that require protection of the personal data.

The LGPD further created special rules regarding the processing of personal data of children and adolescents, based on the principle that this should be done always in their best interests.

As a general rule, the processing of personal data of children must be done with the specific and emphatic consent of at least one of the parents or legal guardian.

In exceptional cases, children's personal data may be collected without consent when such collection is necessary to establish contact with the parents or legal guardian, and used only once and without storage, or for their protection, and in no case may data be passed on to a third party without consent.

As regards termination of the processing of data, this will occur in the following circumstances:

I - confirmation that the purpose of the processing has been fulfilled or that the data have ceased to be necessary or relevant to fulfillment of the specific purpose intended;

II - end of processing period;

III - communication by the data subject, including the exercise of his/her right to revoke consent, subject to the public interest; or

IV - determination of the national authorities, when there is a violation of the Law.

On termination of the processing, the personal data will normally be eliminated, retention being authorized for the following purposes:

I - compliance with a statutory or regulatory obligation by the controller;

II - study by a research group, with guaranteed anonymization, whenever possible, of the personal data;

III - transfer to a third party, provided the data processing requirements are observed; or

IV - exclusive use by the controller, access by third parties being prohibited, and provided the data are maintained in anonymity.

These are, in summary, the questions that we should comment on data processing. As we can see, we are facing a new era with a great number of challenges, and it is very important that companies are prepared to comply with the new legislation as soon as it comes into force.

*Author of the publication ***So geht's Ihr Einstieg in Brasilien***
and ***So geht's Arbeitsrecht in Brasilien***

Stüssi-Neves Advogados*
Rua Henrique Monteiro, 90 -
10º andar
05423-020 - São Paulo - SP/Brasil
T (+55) 11 3093 6600
F (+55) 11 3097 9130
www.stussi-neves.com

Stüssi-Neves
Advogados

Glauco Alves Martins
gmartins@sperling.adv.br
T (+55) 11 3704 0780
M (+55) 11 96800 1702

Renata Rizzo
rrizzo@sperling.adv.br
T (+55) 11 3704-0788

Sperling Advogados
Av. Nove de Julho, 4.939, 6º andar
01407-200 – Jardim Paulista
São Paulo/SP
T (+55) 11 3704 0788
http://sperling.adv.br

Provisional Measure No. 869/2018

Last year, the vetoes of the Brazilian President, at that time, Michel Temer, gave rise to some controversy because of the exclusion of the creation of the National Authority of Personal Data Protection ("ANPD") from the provisions of the General Personal Data Protection Act ("LGPD"). In fact, such authority would be crucial for the implementation of the LGPD, specially in respect to the supervision of compliance and to the application of penalties, which created concerns amongst many entities. During the President's last few days at the government, however, the ANPD was finally created, with the enactment of the Provisional Measure no. 869/2018 ("Provisional Measure") in December.

The new regulation sets forth that the ANPD will be linked to the Federal Government, grounded with technical autonomy, and will observe a specific composition, with the nomination of five directors (Board of Directors), a National Council for the Protection of Personal Data and Privacy; Internal Affairs; Ombudsman; Internal Legal Assistance Body; and other administrative and specialized units made necessary for the compliance of LGPD's provisions.

The Provisional Measure also provides ANPD's responsibilities, such as to:

• Ensure the protection of personal data;

• Create regulations and proceedings about the protection of personal data;

• Decide about the interpretation of LGPD;

• Require, at any time, information to controllers and operators that execute processing operations of personal data;

• Create simplified mechanisms to register complaints about the non-compliance with the LGPD;

• Supervise and have exclusive jurisdiction to apply penalties for the non-compliance of the LGPD, by bringing administrative proceedings that will observe the due process of law; and

• Promote measures to improve the education about the law and its application, such as stimulating new studies about the application of the law, promoting services and products that facilitate the protection of personal data, collecting suggestions of public interest about data protection matters, connecting with other authorities to execute its activities (e.g. Department for Consumer Protection and Defense, Brazilian Central Bank, Federal Revenue etc.), among others.

Moreover, other modifications were made in the LGPD by the Provisional Measure. The following are the most relevant:

• ANPD's responsibilities: The ANPD will no longer have powers to directly execute due diligences to supervise the compliance of the LGDP by private and public companies (as mentioned above; however, the powers to supervise and apply penalties were not modified);

• The Data Protection Officer ("DPO"): The DPO does not have to be an individual anymore. This means that companies can be indicated to execute the DPO's functions;

• Processing Operations: The informative duties related to the legal grounds for processing operations were slightly changed. Previously, the data subject would have to be informed when the justification for the data processing operation was based on (i) the fulfilment of a legal or regulatory obligation of the data controller and (ii) on the execution of public policies by the public administration. Pursuant the new regulation, there is no obligation to inform the data subject on those cases anymore.

• Automated decisions: The right to obtain revisions of automated decisions now includes the possibility of having such revision executed by entities and not only by individuals;

• Data related to health: Now it is possible to share data related to health for the execution of the activities of Supplementary Health, even with economical purposes;

• National Security: The Provisional Measure included the possibility of having data related to national security processed by private entities that are controlled by the public administration, which was not possible pursuant the previous text. Also, in the cases of processing data related to national security, it was revoked the provision that allowed the ANPD to request impact reports on personal data, which clearly limits the transparency duties of the public administration;

• Public administration: New provisions were created to regulate the right of the public administration to transfer personal data to private entities. Now it is possible to transfer data in the following situations, when: (i) the private entity has nominated a DPO, (ii) provided by law or by administrative agreements, (iii) the data is public and (iv) the transfer aims at fraud-prevention, security and safety of the data subject.

