information

Article

Diagnostic of Data Processing by Brazilian Organizations—A Low Compliance Issue

Sâmmara Éllen Renner Ferrão [1,†], Artur Potiguara Carvalho [1,†], Edna Dias Canedo [2,*,†], Alana Paula Barbosa Mota [3,†], Pedro Henrique Teixeira Costa [2,†] and Anderson Jefferson Cerqueira [2,†]

1 Electrical Engineering Department (ENE), Technology College, University of Brasília (UnB), Brasília, DF P.O. Box 4466, Brazil; sammaraellen@gmail.com (S.É.R.F.); arturpotiguaracarvalho@gmail.com (A.P.C.)
2 Department of Computer Science, University of Brasília (UnB), Brasília, DF P.O. Box 4466, Brazil; phtcosta@gmail.com (P.H.T.C.); andersonjcdf@gmail.com (A.J.C.)
3 Information Systems (IS), Pioneer Union of Social Integration (UPIS), Brasília, DF P.O. Box 70390-125, Brazil; alanapaula.job@gmail.com
* Correspondence: ednacanedo@unb.br or edna.canedo@gmail.com; Tel.: +55-61-98114-0478
† These authors contributed equally to this work.

Abstract: In order to guarantee the privacy of users' data, the Brazilian government created the Brazilian General Data Protection Law (LGPD). This article made a diagnostic of Brazilian organizations in relation to their suitability for LGPD, based on the perception of Information Technology (IT) practitioners who work in these organizations. We used a survey with 41 questions to diagnose different Brazilian organizations, both public and private. The diagnostic questionnaire was answered by 105 IT practitioners. The results show that 27% of organizations process personal data of public access based on good faith and LGPD principles. In addition, our findings also revealed that 16.3% of organizations have not established a procedure or methodology to verify that the LGPD principles are being respected during the development of services that will handle personal data from the product or service design phase to its execution and 20% of the organizations did not establish a communication process to the personal data holders, regarding the possible data breaches. The result of the diagnostic allows organizations and data users to have an overview of how the treatment of personal data of their customers is being treated and which points of attention are in relation to the principles of LGPD.

Keywords: Brazilian General Data Protection Law; treatment of personal data; federal public administration; organizations private

Citation: Renner Ferrão, S.; Carvalho, A.; Dias Canedo, E.; Mota, A.; Costa, P.; Cerqueira, A. Diagnostic of Data Processing by Brazilian Organizations: A Low Compliance Issue. *Information* **2021**, *12*, 168. https://doi.org/10.3390/info12040168

Academic Editor: Willy Susilo

Received: 27 February 2021
Accepted: 9 April 2021
Published: 14 April 2021

1. Introduction

The data privacy concern is increasing daily for Brazilian citizens, especially with the entry into force of the General Data Protection Law (LGPD) [1]. The legislation's goal is to regulate personal data processing. In technological areas, personal data processing can bring several implications if it is not done in compliance with this law. LGPD is a law instrument that allows Brazilian citizens to have power over their own data and allows them to identify processing applied to their personal data and furthermore, to rectify their data any time.

The LGPD implementation by organizations will demonstrate the transparency of Brazilian organizations and the commitment to their users. In addition to presenting the improvement in risk management and better organizational methodologies, LGPD presents several principles that will benefit both citizens and organizations. Considering the Brazilian context, some factors may have impacted organizations' initiation processes for implementing LGPD, such as the COVID-19 pandemic that forced organizations to design a remote working process in a hurry to deal with the social isolation initiated in March

and which was necessary to contain the pandemic. In addition, in April, a provisional measure, 959/2020 [2] (an act that has law enforcement executed by the executive branch that requires subsequent approval), was published that postponed the entry into force of the LGPD until 2021. This provisional measure had the postponement article vetoed exactly in the month scheduled for entry into force by the law, in August 2020.

The main goal of this work was to create a diagnostic for the organizations of federal public administration (FPA) and of private organizations in relation to personal data processing and their adequacy for complying with LGPD principles. This diagnostic will allow organizations to have an overview of their situation due to LGPD compliance, based on the perception of their employees in the Information Technology area. In addition to the individual context of law compliance, this research presents an overview of Brazilian companies, public and private, regarding the security aspects of the privacy of personal data and their policies and procedures regarding data processing.

Our main findings were—analyzing the results of research question (RQ.1), we identified that more than 31% of the companies handle personal data according to the principles of the LGPD and 30% of these companies have a communication plan for the Institutional Data Privacy Program (PPDI). Although almost 50% of the companies have supervisors, 45% (partially applied and fully applied) of the areas participated in some training and 30% of these companies provided the necessary resources to implement the LGPD. However, only 40% of the participants claim to be processing data based on a legal basis.

Regarding RQ.2, only 10% of the organizations claim to have prepared the Personal Data Privacy Impact Report (RIPD) and only 15% of the organizations have indicators to measure the results of the RIPD. In addition, more than 40% of the participants did not know whether the RIPD was prepared based on the guidelines of the LGPD Guide to Best Practices.

Regarding RQ.3, which evaluates the compliance law, we identified that 26% of the organizations implement, integrally, actions not to treat or collect inappropriately or excessively and to treat the minimum amount of data necessary to achieve the desired legal purpose. Less than 30% of companies mapped the processed data regarding legal competence and only 16% of the companies established methodologies to guarantee legal principles compliance.

At last, RQ.4 identified that only 15% of the organizations have published the Data Protection Officer (DPO) identity and contact information as publicly disclosed and less than 30% of the organizations developed a Privacy Policy. Still, 36% of these policies were prepared in simple and accessible language. Only a quarter of these companies protects its owns institution regarding the security measures evidences. From these findings, this research was able to conclude that a large part of the organizations are still beginning to implement the LGPD and that there is a great challenge in the law application within the Information Technology (IT) governance for these organizations, in view of the large number of IT practitioners who did not know how to answer the survey questions, when expected (in fact, required by the law) is that all practitioners in the organization, including outside of IT area, know (and apply whenever there is a personal data processing) the practices adopted by the organization be compliance with the legislation.

Our finding for this research can be justified by the absence of specific definitions for some LGPD implementation aspects that are still in need to be regimented within complementary standards. The Brazilian companies culture about the actual personal data processing before LGPD incoming may also negatively impact the law compliance.

This work is organized as follows—Section 2 presents the LGPD concepts and the correlated works. Section 3 presents the setting of this study. Section 4 presents the findings and the discussions on behalf of our findings. In Section 5, the threats to validate the research and its limitations are presented. Finally, in Section 6 the conclusions and future work are presented.

2. Background

In the background section, we will deal with the main concepts involved with the protection of personal data, relevant legislation and treatment of personal data. We will also present the recent works that deal with the subject and the main findings in this area.

2.1. Legislation of Personal Data Protection

Considering the indiscriminate personal data usage by organizations, many countries have identified the need to implement a specific legislation to protect citizens' personal data. In Brazil the General Data Protection Law (LGPD) [1] was created. This Law has been published since august 2018 and it was inspired by the European General Data Protection Regulation (GDPR) [3].

The LGPD's goal is to regulate personal data processing by natural or legal persons in order to protect the fundamental rights of freedom and privacy and the free development for a natural person's personality summered by Brazilian Constitution [1]. LGPD has come into force on 14 August 2020 after some government movements that failed at extending its deadline. LGPD, by its article 6, lays down some principles for personal data processing that can be associated with five of the six GDPR principles. These principles should observe good faith, a Brazilian concept that can be understood in Brazilian civil law as a concept related to the ethical conduct of a citizen in which his ideas are molded from the conscience of the right conduct and dignity as well as being based on attitudes of honesty, principles, good intentions and with the purpose of harming no one [4], and are listed as follows [1,5,6]:

1. Finality, or Transparency in GDPR: the personal data processing must be a legitimate goal, specified and explicitly known by the data owner;
2. Adequacy, or Purpose limitation in GDPR: the processing of data must be consistent with its finality requested;
3. Need, or Data Minimization in GDPR: the data must be restrained to exactly what is needed by the process;
4. Free access: the data owner should be able to consult the form and the duration of its processing as well as the data itself at anytime, free of charge and in an easy way;
5. Data quality or accuracy in GDPR: the processed data must be stored, arranged and manipulated with a view to clarity, accuracy, relevance and timeliness of the data;
6. Transparency: the information about data processing should be arranged by clarity and objectivity, presenting its purpose;
7. Safety, or integrity in GDPR: the data must be safe both technically and administratively (physical and digital data);
8. Prevention: adoption of measures to avoid possible damage resulting from data processing;
9. Non discrimination: the prohibition of data processing for discrimination or abuse purposes; and
10. Accountability: demonstration of the means used to comply with legislation and accountability for the data process.

Besides its principles, LGPD determines the data owner's rights that are grounded in obligations such as allowing the data owner to identify the ongoing data processing, the data adjustment of incomplete or out of date data, the data portability to another provider, the history of data sharing, data access and anonymization.

There are also in LGPD definitions for data processing agents—controller, processor and commissionaire. They are the involved agents that take responsibility over the data processing according to each role [1]:

1. Controller: it is a natural or legal person, public or private, who is strategically and tactically responsible for data processing;
2. Processor: it is the operational data processing responsible, it executes according to the controller's determinations;

3. Data Protection Officer (DPO): is defined by LGPD as a person nominated by the controller and the processor to act as a communication channel between the controller, data holders and the National Data Protection Authority (ANPD) [1].

