SEVEN
publicações acadêmicas

# LGPD as a basis for adaptation to micro and small companies in the northwest of São Paulo

Crossref doi
https://doi.org/10.56238/sevened2023.006-134

**Eduardo Cury**
Advisor. Professor at the University Center of Santa Fé do Sul, SP – UNIFUNEC.
E-mail: adveduardocury@uol.com.br

**Heitor Oliveira Machado**
Law student at Centro Universitário de Santa Fé do Sul, SP – UNIFUNEC.
E-mail: heitor_machado9@hotmail.com

**Paulo Ricardo Santana**
Advisor. Professor at the University Center of Santa Fé do Sul, SP – UNIFUNEC.
E-mail: professorpaulosantana@hotmail.com

**Vanessa França Valero**
Law student at Centro Universitário de Santa Fé do Sul, SP – UNIFUNEC.
E-mail: vanessa.valero@outlook.com

## ABSTRACT

The General Personal Data Protection Law (LGPD – Law No. 13,709, of August 14, 2018) was created, above all, with the intention of preserving and regulating the control of personal data. In addition, before its elaboration, there was no effective processing of personal data in the Brazilian legal system, which is facing a business scenario that has been rapidly shaping itself to technologies and therefore it is necessary for companies to review their operations involving personal data. In addition, in view of the significant growth of micro and small businesses in the Southeast region of the country and the predominance of this type of company in the northwest region of São Paulo, it is essential to analyze the most efficient way to comply with the new rules of the LGPD, through the present work. According to the law, companies must treat consumers' personal data in a careful and transparent manner, establishing policies for consumer protection, human rights, dignity and the exercise of citizenship by natural persons. Thus, the main objectives of this study are to understand what is the legal object protected by the General Data Protection Law in Brazil and its applicability by companies, in addition to setting up a base plan of adequacy that can be used both by entrepreneurs who are starting business activity, and for those who have not yet adapted. The methodology applied was the bibliographic and documentary research, seeking bibliographies, jurisprudence and theoretical analysis, involving databases consulted for the elaboration of this work, in order to find and discuss the legal object protected by the LGPD, in addition to making use of the deductive method to achieve the system of contractual clauses of the adequacy plan. From the research carried out, it was reached the result that the legal object protected by the LGPD is personal data and that they are part of the list of Fundamental Rights, entering the concept of privacy listed in article 5, item X of the Federal Constitution. In addition, according to the research found in this work, it was possible to observe that most companies are still unaware of the LGPD, although the law has been in force since September 2020, which can harm the entrepreneur if data leakage occurs. Thus, companies need to protect themselves from alleged data leaks and civil liability, and must have a contract model to ensure the security of their business, as well as the data subject. It is concluded that the law came to protect personal data, provide foundations on the correct form of protection and necessary adaptations, in addition to promoting the economic and technological development of the administration of legal entities.

**Keywords:** General Data Protection Law, Micro and Small Enterprises, Northwest of São Paulo.

## 1 INTRODUCTION

In the face of the advance of globalization and the development of technology, there is a need to question the security of corporate information and its customers. With the increasingly computerized society, the flow of data has become a crucial element for commerce and industry, and the protection of personal data is a concern for all individuals.

The most diverse areas of commerce, industry and service will have to undergo adjustments in their activities. And, among these needs, through the digital and automated revolution, the processing of data from customers, suppliers, and partners becomes strictly necessary, according to Kohls, Dutra, and Welter (2021).

The search for the security of your information has actually become a cultural change in which companies in turn involve their legal, technological, human resources, marketing, and other areas.

The General Data Protection Law gives the holder of personal data the right to obtain information about the processing of their personal data provided to any company, and this must be clear, objective, easily understandable and accessible throughout the period in which it is using the individual's personal data (SILVA; AUROCA, 2020). It is important to clarify that data processing encompasses the collection, production, reception, classification, use, access to reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction of personal data.

In addition, it is important to note that there are coercive measures for companies in case of non-compliance with the requirements imposed in the rule in question, such as the application of the following penalties: warning, pecuniary fine of up to 2% of the company's revenue, up to a limit of R$ 50 million per infraction, daily fine, possibility of publicizing the infraction, blocking of the personal data involved, partial suspension, for up to six months, of the database involved, partial or total prohibition of the exercise of activities related to data processing (BRASIL, 2018). Thus, the present study has its anguish in the lack of information of micro and small business entrepreneurs in the face of the cogent norm of the aforementioned law and brings the following problem in question: "how to prevent micro and small companies in the northwest of São Paulo from suffering the sanctions imposed for non-compliance with the LGPD?".

According to data from the Sebrae Nacional website (2022), micro and small companies are divided into micro and small companies, created and founded by Complementary Law 123/2006, this was a measure that the government adopted to encourage entrepreneurs to believe in their idea and have their own business. The authors, Santos, Krein and Calixtre (2012), emphasize the importance of the role of micro and small enterprises in the country, having as their main point the increase of the economy, due to the number of companies and scope, fostering the generation of employment, social inclusion and other benefits that contribute to the consolidation of the national economy.

With regard to the northwest of São Paulo, the research will address the relevance of the increase in micro and small companies in the region, as well as the need for a plan to adapt.The LIDE Northwest São Paulo Business Climate Survey, published on September 29, 2020, revealed that companies in the northwest of São Paulo continue to grow, especially with regard to micro and small companies, despite the economic uncertainties caused by the context that Brazil experienced, in the face of the spread of the coronavirus at the time, which prevented the full exercise of most of the economic activities developed in the region.

