LGPD Framework: An Implementation and Compliance Guide for Technology Areas

Sara B. O. G. Carturan[1], **Beatriz M. A. Matsui**[1], **Denise H. Goya**[1]

[1]Pós-Graduação em Ciência da Computação – Universidade Federal do ABC (UFABC)
Santo André – SP – Brazil

{sara.carturan, beatriz.mayumi, denise.goya}@ufabc.edu.br

Abstract. *Considering the unrestrained consumption of personal data, the LGPD came to protect and regulate the treatment of data, whether digital or physical. Due to the lack of technical guides to interpret the LGPD and apply it in the technology area, a gap arises that impacts IT management. This paper proposes a conceptual framework composed of domains and components to facilitate the LGPD interpretation and implementation by technology areas. The framework was mainly inspired by the essential principles of COBIT 2019 and DevOps, which transform a concept into a practical method of understanding and implementation. The LGPD framework will guide organizations to be compliant in a shorter time and to provide cultural and behavioral changes.*

1. Introduction

Technology permeates almost every aspect of our society, connecting people, systems, environments, sensors, and devices. Sometimes, it is not very easy to establish boundaries between the physical and digital worlds. With the evolution of technology, there is a proliferation of data, which leads to the need to develop new business models. In turn, the new business models have led to conceptual changes in product development, including the use of data as added value in services [Huth 2017].

An EU-wide regulation controls how companies and other organizations process personal data – the General Data Protection Regulation (GDPR). This regulation covers any organization globally that has personal data of individuals from the European Union; hence its importance [European-Parliament and Council 2016]. Similarly, in Brazil, the General Data Protection Law (or "Lei Geral de Proteção de Dados" – LGPD, in Portuguese) was sanctioned in August 2018 and enforced in August 2020, being applied to everyone on Brazilian territory, with a few exceptions [Brasil 2018]. Considering a legal point of view, the LGPD defines standards, roles, responsibilities, rights, penalties, and practices to promote the protection of the personal data of every Brazilian citizen.

In this work, we propose an LGPD framework that can serve as a reference model to help organizations segment the LGPD into an IT view. A literature review showed several works related to the LGPD, but few studies and frameworks similar to this one. Each organization has defined an LGPD implementation plan in the best possible way, but there is no established standard of analysis and definition of actions to become compliant [Teixeira et al. 2019a]. Studies such as [Fernandes et al. 2021, Rapôso et al. 2019], for example, illustrate a theoretical approach to understanding the LGPD, considering impacts on using the LGPD in cloud computing and a systematic review on the applicability of the law in technology, without proposing frameworks or architectures to guide

the implementation of the LGPD by Information Technology (IT) practitioners. The thesis [Carvalho 2021] presents an LGPD implementation model considering the aspects of Data Governance, Data Privacy, and Information Security. However, its applicability was restricted to public financial institutions, as pointed out by the authors themselves, in addition to the focus on business aspects and applicability in Big Data scenarios only. The compliance process is also an important topic addressed in some papers on LGPD. However, they have a specific focus, such as in small and medium-sized agribusiness companies [Marques et al. 2021], and possible techniques for converting a clear database to a ciphered database [Pitta et al. 2020]. But none of these articles exposed legal writing, which is organized by chapters, sections, articles, and paragraphs and represents them in a framework.

In contrast, our framework aims to serve as a guide for all IT practitioners, and it considers, in addition to governance and privacy aspects, all the methods and processes involved in data processing and management and the infrastructure architecture necessary for the development and maintenance of systems under the LGPD optics.

2. LGPD Main Concepts and Brazilian Context

The LGPD is the first Brazilian legislation that broadly regulates data privacy. It has the objective of regulating the processing of personal data by guaranteeing fundamental rights to protect people's freedom, and privacy [Brasil 2018]. The LGPD should not be interpreted and implemented only by lawyers or legal entities. It is a multidisciplinary theme where Information Security, audit, fraud, compliance, and quality teams should be involved since at the beginning [Oliveira et al. 2019, Habl et al. 2017].

In this context, an analysis of the LGPD should not be carried out from an isolated point of view. Everyone should discuss and examine the actions, constraints, impacts, and consequences to get a complete picture of the focal point of analysis. The decision must be made by consensus, and monitoring must be done to verify the results. If one of these views is missing, the conclusions can be misrepresented.

