








# Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)

Edna Dias Canedo<sup>1</sup><sup>a</sup>, Anderson Jefferson Cerqueira<sup>1</sup><sup>b</sup>, Rogério Machado Gravina<sup>3</sup><sup>c</sup>,  
Vanessa Coelho Ribeiro<sup>3</sup><sup>d</sup>, Renato Camões<sup>3</sup><sup>e</sup>, Vinicius Eloy dos Reis<sup>3</sup>,  
Fábio Lúcio Lopes Mendonça<sup>2</sup><sup>f</sup> and Rafael T. de Sousa Jr.<sup>2</sup><sup>g</sup>

<sup>1</sup>*Department of Computer Science, University of Brasília (UnB), Brasília, DF, Brazil*

<sup>2</sup>*National Science and Technology Institute on Cyber Security, Electrical Engineering Department (ENE),  
University of Brasília (UnB), Brasília, DF, Brazil*

<sup>3</sup>*General Coordination of Information Technology (CGTI), Administrative Council for Economic Defense (CADE),  
Brasília, DF, Brazil*

**Keywords:** Brazilian General Data Protection Law, Business Process Modeling Notation, Data Privacy Brazilian Federal Public Administration, Data Protection Laws.

**Abstract:** The increasing number of online users yields to a correlated increase in the number of varied personal data collection devices. As a result, it became necessary to create and regulate new personal data policies which define the rights and duties of public and private organizations and users. As occurred in other countries, the Brazilian General Data Protection Law (LGPD) was created to define the nationwide rules regarding the privacy of users' data. In this paper, we present the proposal for a LGPD implementation process, using the Business Process Modeling Notation (BPMN). This proposal is intended to allow the Brazilian Federal Public Administration (FPA) Agencies to perform the steps to implement the LGPD in an easier and more targeted way, resulting in increased privacy of personal data. The proposal also defines new roles and responsibilities within FPA Agencies to enable these Agencies for providing clarifications to complaints about personal data, receiving communications from the National Data Protection Authority (ANPD) and adopting measures, guiding employees in relation to rules, regulations and data protection laws.


## 1 INTRODUCTION


Privacy has often been identified as a major concern for systems that handle personal information. Activities that were previously private or shared with few users, currently leave traces of data that expose the interests, characteristics, beliefs and intentions of users. Privacy reflects the particular needs and desires of each user and changes constantly in terms of life cycle progress and situational events (Razak et al., 2020). Privacy is a complex notion, because there are several


factors and dimensions that can vary according to culture or context. The perception of privacy can also be subjective and differ from one user to another (Ataie et al., 2018).


In the literature, there are several reports of information that are being leaked by people intentionally and/or involuntarily among themselves, both through commercial organizations and through government agencies (Chamikara et al., 2020). The breach of privacy can threaten an individual's autonomy, not just as users, but as citizens (Lu and Li, 2020). According to Acquisti et al. (Acquisti et al., 2015), sharing users' personal data, does not always translate into more progress, efficiency or equality.


With growing personal concerns about ensuring data privacy, when using different software, such as mobile applications and online service systems, several countries have signed data protection laws, such as the General Data Protection Regulation (GDPR)


<sup>a</sup>  <https://orcid.org/0000-0002-2159-339X>


<sup>b</sup>  <https://orcid.org/0000-0002-6973-3240>

<sup>c</sup>  <https://orcid.org/0000-0002-7129-8874>

<sup>d</sup>  <https://orcid.org/0000-0001-7537-6895>

<sup>e</sup>  <https://orcid.org/0000-0002-0793-7715>

<sup>f</sup>  <https://orcid.org/0000-0001-7100-7304>

<sup>g</sup>  <https://orcid.org/0000-0003-1101-3029>

(Regulation, 2018),(Diamantopoulou et al., 2020), (Tamburri, 2020) and the Brazilian General Data Protection Law (LGPD) (Macedo, 2018), (Bernardes et al., 2020), (Netto et al., 2019), (da Silva et al., 2020).

These laws regulate the principles for the collection, storage, treatment and sharing of users' personal data. The LGPD was sanctioned in August 2018 and is expected to come into effect in August 2021. GDPR came into effect on May 25, 2018 and regulates data privacy for European Union countries.

The pillars of LGPD are the transparency, management and governance of users' personal data (Bernardes et al., 2020),(Macedo, 2018). Regarding the user, the LGPD, determines that the personal data belongs to the person to whom it concerns and not to the person responsible for storing the data in the databases, or whoever uses the data (Bernardes et al., 2020), (Macedo, 2018). Thus, the user's right is rectified and synthesized in one word: consent (Bax and Barbosa, 2020).

The law establishes the rules for the collection, storage, treatment and sharing of personal data, imposing more protection and penalties for non-compliant organizations with the LGPD principles (Macedo, 2018). The LGPD covers all personal data collected, stored and processed by public and private organizations, with an international reach (Carauta Ribeiro and Dias Canedo, 2020).

In this paper, we present a proposal for a process to implement the General Data Protection Law (LGPD) in the Brazilian Federal Public Administration (FPA). The process aims to facilitate the understanding of public agencies to implement the LGPD and become adherent to international laws. The process was developed according to the LGPD implementation guide, developed by FPA (BRASIL, 2020).

This paper is organized as follows. Section 2 presents concepts related to LGPD and related works. Section 3 presents the adopted methodology. Section 4 presents the proposed model and the description of the process. Section 5 presents threats to validate the proposed model and limitations. Finally, Section 6 presents conclusions and future work.