It is already possible to observe growing and consistent changes in the market with the implementation of the principles and standards of the LGPD in organizations, and this has translated into awareness actions, clearer and more transparent texts in contracts and in the privacy policy of portals, greater contracting of information security tools and systems, certification of professionals in the field of data protection, among others (NEOWAY, 2018). Thus, the present study is justified in view of the growth of small and micro enterprises in the State of São Paulo and in the northwest of São Paulo, and it is important that those responsible for them implement as soon as possible the guidelines imposed by the General Data Protection Law so that they can avoid future losses to the development of economic activity.

From the point of view of data subjects, the LGPD should represent a new phase of autonomy and security. Because, by law, companies will be required to make transparent to data subjects what they do with their personal information. Any organization that collects personal data will be responsible for ensuring the protection and privacy of that information. (KOHLS; DUTRA; WELTER, 2021).

Finally, the present study is developed with the objective of understanding what is the legal object protected by the General Data Protection Law in Brazil and its applicability, in order to plan a viable system for the adequacy of personal data provided by the data subjects in order to benefit the contractor and the contractor, showing what they are entitled to. The specific objectives that contribute to achieving the main objective are to know the pertinent legislation that safeguards the rights of data subjects and their mediators, understanding the main challenges that micro and small companies face to adapt to the guidelines of the new legislation compared to companies with greater economic potential, in order to create a system of general clauses, without a specific sector, which seeks to meet the general needs of any company and can be adopted by an entrepreneur in any field, who can later add the specificities that the company's niche needs.

The methodology applied for the development of this was a bibliographic and documentary research, seeking bibliographies, jurisprudence and theoretical analysis, involving databases consulted for the elaboration of this work, in order to find and discuss the legal object protected by the LGPD, in addition to making use of the deductive method to create a base plan of adequacy that can be used

both by the entrepreneur who is starting the business activity and for those who are still they didn't fit in.

## 2 HISTORICAL EVOLUTION OF DATA PROTECTION IN BRAZIL

The concept of privacy that is currently seen as an element of protection and discussion in society has been developed over time, especially with technological innovations, such as the expansion of the internet and social networks, which have brought greater risk to the disclosure of the individual's personal information. According to Lugati and Almeida (2020, p. 04), in the principle of conceptualizing the right to privacy, he:

> It had a strongly individualistic character and was seen as a negative right. Therefore, it can be said that the right to privacy would be guaranteed as long as the State refrained from entering into the individual sphere of each person. This perspective was consistent with the first generation of fundamental rights in which it was inserted, which was directly linked to the right to freedom.

This idea began to change in the 1960s, when the development of technology led to a need for data collection and search for information both in civil practices, consumer relations, and for research, thus growing interest in the protection of privacy and its exercise.

According to Lugati and Almeida (2020, p. 04), "Since computerized data processing emerged and gained focus, there has been a need for the concept of the right to privacy to be modified in order to encompass the protection of personal data."

There was a path to be taken with regard to data protection, which gained focus with the promulgation of the 1988 Constitution, which brought the protection of the right to personality, freedom of expression, information, in addition to guaranteeing in item X of article 5 the inviolability of private life and intimacy.

Following the chronology, after the federal constitution, in 1990 came the consumer protection code, which provided in article 43 the protection of the holder of the information against databases and registrations. It was required that the consumer be notified of the opening of registrations, forms, registrations and personal and consumption data, however, it is noted that the greater concern was with the regulation of databases than with the human person himself, with the consent about the sharing of data, an example of this is precedent 404 of the Superior Court of Justice (2009 – online), which considers dispensable the Acknowledgment of Receipt (AR) in the letter that informs the consumer of the inclusion of his name in the database of delinquents.

After that, it is also important to observe the Positive Registry Law, of 2011, which deals with the processing of data from financial operations and consumer compliance, enabling the release of credit, since a person's history is formed. It was a breakthrough with regard to the right to privacy, since it developed the idea of consent in the control of data from the collection. It is the individual who

decides whether or not to share their personal data so that other companies have access to the database and offer products.

In 2014, another law came into force that discusses the need for the individual's consent to the manipulation of their data by third parties, the Civil Rights Framework for the Internet (Law 12.965/2014), however, now, in a virtual environment, that is, in the relationships developed on the internet, conferring, according to Lugati and Almeida (2020, p.12) "rights and guarantees of the citizen in the relationships held in the virtual environment, in a principled way."

Time passed, until in 2018, the law that specifically discusses the protection of people's data, the LGPD (law 13.709/2018), appeared. It establishes the roles of agents in the information processing process, five of which are, according to Schwaitzer (2020) "the data subject, the controller, the operator, the person in charge and the National Data Protection Authority (ANPD)." Article 5 explains what each one is (BRASIL, 2018, on-line):

> V - data subject: natural person to whom the personal data that are subject to processing refers;
> VI – controller: natural or legal person, governed by public or private law, who is responsible for decisions regarding the processing of personal data;
> VII – operator: natural or legal person, governed by public or private law, who processes personal data on behalf of the controller;
> VIII - person in charge: person appointed by the controller and operator to act as a communication channel between the controller, the data subjects and the National Data Protection Authority (ANPD);
> XIX - national authority: public administration body responsible for ensuring, implementing and supervising compliance with this Law throughout the national territory.

