

Challenges Regarding the Compliance with the General Data Protection Law by Brazilian Organizations: A Survey

Edna Dias Canedo[2(✉)], Vanessa Coelho Ribeiro[1,3], Ana Paula de Aguiar Alarcão[1], Lucas Alexandre Carvalho Chaves[1], Johann Nicholas Reed[1], Fábio Lúcio Lopes Mendonça[1], and Rafael T. de Sousa Jr[1]

[1] National Science and Technology Institute on Cyber Security, Electrical Engineering Department (ENE), University of Brasília (UnB), Brasília, DF, Brazil
{vanessa.ribeiro,Johann.reed,fabio.mendonca}@redes.unb.br, 160001986@aluno.unb.br, desousa@unb.br

[2] Department of Computer Science, University of Brasília (UnB), Brasília, DF, Brazil
ednacanedo@unb.br

[3] University Center Uniprojeção, Brasília, DF, Brazil

Abstract. Brazilian organizations must comply with the Brazilian General Data Protection Law (LGPD) and this need must be carried out in harmony with legacy systems and in the new systems developed and used by organizations. In this article we present an overview of the LGPD implementation process by public and private organizations in Brazil. We conducted a literature review and a survey with Information and Communication Technology (ICT) professionals to investigate and understand how organizations are adapting to LGPD. The results show that more than 46% of the organizations have a Data Protection Officer (DPO) and only 54% of the data holders have free access to the duration and form that their data is being treated, being able to consult this information for free and facilitated. However, 59% of the participants stated that the sharing of personal data stored by the organization is carried out only with partners of the organization, in accordance with the LGPD and when strictly necessary and 51% stated that the organization performs the logging of all accesses to the personal data. In addition, 96.7% of organizations have already suffered some sanction / notification from the National Data Protection Agency (ANPD). According to our findings, we can conclude that Brazilian organizations are not yet in full compliance with the LGPD.

Keywords: Brazilian General Data Protection Law – LGPD · LGPD compliance · Personal data processing · Data privacy

1 Introduction

The presence of Information and Communication Technology (ICT) in society brought several benefits, such as access to information in an easier way and

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12951, pp. 438–453, 2021.
https://doi.org/10.1007/978-3-030-86970-0_31

the possibility of communicating with people who are geographically distant. However, this strong presence often requires the use of personal data both in services, in the availability of resources and in business/commercial transactions. This process leads to an exponential growth in the use of personal data, making it necessary to review the regulation of how this data is treated for the protection of individuals [1].

Based on this assumption, several laws have emerged with the aim of protecting personal data, such as the General Data Protection Regulation (GDPR) [2] in the European Union, Australian Privacy Principles (APP) in Australia [3] and California Consumer Privacy Act (CCPA) in the United States [4]. With the creation of these laws, the way in which countries manipulate and store information has changed. After the creation of the GDPR, for example, several countries in the world had to modify or even create laws that regulate the protection of personal data in order to comply with the guidelines defined in the European regulation [5].

Brazil was one of the countries that needed to adapt to the GDPR guidelines, since the nations belonging to the European Union make up the country's main economic partners [6,7]. Thus, in September 2020, Law No. 13,709 / 18, called the Brazilian General Data Protection Law (LGPD), came into force [8], [9]. With the LGPD, companies that have personal information stored in their systems must pay attention and follow the guidelines and principles established so that the data is kept safe.

It is possible to observe the movement of many companies to adapt to the LGPD and to create tools that facilitate this implementation in the daily lives of the institutions. An example is the LGPD Educational platform, created by the Data Processing Service - (SERPRO), which offers professional training and certification for the public and private sectors in disciplines related to privacy and protection of personal data [10]. It should be noted that by the end of 2020, surveys pointed out that around 64% of Brazilian companies were not in compliance with the new legislation [11].

Given the above, the objective of this article is to identify the current situation of the implementation of LGPD in Brazil, in public and private organizations, identifying the level of knowledge and compliance with the legislation. The main findings of this article were: more than 75% of the survey participants informed their organization that they treat personal information for legal purposes (according to the permissions granted by legislation); more than 62% stated that the organization controls personal data considered sensitive by the LGPD; more than 46% stated that The organization maintains an inventory of all sensitive information (including personal data) stored, processed or transmitted by the Institution's IT systems, at physical locations and remote service providers and more than 57% stated that the organization has a specific privacy policy related to privacy and data protection.