## 2 BACKGROUND AND RELATED WORKS

The LGPD is a regulation that defines principles and guidelines related to the use of the most valuable assets in the context of a society in digital transformation, which is the database related to the members of society (Pinheiro, 2020), (Potiguara Carvalho et al.,

2020). For the treatment of this personal data, the law defines ten principles to be followed, in addition to determining that good faith must be observed in the activities. The principles are (Macedo, 2018; Canedo et al., 2020):

1. Purpose: where the treatment must be carried out for legitimate, specific, explicit and informed purposes to the holder, without further treatment incompatible with the initial purpose;
2. Adequacy: where the treatment must be compatible with the purpose informed to the holder;
3. Need: which limits the treatment to the minimum necessary to fulfill its purpose; 4. Free access - which guarantees the holder easy and free consultation on his personal data;
4. Data Quality: which guarantees data accuracy to data subjects, promoting the right to change incorrect or outdated data;
5. Transparency: which provides the holder with clear, accurate and accessible information about his data and the treatment performed;
6. Open Access: Assurance to data subjects, free and accessible information about the form and duration of data processing, as well as the completeness of their sensitive data.
7. Security: which guides the controller to use technical and administrative measures to protect the data of the holder;
8. Prevention: which defines measures to prevent the occurrence of damages due to the treatment;
9. Non-discrimination: which makes it impossible for the operator to carry out treatments that result in discriminatory or abusive purposes;
10. Accountability: where the agent must be accountable and take effective measures to prove compliance with the required standards.

In the context of public institutions, with regard to meeting the needs of stakeholders and creating value, the citizen is at the center of these perspectives. Therefore, there is a need on the part of institutions to reinforce their commitment to individual members of society, with regard to the protection and guarantee of fundamental human rights, which, among others, is privacy, foreseen in the Universal Declaration of Human Rights of 1948 (Pinheiro, 2020).

For data sharing within the scope of the FPA, Decree number 10,406 of October 9, 2019 was created, which institutes the citizen register database and the Central Data Governance Committee (CDGC) (BRASIL, 2019). Governance in data sharing in the FPA needs to be understood according to the criteria

of legal restrictions, information and communication security requirements and the provisions of the LGPD (BRASIL, 2020).

Decree 10,046/2019 defines the general provisions, in which the rules and guidelines are established with the purpose of (i) simplifying the provision of public services; (ii) guide and optimize the formulation, implementation, evaluation and monitoring of public policies; (iii) making it possible to analyze the conditions for accessing and maintaining social and tax benefits; (iv) promote the improvement of the quality and reliability of data held by the federal public administration; and (v) increase the quality and efficiency of the internal operations of the federal public administration (BRASIL, 2019).

To LGPD compliance, it is necessary to adapt several processes, which involve, among other activities, the implementation of a consistent digital compliance program, requiring investment, updating data security tools, document compliance verification, improving procedures and flows internal data, through the application of control and audit mechanisms, but mainly, through the change of the organizational culture (Pinheiro, 2020; Macedo, 2018).

The CDGC, instituted by Decree No. 10,046/2019, is composed of members of the Special Secretariat for Debureaucratization, Management and Digital Government, which presides over the Special Secretariat for Federal Revenue of Brazil, Civil Office of the Presidency of the Republic, Secretariat for Transparency and Prevention of Corruption of the Comptroller General of the Union, Special Secretariat for Modernization of the State of the General Secretariat of the Presidency of the Republic, Advocacy-General of the Union and National Institute of Social Security (BRASIL, 2019).

This committee invited the Institutional Security Office to form a technical group, together with its members, and to prepare a document to guide the FPA in meeting the requirements involving the topic of privacy and data sharing, where the legal bases are mainly the LGPD and decree number 10,046. The document received the name of Guide to Good Practices: General Data Protection Law (LGPD), and was published in April 2020 and provides the entities that are part of the FPA with basic guidelines, in order to guide the processing of personal data (BRASIL, 2020).

The guide to good practices is divided into four chapters, which discuss the main themes of the LGPD, which are the fundamental rights of the data subject, how to carry out the processing of personal data, the processing life cycle and good practices in

security information (BRASIL, 2020). In each chapter, the recommendations for each step of the LGPD implementation are detailed, regarding general context of the data and defining the steps to implement the law.

## 2.1 Related Works

Although the LGPD is recent, the law has been the subject of study and analysis on several research fronts. Both LGPD and GPDR are referenced in existing studies in the literature, as principles for new standards, improvements to standards already implemented and data security in Information and Communication Technology (ICT) activities. In this sense, we investigated the current scenario of the application of the GDPR and LGPD law in public and private organizations, with the objective of proposing standards that, in the future, can be replicated. This research stage consisted of reading the existing bibliography and adapting the proposals made by LGPD (Macedo, 2018), with a focus on the adaptability of data security processes in Brazil, to the international standards proposed by GPDR (Regulation, 2018).

Schreiber (Schreiber, 2020) analyzed the role of the National Data Protection Commission - (NDPC) in the regulatory process in electronic environments. The author described the procedures to be adopted for the use of personal data processed by electronic means, and how the protection of personal data in the electronic communications sector should occur, as well as the data protection paths using Digital Forensics. The author presented GDPR articles that are associated with the context analyzed in the study.