Also according to Schwaitzer (2020, p. 42):

> The processing must have non-discriminatory or abusive purposes, the purposes must be legitimate, specific, explicit, restricted and compatible with the purposes informed to the data subject, and subsequent processing that is incompatible or different from its context is prohibited.

Therefore, it is necessary that the data subject is made aware of what will be done with their data, so that they can decide whether or not to agree to share their personal information, and it is strongly important to respect the principles of probity and good faith throughout the process. In other words, unlike another time when the consumer only received a letter about the inclusion of his name in the registry of the database of defaulters, from the General Data Protection Law it is necessary for him to participate in the process, to be informed about everything.

From the point of view of data subjects, the LGPD should represent a new phase of autonomy and security, since companies are now required to make transparent to data subjects what they do with their personal information. Every organization that collects personal data will be responsible for ensuring the protection and privacy of that information, according to Kohs, Dutra, and Welter (2021).

It is important to highlight the principles that make up the rule in question, which are listed in Article 6, in which the aforementioned good faith, purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability and accountability are highlighted.

From this perspective, it is clear that companies need to implement a data protection program, catalog personal data, identify the internal process for handling this information from collection to closure, verify the storage location, review their internal policies and IT systems, understand what the vulnerability is and how is the security of the database to which the data provided belongs. as well as reviewing contracts with partner companies, hindering access to sensitive information and making a data protection impact report, given that the ANPD may request it. In other words, there is a need for entrepreneurs to adopt a routine of privacy and personal data governance with regard to compliance with the law in their business, since they will be held accountable.

Thus, according to Roseli Bossoi (2020, p. [unpaginated]):

> This is a legislation that becomes part of the day-to-day life of all types of companies that are operating in the Brazilian territory processing personal data, citing as an example: supermarkets, bakeries, butchers, accounting offices, condominiums, hotels, gas stations, banks, pharmacies, virtual stores, social media companies, retail and wholesale stores, photographic studios, service providers, educational institutions, children's schools, health plan operators, hospitals, clinics, offices, unions, cooperatives, workshops, churches, associations, communication companies, public companies and others.

It is possible to notice an evolution with regard to personal data, which is now seen in two ways, that of helping economic development and of guaranteeing fundamental rights from the figure of consent, integrated into the concept of privacy, therefore, they are the legal object that the LGPD specifically protected.

## 3 PERSONAL DATA AS FUNDAMENTAL RIGHTS

With regard to the right to privacy, it is appropriate to bring the definition of José Matos Pereira (1980 apud SILVA 2015, p. 208) "the set of information about the individual that he can decide to keep under his exclusive control, or communicate, deciding to whom, when, where and under what conditions, without being legally subject to it". Thus, it can be seen that the set of protection of individuals is broad and "covers the domestic way of life, in family and affective relationships in general, facts, habits, place, name, image, thoughts, secrets, as well as the origins and future plans of the individual" (OLIVEIRA, 1980 apud SILVA 2015, p. 208).

It should be noted that, in the study of the General Data Protection Law, it:

> It applies to all information related to an identified or potentially identifiable natural person and to data that deals with racial or ethnic origin, religious conviction, political opinion, membership in a trade union or organization of a religious, philosophical or political nature,

> data relating to health or sex life, genetic or biometric data, whenever they are linked to a natural person. [(Schwaitzer (2020, p. 41)]

The law also makes clear in article 18 the right of the holder to access, correct, anonymize, delete, update, confirm their data and even revoke the consent that gave rise to the processing of the information and the possibility of pleading with the ANPD against the controller, if they understand that there has been any damage to their private sphere due to non-compliance with the values and principles contained in the rule."In general terms, the LGPD ensures the integrality of protection for the human person to the extent that it enshrines the obligation of secure management from the beginning to the end of the operation involving personal data" (Sarlet, Ruaro, 2021, p. 86).

Consent, which in the past was treated in order to regulate cadastral banks, is now seen as a necessary element to guarantee fundamental rights, it "is configured as a means to implement the right to informational self-determination" (LUGATI, ALMEIDA 2020 p.15), that is, the right of the person to be able to exercise their freedom of decision about the actions that will be made with their data, as well as what should or should not be omitted from access by third parties. It puts the individual at the center and controls the entire process of processing their data, to the extent that each person chooses whether or not to consent to the collection and handling of information.

In the text of the LGPD, consent is treated intensively, appearing several times. In the words of Mendes (2014, apud Lugati and Almeida 2020):

> The validity of consent is formed from the assumptions that [..] "The holder must issue consent of his or her own free will; (ii) the consent must be for a specific purpose; iii) there must be information to the user about the purposes of the collection, processing and use of data and consequences of not consenting to the processing.

In this sense, it is necessary to bring the decision of the STF that suspended MP 954/2020 (provisional measure), which violated data confidentiality, in the judgment of the ADIs (direct actions of unconstitutionality 6387, 6388, 6389 and 6390). In the case in question, the measure provided for the sharing of data from telecommunications users with the Brazilian Institute of Geography and Statistics (IBGE) for the production of official statistics during the pandemic of the new coronavirus. In short, the plaintiffs alleged that if the mobile phone companies were required by the MP to provide the IBGE with data related to the names, telephone number and address of their consumers, both individuals and legal entities, they would be violating the constitutional rights that ensure the dignity of the human person, the inviolability of private life, intimacy, image and honor of people and the confidentiality of data.