2 Background

Law No. 13,709 / 2018, called the Brazilian General Data Protection Law (LGPD) [12], of August 14, 2018, is the law that regulates activities involving the processing of personal data, including digital media, with the purpose of protecting the fundamental rights of the citizen to freedom and privacy, as well as the free development of the personality of the natural person, as natural persons are called within the law. Although these fundamental rights are already protected by the Federal Constitution of 1988, it was only after the enactment of the LGPD that the privacy of personal data acquired a similar relevance [13]. It is noteworthy that this regulation did not revoke the previous laws that were used to deal with data privacy (Consumer Protection Code, Brazilian Civil Code and Civil Framework of the Internet), which still remain in force, since they do not conflict with the new law, but are complemented by it, as there were many gaps that needed to be filled around this issue.

Article 1 of the LGPD gives a general definition of what will be covered in the Law, a general scope and an objective. Article 2, on the other hand, deals with the fundamentals of data protection that the Law will be based on, such as respect for privacy, freedom of expression, free initiative and human rights [12].

Article 3 establishes that the law applies to any processing operation carried out by legal or natural personnel, under public or private law, regardless of the means, provided that the data processing has been carried out in national territory, or has the objective of the provision of goods and services, or that data has been collected in Brazil. Whereas Article 4 deals with cases to which the Law does not apply: treatment carried out by natural persons for private, journalistic and artistic purposes, academic or for public security, national defense, State security and investigative activities [12].

Article 5 of the Law establishes the definitions for terms used in the law, such as the definition of titleholder, personal data, sensitive personal data, database, consent, shared use of data and others that can be found in the law [12]. Article 6, on the other hand, defines the principles to be observed in the data processing process as the purpose for this, adequacy, data quality, transparency, accountability and accountability, among others.

Articles 7 and 8 concern the possibility of processing personal data. In order for this process of handling personal information to be legitimate, the legislation lists an exhaustive list of circumstances that allow this treatment. Article 9 of the law deals with the data subject's rights in relation to facilitated access to information on data processing. Article 10, in turn, deals with the duties of the data controller in relation to the legitimate purposes of carrying out the processing of the data.

The LGPD covers any transaction involving the processing of data by individuals or legal entities, under public or private law, that is carried out in Brazilian territory, regardless of where the data is initially located. Personal data is classified as information related to a natural person, such as Individual Taxpayer Registration (CPF), Number of the General Registry (RG), Name and Education Level. The processing of personal data is defined by law as any operation

carried out with personal data, including any activity carried out that uses personal information, such as storage, transmission, modification, use and access. In addition, the law requires companies to collect the minimum possible amount of data they need and process it only on legal grounds. The Law also encompasses scenarios where the data are from individuals located or whose data are collected in the national territory. Thus, in order to comply with the LGPD, Brazilian companies must take, among others, the following measures:

1. Analyze and verify which data falls within the scope of the LGPD as this information is processed;
2. Correct incomplete, inaccurate or outdated data;
3. Obtain information about public and private entities with which the controller shared the data;
4. Obtain information about the possibility of the information holder denying consent and the consequences of such denial.

Although the LGPD was based on the GDPR and has many aspects in common, the Brazilian privacy regime has some particularities, which must be taken into account by those who are subject to this law. LGPD does not apply only to companies located in Brazilian territory: In addition to being employed by any company that operates in Brazil or that sells its goods and services there, it also applies to global businesses that are processing information in Brazil or that use personal data of individuals located in Brazil, regardless of the means used for processing and whether this is done directly or indirectly.

The qualification of a legal basis for data processing is one of the main differences between LGPD and GDPR. According to the LGPD, the protection offered is limited to data that qualifies as personal data, offering two levels of protection, depending on whether the data is classified as personal data or sensitive personal data. However, the vast majority of data subject to the application of the LGPD fall within the general definition of personal data, which is considered "information about an identified or identifiable natural person" (Article 5, I) [12]. When compared to the European regulation, this definition applies not only to information directly linked to an individual, but also to any element that can be used to identify or potentially contribute to the identification of a person [13]. Although the GDPR has six legal bases for processing and the data controller company must choose one of them as a justification for using personal information, the LGPD has ten, which are defined in its article 7:

1. Have the consent of the data subject;
2. To aim to fulfill a legal or regulatory obligation of the controller;
3. Execute a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject;
4. Execute public policies provided for in laws or regulations, or based on contracts, agreements or similar instruments;
5. Conduct studies by research entities that guarantee, whenever possible, the anonymity of personal data;

6. Exercise rights in judicial, administrative or arbitration proceedings;
7. To aim to protect the life or physical security of the data subject or third parties;
8. Protect health, in a procedure carried out by health professionals or by health entities;
9. Meet the legitimate interests of the controller or of third parties, except when the fundamental rights and freedoms of the data subject, which require the protection of personal data, prevail;
10. Protect credit (referring to a credit score).