Information security concepts are addressed in the LGPD from the determination to use mechanisms such as physical security and access control, among others, from the product or service conception to its execution [1]. Best governance practices in relation to data processing are also established by LGPD, such as the determination to create a privacy governance program with periodic updating that demonstrates commitment to compliance to the law, adequacy to the nature of the data treated, response plan for incidents and establishing a trust relationship with the data owner, among others. The law creation goals with its principles, data holders rights and best practices is to provide means for the citizen to know the data processing done to its own information and to have the possibility to end its processing when needed.

2.2. Personal Data Processing

The data processing is the main goal of the LGPD applicability and can be identified as any activities that use some personal data [7], regardless of the activity. Some examples are storage, access, extraction and manipulation, among others. The controller may be asked for a report on the RIPD, which must contain a description of the processes for the personal data processing that may create risks to civil liberties and the fundamental rights of the data holder, as well as the mechanisms to mitigate these possible risks [1].

LGPD defines that data processing could be done with the data owner's consent for specific purposes. User data can only be processed without the owner's consent in the following cases: (i) to comply with a legal or regulatory obligation by the controller; (ii) to share data processing necessary for the implementation of public policies established by federal public administration laws or regulations; (iii) to protect life itself or physical danger that may result from damage to the data holder or third parties; (iv) to health supervision exclusively in procedures performed by health professionals, health services or health authorities; or (v) guarantee of fraud prevention and holder security in the identification and authentication processes in electronic systems.

Regardless of the possible data processing with no consent, it is understood that there are challenges for the FPA in promoting the visibility of such data processing in the light of the treatment that does not require consent.

2.3. Data Privacy

Privacy can have several meanings depending on the purpose to which it is used. For this work, we will consider that privacy is the individual's right in relation to the collection, storage, processing and use in personal decision-making about themselves [8]. The data privacy concern has increased over the decades and, according to Schreiber [9], this increase was due to the rapid development of information processing in information technology.

In the 1980s, privacy was already addressed in computing as done by Turn [8] who listed the main mechanisms to guarantee privacy and the protection of individual data holders as legislative, administrative and rarely technical. In the legislative sphere, the Civil Rights Framework for the Internet and the General Data Protection legislation currently stand out in Brazil as mechanisms to guarantee data protection.

From an administrative point of view, standards such as ISO/IEC 27701 [10] and ISO/IEC 27002 [11] indicate processes and procedures as well as best practices to ensure data privacy. Finally, from a technical point of view, the information technology that currently stands as an important mechanism for information systems to be responsible for the data privacy they manage, fails to resolve all privacy issues by itself [12].

Data privacy finds a barrier to its existence in the technological world given the facility of information flow [13], thus making the data privacy concern even more relevant in the information technology sphere.

2.4. Related Works

In this research, we bring a non-exhaustive review of the works related to our work. We present articles related to the IT context regarding the European Privacy Data Protection law, GDPR. Then we present a set of Brazilian privacy Data Protection laws, LGPD, research, and lastly the compliance survey's research regarding GDPR and the legal compliance context.

In the scope of software development regarding GDPR works, Tamburri [14] conducted a formal concept analysis by GDPR to assist software engineers and designers in redesigning software systems to bring them into compliance with GDPR. Jensen et al. [15] discussed the concept of GDPR and its application in software developed in Europe and presented an approach for data annotation, as well as its use for visualization, standardization and data management, to ensure compliance with the law of data protection.

Guamán et al. [16] presented a method for systematically assessing the compliance of Android mobile apps with GDPR requirements for international transfers in accordance with the data protection regulation. However, data protection laws generally require that all participants in a personal flow ensure an equivalent level of protection for personal data, regardless of location.

Daudén-Esmel et al. [17] proposed a GDPR-compliant personal data management platform using Blockchain concepts. The platform provides public access to immutable evidence that shows the agreements between data subjects and service providers. Service Providers can demonstrate that they comply with the regulation and data subjects are aware of what happens to their personal data and can manage it according to their rights.

Daoudagh et al. [18] proposed a solution for ICT Smart Systems to comply with GDPR. The proposed privacy solution was developed using Privacy by Design and was based on Consent Manager and Access Control. The authors created a generic architecture that can be customized using real artifacts, in addition to demonstrating the applicability and flexibility of Privacy by Design when integrating with the tools CaPe and GENERAL _D Framework.

According to Diamantopoulou et al. [19] the application of GDPR is a challenge and should be seen as an opportunity for the redesign of systems that perform the processing of personal data, especially on sensitive systems, and that collect and process a large amount of personal data. In addition, the authors stated that it is important for organizations to at least inform data subjects about their processing activities and all employees in the organization need to know the principles of GDPR.

Following the LGPD context, we analyzed the work of Canedo et al. [5], which carried out a systematic literature review to identify works related to software privacy and privacy requirements in addition to the methodologies and techniques in their specification and conducted a survey on the understanding of Information and Communication Technology (ICT) practitioners regarding privacy and LGPD requirements.

Ribeiro and Canedo [20] used a Multiple Criteria Decision Analysis (MCDA) model to select the best alternatives for implementing safety criteria in a federal education organization in accordance with the LGPD. Carvalho et. al. [21] criticize the personal data privacy laws (both LGPD [1] and its European sister GDPR [22]) as well as the unweighted expectation about data anonymization mechanisms. For the authors, anonymization is a tool that should be added to the framework of tools used to protect data privacy together with a review of data governance policies and processes, as well as a review of security policies and risk responses organizations [21]. Carvalho et. al. [23] also mention an outline of *framework* that may involve the disciplines of Data Governance, Privacy, Risks and Information Security contributing to the LGPD *compliance*.

Oliveira [24] referred to the various difficulties in applying the law from the LGPD in technologies aimed at the Internet of Things while the hardware resources are limited and there is a need to collect personal data to define standards and behaviors for the automation of devices. The authors proposed as a solution to notify users about data collection, making the purpose clear and asking for authorization for their use. In addition, they also suggested, data encryption in storage cases, however, this consequently brings

a high cost for execution when the user requests the deletion or extraction of that data, leaving as an alternative the use of light block ciphers.

Silva et al. [25] presented a solution for decentralized web applications in order to avoid vulnerabilities arising from data leaks. The solution is correlated with *Sphinx Guardian*, a framework capable of managing authorizations in web applications, and of making personal data anonymous, completely disconnecting it from the user. The authors suggested that this measure can be adopted to get closer to the LGPD guidelines.

Pattakou et al. [26] mentioned a series of usability criteria that can be used both to support software developers and designers—from the beginning to the end—in creating the software, and to follow effective privacy requirements methodologies. Therefore, with the objective of defining the software as an usable system to contain the requirements: effectiveness, efficiency and satisfaction, the authors make an analysis and draw parallels with ISO 9241-11, Nielsen criteria, and the criteria of usability that have been recorded in the literature.

Carvalho et al. [27] investigated the importance of the applicability of the LGPD law, with an emphasis on Social Networks. The authors exemplify the types of data; (pseudo) anonymization and solutions for use; treatment and data collection. The authors draw a fine line between the LGPD and the GDPR, and criticize the limited effectiveness of the law in Brazil due to the still open questions, while the National Data Protection Authority (ANPD) materializes. Then, they emphasize the importance of putting into practice the principles of ethics and good faith, when there is a need to manipulate this resource considered the most valuable in the world, and not to neglect the current law.

Sabino [28] investigated the difficulties of companies in following the LGPD guidelines and presented some proposals to assist company policies in meeting security requirements and improvements in data processing, reviewing their structure and processes. The authors proposed the appointment of the Data Protection Officer (DPO) and the categorization of data, among others. In addition, the authors presented a more administrative approach to LGPD and its applicability.

Celidonio et al. [29] investigated the difficulty that Brazilian companies encountered in implementing the LGPD guidelines in a fully effective manner. The authors applied a mapping methodology, analyzed data from the multinational company Omega and concluded that although part of the material studied partially or completely meets the requirements, several improvements are still necessary for the organization to effectively follow the principles of LGPD. The study contributed as an investigative path that several other companies can orient themselves and implement changes in favor of following the LGPD and ensuring data privacy and security.

Alves et al. [30] took an approach to the regulation of LGPD in context with the current world scenario: Covid-19 (and other diseases). The authors mentioned applications that identify and signal about infected people and others who had contact with them; such an application has a high capacity to prevent people from contracting diseases, and can save countless lives. However, the application violates data privacy principles.

Morte et al. [31] proposed the use of *blockchain* for the processing of personal data to ensure transparency and security. To follow LGPD guidelines using private blockchains, the authors used terms such as privacy by design, off-chain, commitment, hash, smart contracts and Hyperledger Fabric. However, he warns about the use of public blockchains due to the difficulty of accountability, since he does not know who is giving consent and/or the location of the nodes cannot be guaranteed, in addition to other malfunctions, such as immutability and decentralization. Despite this, the authors state that it is worth increasing the solutions resulting from this implementation.

According to Silva et al. [32], due to the various facets of the technology, there was a need to protect numerous data, which is why the LGPD law and the ANPD agency were created. Despite this, the authors criticize loopholes in the law within the scope of national security, and this leads to important questions, for example—even with the LGPD in place, how safe is the data? Or to what extent can the current law protect and safeguard data when

there are situations of major interest on the part of the government? The authors mentioned the possibility of circumventing the law—legal rights and guarantees—and of disrespecting the LGPD guidelines in the public interest, in other words, of the government itself.