Part of the decision of Justice Gilmar Mendes on the case in ADI 6387 is shown:

> the affirmation of the fundamental right to the protection of personal data imposes on the legislator a real duty of protection (Schutzpflicht) of the right to informational self-determination, which must be remedied by providing institutional safeguard mechanisms

> translated into rules of organisation and procedure (Rechtauf OrganisationundVerfahren) and rules of protection (Rechtauf Schutz). These norms must be enacted precisely to ensure the effective and transparent control of the individual in relation to the circulation of his or her data, having the notion of consent as the interpretative key to the legality of this control. (STF on – line).

In the same vein, Luiz Fux pointed out:

> The legal-constitutional question raised in these records involves the comparison between (i) the requirement of statistical production for the design of public policies to combat the coronavirus and (ii) the fundamental rights to data protection, informational self-determination and privacy. Despite the limits to the precautionary seat, the present judgment may emerge as a paradigm of data protection in the country, with the definition of principles and parameters for the processing and sharing of personal information. This vote is structured on the premise that data sharing, even in crisis scenarios, must follow constitutional and legal commandments, observing a strict relationship between adequacy and necessity. In this perspective, I understand that Provisional Measure 954/2020 goes beyond the limits set by the fundamental rights to data protection and informational self-determination, extracted from the guarantee of the inviolability of intimacy and private life (article 5, X, CF/88), the principle of human dignity (article 1, III, CF/88) and the procedural guarantee of habeas data (article 5, LXXII, CF/88). (STF on-line)

Thus, personal data, object of the LGPD, and all the principles of the law, are "framed by the principles constitutionally provided for by the 1988 Charter" (SARLET, RUARO, 2021). In other words, it is possible to say, based on the analysis of the decision concomitant with the cited doctrine, that personal information is recognized as a fundamental right in the Brazilian legal system and needs to be protected.

Consequently, it is necessary that companies when receiving personal data, whether arising from consumer or labor relations, protect them through all legally possible mechanisms and one of the ways to process them is to observe the application of the LGPD in contracts of the most diverse modalities, thus becoming another element of importance, indispensable for contracts involving customers' personal information.

## 4 CONTRACTS AND THEIR APPLICATIONS TO THE LGPD

In contemporary times, the traffic of data between suppliers and consumers in the market has been shown to be an important issue regarding the legal duty to ensure the correct protection of personal data, considering that the contracting of such services involves an imminent risk to the activity provided by the company itself. In view of this, it is necessary to use the contract, which is a legal space in which the parties are guaranteed duties and obligations that must be respected through constitutional and civil principles.

As the matter of adhesion contracts was entered into between suppliers and consumers as a mere acceptance of the so-called "Terms of Use", consumers were not allowed to discuss the contractual clauses and since there was no specific legislation for the correct processing of personal

data, there was a need to create the law studied here. which is concerned with the information passed on to suppliers.

According to Silva and Arouca (2020), the path that leads to the full acceptance of the institution with LGPD involves the adequacy of all contracts signed between consumers, employees, partners, service providers, suppliers and public agencies. In this way, the law itself establishes that companies adapt, making changes and contractual updates.

Initially, it is sought to have an agreement between the parties, a contract in which there are clear and explicit rules, as well as the purposes that they wish to be raised. In addition, obtaining consent for the collection and storage of personal data is set out in item I of article 7 of the law, which provides: "the processing of personal data may only be carried out in the following cases: I - upon the provision of consent by the data subject."

First of all, it is important to understand which personal data can be protected and their distinctions. In theory, according to article 5, personal data is any information that has informative content about the identified or identifiable natural person, such as documents showing date of birth, registration data, profession, interests, nationality and others. Later, there is a difference in sensitive data, as they involve issues related to the individual's intimacy, such as color, sex, religion, political opinion, among others.

Thus, the General Data Protection Law also clarifies the meaning of data processing. According to article 5, item X:

> X - processing: any operation carried out with personal data, such as those related to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

As demonstrated by the basic points for the definition of personal data and minimum requirements of the standard, we must go against the authors, Silva and Arouca (2020) who defend the importance of the institution providing necessary adaptations in all contracts used in its sectors, with the most diverse purposes, observing that the law now requires that new contractual clauses be made that inform the data subject what the data collection is, duration and purpose of the processing, form, what are the rights of the data subject and the responsibilities of the controller, in addition to obtaining consent for the processing of data.

Leite et al., (2019) justify the correct way for the processing of personal data, which is based on contractual obligations, the contract makes law between the parties, once signed it must be fulfilled in its entirety. In addition, written contracts must have clauses related to the protection of personal data in which obligations to do and not to do are configured, and when it comes to the modality of

expression of will in non-written contracts, the controller must make the data processing clear and valid.

Lima et al. (2022) refer to the concepts that should be used for the elaboration of contractual data protection clauses. The contract has a way of generating a series of obligations for the parties involved. And the object of the contract must be lawful and may not contravene the law and good customs.

In short, when entering into a contract, the following question must be taken into account: "Is there any personal data in this contractual clause?" If there is, a contractual analysis is necessary, in order to obtain clarity on the services provided and care for the appropriate treatment, as required by the current law.