2.1. LGPD Roles and Responsibilities

There are some important roles in the LGPD as shown in Figure 1: the **Controller**, who is a natural or legal person and determines the purposes and means of the processing of personal data; the **Processor**, who is a natural or legal person that processes personal data on behalf of the Controller; the **Data Protection Officer (DPO)**, whom the Controller must appoint to act as a communication channel between the Controller and the DPO; the data subjects and the **National Data Protection Authority** (ANPD, in Portuguese) [Brasil 2018]. The responsibilities of ANPD are monitoring and enforcing penalties, having technical and decision-making autonomy, establishing guidelines, rules, and procedures, and regulating data protection.

A company or organization that collects, uses, or stores personal data from anyone must comply with LGPD principles and in good faith. *Good faith*, in a simple way, is the state of consciousness of the individual who is acting according to the established norms. A starting point could be for companies to identify which of their data is personal data. Based on that, companies will define the adequate treatment for their data in an LGPD Action Plan. For sure, a contract review must be done to be LGPD compliant. Regardless of

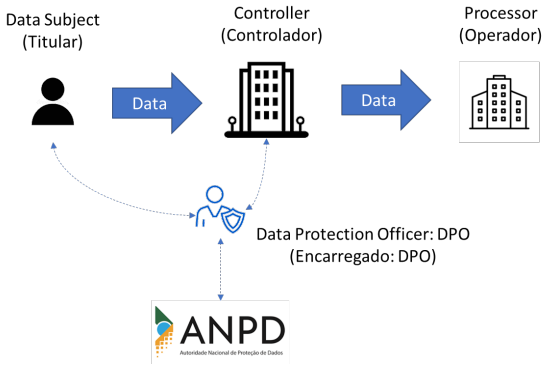

Figure 1. LGPD main roles relationship. (Designed by the authors)

company size, the corporate world is interconnected as if it were a huge network. Thereby, Information Systems (IS) increasingly need integration, interoperability, scalability, flexibility, privacy, security, transparency, and collaboration, to meet business challenges. In this context, new ecosystems emerge, where roles may vary depending on the situation, as producer, consumer, or partner. These characteristics of complex environments make design and integration a big challenge [Habl et al. 2017].

2.2. LGPD Impacts

Thus, business and industry processes, Brazilian regulations, Information Security policies, IT governance, IT operational model, and IT architecture framework should be adjusted to this new scenario. It is almost inevitable that the complexity between IS will increase, further requiring interoperability to support activities between heterogeneous environments. The organization that does not comply with the regulation may be charged with penalties by ANPD, such as administrative fines and temporary suspension of its processing activities. It will depend on the nature, gravity, duration of the infringement, and consequences and will be established by ANPD.

Another meaningful discussion is the knowledge of the role that Systems-of-Information Systems (SoIS) [Teixeira et al. 2019b] plays in our society. Building secure and sustainable software, requiring knowledge, technology, methodologies, innovation, and tools, depend fundamentally on people. The success of scientific and technological development depends intensely on the human values embodied in technologies [Schwartz 1992]. It is essential to consider that the LGPD implementation is much more than adjusting some Information Security procedures, but it should lead to changes in people's behavior, systems development methodology, IT governance, IT architecture, and contracts. The law itself is complex, extensive, and involves a certain degree of subjectivity [Teixeira et al. 2019a, Graciano Neto et al. 2016].

Therefore, it is essential to have a legal understanding of the law and how it will be operationalized, considering the specificities and technological restrictions. Today's corporate systems, in general, are not prepared to offer all sensitive data processing and data subject rights in a fast and transparent manner [Habl et al. 2017, Barata and Prado 2015].

3. Introducing the LGPD Framework

The LGPD Framework was devised considering Control Objectives for Information and Related Technologies (COBIT) [Audit and Association 2018], DevOps (term that stands

for *Development* and *Operations*) [Erich et al. 2017], Information Technology Infrastructure Library (ITIL) [Axelos and Office 2019], and some ISO/IECs (38500, 27001, 20000) [Calder 2008, Kunas 2012], standards for Information Security Management Systems published by the International Organization for Standardization and the International Electrotechnical Commission. These frameworks and standards were selected because they provide good methodological support for technology areas and will help implement the needs required by the LGPD. It was the authors' choice, considering their academic and professional experience. Also, working with clients provided experience in practical implementations in Brazilian and global companies.