It is important to note that the Provisional Measure has modified the period in which the LGPD will enter into force. According to the new provisions, the sections related to the creation of the ANPD have entered into force on December 28th, 2018, while all the other sections shall enter into force after a 24-months period, counted from the publication of the LGDP. This means that, except for the provisions related to the ANPD, which are already effective, the LGDP will enter into force only on August of 2020.

Sperling Advogados
Av. Nove de Julho, 4.939, 6º andar
01407-200 – Jardim Paulista
São Paulo/SP
T (+55) 11 3704 0788
http://sperling.adv.br

Sperling Advogados
Av. Nove de Julho, 4.939, 6º andar
01407-200 – Jardim Paulista
São Paulo/SP
T (+55) 11 3704 0788
http://sperling.adv.br

Sperling Advogados

Also, pursuant Brazilian laws, despite having immediate application, to obtain definitive effectiveness, the Provisional Measure must be converted into law by the National Congress within the next 60 days, extendable for the same period.

Although many organizations that are subject to the LGDP should already be revising their data-processing activities, the Provisional Measure gives extra time to get prepared.

Ten things you should know about data subjects' rights in Brazil: getting ready for the Brazilian General Data Protection Law

Tatiana Campello
tcampello@demarest.com.br

Vanessa Ferro
vferro@demarest.com.br

Demarest Advogados*
Av. Pedroso de Moraes, 1201
05419-001 - São Paulo - SP/Brasil
T (+55) 11 3356 1531
F (+55) 11 3356 1700
www.demarest.com.br

DEMAREST

Highly inspired by the European GDPR, the Brazilian General Data Protection Law – GDPL (Law No. 13,709/2018) was published on August 15, 2018 and will come into force in 2020 .

The goal of the GDPL is to protect the fundamental rights of freedom and privacy, foreseen in Brazilian Federal Constitution, as well as the free development of the personhood of individuals. To secure its intent, the law establishes, among other provisions, data subjects' rights that data controllers and processors shall take into account when:

(i) processing personal data in the Brazilian territory (even when personal data is only collected in Brazil); or

(ii) personal data is processed with the purpose of offering goods or services to data subjects located in Brazil.

In case your company is a data processor or data controller and the circumstances set out in items (i) and (ii) above are fulfilled, it will be necessary to adopt the following measures to guarantee data subjects' rights:

1. Provide easy access to information on the processing of personal data in a clear, adequate and ostensive manner, informing: (a) the specific purpose of the processing; (b) the form and duration of processing; (c) identification of the data controller; (d) the controller's contact information; and (e) information about the sharing of personal data with third parties, if any.

2. Specify the parties' liabilities in the data processing agreements, such as establishing reimbursement of expenses in case of damages caused by the other party, since the processing agents have joint responsibility, according to the GDPL.

3. Expressly include in the instruments that will be signed or provided to the data subjects, all of the following rights:

(a) confirmation of the existence of processing;

(b) the possibility and form of access to personal data;

(c) the possibility of correction of incomplete, inaccurate or outdated personal data;

Demarest Advogados*
Av. Pedroso de Moraes, 1201
05419-001 - São Paulo - SP/Brasil
T (+55) 11 3356 1531
F (+55) 11 3356 1700
www.demarest.com.br

DEMAREST

(d) the right of the data subject to anonymization, blocking or deletion of unnecessary, excessive or unapproved personal data in accordance with the provisions of the GDPL;

(e) portability of personal data;

(f) the right to delete personal data processed with the consent of the data subject, with the exception of cases where the data specified in the GDPL are retained.

(g) information regarding the possible sharing of personal data;

(h) information about the possibility of not providing consent and the consequences of the negative (*e.g* discontinuance of service provided); and

(i) the right to revoke the consent given.

4. In case of impossibility of immediate adoption of the measures listed above, the data controller shall provide the data subject with a response, explaining the reasons that prevent the immediate adoption of the measure.

5. Inform in advance any change in the purpose of the processing, where the processing of personal data is carried out on grounds of consent by the data subject.

6. To confirm the existence or access to personal data, upon request of the data subject (a) immediately, in a simplified format; or (b) within a period of 15 days, by means of a clear and complete statement indicating certain information required by law, such as the origin of the data and the purpose of the treatment.

7. To store the personal data in a way that favors the exercise of the right of access (usually the electronic format is the most indicated).

8. To provide a complete electronic copy of the personal data, whenever requested by the data subject, if the processing is based on consent.

9. Review decisions on automated processing, at the request of data subjects, if such decisions affect the interests of the data subject, such as his/her professional profile, credit assessment, among others.

10. Adopt security, technical and administrative measures to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or illicit processing.

We underline that although the data protection authority can authorize international transfer of personal data, as an additional step in order to facilitate the international transfer, data controllers shall, whenever possible, offer and prove guarantees of compliance with data subjects' rights. Specific contractual clauses for certain transfers and standard contractual clauses are examples of such guarantees.

*Author of the publication ***So geht's Tax Incentives in Brasilien***

The Role and Responsibilities of the Data Protection Officer – DPO

The Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* – "LGPD" or "the Law") was approved on 14 August. It sets out protection to privacy and the personal data of Brazilian citizens, establishing a clear data protection framework inspired by the General Data Protection Regulation (GDPR). The LGPD sets forth comprehensive set of rules that promise to reshape how companies, organizations and public authorities collect, use, process and store personal data when carrying out their activities.