In addition, another basic point to be mentioned is the social function of the contract, which is an essential part for the drafting of contracts, as stated in article 421 of the Civil Code: "contractual freedom shall be exercised within the limits of the social function of the contract". In the same article, it is stated that the contracts will be drawn up according to the will of the parties (BRASIL, 2002).

Lima et al. (2022) establishes that in order to draft a contract with data protection clauses, the LGPD and all the essential elements of a contractual relationship must be observed, even if it is to establish the provision of services by the person in charge of the processing of personal information. Thus, the author suggests the main specific elements for the elaboration of the contract, such as observing the legal bases of the norm in question, observing its principles and, finally, observing the rules of responsibilities established by law.

In this way, it is important to go against the Civil Code again in its article 104, which refers to the main points of a contractual relationship: capable agent, lawful object and prescribed form or non-defense in law.

In addition, the law gives importance to the correct form of processing, since it determines civil liability for the storage and use of personal data by anyone. It brings consequences, such as: sanctions, fines, public retraction and respect for good practices in corporate governance. It can also be said about the harm generated by the lack of responsibility, in which the company loses its credibility and respect for the inviolability of expression, information, opinion, intimacy, honor and image of the person.

Therefore, the contractual clauses for the protection of personal data must be clear and objective as to the form of processing and services provided, so as not to run the risk of damages caused by the damage caused due to the lack of liability, since the law itself guarantees the security of the information with the consent of the data subject.

## 5 CIVIL LIABILITY FOR THE USE OF PERSONAL DATA.

It is noteworthy that over time the relationships would become more complex and broader, as well as the figure of civil liability, in view of the socioeconomic changes in which the protection of personal data stands out, widely used by all business sectors.

In this interpreter, Donda (2020) conveys the idea that the law under study is based on the preservation of fundamental rights, privacy, and the free development of the natural person.

It is important for the company to transmit security in the provision of services involving personal data, to ensure the common good and to promote economic and technological development. However, this General Law for the Protection of Personal Data is little known among small business owners, which ends up harming them, since non-compliance can lead to sanctions.

In an analysis carried out by Sebrae/SC between January 4 and 25, 2021, 810 micro-entrepreneurs were interviewed by quotas representative of the number of MEI, ME, and PE as well as in sectors of activities in the regions of Santa Catarina, in order to identify the level of knowledge and compliance with the LGPD. The survey showed that 7 out of 10 entrepreneurs are aware of the law, and that about 75% of respondents were aware of the two-year *vacatio legis period* to comply, which has already ended, and only 22.6% were in compliance with it. Thus, it was calculated that 50.4% of the micro and small enterprises in that region were aware of the existence of the standard and had information on the respective deadline. Of the 810 companies surveyed, the service sector accounted for 70.2% of which had heard of the respective law, followed by industry with 68.4% and Commerce with 64.6%. Finally, it was presented that 50% of small businesses were unaware of the LGPD and only 22.6% reported being prepared to adapt (SEBRAE, 2021).

Thus, to ensure the proper development of the LGPD, it is necessary to understand all the rules exposed for adequate compliance with the new requirements, with the scope that there is due compliance and avoid situations of unforeseen and inevitable injury, provided for by the law itself, which brought a chapter for the regularization of the liability of agents specified between articles 42 and 45.

At the outset, when it comes to liability and reparation for damages, article 42 presents the obligations of the controller or operator who, by failing to comply with data protection legislation, causes damage to the data violated by the persons:

> Art. 42. The controller or operator who, as a result of the exercise of a personal data processing activity, causes another person property, moral, individual or collective damage, in violation of the personal data protection legislation, is obliged to repair it.

Corresponding to the CDC Consumer Protection Code (Law 8.078/90), the LGPD establishes solidarity with agents who cause damage (art.42, § 1, I and II) and, in order to contain the difference

in the relationship between operators, controllers and holders of personal data, the judge may allow the reversal of the burden of proof (art.42, § 2).

Following the next article, the LGPD deals with the hypotheses of exclusion of liability under the processing agent, when it is proven that the personal data was not processed, when there is no violation of the current law or that the damage was generated exclusively by the fault of the data subject. According to article 43 (BRASIL, 2018, on-line):

> Art. 43. Processing agents will not be held liable unless they prove:
> I - who have not carried out the processing of personal data attributed to them;
> II - that, although they have carried out the processing of personal data attributed to them, there has been no violation of data protection legislation; or
> III - that the damage is due to the exclusive fault of the data subject or of a third party.

Article 44 presents the concept of irregularity in relation to data processing, establishing limits in the face of legislation or when it does not present the necessary security measure.

> Art. 44. The processing of personal data will be irregular when it fails to comply with the legislation or when it does not provide the security that the data subject may expect, considering the relevant circumstances, including:
> I - the way in which it is carried out;
> II - the result and the risks that are reasonably expected from it;
> III - the personal data processing techniques available at the time it was carried out.

In observation of the provisions previously listed by the law, which establish liability for violation of legal norms, the sole paragraph of article 44 refers to the assumption of the duty to indemnify derived from the violation of express technical norms of the national data protection authority:

> Art. 44 [...]
> Sole paragraph. The controller or operator who, by failing to adopt the security measures provided for in article 46 of this Law, causes the damage shall be liable for the damage resulting from the breach of data security.
> Art. 46. Processing agents must adopt security, technical and administrative measures capable of protecting personal data from unauthorised access and from accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or unlawful processing.