The LGPD framework was based on a conceptual model, identifying its main components and their interrelationships without losing the consistency of its essence. Also, it is open and flexible, allowing the addition of new content or components without compromising its integrity and consistency. Finally, it aligns with leading global IT standards, guidelines, and regulations. The LGPD framework has six essential principles based on the Principles of the Technology Governance referenced by COBIT 2019, which are: add value, be componentizable, be clear, be versatile, have dynamism, and reach the entire organization [Audit and Association 2018].

3.1. Framework Structure

The LGPD framework will support the organization in creating its data protection view considering regulation drivers. The LGPD framework comprises a conceptual framework for the LGPD implementation formed by domains and components to facilitate the law interpretation by technology areas. Successful governance starts with aligning business and technology strategy, which creates the foundation for all technology decisions. In addition to that, there are LGPD requirements that should comply and integrate with the IT governance model.

The LGPD framework was developed considering primary technology standards and frameworks, and also the theory of technological frames of reference [Orlikowski and Gash 1994]. The theory introduces a systematic approach to examining how people understand technology, where each interpretation is seen as a "technology framework" representing an analytical view of technological development. A parallel can be made with our LGPD framework, which exists from the researchers' vision and experience and proposes a component-based model for implementing the LGPD from a practical perspective.

The framework comprises four domains: **LGPD Governance & People**, which comprehends guidelines, roles and responsibilities, and behavior changes demanded by the LGPD; **Methods & Processes**, which explicit policies, standards, and processes of personal data treatment and monitoring to drive and organize what should be done; **Data Controls**, which manage and monitor physical or logical data considering its entire lifetime, and **Infrastructure Architecture**, which defines infrastructure principles, platforms, models, and standards for use across the organization considering LGPD requirements (Figure 2). COBIT 2019 helps organizations create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. Moreover, COBIT is aligned with the most relevant IT-related standards and frameworks used by organizations, such as the Committee of Sponsoring Organizations of

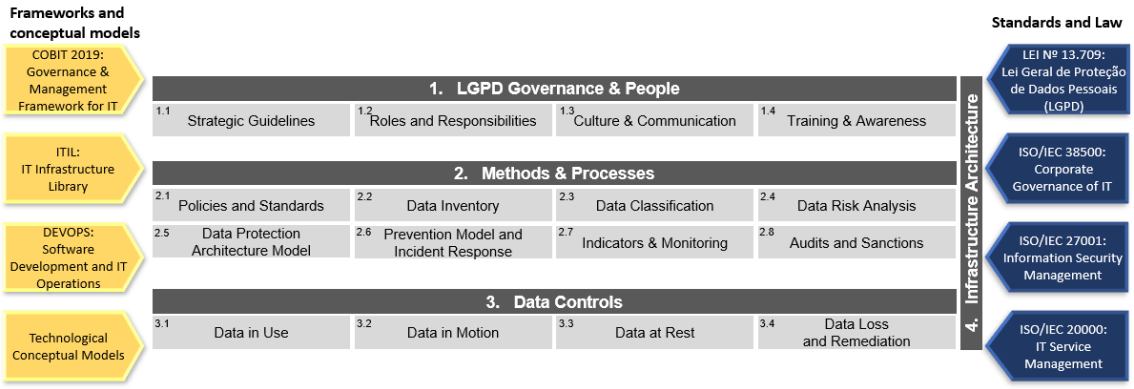

Figure 2. LGPD framework for implementation by technology areas. (Designed by the authors)

the Treadway Commission (COSO) [Janvrin et al. 2012], ISO/IEC 38500 [Calder 2008], ITIL [Axelos and Office 2019], ISO/IEC 27000 series [Meriah and Rabai 2019], ISO/IEC 31000 [Purdy 2010], ISO/IEC 9000 [Hoyle 2017], among others that can still be highlighted [Audit and Association 2018]. ITIL is a set of practices for IT Service Management (ITSM) that identifies and develops actions aiming to improve each provided IT service's overall quality, efficiency, and effectiveness, reflecting trends in software development and IT operations. It includes recommendations on how to apply philosophies such as Agile, DevOps, and Lean in the service management domain [Axelos and Office 2019]. DevOps seeks to remove technical, process, and cultural barriers between development and operation areas. So, it eliminates blocks, improves collaboration, empowers people, accelerates productivity, and automates. It is more related to People & Processes, but for sure, it also includes tools [Leite et al. 2019].