One of the main novelties of the LGPD is the obligation imposed on data controllers to appoint a Data Protection Officer ("DPO"), which is defined as the "*person appointed by the controller, who acts as a channel of communication between the controller and the data subjects and the National Data Protection Authority*" (article 5, VIII of the LGPD). Article 41 of the LGPD regulates the roles of the DPO. In Europe, although the former Directive 95/46/EC was silent about this matter, the GDPR imposes on controllers and processors the obligation to appoint a DPO in certain situations.

This is not new, however, for German companies, since the obligation to appoint a DPO was already provided for in the German data protection system even before the GDPR came into effect.

We will discuss below the DPO provisions of the LGPD, which are still subject to further regulation from the National Data Protection Authority (the "Authority"). Considering that the LGPD does not provide much detail about the situations when a DPO will be required, as well as other aspects concerning their roles and responsibilities, we will also rely on the DPO provisions of the GDPR and the Guidelines DPOs adopted by the Article 29 Working Party on 13 December 2016 ("WP29 DPO Guidelines").

When a DPO is required?

The LGPD does not clarify when a DPO is actually required. Pursuant to Paragraph 3 of Article 41, *"the supervisory authority may establish supplementary rules on the definition and duties of the data protection officer,* ***including the cases in which there is no need for appointing such data protection officer, in accordance with the nature and size of the entity or the volume of data processing operations".*** Therefore, the LGPD left to the Authority the task of defining the situations in which a DPO will not be mandatory, and that this decision will be based on: (i) the size of the entity; or (ii) the volume of data processing.

Paulo Lilla
paulo.lilla@lefosse.com
T (+55) 11 3024 – 6347

José Carlos Berardo
zeca.berardo@lefosse.com
T (+55) 11 3024 – 6347

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

The GDPR provides a good guidance by which the Authority could rely upon to regulate the matter in more detail, as Article 37(1) of the GDPR sets forth that the controller and the processor shall designate a data protection officer in any case where:

(i) the processing is carried out by a **public authority;**

(ii) the **"core activities"** of the controller or the processor involve **"regular and systematic monitoring"** on a "large scale; and

(iii) the **"core activities"** of the controller or the processor consist of **"large scale"** processing of sensitive data or personal data relating to **criminal convictions and offences.**

It is clear that companies that process large volumes of data as part of their core activities, especially when dealing with sensitive data, such as hospitals and other health care providers, will be required to appoint a DPO. Likewise, companies that carry out regular and systematic monitoring of individuals on a large scale, including those activities involving tracking and profiling on the internet, are also likely to be required to appoint a DPO. Examples of activities that involve regular and systematic monitoring of data subjects include telecom providers, data-driven marketing, profiling and scoring for purposes of risk assessment (e.g., credit scoring), establishing of insurance premiums, mobile wearables, behavioral advertising, location tracking by mobile apps, among others.

Finally, according with the LGPD, appointing a DPO is an obligation that lies solely on controllers, and not on processors. In any event, it may be advisable that processors also appoint a DPO in certain situations where the processing activities entail enhanced risks.

What are the duties of a DPO?

Pursuant to Paragraph 2 of article 41, the DPO will be responsible for:

(i) **receiving complaints and communications from the data subjects**, provide clarifications and take action;

(ii) r**eceiving notices** from the Authority and act upon them;

(iii) **advising employees and third parties on the practices and measures** taken in relation to data protection; and

(iv) **perform other duties** determined by the controller or in further regulation issued by the Authority.

Therefore, the DPO should be the point of contact for data subjects and for the Authority within the organization, and should also be responsible for monitoring privacy governance and compliance within the organization, which includes collecting information on data processing activities, check compliance measures, as well as inform, advise, provide training and issue recommendations.

The duty to be a contact point for both data subjects and the Authority is in line with the obligation that the identity and contact data of the DPO must be publicly, clearly and objectively disclosed, preferably in the controllers' website, as provided by Paragraph 1 of article 41.

Articles 37, 38 and 39 of the GDPR also provide further guidance that could be relied upon by the Brazilian DPO in future regulations on the matter, as it is recommended that DPOs be involved in all issues related to the protection of personal data, including situations where data breach or other security incidents occur.

In any case, as per the WP29 DPO Guidelines, DPOs should not have decision-making authority. All decisions concerning privacy and data protection matters must be taken by the management of the company, although a DPO can and should provide advice and recommendations on these matters. In this regard, if management decides not to follow the DPO's advice on a certain issue, the WP29 recommends documenting the reasons for not doing so.

In addition, DPOs must be allowed to act independently, which means that a DPOs *"must not be instructed"* on how to perform their tasks, *i.e.*, must not be bound by instructions from superiors with regard to the performance of their tasks.

One doubt that always come up concerns what is the role of a DPO in the preparation of a Data Protection Impact Assessment ("DPIA"). Pursuant to the GDPR, a DPIA is required whenever data processing is likely to result in a high risk to the rights and freedoms of individuals and at least in the following cases: (i) a systematic and extensive evaluation of the personal aspects of an individual, including profiling; (ii) processing of sensitive data on a large scale; and (iii) systematic monitoring of public areas on a large scale. Similarly, article 5, XVII, of the LGPD defines a DPIA as the documentation of the controller containing a description of data processing activities that may result in risks to civil liberties and fundamental rights of individuals, including measures, safeguards and mechanisms to mitigate those risks.

Pursuant to Article 35(1) of the GDPR, it is the task of the controller, not of the DPO, to carry out, when necessary, a DPIA. However, the WP29 DPO Guidelines clarifies that a DPO can play an important and useful role in assisting the controller in this task. This understanding is in line with Article 35(2) of the GDPR, which specifically requires that "*the controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment"*. Article 39(1)(c), in turn, sets forth that one of the tasks of the DPO is *"to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35".*

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

Who should be appointed as DPO?