Article 45, on the other hand, establishes the situations of violation of the holder's right within the scope of consumer law, in which the responsibilities governed by the pertinent legislation of the Consumer Protection Code (Law 8.078/90) will remain.

## 6 MICRO AND SMALL ENTERPRISES IN THE NORTHWEST OF SÃO PAULO

The concept of MSEs is complex to discern, since there is no specific agreement to define micro and small enterprises, as several authors adopt different standards, as presented by Souza (2007) who

explains the definition being broad and diverse, and varies by region, state or municipality. The indoctrinators Medeiros; Relative; Minora (2007, p. 196) state that:

> There is no unanimity on the delimitation of the segment of micro and small enterprises. In practice, there is a variety of criteria for its definition both by specific legislation and by official financial institutions and representative bodies of the sector, sometimes based on the value of turnover, sometimes on the number of employed persons, sometimes on both. The use of heterogeneous concepts stems from the fact that the purpose and objectives of the institutions that promote their framing are distinct (regulation, credit, studies, etc.).

However, Complementary Law No. 123, of December 14, 2006, which establishes the National Statute of Micro and Small Enterprises, provides in its article 3:

> Article 3 For the purposes of this Complementary Law, micro or small companies are considered to be business companies, simple companies, individual limited liability companies and entrepreneurs referred to in article 966 of Law No. 10,406, of January 10, 2002 (Civil Code), duly registered in the Registry of Mercantile Companies or in the Civil Registry of Legal Entities. as the case may be, provided that:
> I - in the case of micro-enterprises, earn, in each calendar year, gross revenue equal to or less than R$ 360,000.00 (three hundred and sixty thousand reais); and
> II - in the case of a small company, earn, in each calendar year, gross revenue greater than R$ 360,000.00 (three hundred and sixty thousand reais) and equal to or less than R$ 4,800,000.00 (four million and eight hundred thousand reais). (Amended by Complementary Law No. 155 of 2016) Effective

As the number of people looking to start their own business across the country increases, the number of people who rely on these small businesses grows. According to Sá (2011), with the increase in unemployment from 1980 onwards, several people were affected, seeking small businesses as a new alternative, so micro and small businesses became influential ways to generate growth in the Brazilian economy.

On June 6, 2022, the Federal Government, with the support of the Ministry of Economy, published the "Map of Companies – bulletin of the 1st four-month period/2022". According to the bulletin, in the period from January to April 2022, there was an increase of 11.5% in the first four months, compared to the last four months of 2021, accounting for a balance of 808,243 open companies, with a total number of 19. 373,257 active companies. (COMPANY MAP, 2022).

The Northwest Rural Territory of São Paulo -SP, which is the object of study, is composed of 36 municipalities: Aparecida d'Oeste, Aspasia, Dirce Reis, Dolcinópolis, Estrela d'Oeste, Fernandópolis, Guarani d'Oeste, Indiaporã, Jales, Macedônia, Marinópolis, Meridiano, Mesópolis, Mira Estrela, Nova Canaã Paulista, Ouroeste, Palmeira d'Oeste, Paranapuã, Parisi, Pedranópolis, Pontalinda, Populina, Rubinéia, Santa Albertina, Santa Clara d'Oeste, Santa Fé do Sul, Santana da Ponte Pensa, Santa Rita d'Oeste, Santa Salete, São Francisco, São João das Duas Pontes, Três Fronteiras, Turmalina, Urânia, Valentim Gentil and Vitória Brasil (BRASIL, 2015).

In a survey carried out for the first five months of 2022, there were more than 35 thousand new microenterprises (ME) and small businesses (EPP) registered by the Board of Trade of the State of São Paulo (JUCESP), an agency linked to the Secretariat of Economic Development. Presenting a rate of 7% more than the period last year.

The LIDE Northwest São Paulo Business Climate Survey, published on September 29, 2020, revealed that companies in the northwest of São Paulo continue to grow, especially with regard to micro and small companies, despite the economic uncertainties caused by the context that Brazil experienced, in the face of the spread of the coronavirus at the time, which hindered the full exercise of most of the economic activities developed in the region.

In a survey carried out by SEBRAE/SP (2018), in relation to the panorama of small businesses in the state of São Paulo in 2018 in each business sector, 41% of the total is represented by the service sector, totaling 1,118,986 small businesses in which their market segment is disregarded: restaurants, hairdressers and road cargo transport, followed by commerce with 37% which represents 1,002,276 small companies, In third place is the industrial sector with 12% of the total that has 313,196 small businesses in which it is represented by the manufacture of parts, catering services, catering and bakeries, in addition, in fourth place the construction sector with 7% and 179,639 small businesses in which it represents the various and specialized services for construction, Finally, the agricultural sector, which represents 3%, with 74,269 small businesses, which represents cattle breeding, activities related to landscaping and horticulture. The São Paulo revenue of MSEs for the year 2017 was also estimated, in which R$ 635.9 billion in revenues were collected.

## 7 CONCLUSION

When a law comes into force that changes the way companies were used to dealing, they initially struggle to adapt, needing to undergo transformations in their routines and train employees. In order to be able to emerge and guarantee the security of your information, it is necessary that an agreement is made between the parties in a clear and transparent way, based on a contract.