As for sensitive personal data, defined as information that relates to "racial or ethnic origin, religious belief, political, union or religious opinion, philosophical or political", the LGPD offers even broader protection. One of the fundamentals for the processing of this type of Personal Information is the prevention of fraud. According to this requirement, data processing must be legitimate, legal, non-fraudulent and transparent. They also require data from the controllers in order to guarantee the accuracy, completeness and security of the data and to provide the holders with access and portability rights. In addition, it is also possible for data controllers to report violations and dispense with the transfer of data to countries that do not have adequate protection conditions.

The protection of children's data has also been strengthened after the LGPD regulation. Although the protection of children and adolescents is guaranteed through Law No. 8,069 / 1990 (Statute of Children and Adolescents) and CF/88 itself, with the new personal data protection law, a child protection structure has been implemented. in which it is an absolute priority for all parties involved in the child's development [13]. In order for data to be processed for children and adolescents, controllers must have the consent of the child's legal guardian even before collecting the personal information of children under 16 years of age. In addition, any Information addressed to this audience must be clear and simple.

Both the GDPR and the LGPD determine that the data controller must provide the data holder, when requested, with a copy of all their personal information, which can be delivered electronically or in print within up to thirty days, with the extension of the deadline being permitted. However, the LGPD is somewhat more rigid in the way that information holders must respond to their respective owners. According to Brazilian law, in its article 19, the data controller company has up to fifteen (non-extendable) days to respond to the request of the holder, and must provide a clear and complete statement regarding the information it has. This statement must provide clarification of the source of the data, the lack of registration, the criteria used and the purpose of the treatment. However, the LGPD still allows the parent company to respond to the holder in a simplified format, making it possible to report fewer elements and less details.

Another similarity that can be observed between the LGPD and the GDPR is the requirement to hire a Data Protection Officer (DPO) by the data controllers. This professional should serve as a communication channel between the controllers, the information holders and the national data inspection body, the

National Data Protection Authority (ANPD) – which is responsible for inspecting and imposing sanctions. This obligation is given to oversee compliance and governance, in addition to including training, management and data governance. In addition, the DPO will be responsible for collecting complaints and communications from data subjects and ANPD, guiding employees on good practices and fulfilling other duties determined by the controller or by complementary rules [13].

The LGPD encourages institutions to comply with their requirements by imposing penalties, which may be warnings, suspensions, financial penalties or a ban on the exercise of their activities, for companies that fail to comply with the rules. To impose punishment or for non-compliance, LGPD regulatory and supervisory authorities have administrative powers to impose fines. In cases of more severe penalties, the fine imposed can reach 2% of the company's revenues or a maximum of R$ 50,000,000.00 for an infraction [13].

2.1 Related Works

Ribeiro and Canedo [7] carried out a study on the implementation of LGPD at the University of Brasilia (UnB), in order to minimize the challenges and identify the criteria for the implementation of security of personal data, and the main difficulties faced for the application, under this Law, how to identify all databases that store personal information, check what types of personal data are collected in the University's systems and forms, check for potential vulnerabilities that may cause loss, leakage or impair information access. Through the Analytical Hierarchy Process (AHP) method, the main criteria for the implementation of LGPD at UnB were determined, which are: Data Protection Level, Security Risk, Incident Severity and Data Privacy Risk.

Alencar [14] carried out a study comparing the Brazilian and Chilean Data Protection Laws in relation to the decision criteria on the adequacy of third countries provided for by the General Data Protection Regulation of the European Union (GDPR). Alencar made an analysis of the necessary requirements for adequacy granted by the European Commission, which are: fundamental principles, conducting the processing of sensitive data, automated decisions, supervisory authorities and mechanisms to protect data subjects. Thus, it was concluded that both countries have outdated legislation in relation to the European Regulation. This shows how the interest of Brazil and Chile in fulfilling the requirements is for economic purposes and not in actually protecting the rights of data subjects. The study also showed that the main flaw in Brazilian legislation is the lack of consolidation of a supervisory authority, which in this case would be due to the implementation of the National Data Protection Authority (ANPD). And finally, it was concluded that Chilean law is completely in line with European regulations, while Brazilian law is only partially due to the absence of effective supervisory authority and there is no express right of opposition on the part of the data subject regarding automated decisions.

Cantelle [15] held a debate on the importance of the existence of a legal framework on data protection in Brazil that establishes tools for the exercise of

data subjects' rights, minimum standards of security and privacy, legitimate use of data and consent of the holder. The author concludes that Marco Civil is very positive for the future development of the Brazilian General Data Protection Law, as the Brazilian population is in need of legal information about the limits of web users. In addition, it establishes that informing and educating citizens regarding new legislation will be essential.

Machado et al. [16] carried out an analysis based on the increase in security reports on sensitive data leaks and how it has affected companies and governments. It identified the socioeconomic impacts of significant leaks and how the latest data protection laws can help to combat the lack of investment in information security. In this article, the authors argue that recent reports show that 50% of security incidents are caused by malicious employees or former employees, and that a possible solution is to decrease access to data in plain text, using encrypted databases. In the case of Brazil, the LGPD provides for a fine of up to 2% of the annual turnover of legal entities in case of leakage of sensitive data, or up to R$50 million.