The initial wording of article 5, VIII, of the LGPD indicated that only individuals could be appointed as DPO. However, the Provisional Measure No. 869/18, which amended the LGPD, excluded the word "individual" in order to make sure that any person could be appointed as DPO, such as companies, organizations, advisers, committees, etc.

Therefore, from the current wording of the LGPD it is clear that both internal employees and external firms or third party advisors can serve as DPOs. When appointing an employee or any other individual within the company, it is important to make sure that ensure that any other tasks and duties of this person do not result in a conflict of interests with the DPO position. The WP29 DPO Guidelines clarifies that this entails in particular that "the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing". Examples of conflicting positions within the organisation may include "senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments)", as well as other lower positions that entails determining the purposes and the means of the processing.

Is a DPO liable for failures to comply with the law?

The LGPD makes clear that liability for infringement lies with the controller, since it is the one who defines the purposes and means of data processing activities. In exceptional circumstances, the data processor may be jointly and severally liable in case it fails to comply with the LGPD or in case it has not observed the lawful instructions of the controller. Therefore, the LGPD does not specifically impose on DPOs any liability in case of non-compliance with the data protection rules.

The GDPR also makes sure that controllers and processors are responsible for complying with the law. In this regard, the WP29 clarifies that DPOs are not "personally responsible" for "case[s] of non-compliance with the GDPR." The WP29 also points out that "[t]he GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organizational measures'" to ensure compliance.

In any event, controllers may have a claim or a right of recourse against the DPO in case of fault or willful misconduct when conducting his or her activities. For instance, failure to recognize a risk or an erroneous advice could expose the DPO to indemnification or damages claims. Therefore, companies appointing internal DPOs should consider contracting an E&O policy for the DPO. Third party DPO providers should also consider professional insurance in this regard.

Final remarks

Based on the above, the DPO rules provided for by the LGPD will entail in great deal of work and preparation for companies. Even though the new law will come into effect only in the second semester of the 2020, it is highly advisable that companies appoint a DPO as early as possible in order to have this person involved in all actions necessary to adapt the company's policies, governance and infrastructure to the strict requirements of the LGPD.

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

Sonia Marques Döbler
sonia@dobler.com.br

Fabiana Nitta
fabiana.nitta@dobler.com.br

Daniel Ricardo dos Santos Andrade
daniel.andrade@dobler.com.br

Sonia Marques Döbler Advogados*
Rua Dona Maria Paula, 123
19º andar - Edifício Main Offices
01319-001 - São Paulo - SP/Brasil
T (+55) 11 3105 7823
www.dobler.com.br

SONIA MARQUES DÖBLER Advogados

Obligations of the companies towards the treatment of private data

The market watched with great expectation the recent approval of the Brazilian General Data Protection Law (Law No. 13,709, from 14/Aug/18), or simply "LGPD" - with obvious inspiration in the European General Data Protection Regulation ("GDPR") -, which makes the law friendlier to foreign investors and businessmen who work in Brazil.

Basically, the LGPD governs the **treatment of private data**, which is defined as "every operation made with private data, like the ones that handle the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of the information, modification, communication, transfer, dissemination or extraction" (Art. 5, "x").

With such a broad concept, every company, no matter its size, turns out to treat some kind of personal data, including, among others, the data of its own employees, clients, suppliers, etc.

However, what can be seen is that they are not fully aware of their obligations and, despite the fact that the LGPD will be effective only in August/2020, they are advised to promptly start the actions to be compliant with the new rules, not only because it is expected to be an extensive and time-consuming work, but also in light of the penalties in the event of violation of the LGPD, which are severe, including fines that may range from 2% of the company's turnover until BRL50 million (per breach).

And it is precisely the planning and execution of such adjustments that are causing many doubts and uncertainties. Although the answer is not so simple - as it can vary according to numerous factors such as the business type, the company's size, the way the data is obtained, how the internal traffic of such data is given, etc. - some common points can be highlighted and some obligations should be observed by all, indistinctly.

The purpose of this article is to briefly give a general idea of how this type of work of adequacy should be done.

1. Due diligence of the private data (mapping)

Many times, the company may think that it does not collect any relevant information or may not realize the broadness of the data that it stores/handles. Therefore, the recommendation is to start with a due diligence of the data that it treats, developing a visual map of all the information collected and stored by the company.

This aims a identifying: **(i)** the nature of the data (ex.: personal, sensitive, anonymized, child/adolescent, public); **(ii)** for which purpose the data is used; **(iii)** the departments that make use of the data; **(iv)** the means in which the data is stored (ex.: physical, digital); and **(v)** the individuals - inside and outside the organization - who have access to the data.

A good starting point is to create a multidisciplinary team with legal knowledge, IT skills and processes expertise to assume this task.

The company must also appoint the so-called Data Protection Officer - DPO (natural person or legal entity) to assume the activities established in the LGPD and shall publicly disclose the DPO's information preferably in the company's website.

2. Management of the private data and creation of Good Governance Policies

Having the picture of the relevant information handled by the corporation and the indication of the departments that have access to the private data, it is time to eliminate the information that is not strictly necessary for the development of the business, as well as to implement standard procedures and internal flows to treat the private data (ex. policies, templates, conduct codes, etc.) and to correct the situations that are not fully in line with the LGPD.