Kshetri and DeFranco [33] addressed the high rate of cyber attacks in Brazil, highlighting the financial damage of these crimes—on large or small scales, internal or external—have on citizens and/or companies. The authors mentioned that the LGPD and its applicability as the first significant attempt to guarantee data security and privacy, and lastly, the amount of the penalty in case of violation of the respective law.

Regarding compliance survey on personal data protection and privacy laws, Freitas and Silva [34] revealed the long journey to be taken for the legal compliance of small and medium-sized enterprises (SME) to the protection of personal data, explaining matters of concern such as the IT practitioner's lack of knowledge of such laws or the absence of consent mechanisms (despite the importance of the personal data involved in the operation of these companies). In the same year, Presthus et. al. [35] conducted the same survey in the context of Norwegian companies, obtaining similar results (justified by the authors due to the short force of the law).

At last, we identify Li et. al. [36] work at 2020 that propose a tool for legal compliance in the context of continuous integration, still verifying this year that most organizations are not compliant or perhaps they would never be completely compliant with legal requirements (mainly from the GDPR).

3. Research Methodology

In this section, we describe the goal of this research, as well as the research questions (RQs) which have been defined to conduct this work. In addition, the methods and procedures adopted to answer the RQs will be described.

3.1. Research Goal

The goal of this research is to carry out an assessment and study of the suitability and perception of organizations, regarding LGPD [1], collecting the individual perception of IT practitioners, submitted to this law, regarding the level of compliance in their organizations. So far (at the time writing), there are still no definitions that the LGPD delegates to the ANPD, the criteria contained in the literal text of the law (without interpretations by the magistrate authorities or additions of complementary laws) will be used in order to validate the compliance with the "current" law.

3.2. Research Questions

In order to achieve the main goal of this research, the following research questions have been defined to help achieve this main objective:

RQ.1. Is the processing of personal data carried out by organizations in accordance with LGPD principles?

RQ.2. Have organizations prepared the Personal Data Protection Impact Report (RIPD)?

RQ.3. Have organizations established a procedure or methodology to verify that the LGPD principles are being implemented?

RQ.4. Do organizations have a Service Privacy Policy?

3.3. Research Methods

To execute the assessment, we developed a questionnaire for diagnosing actions related to LGPD. This questionnaire was composed of eight sections of questions with multiple choices (mostly composed of exclusive alternatives) that address dimensions for the assessment, grouping the questions into evaluation themes. The dimensions (Dim) evaluated were:

Dimension 1 General Information: In this dimension, we grouped the general information about the audience and their company, taking as an example some

questions related to the size of the organization, general actions related to the compliance to LGPD, nature of the organizations activity among others. This dimension contained six questions (1–6).

Dimension 2 Governance: About the governance, we listed questions concern the good practices, polices, communication, roles and involvement at a strategic level. This dimension contained eleven questions (7–17).

Dimension 3 Legal Compliance and LGPD Principles: In this dimension, the level of compliance with the legal aspect of the LGPD and its principles were measured, as the principle of data minimization, or maintaining the purpose/legality of personal data and other aspects. This dimension contained seven questions (18–24).

Dimension 4 Transparency and Subject Rights: This dimension assesses the way the company informs its customers about the privacy of their data. This dimension contained four questions (25–28).

Dimension 5 Data Traceability: This dimension is responsible for grouping questions related to data inventory, data classification and extension of the data format under treatment. This dimension contained three questions (29–31).

Dimension 6 Contracts and Relations with Collaborators: This is a dimension dedicated to the review of the legal instruments in force and also the future ones to comply with the LGPD regulations. This dimension contained two questions (32 and 33).

Dimension 7 Information Security: This dimension assesses aspects of information security related to LGPD such as risk assessment, risk monitoring and technical aspects. This dimension contained five questions (34–38).

Dimension 8 Data Breach: This dimension assesses the actions that the company plans to deal with threats of data leakage, such as data leakage communication plan, incident management and external reporting channels. This dimension contained three questions (39–41).

The questionnaire was applied between 2 October 2020 and 11 December 2020 and had the participation of several IT practitioners from the public and private sectors from different areas and profiles who are involved in the processes of treating personal data, such as developers, systems analysts, requirements analysts and project managers. This questionnaire was circulated by the authors' network including mainly e-mail and business social media.

Most of the IT practitioners (64.8%) claimed to work in a large organization with more than 400 employees, followed by smaller companies (up to 19 employees) with 17.1% of participants and companies with less than 200 employees with 13.3%. Medium companies with less than 399 employees with 4.8%, as shown in Figure 1a. Also, 62.9% of participants claimed to work for the public sector (government entities, public agreements and public companies) and 37.1% of the contributions were from the private sector (market services in general), as shown in Figure 1b.

The answers to the questionnaires were individual, made through the Google forms tool and configured with pre-defined questions. All dimensions and their respective survey questions are available at URL: http://tiny.cc/rpw4tz (accessed date 8 April 2021) and by the Appendix A.

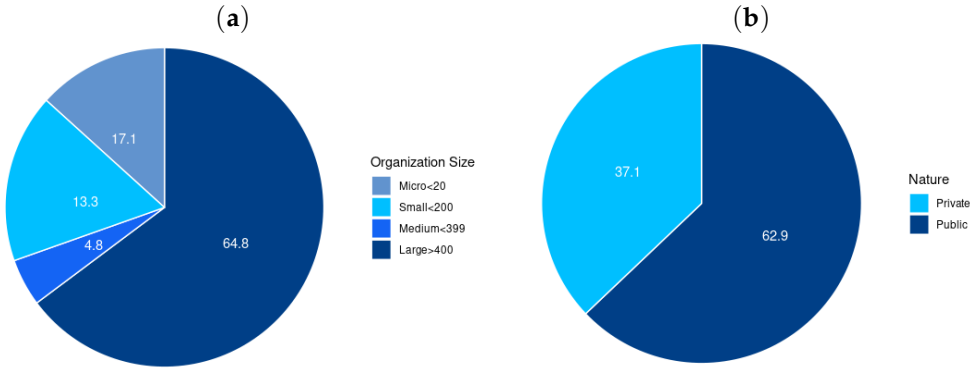

Figure 1. Figure (**a**) shows the number of employees that the organization has, while (**b**) shows the nature of the organization.

4. Results

In the results section, we present the main considerations of the answers to the research questions and answers to the applied survey. We also present an interpretation of the findings, in view of the initial statements of this work and the delimited scenario.

4.1. RQ.1. Is the Processing of Personal Data Carried Out by Organizations in Accordance with LGPD Principles?

The diagnostic questionnaire was answered by 105 IT practitioners. Regarding the General Information dimension (Dimension 1), it started with the (Q01 of the Appendix A) in concern of the number of employees from respondents organization considering the six options presented. The options were up to 19 employees going over until more than 600 employees, so we could have an idea of the companies size, the results shows that more than half (64.8%) of the organizations have more than 400 employees (option 5) as shown in Figure 1a. 62.9% of respondents are from the Federal Public Administration and 37.1% are from private organizations, as shown in Figure 1 (Q02 of the Appendix A) and as we asked about the organization's nature.

Twenty three percent of the participants informed that the organizations initiated a plan to carry out the treatment of sensitive personal data, 29% informed that their company partially apply and 25% informed that they fully apply and only 11% informed that they do not apply, as shown in Figure 2 (Q03 of the Appendix A). According to 28% of respondents, the organization partially applies and 31% stated that the organization fully handles the processing of publicly accessible personal data based on good faith and the principles of the LGPD (which are the principles of purpose, adequacy, need, free access, data quality, transparency, security, prevention, non-discrimination and accountability), as shown in Figure 2 (Q04 of the Appendix A).

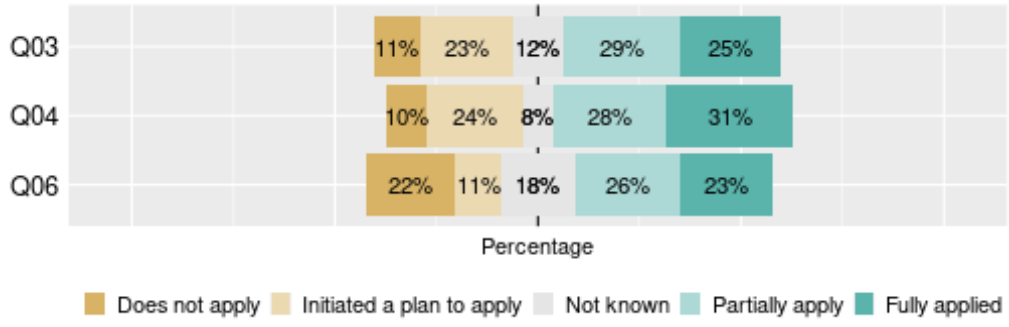

Figure 2. Processing of personal data.

Twenty three percent of respondents stated that the organization applies the processing of personal data through the automation of any decision making, the creation of profiles based on the transferred personal data (profiling) or analytical use (analytics), 26% stated that the organization partially applies and 22% stated that the organization does not. 18% did not know how to answer and 11% stated that the organization initiated a plan to carry out automated data processing, as shown in Figure 2 (Q06 of the Appendix A).

Regarding the Governance dimension (Dimension 2), 36% of respondents stated that the parties involved with the implementation of LGPD in the organization, fully read some Guide of Good Practices on LGPD and 18% partially read. 14% stated that they initiated a plan to adopt the reading of a guide and only 10% reported that stakeholders did not adopt the reading of a guide of good practices. 21% of the participants were unable to inform, as shown in Figure 3 (Q7 of the Appendix A).