Ribeiro and Canedo (Carauta Ribeiro and Dias Canedo, 2020) defined security criteria for personal data and actions to guide the University of Brasília (UnB) in its ICT processes regarding the need to LGPD compliance. The study was applied to UnB's software systems. In the construction of the proposal, the authors analyzed and understood the privacy principles of the LGPD, GDPR and ISO 27701 (Lachaud, 2020) laws. To define which LGPD principles were relevant to the analyzed case study, the authors carried out an analysis of the requirements, using the Analytical Hierarchical Process Method (AHP). To perform the comparison and indication of the data security priority, the authors applied the Preference Classification for Enrichment Assessment method - PROMETHEE and for the implementation according to the LGPD, the authors used the Multiple Criteria Decision Analysis process - MCDA. They defined as the priority requirements for personal data security the level of

data protection, the security risk, the severity of the incident and the risk of data privacy. As a result of the research, data privacy risks criterion was identified as a priority in the implementation of LGPD at UnB (Carauta Ribeiro and Dias Canedo, 2020).

Lindgren (Lindgren, 2020) reflected on changes in the modeling of business processes, to adapt to the principles of GPDR, as well as their influence on the relationships of Business Process Notation (BPN) and between Business Process Modeling Notation (BPMN). The author considered that in a global and competitive world, in which no organization works in isolation, and that the BPN model is based on global businesses, law enforcement becomes even more complex, considering data sharing and privacy. The author described three case studies and proposed a BPN model, containing seven generic dimensions, so that any organization can apply it in different ways, according to the needs and type of business. As a result of the research, the author reported that the implementation of GPDR requires extensive business adaptation, investments in ICT and human resources to be able to support GPDR's data privacy requirements. Data privacy has been identified as a hindrance for organizations that share data for their business. In addition, the impact of data privacy in relation to the BPN model implemented in the organization, increased the functions of the value chain and shaped the dimensions of the business model.

Agostinelli et al. (Agostinelli et al., 2019) stated that to ensure the applicability of GPDR, companies need to rethink their Business Process Modeling Notation (BPMN) and how they manage users' personal data within the business. The authors used BPMN in a company in the telephone sector, with the objective of applying GPDR to guarantee the privacy of users' data, in the process of accreditation of new users and the responsibility of data controllers about the process. To ensure that there is no violation of the data privacy principle, the authors have proposed that ad-hoc countermeasures should be implemented during the BPMN automation stage in a preventive manner. In addition, the authors concluded that the design of process modeling is important for successful implementation of the data privacy law. In the analysis, they raised the critical points of GDPR regarding privacy restrictions and proposed a set of design standards to capture and integrate these restrictions in the models represented in the BPMN.

Unlike the work carried out by Agostinelli et al. (Agostinelli et al., 2019) in which the authors model a business process to implement the data privacy requirements of GDPR, analyzing a real case study, in this work, we carry out the process mapping to per-

form the implementation of LGPD in an FPA, using the BPMN notation.

### 3 RESEARCH METHODOLOGY

In this work we carried out a preliminary bibliographic survey to facilitate the construction of the proposed process for the implementation of the LGPD. This bibliographic survey can be understood as an exploratory study, with the aim of providing familiarity with the study area and ensuring that the proposed process is constructed in a clear and precise manner.

We chose exploratory research (Wazlawick, 2009) due to the need to know and understand the legislation associated with the privacy of users' data and contribute to the regulatory compliance practices of Brazilian legislation, applied in an FPA agency. Thus, we performed data collection as follows (Figure 1):

1. **Bibliographic Research:** presents a study based on articles published in conferences and newspapers. The purpose of bibliographic research is to put the researcher in direct contact with what has already been published in relation to a certain subject (Wazlawick, 2009). In this work, the bibliographic research was carried out with the objective of studying and understanding the works existing in the literature, to identify which principles and factors should be present in the implementation of the LGPD, such as the legislation related to the privacy of users' data.
2. **Observation:** by a case study, which is a method of procedure that constitutes more concrete stages of the investigation, with a more restricted purpose in explaining, in general terms, the less abstract phenomena that are limited to a private domain, such as a region, city or organization (Yin, 2018). In this work, we conducted a case study at an FPA agency.
3. **Questionnaire:** it is a way of obtaining answers to the investigated questions, and may have closed and open questions. The open questions allow us to obtain more detailed answers and the closed questions allow us to easily manipulate the data to perform the analysis (Kitchenham and Pfleeger, 2002). In this work, we conducted a questionnaire with the participants of an FPA agency to understand how user's data is handled by agency's systems, as well as: 1) databases are separated or have different treatment; 2) whether the agency is engaged in investigating and prosecuting criminal offenses; 3) the type of data processing agent that will be defined for the agency; 4) if it has ac-



tivities that use personal data in the execution of operations; 5) the current situation regarding the processing of personal data before the law; and 6) the level of consent of data subject and the possible waiver of consent for the processing of the data.

4. **Interview:** it is very suitable for obtaining information related to what people know, believe, expect and desire, as well as their reasons for each answer, which can be structured or semi-structured. The interviews contain a list of information, expressed through the questions, that we want to know from each interviewee (Kitchenham and Pfleeger, 2002). In this work, we conducted the interviews in order to understand the scenario of the FPA agency, as well as which agency systems perform personal information: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

We use data triangulation to perform data analysis. The triangulation of data aims to cover the breadth in the description, explanation and understanding of the object of study. It starts from principles that maintain that it is impossible to conceive of the isolated existence of a social phenomenon, without historical foundations, without cultural meanings and without close and essential links with a macro social reality. The theoretical support, complex and complete, does not make qualitative studies easy (Triangulation, 2014).