Within the concept of the Privacy by Design – adopted by the LGPD - the settings referring to privacy must have protection and security as a general rule and, thus, any other treatment of the data must be an exception and subject to the holder's express authorization.

It consists of preventing and anticipating potential events that may compromise the privacy prior to their occurrence. The implementation of efficient processes to protect privacy, since the collection of the data until its elimination (data life cycle inside the company), is the grounds for the Privacy by Design.

It requires the commitment from all the employees in the organization, who must understand the importance of such prevention and the consequences of a potential breach. To this end, the company shall create guidelines, with good practices and governance rules that establish security procedures and educative actions to mitigate risks.

For the departments that treat the information in a daily basis (ex. Marketing, HR, Sales), an individual and specific approach is advisable, based on risks previously identified.

3. Protection of the private data

The organization must invest in security mechanisms so as to protect the private data (ex. encryption, pseudo-anonymization, infrastructure, back-up solutions, access control, etc.). Nevertheless, although technology has a crucial role, it is necessary to combine security techniques, standard work flows, internal education and continu-

Sonia Marques Döbler Advogados*
Rua Dona Maria Paula, 123
19º andar - Edifício Main Offices
01319-001 - São Paulo - SP/Brasil
T (+55) 11 3105 7823
www.dobler.com.br

ous training. The company must have the ability to evidence the adoption of efficient security measures to safeguard the private data.

This extends to the company's suppliers, who must also comply with the requirements of the LGPD.

4. Review, update and adequacy of the Privacy Policy, Terms of Use and Consent Terms

It is the moment to review, update and adjust the existing Privacy Policy and Terms of Use, using simple wording of easy comprehension, considering the target group, i.e., the data holder or the employees in the organization.

Highlighting consent terms is also indispensable, so that the holder is duly informed, prior to giving the "OK" (consent), to what purpose his/her private data will be used.

5. Management of consent and anonymization

This aims at defining mechanisms to control the consent and the anonymization of the private data, according to the requests made by the respective holder and by the Brazilian authorities. It may result in modifications of the company's service channels, whose procedures shall be able to receive all the requests, in order to guarantee the safety of the information.

The data holders shall have full access as to how the companies handle their information, for how long it is stored and with whom the information is shared.

6. Management of the data holders' requests

This aims at creating a data basis to manage, fulfill and control the requests made by the data holders, given that they can demand, at any time, the confirmation, access, correction, elimination and revocation of consent and/or information stored by the company.

7. Issuance of Impact Report

The construction of the impact report aims at detailing all the treatment processes through which the private data circulates along its life cycle, as well as the legal basis and the safety measures adopted. The continuous fulfillment of the LGPD's obligations requires documentation and audit of what data the company is collecting, for which purpose it is being used and for how long it will be stored. If requested by the authorities, the company must be able to present the impact report concerning the private data that it handles.

Nevertheless, the company is encouraged to constantly update the impact report, so as to have a better view and comprehension of its operation, avoiding excesses and allowing the adoption of the appropriate solutions within the context of privacy and data protection.

Sonia Marques Döbler Advogados*
Rua Dona Maria Paula, 123
19º andar - Edifício Main Offices
01319-001 - São Paulo - SP/Brasil
T (+55) 11 3105 7823
www.dobler.com.br

8. Communication Plan – Security Incident

The company must also be able to promptly communicate the authorities and the data holder about any security incident potentially harmful to third parties, to the company itself and/or to the holder.

9. Validation of Treatment Termination

The company shall have the means to eliminate the treated data, confirming the security of the information that remains stored, with the issuance of documents that evidence the elimination.

Far from exhausting the theme, this article summarizes some of the main obligations that the companies must fulfill with the advent of the LGPD, with the purpose to give a good overview of what is expected from them in connection with the new law. Nevertheless, the Brazilian Agency that will regulate the application of the LGPD is yet to be created, reason why it is possible that changes and/or additions are required.

Despite the fact that the LGPD will be effective only in August/2020, it is worth emphasizing that the adaptation process is complex and may always leave some uncertainties as to whether or not all the legal requirements have been properly addressed. Besides, as informed before, the penalties for the violation of the LGPD are severe.

For these reasons, the sooner the companies start their adaptation process, the lesser it will be their exposure to the penalties established by the law. Furthermore, the assistance of specialized professionals in the whole procedure is highly recommendable.

*Author of the publication ***So geht's M&A in Brasilien***

Débora Motta Cardoso
dmotta@dmktadvocacia.com.br

Karin Toscano Mielenhausen
ktoscano@dmktadvocacia.com.br

Débora Motta & Karin Toscano
Advocacia Criminal – DMKT
Av. Brigadeiro Faria Lima, 1826
cj. 906 - 01451-908
Jardim Paulistano, São Paulo – SP
T (+55) 11 2501-0475
www.dmktadvocacia.com.br

Possible Penalties in the Event of Data Leaks

In an effort to recognize and regulate cyber-legal relations, the Internet Civil Law Framework ("Marco Civil da Internet") – as it was entitled by Law nº. 12,965 (2014) – established certain principles, rights, and duties for the use of information superhighway in Brazil. Every user, Internet Service Provider (ISP), and online service provider is directly covered by the norm and, as a result, has had to adapt to its legal requirements over the course of recent years. Though the law in question dealt closely with questions related to privacy in the context of the World Wide Web[1] , some aspects remained undefine, namely the protection of personal data, the core subject addressed by Law nº. 13,709 (2018), the new General Data Protection Act (GDPA) ("Lei Geral de Proteção de Dados" - LGPD).