Souza et al. [17] presented the development of a tool that automates the service to users regarding LGPD issues. This way, the bot is able to answer questions instantly about information related to the Brazilian General Data Protection Law. In this study, an entire infrastructure using the LUIS service (Language Understanding Intelligent Service) and Natural Language Processing so that the communication between the user and the bot occurs in a more natural way, without seeming to be a conversation with the computer. With this study, a knowledge bank for making inquiries about LGPD and identifying the user's intention is used to provide this service.

Lehfeld et al. [18] studied how the Brazilian General Data Protection Law (LGPD) was applied and effective in protecting consumers and its relationship with the occurrence of cyber-crimes, mainly related to consumer protection in the face of abusive practices by companies with fundamental data. This research showed that, although the Internet is constantly growing, the ways of combating digital crimes are still elementary, with few activities effectively typified as crimes. The study also deals with the vulnerability of cyber space under the optimum of digital consumption and how the Brazilian General Data Protection Law reaffirms the need for individuals to be protected as virtual consumers and owners of their data.

Renner et al. [19] carried out a study in Brazilian organizations regarding the adequacy to LGPD based on a survey carried out with IT workers in each company in the public and private sphere. A survey was applied with the objective of carrying out an assessment and in relation to the adequacy and perception of organizations in relation to the LGPD, collecting the individual perception of the IT employees of each company. From there, the level of compliance that these companies have with the Law can also be analyzed.

The survey respondents consisted of several IT professionals from the public and private sectors from different areas and profiles who are involved in the processing of personal data, such as developers, systems analysts, requirements

analysts and project managers. Out of a total of 105 IT professionals, 64% of employees worked in companies with more than 400 employees, while 17.1% work in companies with less than 20 employees. Of the total, 37.1% work for the private sector and the remaining 62.9% work for the public sector. As a result, the authors identified that only 25% of the companies, according to the professionals, adhered to the personal data processing from LGPD, while 11% did not. These and other results showed that the principles of LGPD are still in the initial phase of implementation in companies and a large proportion of correspondents stated that their company had not yet started a plan or initiative to implement LGPD [19]. This study indicated that it is possible to observe the lack of maturity in relation to governance and data management, privacy and information security on the part of most Brazilian organizations and that a possible solution to this lack of maturity will be the establishment of the National Data Protection Agency (ANPD) to monitor the adherence of organizations to the LGPD.

Canedo et al. [20] conducted a survey with ICT professionals from different organizations to gain an insight into how these people understand the LGPD guidelines and how these guidelines are being addressed in the software development process in companies. With the completion of the study, the authors observed that the majority of professionals who responded to the survey are aware of the changes that LGPD would bring to company processes. In addition, these professionals declared that they do not have the necessary knowledge to implement the principles and guidelines of the LGPD, in addition to the organizational environment itself interfering in privacy practices. The authors observed a certain deficiency in the disclosure of information and the promotion of training on LGPD by companies to train their members, as well as in their own privacy policies (which were often unknown to employees). In addition, a literature review was also carried out in order to identify proposed methodologies for obtaining software privacy and privacy requirements. According to the authors, several studies have been found in the literature that propose some techniques for software privacy, but no reports have been found of the use of these methodologies by the industries, being restricted only to theory.

3 Study Settings

The aim of this study is to understand and understand the guidelines of the Brazilian General Data Protection Law and how its principles are being treated by Brazilian organizations. Thus, we conducted a literature review, in order to identify related works related to LGPD. In addition, to investigate and understand how the Law is doing, what aspects were addressed by the organizations that implemented the LGPD and the current scenario in the adequacy of these organizations in relation to the LGPD, we conducted a survey. The questionnaire was prepared considering the principles of the LGPD and the related works identified in the literature that addressed the implementation of the legislation and the implementation guides.

The survey developed has 40 questions, 38 of which are closed and 02 are open, using mainly the Likert scale [21]. The survey was designed along three axes: demographic issues, general issues unrelated to the LGPD, and questions about the principles and compliance with the LGPD. We made the survey available through google forms and the response time of the participants was approximately ten minutes. In addition, the survey was available for 30 days. In total, 61 practitioners responded to the survey.

4 Results

The survey was answered by 61 professionals in the area of Information and Communication Technology (ICT) from public and private Brazilian organizations. Figure 1 shows the distribution of the nature of the organizations that the survey participants work with. 57.4% of participants work in private organizations and 42.6% in public organizations. With this number, we can see that there is a good balance in the nature of the organizations that the participants work with, helping to measure the adequacy of Brazilian companies in general.