The definitions of the conceptual IT framework were considered to build the LGPD framework, as it must have some characteristics and, in addition, continuous adjustments [Orlikowski and Gash 1994]. Internal and external alignment of IT guidelines is critical, and its lack can be one of the main reasons for IT strategy failure [Venkatraman et al. 1993, Checkland and Holwell 1998]. Attention to external factors, legislation, and market changes are also critical success factors for IT to stay modern and provide continuous improvement. Many authors describe technological conceptual models, and we highlight here some of them [Orlikowski and Gash 1994, Venkatraman et al. 1993, Checkland and Holwell 1998] due to their relevance and drivers for the LGPD framework design. Another significant contribution was ISO/IEC because it develops, maintains, and promotes science and technology standards. There are many valuable standards: ISO/IEC 38500, which focuses on IT corporate governance; ISO/IEC 27001, whose family contributes to Information Security; and ISO/IEC 20000, which is dedicated to IT Service Management. All this served as inspiration for the creation of the LGPD framework.

3.2. Relation Between the Law and the LGPD Framework

It is important to understand the relationship between the law and the framework. The document that describes the law has 65 articles, three of which were vetoed (56, 57, 59). The LGPD framework is directly related to each article of the law. Figure 3 demonstrates

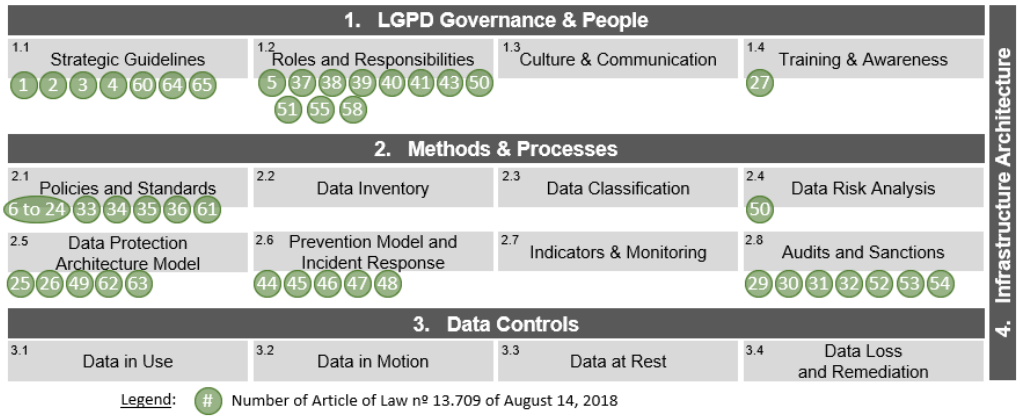

Figure 3. Relation between the Brazilian General Data Protection Law [Brasil 2018] and the LGPD framework. (Designed by the authors)

where each article of the law is represented in the LGPD framework component. Some components do not have a specific article, as they are IT tasks and must be performed exclusively by the technology area. Because of this, some components do not have a directly related regulatory article. **LGPD Governance & People** relates to guidance, roles, and responsibilities. **Methods & Processes** is the domain related to the articles of the law. **Data Controls** consider structured and unstructured data related to personal data. This domain considers the five stages of the data life cycle (creation, storage, use, archiving, and destruction), covering the three data states (in use, in motion, and at rest). And the **Infrastructure Architecture** domain is needed because physical environments must be solid, scalable, modular, secure, and reliable.

3.3. Interconnection with DevOps

From a technical perspective of software development, DevOps practices are increasingly present to ensure greater union between various development and operations teams and establish more security and agility in the software delivery process. Although there is no standard definition for DevOps, we can understand it as a set of practices that aim to integrate development and operations teams and automate the continuous delivery of software, ensuring its availability with agility, resilience and correctness [Leite et al. 2019, Dyck et al. 2015]. DevOps relates to the LGPD by helping to maintain the software under data protection and security standards, handling data throughout the entire application lifecycle, promoting better communication and accountability between different teams, and encouraging more agility and quality in the whole software development process [Mendes et al. 2021].