With a vacatio legis in line with the degree of complexity of the modifications imposed on its adherents, the new law – which was designed to protect fundamental privacy and liberty rights and free personal development, dignity, and citizenship – will take effect only in 2020, sufficient time it is hoped to guarantee that companies and society in general will make the necessary adaptations to comply with the norm. However, civil, administrative, and – in the last analysis – criminal sanctions will be imposed on anyone who deliberately refuses to or in some manner neglects to adapt to the law's requirements.

It should be noted that, among the innovations contained in the text of the GDPA, subject to administrative sanctions, is that companies must begin to collect only the minimum of data necessary for their particular needs and eliminate any data collected after those purposes are served. They must also maintain detailed records of all of their data handling activities, as well as name a so-called Data Protection Officer, whose job it will be to act as a communications conduit between the owners of the data and the company, while also supervising and monitoring compliance with the legal norms.

Data security received special attention in the new legal framework with the requirement for security guidelines in the data handling process, as well as personal data protection protocols that must extend from the initial concept for products and services until their effective execution. Finally, companies must notify the national data protection authority of any data security incidents, as well as the data owners and the general public, depending on the seriousness of the nature of the incident.

Articles 52 to 54 of the GDPA deal specifically with compliance and the application of administrative sanctions for any violations, penalties that vary from: a) a warning, with a specific time period in which corrective measures must be taken; b) a simple fine, of up to 2% (two percent), of the private law legal entity, economic group, or conglomerate in Brazil's billing in the last fiscal year, excluding taxes paid and limited to a total of R$ 50,000,000.00 (fifty million Brazilian reals) per violation; c) a daily fine, up to a total limit of R$ 50,000,000.00 (fifty million Brazilian reals); d) public disclosure of the violation, after its occurrence has been duly investigated and confirmed; e) a hold or stay on the personal data involved in the violation, until the said violation is remedied; and f) the elimination of the personal data involved in the violation.

Naturally, in accordance with the guarantees enshrined in the Brazilian Constitution, those sanctions may only be applied following an administrative law proceeding that allows for a full defense, respects the particulars of the concrete case, and takes into account the parameters and criteria established in the law itself[2] . Nevertheless, it is important to note that those administrative sanctions may not be substituted for the application of the penal sanctions provided for in specific legislation. Under the express terms of art. 55-J, the national data protection authority not only must notify the internal control bodies of any non-compliance with the provisions of the law on the part of federal public organs and entities, but must also report to the competent authorities any criminal violations it is aware of.

In addition, the absence of a specific criminal law that effectively covers the conduct included in so-called cybercrime – violations carried out online – has forced recourse to the traditional crimes provided for in Brazilian law. For example, laws against fraud, misrepresentation, threats, and the various specific forms of libel, slander, and defamation of character (in the Brazilian context, "injuria", "calúnia", and "difamação"), among others, are resorted to when the seriousness of the facts goes beyond the limits of a mere administrative law

[1] By way of example, the Internet Civil Law Framework did the following:
a) Instituted the mandatory removal of offensive content from sites, blogs, or social networks, following a court order, with criminal penalties for anyone producing or distributing said material;
b) Allowed for the violation of the privacy and data protection rights of Internet users, including e-mails and chats, only in the context of a criminal investigation;
c) Barred sites from collecting user data without consent.

[2] "Art. 52. (...)
I – The seriousness and the nature of the violation and of the personal rights affected; II – the good-faith of the violator; III – the advantage available to or sought by the violator; IV – the economic conditions of the violator; V – repeat offenses; VI – the degree of the harm done; VII – the cooperation of the violator; VIII – the repeated adoption and demonstration of internal mechanisms and procedures capable of minimizing any damage, focused on the safe and adequate handling of data in line with the provisions of paragraph 2, section ("inciso") II, of art. 48 of this Act; IX – the adoption of best practices and corporate governance; X – the ready adoption of corrective measures; and XI – proportionality between the seriousness of the violation and the severity of the saction".

Débora Motta & Karin Toscano Advocacia Criminal – DMKT
Av. Brigadeiro Faria Lima, 1826
cj. 906 - 01451-908
Jardim Paulistano, São Paulo – SP
T (+55) 11 2501-0475
www.dmktadvocacia.com.br

violation. It must also be clarified that the GDPA is absolutely silent with respect to the creation of specific crimes to punish conduct in the virtual realm.

In this respect, if it is understood that the duty of professional confidentiality includes the obligation of data secrecy, any conduct that discloses such data without just cause may be held to be criminal if it is prejudicial to the other party[3]. Moreover, it should be recalled that art. 154-A of the 2012 Penal Code defines as a crime the invasion of an information storage device for the purpose of adulterating or destroying data or information to obtain an unlawful advantage. This criminal classification may likewise aid in combating the abuses related to the new law.

[3] In this regard, see the provisions of art. 154 of the Penal Code: "Art. 154 – To disclose to another, without just cause, a secret of which one is aware as a function of one's ministry, trade, or profession, and the disclosure of which may cause harm to another (...)"

The Brazilian National Data Protection Authority

Law no. 13709, as of August 14, 2018 ("LGPD"), governs the personal data protection in Brazil. The original articles 55, 56 and 57 of the LGPD provided for the National Data Protection Authority ("ANPD") and the National Council for Data and Privacy Protection, but were vetoed by the President for procedural reasons. However, Provisional Measure no. 869, as of December 27, 2018 ("MP"), included new language to the LGPD to create and regulate the ANPD in articles 55, letters A through K.

It is important to highlight that the MP is subject to approval by the National Congress within a 60-day term (with the possibility to extend for one additional 60-day term), otherwise it will become ineffective.