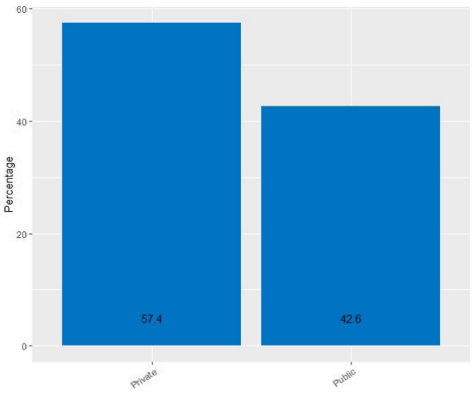

Fig. 1. Nature of the organization

Regarding the role of the ICT practitioner in the organization, 24.6% have the role of responsible for Infrastructure and Networks, 18% are professionals in the area of Information Security, 14.8% are developers, 13.1% are professionals in Database and Business Intelligence, 9.8% work in ICT Management or Governance and 8.2% are Software Engineers. 77% of the participants are male and only 23% are female. 16.4% of the participants stated that they have less than one year of experience, 11.5% stated that they were between 1 and 3 years old, 13.1% stated that they were between 4 and 6 years old, 4.9% between 7 and 9 years old, 6.6% between 10 and 13 years old, 11.5% between 14 and 15 years old and 36.1% stated that they have more than 16 years of experience, as shown in

Fig. 2. With these results we can conclude that most participants have extensive experience in the area of ICT.

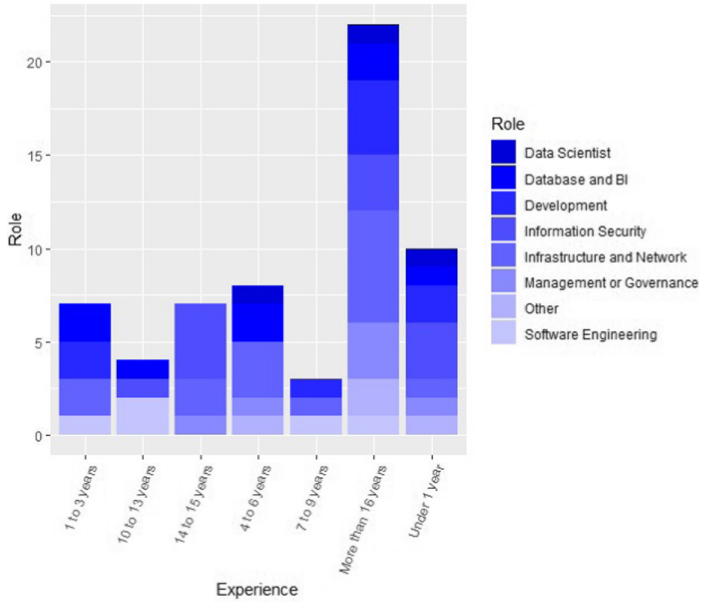

Fig. 2. Role in organization and experience

92% of the participants reported that they are aware of the Brazilian General Data Protection Law (LGPD), as shown in Q5 of Fig. 3. 61% of the participants reported that their organization is in compliance with the LGPD, 16% did not know how to inform, and 23% of the participants informed that their organization is not in conformity with the LGPD, as presented in Q6 of Fig. 3. 56% of the participants informed that the organization has a responsible sector to verify the conformity of its activities with to LGPD, 16% were unable to inform and 28% reported that the organization does not have a responsible sector to verify compliance (Fig. 3 Q7). 46% of the participants reported that the organization has a specific professional who is responsible for data protection (DPO - Data Protection Officer) (Fig. 3 Q8). This finding is worrying because less than 50% of organizations have a DPO and one of the obligations determined by the LGPD is that the organization has a DPO. 54% of respondents stated that organizations provide training and lectures to raise employee awareness and guidance on practices that must be adopted to comply with data protection principles (Fig. 3 Q9). 33% of organizations use a specific methodology or technique to elicit privacy requirements. This is also far below what is expected, as a data privacy policy needs to be defined so that organizations can comply with the LGPD (Fig. 3 Q10).