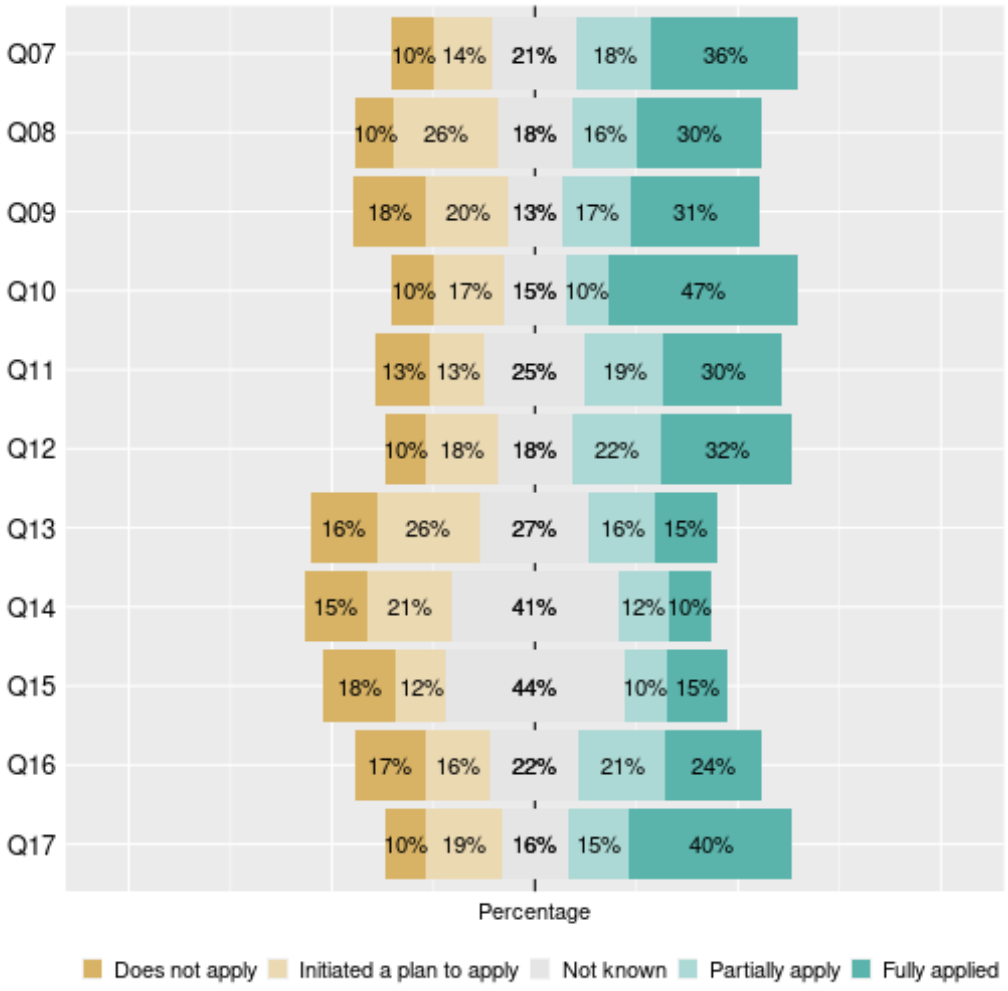

Figure 3. Results related to the governance dimension.

Thirty percent of respondents stated that their organization fully planned its Institutional Data Privacy Program, 16% reported that the organization partially carried out, 18% did not know how to answer, 26% reported that the organization started and 10% stated that the organization did not plan their Institutional Data Privacy Program, as shown in Figure 3 (Q8 of the Appendix A).

Thirty one percent of the organizations developed an internal communication plan for the Institutional Data Privacy Program, 17% of the respondents indicate their organization partially adopts the communication plan, 13% of the participants did not know how to answer, 20% stated that the organization started a plan and 18% of the participants stated

that the organizations did not develop an internal communication plan, as shown in Figure 3 (Q9 of the Appendix A).

Forty seven percent of Brazilian organizations have already nominated a person in charge with the knowledge, experience and autonomy to implement the LGPD. 10% of respondents stated that the organizations partially indicated, 15% of the participants did not know how to answer, 17% reported that the organization initiated a plan to carry out the appointment of a person in charge and 10% of the participants stated that the organization did not the indication of a person in charge to implement the LGPD, as shown in Figure 3 (Q10 of the Appendix A).

Almost one third of the organizations (30%) made the resources fully available to the person in charge for the implementation of the LGPD and direct access to senior management, 19% of the participants stated that the organization partially provided it, 25% did not know how to answer, 13% stated that the organizations initiated a plan to make available and only 13% reported that the organization did not provide the person in charge with the necessary resources to implement the LGPD and direct access to senior management, as shown in Figure 3 (Q11 of the Appendix A).

Thirty two percent of the organizations designated the leaders responsible for each front of action in the treatment of data, 22% of the participants stated that the organization partially designated, 18% did not know how to answer, 18% of the participants informed that the organization started a plan to designate the leaders and 10% stated that they were not, as shown in Figure 3 (Q12 of the Appendix A).

Fifteen percent of the organizations defined the indicators that will be used to measure the results of the Institutional Data Privacy Program, 16% of the participants stated that partially, 27% did not know how to answer, 26% stated that the organizations started defining the data indicators and 16% stated that they were not, as shown in Figure 3 (Q13 of the Appendix A).

Forty five percent (partially apply and fully applied) of the areas involved with data processing participated in some training related to the topic of protection of personal data and only 17% did not perform any training. Twenty two percent of the participants did not know how to answer and 16% reported that the organization initiated a plan to carry out the training of its employees, as shown in Figure 3 (Q16 of the Appendix A).

Forty percent of the participants stated that the processing of personal data carried out by the organization is based on the legal bases stipulated in the LGPD and only 10% stated that they did not. Sixteen percent of the participants did not know how to answer and 19% of the participants informed that the organization initiated a plan to carry out the processing of personal data in accordance with the principles of the LGPD, as shown in Figure 3 (Q17 of the Appendix A).

Considering this analysis over the dimensions used to answer the RQ.1, we believe that most of the organizations are still initiating the work to comply with LGPD principles.

4.2. RQ.2. Have Organizations Prepared the Personal Data Protection Impact Report (RIPD)?

According to LGPD [1,7], the RIPD is a fundamental activity to ensure that the controller does not violate civil liberties and the fundamental rights of personal data holders. There are several situations described in the LGPD, where the ANPD may request the controller to prepare a report on the impact of personal data protection. The RIPD must contain a description of the types of data collected, the methodology used for collection, to ensure the security of information and analysis of the controller, with regard to measures, safeguards and mechanisms that reduce the occurrence of risks. Thus, this is an essential document for all organizations.

As indicated in the Guide of Good Practices for Implementation in the Federal Public Administration [7], the RIPD must be prepared before the organization begins processing personal data, preferably in the initial phase of the program or project. The elaboration steps consist of:

1. Identify the Treatment Agents and the Person in Charge: article 5, Items VI, VII and VIII, of the LGPD;
2. Identify the need to prepare the Report;
3. Describe the treatment: nature, scope, context and purpose of the treatment;
4. Identify the stakeholders consulted;
5. Describe how the organization assesses the need and proportionality of personal data;
6. Identify and assess risks—classification: low, moderate and high;
7. Identify measures to address risks—examples: Logical access control, secure development and Network Security;
8. Approve the Report: formalize the approval of the report, by obtaining signatures from the person responsible for preparing the RIPD, the person in charge, the authorities—controller and processor;
9. Maintain the Review: the RIPD must be reviewed and updated annually or whenever any type of change occurs that affects the processing of personal data carried out by the organization.

In our diagnostic, we found that only 10% of organizations drafted the RIPD and 12% of respondents stated that the organization drafted it partially. Forty one percent of the participants were unable to inform whether the organization developed the RIPD or not. Twenty one percent of the participants stated that the organization initiated a plan to prepare the RIPD and 15% stated that the organization does not adopt the RIPD. In addition, 44% of the participants did not know whether the RIPD was prepared based on the guidelines of the LGPD Guide to Good Practices. Only 15% of the participants said yes, 10% said the RIPD was partially prepared based on the guidelines, 12% said the were initiating the plan to adequacy over the guideline and 18% informed the RIPD does not apply to its guidelines as shown in Figure 3 (Q14 and Q15 of the Appendix A).

In light of the 41% of IT practitioners that do not know if their organization has developed the RIPD and 43.8% could not tell if the RIPD was based on LGPD guidelines, we may conclude that RQ.2 has inconclusive answers.

4.3. RQ.3. Have Organizations Established a Procedure or Methodology to Verify that the LGPD Principles Are Being Implemented?

Regarding the dimension of Legal Compliance and with respect to the principles of LGPD (Dimension 3), 26% of respondents stated that organizations, within the limits of their legal competences, have fully implemented actions not to treat and collect inappropriately or excessively the personal data of citizens and treat the minimum amount of data necessary to achieve the desired legal purpose. Nineteen percent stated that the organizations partially implemented, 24% stated that they had started a plan to implement, 13% reported that their organizations did not initiate an implementation plan and 18% of the participants did not know how to answer, as shown in Figure 4 (Q18 of the Appendix A).

According to 29% of respondents, the organization carried out a mapping between the processed data and the legal competence/purpose for which they are needed and 17% stated that the organization partially carried out, 18% did not know how to answer, 24% stated that the organization initiated a plan to carry out the mapping and 12% stated that the organization did not initiate any activity related to the mapping between the processed data and the legal competence/purpose for which they are needed, as shown in Figure 4 (Q19 of the Appendix A).