The data triangulation technique is presented in three different aspects: (1) User-centered product processes, (2) Elements produced by the user's environment (context in which he is inserted) and (3) Processes and products originated by the structure socioeconomic and cultural aspects of the user's social macro-organism. Figure 1 shows data triangulation process used.

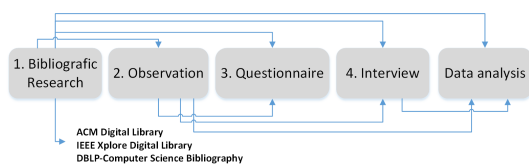


Figure 1: Process for Implementing LGPD at FPA Agencies.

## 4 PROPOSED MODEL

The proposed LGPD Implementation process started with the study of law number 13,709 and the other laws that regulate the FPA business (Macedo, 2018), (BRASIL, 2020), (BRASIL, 2019). The aim of this law is to understand the legal basis for processing personal data, possible rights of data subjects, hypotheses of data processing and verification of data processing compliance with the principles of the law and the specificities for the processing of sensitive personal data. Given the start of the process, 14 steps are required to implement and maintain general data protection in the FPA.

Figure 2 shows the General Data Protection Implementation process for FPA agencies. The proposed process consists of:

1. **Process 1. Study of the LGPD and Other Related Laws that Guide the Business:** this process begins with the study of the Information and Communications Security policy (POSIC) and the laws and regulations related to information security, which are applicable to the context from the FPA agency.
2. **Process 2. Questionnaire Application:** aims to carry out a diagnosis of the agency to identify the stage that the FPA agency is in relation to LGPD. In addition, it aims to identify whether there is any treatment that falls under the law, even if it refers to a few data. This process consists of the following steps: 1) Preparation to apply the questionnaire observing the following principles: a) Identification of the target demographic profile; b) Number of respondents required; c) Time to send the survey; d) Form of data collection; e) Data preparation and analysis; f) Preparation and presentation of the report. 2) Analysis of results according to the following information: a) The existence of treatment for economic purposes; b) The organization of personal data, employees and customers; c) The agency's ability to respond to requests from users or owners of the data; d) Professionals, whether from the agency or outsourced, responsible for handling personal data are clearly identified; e) The agency's documentation and practices regarding the management of information privacy; f) The existence of information transmission with other FPA agencies; g) The courses, seminars and training conducted at the agency in relation to information security.
3. **Process 3. Designation of the Data Protection Officer (DPO):** the data controller must act as a communication channel between the controller,