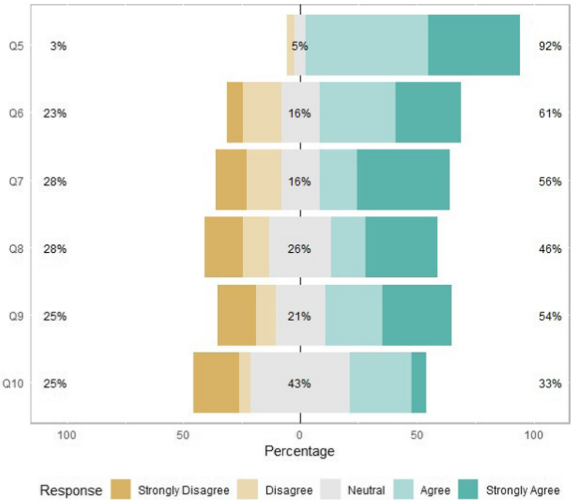

Fig. 3. Question results 5 to 10

Regarding issues related to the LGPD principles, 75% of the participants reported that the organization handles personal data for legal purposes (Fig. 4 Q13), according to the permissions granted by legislation and 79% reported that the organization only uses personal data for the purpose proposed and agreed with the user, limiting their processing to the minimum possible to carry out their activities (Fig. 4 Q14). 69% strongly agree and agree that the process used by the organization is transparent to users, providing them with clear and accurate information about what is being done with their personal data and about the treatment agents (Fig. 4 Q15). 77% of the participants reported that the organization is concerned with the security of the personal data it has control over, adopting effective technical and administrative measures to provide protection against unauthorized access to this information and against accidental or unlawful situations of destruction, loss, alteration or dissemination of personal data (Fig. 4 Q16). 54% stated that the holders have free access to the form and duration that their data is being treated, being able to consult this information for free and facilitated, as shown in 4. Finally, 67% reported that the stored personal data they have accuracy, clarity, relevance and are constantly being updated to fulfill the purpose of their treatment (Fig. 4 Q18).

In matters related to LGPD compliance, 62% of organizations control personal data deemed sensitive by LGPD (Fig. 5 Q19). In 57% of organizations there is a different treatment for sensitive information (Fig. 5 Q20); 46% of organizations maintain an inventory of all sensitive information (including personal data) stored, processed or transmitted by the Institution's IT systems, at physical locations and remote service providers (Fig. 5 Q21). 80% of organizations allow access to personal data only by authorized persons (Fig. 5 Q22). This

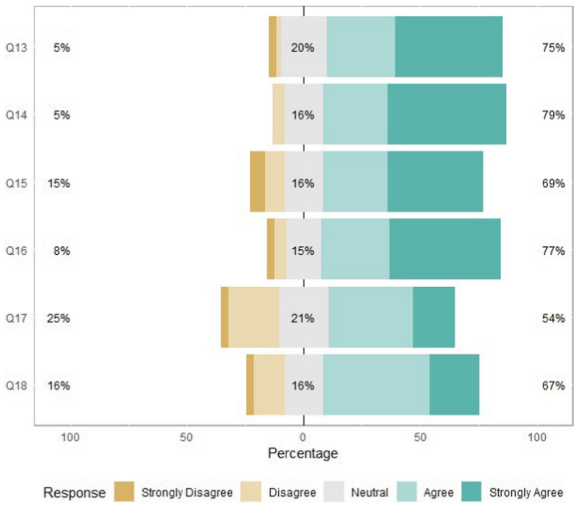

Fig. 4. Principles of LGPD

result allows us to infer that the organizations participating in the survey are in compliance with the principles of the LGPD.

Only 25% of the organizations treat personal data of children and adolescents (Fig. 5 Q23) and only 22% of them carry out the different treatment of the personal data of children and adolescents (Fig. 5 Q24). According to this result, we concluded that more than 70% of the organizations participating in the survey do not deal with data from children and teenagers.

41% of suppliers, contractors and service providers linked to the organizations participating in the survey are in compliance with the LGPD guidelines (Fig. 5 Q25) and share personal data stored only with partners of the organization, in accordance with the LGPD and when strictly necessary (Fig. 5 Q26). 77% of organizations periodically back up data controlled by them (Fig. 5 Q27) and risks related to the security of personal data are identified and documented frequently by 62% of organizations (Fig. 5 Q28). Finally, 51% of organizations log all access to the personal data they maintain, as shown in Q29 in Fig. 5.

49% of organizations regularly review log records in order to identify anomalies or abnormal events (Fig. 6 Q30) and 56% of organizations have an incident response and remediation plan for data leakage situations (Fig. 6 Q31). 31% of participants reported that organizations have performance indicators (Key Performance Indicator - PKI) to check for gaps in data governance and privacy policy (Fig. 6 Q32) and 30% of organizations continually discard unnecessary and excessive data (Fig. 6 Q33). 49% of organizations constantly assess whether there is a legal need to keep personal data, as well as how long it will be kept (Fig. 6 Q34). Regarding physical documents (on paper, such as resumes), 48% of participants reported that the organizations they work with perforate the documents before they are discarded (Fig. 6 Q35). In 57% of organizations there is