Of the respondents, 16% stated that the organization has established a procedure or methodology to verify that the principles of LGPD are being respected during the development of services that will treat personal data from the design phase of the product or service until its execution. Eighteen percent stated that the organization had partially established it and 21% did not know how to answer. Fifteen percent of participants stated that the organization did not establish a procedure and 30% stated that the organization initiated a plan to establish a procedure or methodology, as shown in Figure 4 (Q20 of the Appendix A).

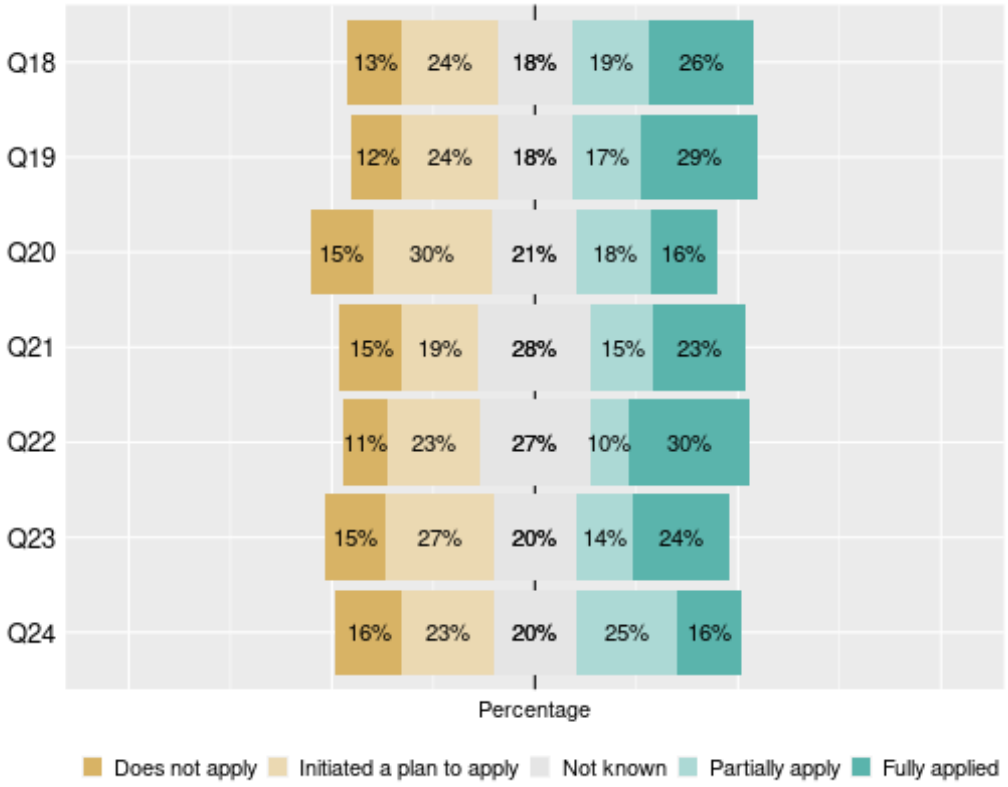

Figure 4. Results related to the Legal compliance dimension and with respect to the General Data Protection Law (LGPD) principles.

Twenty three percent of respondents stated that the principles of the LGPD are applied to all treatment of personal data carried out by the organization, both for users of the public services provided and for servers, employees and/or collaborators of the Organization. Fifteen percent stated that they are partially applied and 28% did not know how to answer. Nineteen percent reported that the organization initiated a plan to apply and 15% stated that the organization did not initiate any activity in relation to this principle, as shown in Figure 4 (Q21 of the Appendix A).

Thirty percent of respondents stated that their organization made the areas involved with the processing of personal data aware that the public administration can carry out the processing of personal data in the exercise of its legal powers or the execution of public policies for the delivery of public services and that in these cases it is not necessary to collect the consent of the data subject and only 10% said that partially. Twenty three percent of the participants stated that the organization initiated an awareness plan and 11% stated that they did not initiated. Twenty seven percent of the survey participants were unable to answer, as shown in Figure 4 (Q22 of the Appendix A).

According to the respondents, 24% of the organizations carried out the processing of personal data in the exercise of their legal powers or the implementation of public policies gave publicity about the purpose and the way in which the data was treated. Fourteen percent stated that it was partially, 27% stated that the organization only initiated a plan to carry out this activity and 15% stated that the organization did not initiate. Twenty percent of respondents were unable to answer, as shown in Figure 4 (Q23 of the Appendix A).

Sixteen percent of respondents stated that the organization adopts systems and procedures to comply with the data subject's right to rectify information and 25% stated that the organization partially adopts it. Twenty percent were unable to answer, 23% of respondents stated that the organization initiated an adoption plan and 16% stated that the organization did not initiate any action for this procedure, as shown in Figure 4 (Q24 of the Appendix A).

From this perspective the RQ.3 have been answered over the results of these dimensions and we may conclude that less then half of organizations have established some procedures or methodologies to verify the implementation of LGPD principles.

4.4. RQ.4. Do Organizations Have a Service Privacy Policy?

Regarding the Transparency dimension and data subject's rights (Dimension 4), 15% of the survey respondents stated that the identity and contact information of the data controller was publicly disclosed, clearly and objectively, in the Organization's homepage. Thirteen percent stated that they were partially disclosed, 24% did not know how to answer, 18% stated that the organization initiated a disclosure plan and almost one third of participants (30%) stated that the organization did not initiate any plan to disclose information related to the contact in charge of the data, as shown in Figure 5 (Q25 of the Appendix A).

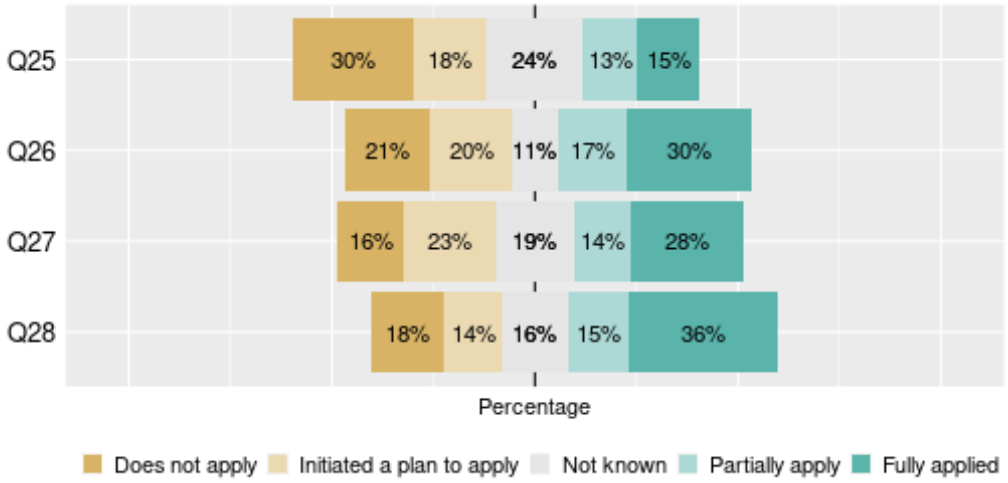

Figure 5. Results related to the Transparency dimension and data holder rights.

Thirty percent of respondents stated that the organization communicates internally the objectives of the Institutional Data Privacy Program, 17% stated that only partially, 11% did not know how to answer, 20% of participants stated that the organization started a communication plan and 21% stated that the organization did not initiate any internal communication plan, as shown in Figure 5 (Q26 of the Appendix A).

According to 28% of respondents, the organization developed a Privacy Policy for each service in order to inform the rights of data subjects and revised the existing Privacy Policies. Fourteen percent stated that partially, 19% did not know how to answer; 23% stated that the organization initiated a plan to elaborate the privacy policy and only 16% stated that the organization did not initiate any plan to elaborate the privacy policy, as shown in Figure 5 (Q27 of the Appendix A).

The services' Privacy Policies were prepared in simple and accessible language, as stated by 36% of respondents and 15% that were partially elaborated. Of the participants, 16% were unable to answer, 14% of the participants informed that the organization initiated a plan to elaborate the privacy policies and 18% stated that they had not, as shown in Figure 5 (Q28 of the Appendix A).

Regarding the Data Traceability dimension (Dimension 5), according to almost one third of the respondents (30%), the organization carried out an inventory of services that treat personal data and 12% stated that partially. Twenty two percent did not know how to answer, 23% reported that the organization started a plan to carry out the inventory and 13% reported that a plan was not started by their organization, as shown in Figure 6 (Q29 of the Appendix A).

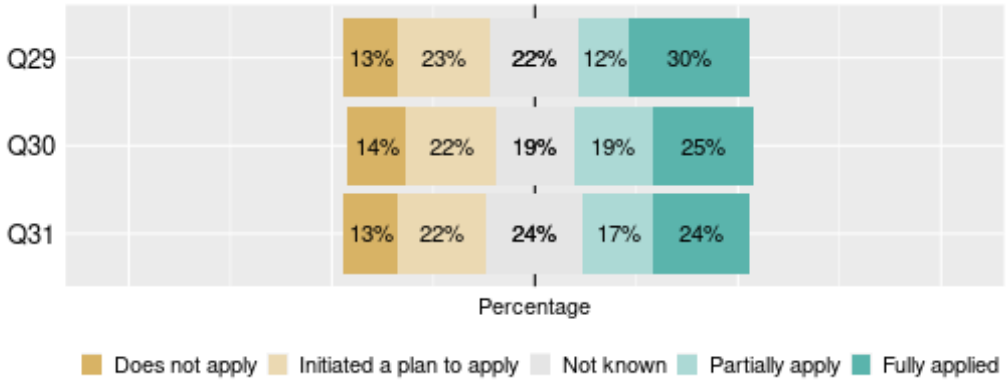

Figure 6. Results related to Data Traceability dimension.