According to the language added by the MP, the ANPD is a federal governmental body, who has technical independence, and the members of its board shall be Brazilian citizens, with good reputation, superior degree and have significant specialty to occupy the position they are being appointed to. The main reason for the existence of the ANPD is to ensure effectiveness of the LGPD and the enforcement of its provisions in the administrative level.

Their competences are listed in the MP and generally involve normative and supervision powers, as well as preventive duties to improve data protection, among others. In detail, the ANPD has powers to:

(i) watch over personal data protection;

(ii) issue rules and procedures about personal data protection;

(iii) resolve on the interpretation of the LGPD and omissions;

(iv) request information from personal data operators and their controlling parties who treat personal data;

(v) implement simplified mechanisms to register claims about personal data treatment in breach of the LGPD;

(vi) inspect and impose penalties in case of data treatment in breach of the LGPD;

(vii) inform competent authorities about criminal offenses it becomes aware of;

(viii) inform internal control bodies about the breach of the LGPD performed by bodies and entities of the federal government;

(ix) disseminate knowledge about data protection rules and public policies and about security measures;

Renata Almeida Pisaneschi
rpisaneschi@machadoassociados.com.br

Mirella da Costa Andreola de Almeida
malmeida@machadoassociados.com.br

Machado Associados
Av. Brigadeiro Faria Lima, 1656 – 11º. andar
01451-918 - São Paulo - SP/Brasil
T (+55) 11 3819 4855
www.machadoassociados.com.br

Machado Associados
Av. Brigadeiro Faria Lima, 1656 – 11º. andar
01451-918 - São Paulo - SP/Brasil
T (+55) 11 3819 4855
www.machadoassociados.com.br

(x) stimulate adoption of standards for services and products that help the control and protection of personal data by the data holders;

(xi) prepare reports on national and international data protection and privacy practices;

(xii) promote cooperation actions with personal data protection authorities from other countries;

(xiii) carry out public consultations to gather suggestions about matters of relevant public interest in the field of action of the ANPD;

(xiv) hear the entities and bodies of the government responsible for the regulation of specific economic fields before issuing resolutions;

(xv) interact with public regulating authorities to exercise its powers in specific economic and governmental fields subject to regulation; and

(xvi) prepare annual management reports about its activities.

The MP established that the ANPD has exclusive competence to impose penalties and its powers shall prevail over the powers of specific governmental entities or bodies in connection with personal data protection. Additionally, the ANPD shall be the central body to interpret the LGPD and to issue rules and guidelines for its implementation.

The LGPD provides for several types of administrative penalties that may be imposed by the ANPD, including fines, suspensions and measures to eliminate or block personal data. In any case, the penalties shall be preceded by an administrative proceeding to be carried out by the ANPD, in which the company or individual must be granted broad defense, and the penalties shall consider certain parameters and criteria, including gravity of the breach, good faith, economic condition, damage level, prompt adoption of correction measures, proportionality.

The ANPD has the duty to report possible criminal offenses to the applicable authorities and the penalties imposed by the ANPD do not avoid or replace civil indemnification claims involving the persons affected by the breach and the responsible parties. Moreover, other administrative penalties provided for in specific laws may also apply.

The individuals and companies subject to the obligations of the LGPD will have to interact with the ANPD to the extent that they will be supervised by it and will have to provide information, documents and grant access to possible inspections. Therefore, it is important to be prepared to always have proper support documents and evidences to present to the ANPD in case of request, to

have a contact person in charge of dealing with and relating to the ANPD in compliance with the LGPD, to monitor and react as promptly as possible to minimize adverse effects of possible claims.

Of course, it will take some time for companies subject to the LGPD to have a clear picture of their needs in relation to the ANPD. Only after the actual structuring and the beginning of the activities of the ANPD it will be possible to have a better understanding of their demands and of the extent of the interactions between the companies and the ANPD. In any case, it is advisable to closely follow up and be updated about any developments related to the ANPD and the LGPD and to actively participate in public consultation procedures in order to allow the implementation of reasonable and effective policies and regulations.

At last, it is worth remembering that the conversion of the MP into a law is required to confirm the creation of the ANPD and its powers. This is supposed to occur by the end of February or at the latest by the end of April 2019.

Machado Associados
Av. Brigadeiro Faria Lima, 1656 – 11º. andar
01451-918 - São Paulo - SP/Brasil
T (+55) 11 3819 4855
www.machadoassociados.com.br

Paulo Lilla
paulo.lilla@lefosse.com
T (+55) 11 3024 – 6347

José Carlos Berardo
zeca.berardo@lefosse.com
T (+55) 11 3024 – 6347

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

Some notes on data portability in the Brazilian General Data Protection Law

LGPD assures data subjects the right to the "portability of data to another service provider or product, upon express request". It is a broad right, with practical implications that are very relevant to different industries beyond technology, the interpretation of which is likely to be much more complex in practice than the simplicity of its language suggests.

The objective of the legal protection of the individual right to change a service provider or manufacturer seems obvious: to assure the subject not only controls his or hers own data, but also to increase competition between different service providers or manufacturers. Portability increases competition insofar as it eliminates – or at least attempts to eliminate - the competitive advantage that the "incumbent" provider or manufacturer has in relation to other providers or manufacturers: this advantage is exactly the data accumulated by the incumbent over the years, or perhaps decades, and which often translate into a form of "lock-in" that facilitates the increase of network effects (e.g., just think about what it would take in terms of personal data for someone to develop a platform capable of competing with Facebook).