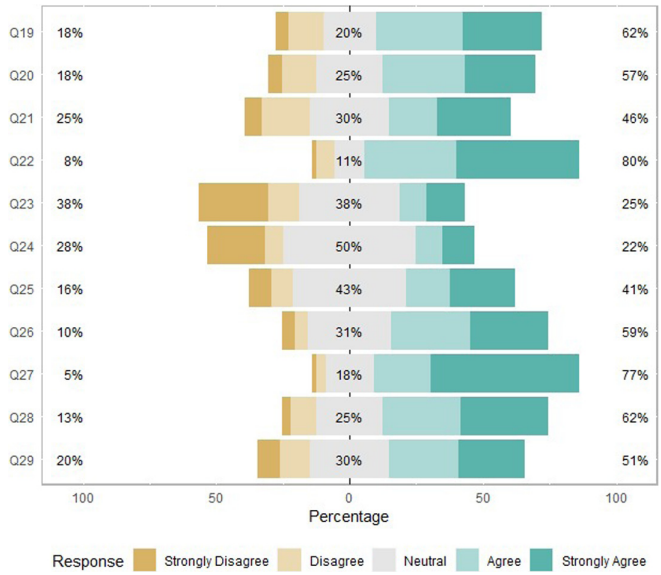

Fig. 5. Compliance LGPD Q19 to Q29

a specific privacy policy related to privacy and data protection (Fig. 6 Q36) and 62% have information security policies accessible to all employees in the organization (Fig. 6 Q37). 46% of organizations use encryption techniques to anonymize controlled data (Fig. 6 Q38) and only 33% of organizations anonymize all user data, as shown in Q39 in Fig. 6. This result is quite worrying, since that one of the principles of LGPD is data anonymization and few organizations carry out this activity.

96.7% of the professionals who participated in the survey, reported that their organizations have already suffered some sanction/notification from the National Data Protection Agency (ANPD), as shown in Fig. 7. This result allows us to conclude that Brazilian organizations are not yet in compliance with the LGPD, since the number of sanctions by the body responsible for controlling the implementation of the LGPD is very high.

In relation to open questions, participants were asked in relation to which methodology and/or technique the organization uses to elicit privacy requirements. Some responses were: "In the process of implementing the LGPD, we use risk management to carry out the controls" and "We use the Trusted Development Guide, developed by the organization itself". Regarding which techniques or methodologies practitioners know and use to elicit privacy requirements in the organization, some of the answers were: Lean Inception, Questionnaires, Personas, Use Cases, Prototyping, Brainstorming and Interviews.

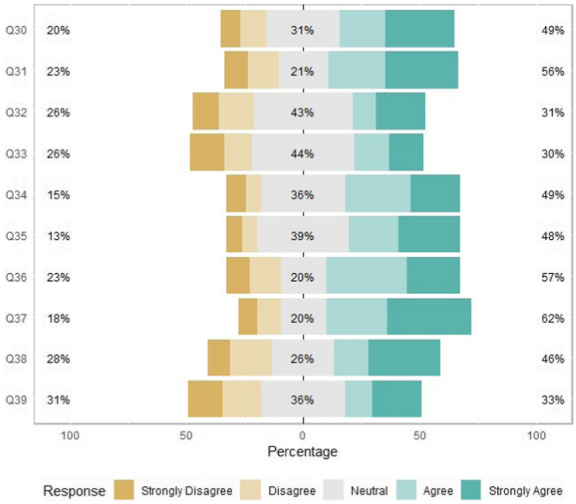

Fig. 6. Compliance LGPD Q30 to Q39

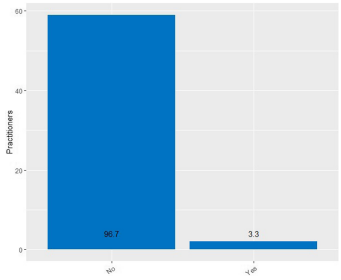

Fig. 7. Organizations that have suffered sanctions/ANPD notifications

5 Threats to Validity

As with any survey that investigates users' perceptions of a given scenario, we have some threats to validity. Regarding the fidelity of the practitioners' responses, we cannot guarantee that they all responded according to the real scenario of the organizations and whether the information really represents what the organization does on a daily basis. To mitigate this threat, we made it clear to all participants that the name of the professional and the organization in which they work would not be disclosed and that the responses would not be disclosed to expose the organization's possible weaknesses.

Another threat is related to the number of responses. In Brazil, we understand that there are a large number of public and private organizations and we understand that 61 participants are a small sample in relation to the number of organizations existing in Brazil. As the participants are from different public and private organizations, we believe that this sample is quite significant, as it allows

us to have an overview of the current situation, but of course, we also understand that we cannot generalize this result from the sample that participated in the survey.

6 Conclusions and Future Work

In this article, we conduct a survey to investigate how companies are adapting to the LGPD principles and whether they are in compliance with them. Most of the practitioners who participated in the survey have more than 16 years of experience in ICT. The results reveal that practitioners know the principles of LGPD and that the organizations they work with are adapting to what is required by legislation. Most organizations have a DPO and are training their employees in relation to the LGPD.