According to a quarter of respondents (25%), the organization carried out a classification of the processed data between personal data and sensitive personal data and 19% stated that partially. 19% did not know how to answer and 22% informed that the organization started a data classification plan and 14% of the participants stated that they did not started, as shown in Figure 6 (Q30 of the Appendix A).

Twenty four percent of respondents stated that the organization maintains traceability of the data of the holder, whether in electronic or physical format (on paper) and 17% stated that partially. Twenty four percent of the participants did not know how to answer, 22% stated that the organization started a traceability plan and 13% of the participants informed that they did not started, as shown in Figure 6 (Q31 of the Appendix A).

Regarding the dimension Adequacy of contracts and relations with employees (Dimension 6), only 10% of the survey participants reported that the organization has already carried out an adaptation of the calling instruments that are being prepared by the teams responsible for compliance with the LGPD and 17% reported that partially. Thirty seven percent of the participants were unable to answer. Seventeen percent of respondents stated that the organization initiated a plan to carry out the adequacy of the calling instruments and 18% reported that they did not initiated, as shown in Figure 7 (Q32 of the Appendix A).

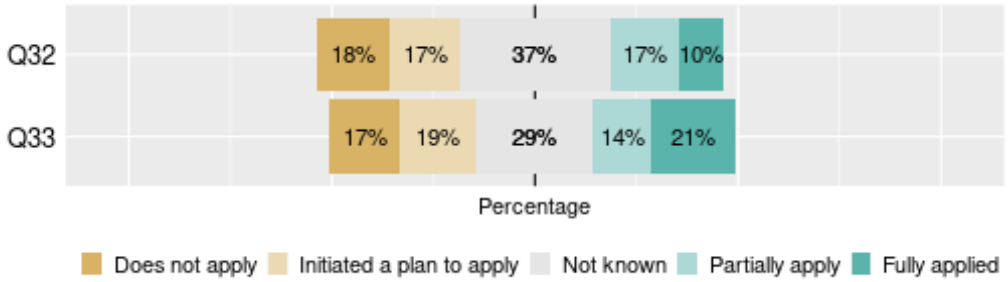

Figure 7. Results related to the dimension Adequacy of contracts and relations with employees.

According to 21% of the survey participants, the organizations carried out a review of the contracts in force to adapt them to the LGPD, 14% stated that partially and 29% of the participants did not know how to answer. Nineteen percent of the participants stated that the organization initiated a plan to carry out the review and 17% informed that they did not initiated, as shown in Figure 7 (Q33 of the Appendix A).

Regarding the Information Security dimension (Dimension 7), 21% of the participants reported that the organization has implemented security controls for the risks identified in the RIPD, 18% reported that partially and 25% did not know how to answer. Twenty percent of the participants reported that the organization has initiated a plan to implement security controls and 16% reported that they have not, as shown in Figure 8 (Q34 of the Appendix A).

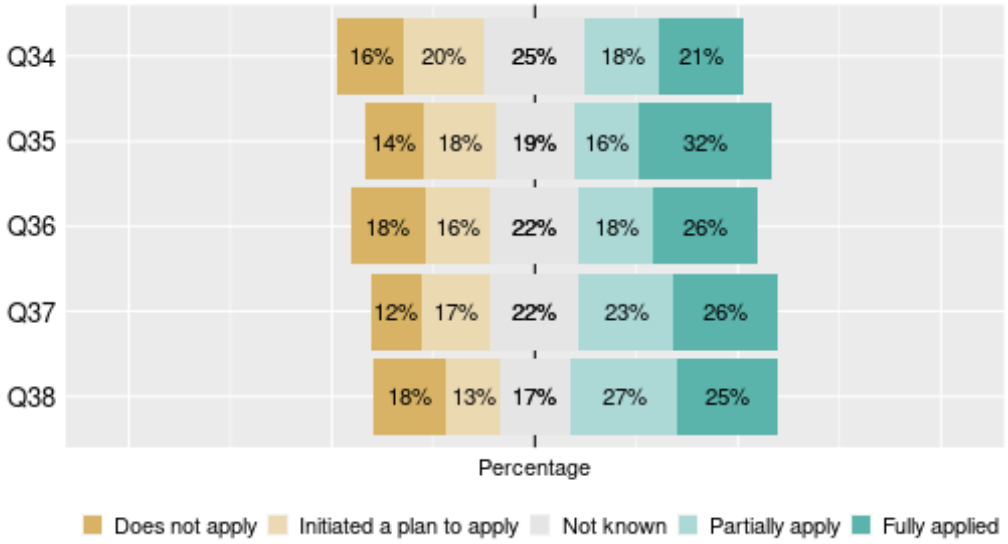

Figure 8. Results related to the Information Security dimension.

Regarding the organization establishing a team to monitor the technical vulnerabilities of the services that treat personal data, 32% reported that the organization has already instituted, 16% reported that the organization partially instituted and 19% of the participants did not know how to answer. Eighteen percent reported that the organization initiated a plan to establish a team and 14% stated that they did not initiated, as shown in Figure 8 (Q35 of the Appendix A).

Twenty six percent of survey respondents reported that the organization had set up a team to monitor the technical vulnerabilities of services that handle sensitive data, 18% reported that partially and 22% were unable to report. Sixteen percent reported that the organization has initiated a plan to institute the team that will perform the monitoring of technical vulnerabilities and 18% reported that the organization has not yet initiated a plan, as shown in Figure 8 (Q36 of the Appendix A).

Twenty six percent of survey respondents stated that the organization generates evidence to prove that it has taken security measures to protect personal data from external and internal threats, 23% said that partially and 22% did not know how to answer. Seventeen percent of participants stated that the organization initiated a plan to generate the evidence and 12% of participants stated that the organization did not initiate any activity in relation to this issue, as shown in Figure 8 (Q37 of the Appendix A).

A quarter of survey respondents (25%) stated that security measures are planned from the product or service design phase to their implementation by organizations, 27% said that partially and 17% did not know how to answer. Thirteen percent stated that the organization initiated a plan for planning and 18% stated that did not initiated, as shown in Figure 8 (Q38 of the Appendix A).

Regarding the dimension Data breaches (Dimension 8), according to 20% of participants, the organization established a process for communicating possible personal data breaches, 13% stated that partially and 25% did not know how to answer to that question. Twenty four percent of participants stated that the organization initiated a plan to establish the reporting process for data breaches and 18% stated that this action has not yet been initiated by the organization, as shown in Figure 9 (Q39 of the Appendix A).

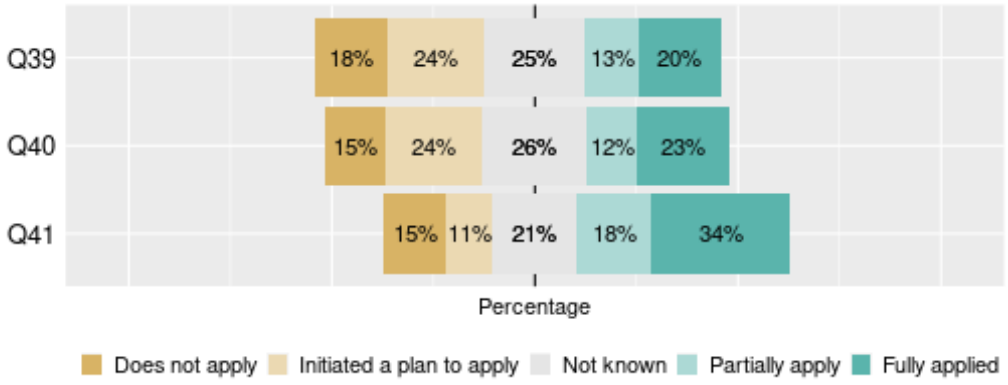

Figure 9. Results related to dimension Data breaches.

Twenty three percent of organizations perform an incident management to deal with possible data breaches effectively, 12% partially perform and 26% did not know how to inform. Twenty four percent of participants reported that the organization has initiated a plan to perform incident management and 15% stated that the organization has not yet initiated a plan, as shown in Figure 9 (Q40 of the Appendix A).

Thirty four percent of survey respondents stated that the organization provides a channel for receiving reports and alerts of irregularities, such as reports of possible data leaks and security breaches, 18% said that partially and 21% did not know how to answer. Eleven percent of participants reported that the organization initiated a plan to provide a reporting channel and 15% reported that they did not initiated, as shown in Figure 9 (Q41 of the Appendix A).

Due to the answers through the dimensions and regarding the answer to RQ.4 we may conclude that only a small piece (a quarter of dimensions average) of the organizations have a Service Privacy Policy implemented.

4.5. Work Discussions

The results obtained with the diagnostic of Brazilian public and private organizations allowed us to identify that organizations are still in an initial stage of adaptation to the principles of LGPD to carry out the processing of personal data. A number of LGPD principles have not yet been implemented by organizations, so we can conclude that regarding the RQ.1 findings most of the organizations are still initiating work to comply with LGPD principles, which raises concerns about the need for these organizations to be in compliance with LGPD. Our diagnostic obtained 105 responses from professionals from different organizations in the country and the results obtained may spark a concern of organizations in relation to their compliance with the LGPD.