On paper and as a premise of protection of personal data, this is of course a measure beneficial to society and citizens; however, there are several important challenges, especially looking from the regulations to be designed by the national data protection authority.

What is data portability?

The portability of personal data is treated, in the LGPD, as an additional right to the right of access to personal data (article 18, II), and is, in fact, its consequence: if the Law is aimed precisely at ensuring respect for rights of the data subject, and the subjects' free access to their own personal data is one of the fundamental principles guiding the LGPD (Article 6, IV), it is only natural that the transfer of data between so-called data controllers (i.e., those who carry out the processing of personal data) be expressly provided for by law as a means of ensuring the freedom of choice of the data subjects.

In fact, even if there were no express provision on data portability, two other rules could be directly interpreted so as to allow it: first, the determination that data will be stored in a format that favors the exercise of the right of access (art. 19, § 1) by subjects, and, second, the determination that personal data must be made available to its holder "in a format that allows its subsequent use".

In other words, the requirements imposed on data controllers in terms of access by subjects are sufficient to ensure portability, i.e., the right of the subject to request that data processed by a given controller be transferred to another controller.

The LGPD distinguishes the concepts of portability and "interoperability". While the former is meant to allow the subject to "carry" data when switching controllers, the latter involves the technical standards controllers must adhere to so that data can be transmitted from one data controller to another without loss of functionality for the data subject. Although portability does not exist without interoperability standards, the mere existence of these standards does not ensure portability nor does it imply full compatibility between data controllers' systems.

What are "portable" data?

Strictly speaking, any "personal data" can be portable, and it is at this point that the discussion becomes more complex and therefore interesting.

The definition of the LGPD on what characterizes personal data can be seen as over-inclusive: personal data is any "information related to an identified or identifiable natural person". Although the European General Data Protection Regulation (GDPR) establishes a similar concept for personal data, it states in its Article 20 (1) that personal data subject to portability would not be just any data related to the natural person, but only the data that the natural person presented to the data controller.

From this perspective, although the LGPD determines that portability is limited by the controller's "commercial and industrial secrets", it is clear that the LGPD has not drawn up a specific definition for portable data, as GDPR did; this leaves room for an interpretation that, considering the very broad definition for the concept of personal data, any personal data would be portable. As such, "personal data" can be read in such a way as to include simple identification data (taxpayer's number and date of birth, by example) effectively filled in by the data subject, and his or hers health information, to music or culinary preferences, most visited places, or financial hurdlers. In other words, the LGPD did not in principle draw an objective distinction between personal data per se, on the one hand, and inferences or derived data, on the other – the former being provided by the data subject himself, in a fully conscious manner (post on the social network) or not (cell phone location history), and the latter ones produced by the controller from or in function of the first one.

Identification data or data presented by the natural person (e.g., a photo posted on social media) seem, without any doubt, to fit into the definition of personal

Lefosse Advogados
R. Tabapuã, 1227 – 14th floor
04533-014 São Paulo – SP
Av. Pres. Wilson, 231 office 2703
20030-905 Rio de Janeiro – RJ
T (+55) 11 3024 6100
www.lefosse.com

LEFOSSE
ADVOGADOS

data for the purposes of the LGPD; are the inferences made from these, however, information "related to the natural person identified"? As an example: if a particular data controller knows that the holder regularly displays photos of Italian dishes, does the portable "personal data" include the inference – made by humans or through electronic means – that the holder enjoys going out to dinner at Italian restaurants? If a user only hears gospel music, is the inference that the user is religious portable? A user looking for credit information is more likely to be going through financial trouble and therefore should have less or more expensive credit? Are these inferences protected by "commercial and industrial secrets," or are they just data "related to natural person" obtained by repetition of behavior? Are the inferences encompassed by portability, or do they depend only on pure data? Are there degrees of inferences (i.e., obvious and non-obvious) to justify invoking the "trade secrets" protection against the portability of inferences?

The debate on the portability of inferences and derived data (and even on the subject's own access to the inferences made by controllers) is likely to be closed only after judicial review or a clear and unequivocal statement by the National Authority for the Protection of Data (ANPD). The GDPR does not provide an adequate guidance in this respect because there is no exact conceptual correspondence between it and the LGPD.

Nevertheless, it is a fact that the antitrust legislation and its principles, on this point, will be the key to the full effectiveness of the provisions of the LGPD, as an interpretation of the data protection law that makes it difficult or impossible to develop competing suppliers (other controllers) would render the express command of the Law useless.

Is this all there is to know about personal data portability?

There are a number of other points about portability – for example, deadlines for responding to a request for portability – which should certainly be subject to specific ANPD regulation, and which are not easily resolved by examining the legal text.

Likewise, there are doubts about the scope of application of the data portability rule, since a broad interpretation of the concept of portability would render, for example, various provisions and the own purpose of the credit scoring legislation (Law No. 12.414) unnecessary or outdated: depending on the interpretation of "portable personal data", it would be enough for a customer to ask his bank to carry his credit history to another bank in order to produce effects similar to that of the credit score legislation. The same reasoning would be valid for the health sector (Article 11, §4, I of the LGPD) and for medical data, for example.

There is a lot to be studied and debated about portability, and its implications will be great, not only for large Internet platforms, but also for the banking, healthcare, auto and many other important industries.

Deutsch-Brasilianische Industrie- und Handelskammer São Paulo

Rua Verbo Divino, 1488 - 3º andar
04719-904 São Paulo - SP - Brasilien
T (0055 11) 5187-5216
F (0055 11) 5181-7013
E juridico@ahkbrasil.com

www.ahkbrasil.com