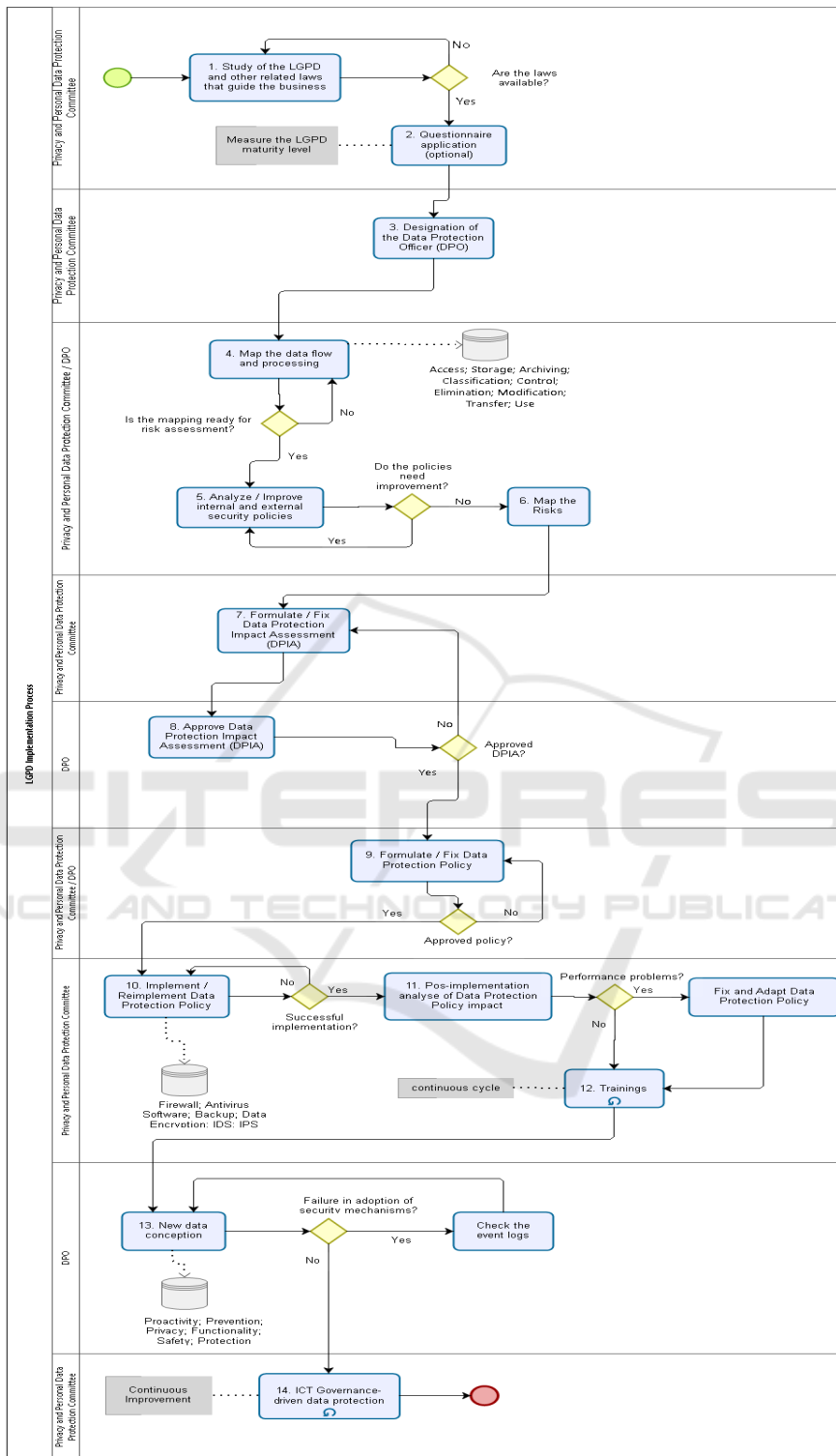


Figure 2: Process for Implementing LGPD at FPA Agencies.

data holders and the National Data Protection Authority (ANPD) to ensure that the information that

are under the authority of the agency will not be accessed by third parties and used in a malicious

manner. In addition, the DPO will be responsible for advising and verifying that the agency is complying with the LGPD in relation to the processing and treatment of third party personal data.

In order to indicate the names of the election of data protection officer (Recio, 2017), the commission must have knowledge of the nominees in relation to the following information: 1) Experience in managing the main systems and processes involved in the protection of the agency's personal data; 2) Knowledge of the agency's culture, as well as its needs in the area of data protection; c) Experience in implementing data protection measures and/or frameworks; d) Expertise in the field of data protection law and practices. In order to elect the Data Protection Officer, the following steps must be taken: 1) Presentation of the name(s) chosen to fill the data manager position; 2) Define who can participate in the name choice vote; 3) Carry out the vote if more than one name is indicated.

**4. Process 4. Map the Data Flow and Processing:**

it is proposed to structure all personal data, the purpose, the legal bases that legitimize the treatment and the form of compliance with the rights of the holder such as access, rectification, exclusion, revocation of consent, opposition, information about possible shares with third parties and portability. to perform this process it is necessary to identify the systems and/or files that contain personal information.

The following activities must be carried out: 1) Analyze the systems and/or files regarding rights to be guaranteed to data subjects. Rights arising from the principles established by article 6 of the LGPD and in specific rights of the holders contained in the other articles of the LGPD (Macedo, 2018); 2) Examine possible weaknesses in the ways of storing information; 3) Observe the security, physical, logical and organizational of the agency's systems and/or personal data files; 4) Check the users' access to systems and/or files and evaluate the emission of logs in the case of systems; 5) Carry out advice from the legal area to verify the adequacy of the data processing definitions to the LGPD.

**5. Process 5. Analyze/Improve Internal and External Security Policies:**

the objective is to survey the guidelines, norms, standards, procedures, ordinances, norms and rules that can assist in the implementation of the LGPD and how they are being followed by employees who use the agency infrastructure. This activity should verify that security policies are being applied at the agency.

The main checks must be: 1) In the building installation, access control and data center; 2) In discontinued devices, with malfunctioning drivers, manufacturing defects or installation problems; 3) When using any unauthorized external device; 4) Accessing folders on a cloud server or even webmail on a home network; 5) In the use of non-approved software for alternative instant messaging applications; 6) Security updates for operating systems and applications; 7) In the protection software, checking if they are active and monitoring as configured and determined; 8) Training of employees and alignment with security policies.

**6. Process 6. Map the Risks:** the objective is to identify threats that may affect personal data processed in the agency's systems and/or files, and to take the most appropriate protection measures. In addition, it is intended to analyze the risks that have a greater possibility of occurrence (theft or loss of devices, information in the hands of third parties, Social engineering, malicious codes, misuse of technology, etc.).

After analyzing the systems and/or files and the level of maturity in relation to the application of the policies, it must analyze the risks in relation to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction of document numbers or tax returns, and employee records.

**7. Process 7. Formulate/Fix Data Protection Impact Assessment (DPIA):** the objective is to constitute the agency's data protection obligations and provide the framework for any data protection strategy to improve service delivery, data quality, decision making, project feasibility, communication regarding privacy and protection of personal data, etc.

After carrying out the report of possible risks, a social impact report must be created with the information: 1) Description of the processes for processing personal data that may generate risks to civil liberties and fundamental rights; 2) Analysis of information processing; 3) Identifying the controls carried out and proposing legal, technical, physical and organizational measures; 4) Analysis of events and threats for the data subject; 5) Proposals for safeguards and risk mitigation mechanisms; 6) Process reviews, in line with a vision of the laws; 7) Create an impact report for the agency with the information: a) The financial

severity that can cause a data leak by the agency; b) Damage to the name of the agency; c) The legal aspects of data leakage and legal liability; d) Damage to the normal flow of a process carried out by the agency.

8. **Process 8. Approve Data Protection Impact Assessment (DPIA):** the data controller must check the information submitted in the report, perform the policy audit in the context of personal data, etc. After the conference and with a positive result, the report is approved. If not, a new conference, adjustments, corrections or inclusions will be proposed.

After the approval of the data supervisor: 1) Present the agency's senior management about the risks and possible impacts related to the leakage of personal data; 2) Hold meetings with those responsible for systems and/or files that contain personal data, presenting the risks and impacts raised; 3) Conduct a lecture with employees highlighting the financial and image losses for the agency in relation to the exposure of confidential or protected personal data; 4) Collect information, suggestions and ideas for updating, modifying and adding to the impact report.