Contemporary society, throughout its evolution, has become governed by data, under a historical scenario about the evolution of norms that deal with personal information. Since the promulgation of the Federal Constitution, there has been a tendency of laws to guarantee the protection of the fundamental right to privacy of individuals, especially in a society where the great challenge is to deal with the use of personal data in an economic bias, that is, in front of registration databases, which manipulate them to understand the characteristics of individuals and sometimes offer provision of services appropriate to the niche in which the person is. Thus, it was possible to understand that the LGPD came to deal specifically with the protection of personal data and that they are Fundamental Rights, integrated into the right to privacy.

Once the data protection rules have been clarified, When companies receive them, whether arising from consumer or labor relations, they need to adopt all legally possible mechanisms for processing, and one of the ways to do this is to observe the application of the LGPD in contracts of the most diverse modalities, thus becoming another element of importance, indispensable for contracts that involve customers' personal information.

By performing all of this analysis, it is noted that it is essential for the company to have a contractual model that specifies clauses related to LGDP, to protect itself from alleged data leaks and civil liability, the interpretation of which evidences the repair of the damage, which shows once again the importance of companies complying.

## REFERENCES


BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, 2020 Disponível em:< http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 20 jun. de 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 jan. de 2022.

BRASIL, Lei n º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União Brasília, DF, 11 jan. 2002. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 20 abril de 2022.

BRASIL, Superior Tribunal de Justiça. Súmula nº 404. Súmulas. Revista de Súmulas do Superior Tribunal de Justiça, ano 8, v. 38, p. 131-173, fevereiro 2014. Disponível em: "https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula404.pdf". Acesso em: 15 mai. 2022.

BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. Relator(a): min. Rosa Weber. Data de julgamento: 07 mai. 2020. Disponível em: "https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629". Acesso em 20 jul. 2022.

BRASIL, 2006. Lei Complementar 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. Diário Oficial da União. Brasília, 14 dez. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm Acesso em: 20 abril de 2022.

BOSSOI, R.A.C. O descumprimento das empresas à implementação do projeto de conformidade à LGPD (Lei Geral de Proteção de Dados Pessoais) e suas consequências. OAB 32º subseção de Lins, Lins, 30 set. 2020. Disponível em: "https://www.oabsp.org.br/subs/lins/noticias/artigo-o-descumprimento-das-empresas-a". Acesso em: 15 jul. 2022."

DONDA, D. Guia Prático de Implementação da LGPD. São Paulo: Labrador, 2020.

É RIO PRETO. Pesquisa divulgada pelo LIDE Noroeste Paulista mostra que 58,3% aumentaram seus rendimentos. Disponível em: <https://eriopreto.com.br/noticia/pesquisa-divulgada-pelo-lide-noroeste-paulista-mostra-que-58-3-aumentaram-seus-rendimentos/4779>. Acesso em: 01 de dezembro de 2021.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed.13.reimpr. São Paulo: Atlas, 2009.

KOHLS, C.; DUTRA, H.L.; WELTER. S. LGPD: da teoria a implementação nas empresas. 1.ed. São Paulo: Rideel, 2021. LIMA, Adrianne *et al.* LGPD para contratos: Adequando contratos e documentos à Lei Geral de Proteção de Dados. Ed. Saraiva, SP: Bela Vista, 2022.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito, *[S. l.]*, v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 10 jul. 2022.

LEITE, Luciano Vasconcelos *et al*. Manual de implementação da Lei Geral de Proteção de Dados.1. Ed. São Paulo, SP: Via Ética, 2019.

LIMA, A *et al.* LGPD para contratos: Adequando contratos e documentos à Lei Geral de Proteção de Dados. 1. Ed. São Paulo, SP: Saraiva, 2022.

MANUAL Básico de LGPD. Florianópolis: Neoway, 2018. Disponível em: < https://f.hubspotusercontent10.net/hubfs/7323764/files/pdf/neoway-lgpd-manual-0902.pdf > Acesso em 19 abr. 2022.

MENDES, L. Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Série IDP: linha de pesquisa apud

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito, *[S. l.]*, v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 10 jul. 2022.

MARCONI, M. A.; LAKATOS, E. M. Metodologia científica. 5. ed. São Paulo: Atlas, 2009.

NACIONAL, Sebrae. Confira as diferenças entre microempresa, pequena empresa e MEI Disponível em: < https://www.sebrae.com.br/sites/PortalSebrae/artigos/entenda-as-diferencas-entre-microempresa-pequena-empresa-e-mei,03f5438af1c92410VgnVCM100000b272010aRCRD >. Acesso em: 17 set. 2022.

OLIVEIRA, Moacyr de. "Intimidade", in Enciclopédia Saraiva do Direito. São Paulo: Saraiva, 1980 apud

SILVA, J. Afonso da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, ed. 39, 2016.

PEREIRA, J. Matos. Direito de informação. Lisboa: Associação Portuguesa de Informática, ed. do autor, 1980 apud.

SILVA, J. Afonso da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, ed. 39, 2016.

SILVA, D. C, AUROCA, A. C. Manual da Lei Geral de Proteção de Dados para Instituições de Ensino [livro eletrônico]. 1. Ed. Brasília.2020. PDF

SCHWAITZER L. S. LGPD E ACERVOS HISTÓRICOS: impactos e perspectivas. Archeion Online, *[S. l.]*, v. 8, n. 2, p. 36–51, 2020. DOI: 10.22478/ufpb.2318-6186.2020v8n2.57020. Disponível em: https://periodicos.ufpb.br/ojs/index.php/archeion/article/view/57020. Acesso em: 1 ago. 2022.