According to our findings, we can conclude that Brazilian organizations are adopting sensitive data control mechanisms and are committed to achieving compliance with the LGPD. Although, concerns about the anonymization of user data are not yet a concern of organizations and several organizations have received sanctions/notifications that can be applied by the ANPD.

Acknowledgments. The authors would like to thank the support of the Brazilian research, development and innovation agencies CAPES (grants 23038.007604/2014-69 FORTE and 88887.144009/2017-00 PROBRAL), CNPq (grants 312180/2019-5 PQ-2, BRICS2017-591 LargEWiN, and 465741/2014-2 INCT in Cybersecurity) and FAP-DF (grants 0193.001366/2016 UIoT and 0193.001365/2016 SSDDC), as well as the cooperation projects with the Ministry of the Economy (grants DIPLA 005/2016 and ENAP 083/2016), the Institutional Security Office of the Presidency of the Republic (grant ABIN 002/2017), the Administrative Council for Economic Defense (grant CADE 08700.000047/2019-14), and the General Attorney of the Union (grant AGU 697.935/2019).

References

1. Erickson, A.: Comparative analysis of the eu's gdpr and brazil's lgpd: enforcement challenges with the lgpd. Brook. J. Int. L. **44**, 859 (2018)
2. European Union. General data protection regulation (gdpr). Intersoft Consult. **1**(1), 1–100 (2018). Accessed 24 Oct 2020
3. Australian Government Federal Register of Legislation. Privacy act (1988) https://www.legislation.gov.au/details/c2021c00139, Accessed 4 Apr 2021
4. Code Section Group: California consumer privacy act of 2018. Accessed 14 2021
5. Ribeiro, R.C., Canedo, E.D.: Using mcda for selecting criteria of lgpd compliant personal data security. In: The 21st Annual International Conference on Digital Government Research, dg.o '20, New York, NY, USA, pp. 175–184. Association for Computing Machinery (2020). https://doi.org/10.1145/3396956.3398252
6. Ministério da Economia. Comercio exterior brasileiro, https://www.gov.br/produtividade-e-comercio-exterior/pt-br/assuntos/comercio-exterior/estatisticas, Accessed 30 Mar 2021

7. Ribeiro, R.C., Canedo, E.D.: Using MCDA for selecting criteria of LGPD compliant personal data security. In: Eom, S.J., Lee, J. (eds.) dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul, Republic of Korea, 15–19 June 2020, pp. 175–184. ACM (2020)
8. Presidência da República. Lei Geral de Proteção de Dados (2018). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, Accessed 22 Mar 2021
9. Governo Federal. Guia de boas práticas para implementação na administração pública federal (2020). https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf, Accessed 20 Mar 2021
10. Serpro. Governo federal lança plataforma lgpd educacional. Serpro (2021)
11. Serpro. Pesquisa indica que 64% das empresas não estão em conformidade com a lgpd. InfoMoney (2020)
12. Pereira Neto Macedo. Brazilian general data protection law (lgpd). Braz. Natl. **1**(1), 1–16 (2018). Accessed 18 Oct 2020
13. Khyara Passos. Compliance with brazil's new data privacy legislation: What u.s. companies need to know. SSRN (2021)
14. Alencar, A.D.S.: ProteÇÃo de dados pessoais no brasil e no chile: Uma anÁlise comparativa sob a perspectiva da decisÃo de adequaÇÃo da comissÃo europeia. Observatório da LGPD, pp. 1 (2020)
15. Cantelle, A.: Marco civil da internet e proteção de dados pessoais 2017. conteúdo Jurídico, p. 1 (2020)
16. Machado, R., Kreutz, D., Paz, G., Rodrigues, G.: Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteçãoo de dados. Anais da Escola Regional de Redes de Computadores (ERRC) (2019)
17. Ferreira De Jesus, A.P., et al.: Robôde conversação baseado em inteligência artificial para treinamento na lei geral de proteção de dados pessoais. Unisanta Science and Technology, pp. 1–10 (2020)
18. de Souza Lehfeld, L., Celiot, A., Siqueira, O.N., Barufi, R.B.: A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da lgpd. In: Revista Eletrônica Pesquiseduca, p. 10 (2021)
19. Ferrão, S.R., Carvalho, A., Canedo, E.D., Costa, M.P., Cerqueira, A.: Diagnostic of data processing by brazilian organizations-a low compliance issue. Academic Editor Willy Susilo (2021)
20. Canedo, E.D., Calazans, A., Masson, E., Costa, P., Lima, F.: Perceptions of ict practitioners regarding software privacy. Entropy **22**, 429 (2020)
21. Allen, I.E., Seaman, C.A.: Likert scales and data analyses (2007)