The discussion found widely in the literature [21,23,25,28,29,33] was also verified through this research—a large section of Brazilian companies continue to have difficulties in maintaining their programs of legal compliance with the laws of protection of personal data, especially in the Brazilian scenario of the LGPD law. The lack of knowledge of IT practitioners on matters related to the protection of personal data or data privacy, or even on governance and data management can be one of the root causes of this difficulty.

As it is possible to identify from the results obtained, most organizations do not comply with the principles and privacy policies of personal data and the results of RQ.2 shows that less then half of organizations started compliance mechanism to validate implementation of LGPD principles. The index of IT practitioners who selected survey responses such as "Does not apply" or "Not known" when answering survey questions is relatively large. With the sum in percentage of these two options responses, within the 41 questions, it is clear that more then one third of the respondents' organizations (more than 38%) of the 105, as a result to answer the RQ.3 have not initiated a plan of effective initiatives or methodologies to implement the LGPD principles and answering RQ.4, only a small

number of IT practitioners have a Service Privacy Policy implemented. These two research questions show a low compliance issue with LGPD implementation.

Dynamic analysis of the treatment of personal data, as well as mapping and efficient IT governance, are measures that must be taken by organizations that are concerned with the reality in which they are inserted and with the management of data. The reflection of these internal implementations may have a positive impact on commercial relations, not only because of the transparency of the treatment of users' personal data, but because it is in compliance with the LGPD and its principles.

5. Research Limitations

In this section, we present the main limitations of this work and possible threats to the representativeness and application of the findings from this research.

There are some threats regarding the conduct of this research. Although the participation of IT practitioners in this research was voluntary, there may be some bias in their responses. In addition, the survey was long, had 41 questions, which may have caused a certain lack of interest in some IT practitioners when answering the questionnaire.

Due to the fact that the application of the LGPD is recent in Brazil, not all IT practitioners have yet been informed of the changes that should occur in the information systems of Brazilian organizations, because, in addition to technological changes, there must also be cultural changes in organizations, in addition to having legal support .

The response rate was low (105 respondents answered from 900 emails sent and not returned). Therefore, we cannot be sure of the representativeness of the sample. While it is preferable to obtain a higher response rate, based on previous research, a low response rate is common using this recruitment method [37].

The questionnaire addressed issues from various segments related to LGPD, which may have been impaired in some parts, as the participants' knowledge is usually not complete, but is restricted to a specific area. As a way of mitigating these threats, we intend to monitor the entire software development process in an organization and define indicators to measure LGPD compliance and return to citizens during the execution of the activities of IT practitioners and make a comparison with the development of systems prior to the application of the LGPD. However, in this research it was not possible to mitigate this threat.

6. Conclusions

An increasing number of current systems deal with personal information (for example, information about citizens, customers), where information is protected by various privacy laws and regulations. Thus, privacy has become a major concern for system designers. In other words, dealing with privacy issues is an obligation nowadays, because privacy breaches can result in serious consequences. Several studies have shed light on the economic costs of privacy breaches, making it clear that the absence of appropriate privacy protection mechanisms imposes huge direct costs on organizations, as well as indirect costs and long-term consequences.

The LGPD came about as a way to facilitate the processing data based on principles of ethics and good faith. In addition, its guidelines are intended to act in favor of the security and privacy of users' data, raising questions and addressing solutions for Brazilian organizations, public and/or private, to implement them during data collection and manipulation. However, in the course of the research, it is possible to observe the lack of maturity regarding governance and data management and the privacy and security of information on the part of most Brazilian organizations.

A possible solution to this lack of maturity on the part of organizations, may be due to the National Authority for the Protection of Personal Data (ANPD), an organ of the direct public administration, which will bridge the gap between society and government and has as the main function the LGPD inspection and regulation, that was recently established. ANPD will be essential for the maturity and compliance process of Brazilian organizations,

since it is in accordance with the National Council for the Protection of Personal Data and Privacy , and will monitor and ensure that organizations apply the principles of the law effectively.

It is important to highlight that, according to the research carried out, there is a clear need for organizations to pay attention to the application of LGPD, as well as its effectiveness. Another important aspect is to inform employees about what it is and how the treatment of personal data is being carried out within their respective organizations. The number of people who did not know how to answer the questions related to the mechanisms adopted by the organization is still very high considering LGPD's article 46, where it is established that all measures regarding protecting the data treatment process should be known, especially when considering the degree of importance of the topic, within the IT biased scope.

In line with our findings, it was also possible to observe that many organizations have not yet defined the data protection agents, the DPO, and have not yet prepared the RIPD based on the guidelines of the LGPD Good Practice Guide [7]. It is important to emphasize the importance of following effective privacy principle methodologies at all stages of the software development process.

Our findings can serve as support for organizations in the application of LGPD, as it allows them to have an overview of the current diagnostic in relation to the treatment of personal data and the stage at which they find themselves in relation to the procedures that must be adopted for compliance with LGPD principles. For future work, we will be monitoring the implementation of the LGPD in a federal public administration organization with the aim of creating a process for implementing the principles of the LGPD during the development of the organization's information systems.

Author Contributions: All authors contributed to Writing Original Draft Preparation and Writing Review and Editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The questions applied to this study are available at the URL: http://tiny.cc/rpw4tz (access date 8 April 2021).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Questions of Survey

Diagnostic of companies compliance to LGPD
Diagnostic of compliance to LGPD: Dimension 1: General Information

This diagnostic aims to verify the level of Organizations compliance with the General Data Protection Law (LGPD), Law No. 13.709. Try to be as assertive as possible in your answer and if you do not know, no problem, indicate this option. The diagnostic is divided into 8 sections and takes an average of 7 min to resolve.

1. How many employees does the organization have?

Mark only one oval.

Up to 19 employees
From 20 to 99 employees
From 100 to 199 employees
From 200 to 399 employees
From 400 to 599 employees
More than 600 employees

2. What is the nature of the organization?

Mark only one oval.

Public
Private

3. Does the organization handle sensitive personal data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

4. The processing of publicly accessible personal data is carried out based on good faith and the principles of the LGPD (that is, the principles of purpose, adequacy, need, free access, data quality, transparency, security, prevention, no discrimination, accountability)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

5. What is the most common type of user of the applications developed by the organization?

Check all that apply.

Citizen (access to government services)
Bank customers
Media Clients
Internal (of the organization, access to corporate systems)
E-Commerce Customers
Other… _____

6. Does the processing of personal data carried out by the organization include automation of any decision making, creation of profiles based on the transferred personal data (profiling) or analytical use (analytics)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 2: Issues related to the Governance Axis

7. Did the parties involved in the implementation of the LGPD read any Good Practice Guide on the General Data Protection Law (LGPD)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

8. Did the organization plan its Institutional Data Privacy Program?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

9. Has the organization developed an internal communication plan for the Institutional Data Privacy Program?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

10. Has the organization already nominated a Data Protection Officer (DPO) with sufficient knowledge and experience and autonomy to implement the LGPD?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

11. Did the organization provide the DPO with the necessary resources to implement the LGPD and direct access to senior management?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

12. Has the organization appointed the leaders responsible for each front of action in the treatment of data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

13. Has the organization defined the indicators that will be used to measure the results of the Institutional Data Privacy Program?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

14. Did the organization elaborated the Personal Data Privacy Impact Report (RIPD)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

15. Was the RIPD elaborated based on the guidelines in the LGPD Good Practice Guide?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

16. Has the area(s) involved with data processing participated in any training related to the theme personal data protection?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

17. Is the organizations treatment of personal data based on the legal bases stipulated in the LGPD?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 3: Legal compliance and respect for LGPD principles

18. Has the organization, within the limits of its legal competences, implemented actions to do not treat and collect citizens' personal data inappropriately or excessively and to treat the minimum amount of data necessary to achieve the desired legal purpose?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

19. Did the organization carry out a mapping between the treated data and the legal competence / purpose for which it is needed?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

20. Has the organization established a procedure or methodology to verify that the LGPD principles are being respected during the development of services that will treat personal data from the product or service design phase until its execution?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

21. Are the LGPD principles applied to all treatment of personal data carried out by the organization, both for users of the public services provided and for public and private employees and/or collaborators of the organization?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

22. The organization has made the area (s) involved with the treatment of personal data aware that the public administration can carry out the processing of personal data in the exercise of its legal powers or the execution of public policies for the delivery of public services and that in such cases it will not be necessary to obtain the consent of the data subject?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

23. Does the organization, when carrying out the treatment of personal data in the exercise of its legal powers or the implementation of public policies, publicize the purpose and how the data will be treated?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

24. Does the organization adopt systems and procedures to comply with the data subjects right to rectify information?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 4 : Data subject transparency and rights

25. Were the identity and contact information of the DPO of the data publicly disclosed, clearly and objectively, preferably on the organizations homepage?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied

Fully applied

26. Does the organization communicate internally the objectives of the Institutional Data Privacy Program?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

27. Has the organization developed a privacy policy for each service in order to inform the rights of data subjects and revised the existing privacy policies?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

28. Are the services Privacy Policies prepared in simple and accessible language?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 5: Data Traceability

29. Has the organization carried out an inventory of services that handle personal data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

30. Did the organization carry out a classification of the processed data between personal data and sensitive personal data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know

Partially applied
Fully applied

31. Does the organization maintain traceability of the subjects data, whether in electronic or physical format (on paper)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 6: Adequacy of contracts and relations with collaborators

32. Has the organization already carried out an adaptation of the legal calling instruments that are being prepared?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

33. Did the organization carry out a review of the contracts in force to adapt them to the General Data Protection Law?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 7: Information Security

34. Has the organization implemented security controls for the risks identified in the Personal Data Protection Impact Report (RIPD)?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

35. Has the organization established a team to monitoring the technical vulnerabilities of services that handle personal data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

36. Has the organization established a team to monitoring the technical vulnerabilities of services that handle sensitive data?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

37. Does the organization generate evidence to prove that it has taken security measures to protect personal data from external and internal threats?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

38. Are security measures planned since the product or service design phase through to execution?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

Dimension 8: Data Breaches

39. Has the organization established a process for communicating possible personal data breaches?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

40. Does the organization carry out incident management to deal with possible data breaches effectively?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

41. Does the organization provide a channel for receiving reports and alerts of irregularities, such as reports of possible data leaks and security breaches?