SALES SARLET, G. B.; LINDEN RUARO, R. A PROTEÇÃO DE DADOS SENSÍVEIS NO SISTEMA NORMATIVO BRASILEIRO SOB O ENFOQUE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, *[S. l.]*, v. 26, n. 2, p. 81–106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 05 jul. 2022.

SANTOS, A. L.; KREIN, J. D.; CALIXTRE, A. B. Micro e pequenas empresas: mercado de trabalho e implicação para o desenvolvimento. Brasília: Ipea, 2012. Disponível em: < https://www.dbd.puc-rio.br/ipea/livro_micro_pequenasempresas.pdf>. Acesso em: 17 set. 2022.

## ANNEX 01 – Example of Contract

### CLAUSE BETWEEN COMPANY AND CUSTOMER

For the purposes of this agreement, the definitions below, when used in capital letters, singular or plural, shall have the following meanings:

a) "Personal Data": data and information obtained by any means, capable of identifying or making identifiable natural persons, including data that can be combined with other information to identify an individual, as established in Law 13,709/18;

b) "Owner": natural person to whom the Personal Data that are subject to Processing under this Agreement as established in Law 13,709/18 refers;

c) "Processing" (as well as the related terms "Treat", "Treaties"): have the meaning established in Law 13,709/18; and

d) "Incident": any and all improper Processing of Personal Data that results in a breach or possible breach of security that causes, accidentally or intentionally and in an unauthorised manner, the destruction, loss, blocking, alteration, disclosure or access to personal data.

1. The SERVICE PROVIDER**, by itself and its employees, undertakes to act in this Agreement in accordance with the rules in force on the Protection of Personal Data and the determinations of supervisory bodies on the matter, according to Law** 13.709/2018, in addition to the other data protection regulations and policies of each country where it has any type of processing of customer data, This includes the company's customer data.

1.1 The PARTIES agree that, within the scope of the execution of this Agreement**, the Client** is the data subject, while the Company will act as the controller of the Personal Data, thus applying to the PARTIES the obligations and responsibilities provided for in the applicable legislation with regard to its performance.

1.2 In the process of handling the data, the **Company** shall:

(a) To process the personal data to which it has access in accordance with the wishes and instructions of **the CONTRACTING PARTY and in accordance with these clauses, and which, if it is eventually unable to comply with these obligations, for whatever circumstantial reason, intends to formally inform** the CONTRACTING PARTY promptly of this fact, which shall have the right to terminate the contract without any charge, fine or charge.

(b) Preserve and make use of administrative, technical, and physical security measures necessary and effective to protect the integrity and confidentiality of all Personal Data held or that may be accessed or consulted electronically, to ensure the protection of such data

against unauthorized search, disclosure, use, modification, destruction, or accidental or improper loss.

(c) Access the information following the guidelines stipulated in the contract and within the limits permitted by the **prior consent of the Client** and the Personal Data may not be read, copied, modified or removed without the express written authorization of the **Client**.

(d) To undertake, by itself or its employees, agents, partners, directors, representatives or contracted third parties, the confidentiality of the personal information processed, certifying that all its employees, agents, partners, directors, representatives or third parties hired who deal with the Personal Data under the responsibility of the **CLIENT** have signed a Confidentiality Agreement with the **SERVICE PROVIDER**, as well as to keep all Personal Data secure and not to use it for a purpose other than that which is the subject of the contract, except for the provision of services to the **CONTRACTING PARTY**. You should also train and guide your staff on regulatory content that can be applied to data protection.

2. Personal Data may not be disclosed to third parties, except with prior authorization written by the **CONTRACTING PARTY**.

2.1 In the event **that the Company** is obliged to provide personal data to a public authority in order to comply with a legal order, it shall inform the Client in advance so that it may take the measures it deems necessary.

2.2 The **Company** shall notify the **Client** within twenty-four (24) days in the following situations:

a) Any occurrence or suspected Incident by the **Company,** its employees, or authorized third parties, with the presentation to the **Client of** all available information and details about such Incident, including the fact that occurred, the identification of which Personal Data was affected, the measures taken (and those in the process of being taken) to mitigate the effects of such Incident, as well as the effects of the Incident foreseen and those already identified.

b) Any other breach of security in the exercise of the Company's responsibilities and activities.

c) Any specific fact or situation that reasonably prevents the **Company** from complying with any of its obligations under this Agreement or under the applicable legislation in the context of the Processing of Personal Data.

2.3 The **SERVICE PROVIDER** shall be responsible, for itself and its Employees, for the Processing of Personal Data carried out within the scope of this Agreement and the relationship between the PARTIES, assuming responsibility for the payment of moral and material losses and

damages, as well as for the reimbursement of the payment of any penalty or fine imposed on the **CONTRACTING PARTY** and, or to third parties when it arises from the Company's non-compliance with any of the clauses set forth in this instrument, related to the use and protection of personal data.

3. The Company **acknowledges that after the purpose of the Processing has been achieved in relation to the Permitted Uses and/or the contractual relationship between the PARTIES has been terminated and/or after receiving a request for deletion of** the Client's Personal Data, the **Company** shall destroy the Personal Data, unless it has to keep them by legal obligation.

4. The jurisdiction of the District of the domicile of the CONTRACTOR is hereby elected.