9. **Process 9. Formulate/Fix Data Protection Policy:** create or redo the data protection policy, providing for the main issues according to the LGPD: 1) Geographic, material, systemic and data scope; 2) General principles, sensitive data, confidentiality, contracting and subcontracting, data transfer and responsibilities; 3) Right of the holders in relation to personal data; 4) Actions for implementation such as governance, training and control; 5) The relationship with the National Data Protection Authority (ANPD); 6) Notification of violation of personal data; 7) Responsibilities of the data supervisor; 8) Reviews, types of reports and validity.

10. **Process 10. Implement/Reimplement Data Protection Policy:** the aim is to create a policy that measures the processing of personal data collected by the agency, directly or indirectly, mainly from employees, companies, consumers, contractors/subcontractors, or any third parties, with "Personal Data". In addition, defining data that is associated with an identified individual by means likely to be used.

In possession of data policy, the application of the policies should be verified in two areas: physical security, logical security (data network, user computers and storage) and organizational security. Analyze physical security and relate the requirements of the data policy in the main aspects:

1) The level of physical security (access by people); 2) Access to the agency's infrastructure components (data-center); 3) Whether the agency's facilities, equipment and other assets are secure; 4) The documents or set of measures and activities employed in physical security; 5) The agency's physical security duties and responsibilities.

Analyze the logical security and relate the requirements of the data policy in the main aspects: 1) Whether the communication network enables the prevention of data loss that filters the exit and entry points of the network in relation to personal data systems; 2) The generation of reports on the state of the data, such as what is being used, for what purpose and by whom they are being accessed, where they are going and where they come from. 3) Check for the presence of antivirus; 4) The organization of sensitive folders and files (content, data and information tags); 5) Access management and generation of alerts for the agency's network administrators; 6) Control of devices, such as pen-drives and cell phones; 7) Preventing the loss of data stored and shared on the agency's network; 8) The identification of anomalies in the accesses.

11. **Process 11. Pos-implementation Analyze of Data Protection Policy Impact:** the aim is the implementation of several controls, which include routine procedures, hardware and software infrastructure, monitoring of indicators, systems audit, in addition to the accurate analysis of the environment computational and organizational.

After the physical and logical implementation of the points covered in the data policy, it should be verified: 1) The real status of each equipment involved in the actions of the personal data systems; 2) If it is necessary to invest in more effective and innovative solutions; 3) Adjustment of metrics and performance indicators for personal data systems; 4) Reports on management tools for the search for flaws and vulnerabilities; 5) Ways to improve the work provided and learn about possible errors; 6) Proactive maintenance routines, focusing on equipment with the possibility of failures; 7) Controls over the infrastructure and processes that can guarantee the continuity of the services of the personal data systems; 8) If the data policy fits ICT solutions effectively; 9) If the teams are in line with the new procedures; 10) The documentation that involves the registration of routines.

12. **Process 12. Trainings:** the aim is to provide at the same time an attractive and objective communication of data security concepts and good prac-



tices used to guarantee the privacy of user's data, in order to change behaviors to make people have attention on the processing of personal data processed at the agency.

It is necessary to structure the training in modules or evolutionary cycles presenting the following knowledge: 1) The General Data Protection Law; 2) The personal data security policy; 3) The rules and procedures that everyone who access the company's ICT systems and assets must follow; 4) The interest of executive leadership in governing and actively nurturing the security of personal data systems and/or files; 5) Behavior focused on the security of systems and/or personal data files; 6) The level of responsibility and prior knowledge, of the access of the data systems and the tools used in the access; 7) Any policy violations and what are the responsibilities; 8) The channels for identifying security problems and the deadlines for action and responses.

13. **Process 13. New Data Conception:** the objective is to foresee and warn situations of invasion of privacy, in any proposal for new and/or changes to the agency's systems, products or services that use personal data, foreseeing possible risks and adopting measures that prevent or mitigate threat situations.

With the request for new systems, data and changes in systems and/or personal data files, the data supervisor must analyze: 1) If the purpose is specified in a clear, limited and relevant way in relation to what is intended when dealing with personal data; 2) If the information to be used to identify the data subject is minimized; 3) Limitation on use, retention and disclosure; 4) New requests regarding security, technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or illicit treatment; 5) If the request is incorporated into the design and architecture of the ICT systems and business practices; 6) Possible invasive privacy events in new requests; 7) If the new requests comply with the privacy standards established in the data policy; 8) Inadequate privacy projects and/or inappropriate privacy practices; 9) Negative impacts and request corrections; 10) The broader additional contexts (other systems, files, people, etc.) based on a holistic view; 11) If stakeholders were consulted; 12) The possibility of reinventing current choices when alternatives are unacceptable; 13) If there is support for standards and frameworks (according to the legislation in

this item) recognized at the agency; 14) The impact of the use, incorrect configuration or errors related to the technology, operation or architecture of information on data privacy; 15) Clearly the risks to privacy and all the measures taken to mitigate and subsequently document them; 16) If it is possible to guarantee the confidentiality, integrity and availability of personal data; 17) If the new order is subject to methods of secure destruction, proper encryption, and strong methods of access control and registration.