Mark only one oval.

Does not apply
Initiated a plan to apply
I don't know
Partially applied
Fully applied

References

1. Da República, P. Lei Geral de Proteção de Dados. 2018. Available online: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (accessed on 22 July 2020).
2. Executivo, P. Medida Provisória 959/2020. 2020. Available online: https://www.camara.leg.br/propostas-legislativas/2250977 (accessed on 12 November 2020).
3. Erickson, A. Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. *Brook. J. Int'l L.* **2018**, *44*, 859.
4. Rodrigues, S. *Direito Civil*; Number v. 1 in Direito Civil; Editora Saraiva: São Paulo, Brazil, 2003.
5. Canedo, E.D.; Calazans, A.T.S.; Masson, E.T.S.; Costa, P.H.T.; Lima, F. Perceptions of ICT Practitioners Regarding Software Privacy. *Entropy* **2020**, *22*, 429. [CrossRef] [PubMed]
6. Pessoa, C.R.; Nunes, B.C.; de Oliveira, C.; Marques, M.E. Effects and Projections of the Brazilian General Data Protection Law (LGPD) Application and the Role of the DPO. In *Digital Transformation and Challenges to Data Security and Privacy*; IGI Global: Hershey, PA, USA, 2021; pp. 195–208.
7. Federal, G. Guia de Boas Práticas para Implementação na Administração Pública Federal. 2020. Available online: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf (accessed on 20 October 2020).
8. Turn, R. Security and Privacy Requirements in Computing. In Proceedings of the 1986 ACM Fall Joint Computer Conference, ACM '86, Dallas, TX, USA, 2–6 November 1986; IEEE Computer Society Press: Washington, DC, USA, 1986; pp. 1106–1114.
9. Schreiber, A. *Right to Privacy and Personal Data Protection in Brazilian Law*; Springer International Publishing: Cham, Switzerland, 2020; pp. 45–54. [CrossRef]
10. Standard, International Organization for Standardization. *ABNT NBR ISO/IEC 27701:2019—Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines*; Standard, International Organization for Standardization: Rio de Janeiro, Brazil, 2019.
11. Standard, International Organization for Standardization. *ABNT NBR ISO/IEC 27002: 2015—Information Technology—Security Techniques—Code of Pratice for Information Security Controls*; Standard, International Organization for Standardization: Rio de Janeiro, Brazil, 2015.
12. Studer, T. A Universal Approach to Guarantee Data Privacy. *Log. Universalis* **2013**, *7*, 195–209. [CrossRef]
13. Brito, F.; Machado, J. Preservação de Privacidade de Dados: Fundamentos, Técnicas e Aplicações. *J. Atualização Inform.* **2017**, *3*, 40.
14. Tamburri, D.A. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Inf. Syst.* **2020**, *91*, 101469. [CrossRef]
15. Jensen, M.; Kapila, S.; Gruschka, N. Towards Aligning GDPR Compliance with Software Development: A Research Agenda. In Proceedings of the 5th International Conference on Information Systems Security and Privacy, Prague, Czech Republic, 23–25 February 2019; SciTePress: Prague, Czech Republic, 2019; Volume 1; ICISSP, INSTICC; pp. 389–396. [CrossRef]
16. Guamán, D.S.; Del Alamo, J.M.; Caiza, J.C. GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access* **2021**, *9*, 15961–15982. [CrossRef]

17. Daudén-Esmel, C.; Castellà-Roca, J.; Viejo, A.; Domingo-Ferrer, J. Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management. In Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), Zhuhai, China, 8–10 January 2021; pp. 68–73. [CrossRef]
18. Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernardo, R.D.; Alessi, M. How to Improve the GDPR Compliance through Consent Management and Access Control. Available online: https://www.scitepress.org/Papers/2021/102602/102602.pdf (accessed on 10 April 2021).
19. Diamantopoulou, V.; Androutsopoulou, A.; Gritzalis, S.; Charalabidis, Y. Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance. *Information* **2020**, *11*, 117. [CrossRef]
20. Carauta Ribeiro, R.; Dias Canedo, E. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. In Proceedings of the The 21st Annual International Conference on Digital Government Research, dg.o '20, Seoul, Korea, 17–19 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 175–184. [CrossRef]
21. Carvalho, A.P.; Canedo, E.D.; Carvalho, F.P.; Carvalho, P.H.P. Anonymisation and Compliance to Protection Data: Impacts and Challenges into Big Data. In Proceedings of the ICEIS (1), SCITEPRESS, Prague, Czech Republic, 5–7 May 2020; pp. 31–41. [CrossRef]
22. Regulation, G.D.P. EU Data Protection Rules. 2018. Available online: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (accessed on 8 March 2021).
23. Potiguara Carvalho, A.; Potiguara Carvalho, F.; Dias Canedo, E.; Potiguara Carvalho, P.H. Big Data, Anonymisation and Governance to Personal Data Protection. In Proceedings of the dg.o '20: The 21st Annual International Conference on Digital Government Research, Aguascalientes, Mexico, 18–21 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 185–195. [CrossRef]
24. Oliveira, N.S.d. Segurança da Informação para Internet das Coisas (IoT): Uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). *Rev. Eletronica De Iniciação Cient. Em Comput.* **2019**, *17*. Available online: https://seer.ufrgs.br/reic/article/view/88790 (accessed on 10 April 2021).
25. Silva, J.; Calegari, N.; Gomes, E. After Brazil's general data protection law: Authorization in decentralized web applications. In Proceedings of the Companion, 2019 World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 819–822.
26. Pattakou, A.; Mavroeidi, A.; Diamantopoulou, V.; Kalloniatis, C.; Gritzalis, S. Towards the Design of Usable Privacy by Design Methodologies. In Proceedings of the 2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE), Banff, AB, Canada, 20 August 2018; IEEE: Banff, AB, Canada, 2018; pp. 1–8. [CrossRef]
27. Carvalho, L.P.; Oliveira, J.; Cappelli, C. Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações. In *Proceedings of the Anais do IX Brazilian Workshop on Social Network Analysis and Mining*; SBC: Porto Alegre, RS, Brasil, 2020; pp. 73–84. [CrossRef]
28. Sabino, R. Gestão da Segurança da Informação Orientado a LGPD: Impactos da Implantação das Normas LGPD nos Processos da ADM SISTEMAS LTDA. 2020. Available online: http://www.riuni.unisul.br/handle/12345/9664 (accessed on 10 April 2021).
29. Celidonio, T.; Neves, P.S.; Doná, C.M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira-Um estudo de caso/Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution-A case study. *Braz. J. Bus.* **2020**, *2*, 3626–3648.
30. Alves, P.H.C.; Frajhof, I.Z.; Correia, F.A.; de Souza, C.S.; Lopes, H. Second layer data governance for permissioned blockchains: The privacy management challenge. *arXiv* **2020**, arXiv:2010.11677.
31. Morte, A.B.; Meira, A.; Costa, R.; Mariz, D. Uma Análise Sobre o Uso de DLTs no Tratamento de Dados Pessoais: Aderência aos Princípios e Direitos elencados na LGPD. Available online: https://sol.sbc.org.br/index.php/wblockchain/article/view/12435 (accessed on 10 April 2021).
32. Da Silva, M.V.V.; da Luz Scherf, E.; da Silva, J.E. The Right to Data Protection versus "Security": Contradictions of the Rights-discourse in the Brazilian General Personal Data Protection Act (LGPD). *Rev. Direitos Cult. Cult. Rights Rev.* **2020**, *15*, 36. [CrossRef]
33. Kshetri, N.; DeFranco, F.J. The Economics of Cyberattacks on Brazil. *Computer* **2020**, *53*, 85–90. [CrossRef]
34. Freitas, M.d.C.; Mira da Silva, M. GDPR Compliance in SMEs: There is much to be done. *J. Inf. Syst. Eng. Manag.* **2018**, *3*, 30. [CrossRef]
35. Presthus, W.; Sørum, H.; Andersen, L.R. GDPR Compliance in Norwegian Companies. In *Norsk konferanse for organisasjoners bruk at IT*; Nokobit: Svalbard, Norway, 2018; Volume 26.

36. Li, Z.S.; Werner, C.; Ernst, N.; Damian, D. Gdpr compliance in the context of continuous integration. *arXiv* **2020**, arXiv:2002.06830.
37. Lee, A.; Carver, J.C.; Bosu, A. Understanding the impressions, motivations, and barriers of one time code contributors to FLOSS projects: A survey. In Proceedings of the ICSE, Buenos Aires, Argentina, 20–28 May 2017; IEEE: New York, NY, USA, 2017; pp. 187–197. [CrossRef]