14. **Process 14. ICT Governance-driven Data Protection:** the objective is to carry out a set of policies, rules and processes for conducting the protection of the agency's personal data. In addition, to establish actions and strategies that bring advantages to the Information and Communication Technology (ICT) tools for the project to implement and continue the personal data protection law.

ICT governance must guarantee or mitigate the security of personal data circulating in the agency's systems and/or files, and ensure the durability and efficiency of all resources involved in this process, carrying out the main actions: 1) Establishing actions and strategies that bring increased security and mitigate the leakage of personal data; 2) Propose transparency and visibility for personal data security processes; 3) Automate processes to increase or mitigate the protection of personal data; 4) Facilitate the use of ICT resources, which support the security of personal data, for employees; 5) Anticipate problems and risks, in relation to personal data, that help in the decision-making process; 6) Verify that the Governance Program in its rules and procedures can be complied with; 7) Adapt, propose and add to the values, objectives and the pre-existing ICT Governance structure (risk management, value delivery, strategic alignment, resource management and performance measurement); 8) Perform data mapping; 9) Design the training schedule and assertive communication on data protection.

The proposed process is generic and can be implemented at any FPA agency. In addition, the process contains the necessary procedures to carry out the control of security and privacy of personal data in accordance with the LGPD. Although the process has been proposed for FPA agencies, we believe it can be applied to any private organization.

## 5 LIMITATIONS AND THREATS TO VALIDITY

The LGPD implementation proposal is a process of identification, evaluation, correction, implementation and even prediction about the security of personal data within the Federal Public Administration (FPA). In addition, the purpose of the implementation proposal is to promote prior knowledge, discussion and technical and administrative analysis of the positive and negative impacts of this implementation. Thus, one can highlight the limitations of the LGPD implementation model listed below, being more critical when referring to the FPA:

- **Framing the Number of Laws and Regulations:** The excess of data security laws and regulations does not facilitate the study and correlation of these laws and regulations in relation to LGPD. The normative complication and spontaneity of laws and regulations can affect the first stage of study of the proposed model. The biggest limitation in this step is to consolidate all the laws and safety standards in effect in Brazil and to undo contradictions, for example, in the transparency laws that must be applied in the FPA.
- **Barriers in the Selection Process and Competing Activities of the Data Supervisor:** firstly, this is a new area of expertise (role). There is still no concrete definition of activities for this role. However, it is expected that the person chosen for this role, must respond to complaints and communications from data subjects, receive communications from the national authority, advise employees and contractors on the protection of personal data and perform the other duties determined by the controller or established in complementary norms. This first point can generate limitations if the data supervisor has another role within the FPA, which divides the time between these activities. Another limitation is that the professional profile of the data manager must have at least three areas of knowledge: ICT, Management and Legal Aspects. The need for these three areas of knowledge generates a difficulty inherent in the professional's profile, where we probably will not have many options for possible candidates for the position, which may result in an indication of the professional by the FPA, and consequently there will not be an election for the office (Recio, 2017), (Alexe, 2019).
- **Weaknesses in Data Entry Mapping:** the first aspect is the large amount of database and the non-interoperability between them. Therefore,

the adoption of data entry mapping initiatives can lead to deficiencies such as little information about data ownership, lack of confidence in data quality, bureaucratic relationship at the FPA agency, lack of validity of information and other aspects. information technicians, lack of adequate information management and non-integrated database, due to the absence of an integrated system. These and other factors can lead to a limitation in the implementation of the LGPD, in accordance with data privacy principles.

- **Moderations in Risk Analysis:** the first point is that many of the techniques, standards and frameworks, can hinder the path of risk analysis. Another factor is that due to lack of knowledge of the risks arising from accessing the databases, it makes the risk analysis process costly, tiring and ineffective. In addition, there may be wear and tear in convincing FPA superiors to pay attention to this analysis. Finally, there may be problems in interacting with people that allow a shared view of a team or a group of people about a personal data system and its security.
- **The Impact Report Problems:** Cause for an unprecedented model in use and the incipient implementation of the LGPD, it can cause an inadequate description of the planned processing operations and the purpose of the data processing and then generating deficient and / or incomplete reports. Another situation to be considered, since the risks are also limiting items, the measures responses to face risks, guarantees, security and procedures designed to ensure the protection of personal data, demonstrate compliance with the LGPD. Finally, factors such as time, analysis and creation of the report can impact and indicate that this instrument is not useful for assessing impacts on other data processing operations, making it just a legal object.
- **Support for Data Protection by ICT Management:** Applying the proposed model, it may happen that the tools become obsolete or systems and information are not available within the agency. That should impact on the productivity of the LGPD implementation, increasing rework and decreasing the quality of data manipulation. Other factors can limit the support of data protection by ICT management such as inadequate ICT infrastructure, poor availability of systems and information, non-automated processes, inefficient communication and relationships with users and those responsible for the databases.

The knowledge of these limitations allows to avoid

and to mitigate problems in the LGPD implementing model. The investigation and the anticipation, with possible improvements in these limiting aspects, automatically reflect the process implementing of personal data protection, reducing the conflicts of interest in the Federal Public Administration. These limitations are not, therefore, an instrument of decision, but an instrument that help the LGPD implementing process.

## 6 CONCLUSIONS

In this article, we present a proposal for an LGPD implementation process, according to LGPD guidelines, developed by the FPA to support the agencies understanding data privacy requirements, that must compliance with LGPD during implementation by agencies.

The proposed process model can be adopted by any federal public administration agency and/or private organizations. As future work, we intend to apply the model proposed in other agencies, with different contexts, with the aim of adapting / evolving the process to a more representative model.

## ACKNOWLEDGEMENTS

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 co-operation 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

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.

Agostinelli, S., Maggi, F. M., Marrella, A., and Sapio, F. (2019). Achieving GDPR compliance of BPMN process models. In *CAiSE Forum*, volume 350 of *Lecture Notes in Business Information Processing*, pages

10–22, [https://doi.org/10.1007/978-3-030-21297-1\\_2](https://doi.org/10.1007/978-3-030-21297-1_2). Springer.

Alexe, I. (2019). The role of the data protection officer in respect of the rights of the data subject. *RRDA*, 1:23.

Ataei, M., Degbelo, A., and Kray, C. (2018). Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. *Journal of Location Based Services*, 12(3-4):141–178.

Bax, M. P. and Barbosa, J. L. S. (2020). Proposta de mecanismo de consentimento na lei geral de proteção a dados - LGPD (consent mechanism proposal in LGPD). In *ONTOBRAS*, volume 2728 of *CEUR Workshop Proceedings*, pages 316–321. CEUR-WS.org.

Bernardes, M. B., de Andrade, F. P., and Novais, P. (2020). Data protection in public sector: Normative analysis of portuguese and brazilian legal orders. In *World Conference on Information Systems and Technologies*, pages 807–817. Springer.

BRASIL (2019). Decreto número 10.046 de outubro de 2019. *Diário Oficial da União - Seção 1*, 1:1–5.

BRASIL (2020). Guia de boas práticas – lei geral de proteção de dados (lgpd). *Comitê Central de Governança de Dados. Secretaria de Governo Digital*, 1–65.

Canedo, E. D., Calazans, A. T. S., Masson, E. T. S., Costa, P. H. T., and Lima, F. (2020). Perceptions of ICT practitioners regarding software privacy. *Entropy*, 22(4):429.

Carauta Ribeiro, R. and Dias Canedo, E. (2020). Using mcdm for selecting criteria of lgpd compliant personal data security. In *The 21st Annual International Conference on Digital Government Research*, dg.o '20, page 175–184, New York, NY, USA. Association for Computing Machinery.

Chamikara, M. A. P., Bertók, P., Liu, D., Çamtepe, S. A., and Khalil, I. (2020). Efficient privacy preservation of big data for accurate data mining. *Inf. Sci.*, 527:420–443.

da Silva, M. V. V., da Luz Scherf, E., and da Silva, J. E. (2020). The right to data protection versus “security”: Contradictions of the rights-discourse in the brazilian general personal data protection act (lgpd). *Revista Direitos Culturais (Cultural Rights Review)*, 15(36).

Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., and Charalabidis, Y. (2020). Preserving digital privacy in e-participation environments: Towards GDPR compliance. *Inf.*, 11(2):117.

Kitchenham, B. and Pfleeger, S. L. (2002). Principles of survey research. *ACM SIGSOFT Software Engineering Notes*, 27(5):17–20.

Lachaud, E. (2020). Iso/iec 27701: Threats and opportunities for gdpr certification. *Available at SSRN*, 1:1–23.

Lindgren, P. (2020). The impact on multi business model innovation related to GDPR regulation. In *HICSS*, pages 1–8, <http://hdl.handle.net/10125/64279>. ScholarSpace.

Lu, Y. and Li, S. (2020). From data flows to privacy issues: A user-centric semantic model for representing and discovering privacy issues. In *HICSS*, pages 1–10. ScholarSpace.

- Macedo, P. N. (2018). Brazilian general data protection law (lcpd). *Nartional Congress*, accessed in May 18, 2020, 1:1-5.
- Netto, D., Silva, C., and Araújo, J. (2019). Identifying how the brazilian software industry specifies legal requirements. In *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, pages 181-186.
- Pinheiro, P. (2020). *Proteção de Dados Pessoais: Comentários a Lei 13.709/2018 (LGPD)*, volume 1. Saraiva, 8553605280.
- Potiguara Carvalho, A., Potiguara Carvalho, F., Dias Canedo, E., and Potiguara Carvalho, P. H. (2020). Big data, anonymisation and governance to personal data protection. In *The 21st Annual International Conference on Digital Government Research*, pages 185-195.
- Razak, S. A., Nazari, N. H. M., and Al-Dhaqm, A. M. R. (2020). Data anonymization using pseudonym system to preserve data privacy. *IEEE Access*, 8:43256-43264.
- Recio, M. (2017). Data protection officer: The key figure to ensure data protection and accountability. *Eur. Data Prot. L. Rev.*, 3:114.
- Regulation, G. D. P. (2018). Eu data protection rules. *European Commission*, Accessed in October 9, 2019, 1.
- Schreiber, A. (2020). Right to privacy and personal data protection in brazilian law. In *Data Protection in the Internet*, pages 45-54. Springer, [https://doi.org/10.1007/978-3-030-28049-9\\_2](https://doi.org/10.1007/978-3-030-28049-9_2).
- Tamburri, D. A. (2020). Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation. *Inf. Syst.*, 91:101469.
- Triangulation, D. S. (2014). The use of triangulation in qualitative research. In *Oncology nursing forum*, volume 41, page 545, 10.1188/14.ONF.545-547. National Center for Biotechnology Information.
- Wazlawick, R. S. (2009). *Metodologia de pesquisa para ciência da computação*. Elsevier, 978-85-352-6643-6.
- Yin, R. K. (2018). Case study research and applications. *Design and methods*, 6:1-352.