DevOps practices are essential in the context of LGPD and other data protection regulations as it promotes software development considering security, privacy, and monitoring aspects [Riungu-Kalliosaari et al. 2016]. Besides, DevOps creates a good foundational IT environment, contributing to better communication, the collaboration of multidisciplinary professionals, and improving the quality of the delivered product. In this way, DevOps helps bring greater standardization, structure, and transparency in data management, including identifying and handling personal data. In the context of LGPD and GDPR, not having DevOps impacts the culture – promoting or perpetuating division between teams – and a lack of mutual understanding for the adoption and

implementation of LGPD practices, in addition to not focusing on automation and consequent monitoring of security failures and breaches, through compliance scans, for example [Abrahams and Langerman 2018]. Moreover, the absence of DevOps practices in systems development under regulations such as the LGPD makes it difficult to adapt quickly to changes and swiftly identify and correct failures and other system characteristics that do not comply with the law.

The LGPD framework aligns with agile development processes, and the DevSecOps methodology [Canedo et al. 2021, Carturan and Goya 2019]. Since the design phase, several specific tasks for planning have been defined, including SoS Security Drivers, Information Security, Architecture Solution, Development, Tests, and Infrastructure. The idea is that DevOps permeates all components of our framework, and, in parallel, the LGPD (with its new rules of approach on how to handle personal data) is present in the DevOps lifecycle. The adoption of DevOps brings several relevant benefits to companies, but it also requires standardization, efficiency, automation, and knowledge, among other characteristics [Riungu-Kalliosaari et al. 2016, Leite et al. 2019, Lwakatare et al. 2019]. All of this contributes to the implementation of the LGPD – because to achieve DevOps benefits realization, IT processes need to be revised, simplified, and improved. However, this is not enough, as the LGPD implementation requires specific changes for personal data protection. Despite that, DevOps adoption is an accelerator for LGPD compliance.

On the one hand, DevOps relates to LGPD Governance & People when it focuses on People, Processes, and Technology [McCarthy et al. 2015]. Cultural change, understanding of roles and responsibilities, and training and awareness are essential steps for a good adoption and implementation of DevOps practices and the LGPD. The same goes for Methods & Processes in the framework, which interconnects with DevOps by bringing standards for data classification, auditing, and monitoring. On the other hand, the LGPD framework provides a way to establish at which stages of the DevOps lifecycle it will be implemented. They consist mainly of planning (Governance & People), software development/coding phases considering privacy by design [Cavoukian 2020] and proper data storage and manipulation, deployment and monitoring (Methods & Processes and Data Controls), and its entire infrastructure (Infrastructure Architecture).

4. Discussion

The concept of privacy is increasingly in the spotlight and undergoing a paradigm shift in light of the new Brazilian General Data Protection Law (LGPD). Personal information is a valuable asset, and privacy awareness of the public has increased significantly once frequent personal data breaches catch media attention. The purpose of the LGPD framework is to provide general propositions, covering the entire regulation in legal language and organizing it into components that technology areas can implement according to the adherence and need of each organization.

The LGPD framework has four dimensions that consist of a pool of similar skills and capabilities for LGPD compliance [Pitta et al. 2020]. The criterion for creating a dimension was to break it down into single, non-overlapping components that consist of core functions to serve and support all LGPD articles. The first dimension was defined as **LGPD Governance & People** considering all entities, roles, and responsibilities defined by the law [Brasil 2018]. It also considered relevant leading frameworks and standards

such as COBIT, ITIL, and DevOps and identified the future requirements for LGPD governance. The second dimension, **Methods and Processes**, covers all the definitions that an organization needs considering the LGPD. In this way, the policy and standards components of the LGPD were defined. Another basic set of essential components was to manage data, such as inventory, classification criteria, risk analysis, and data protection architecture.

Finally, some components were defined to help management, such as prevention and response to incidents, indicators, and audits (internal or external). The third dimension, **Data Controls**, comprises data, more specifically personal data, which can be data in use, data in motion, and data at rest [Sharma et al. 2016]. Data in use is data that a user is manipulating. It is currently being updated, processed, erased, accessed, or read by a system (data lifecycle). Data in motion is the data that is in transit. For instance, it refers to digital information transferred and could be sent either within or between computer systems to a cloud environment. Once the data arrives at its final destination, it becomes "data at rest" that is when it is stored physically in databases, data warehouses, archives, tapes, spreadsheets, or off-site backups [Perkins 2013]. The fourth and last dimension, **Infrastructure Architecture**, covers the assistance in the evaluation and transformation of the IT infrastructure (data centers, networks, servers, applications) and optimizes the use of IT hardware and software assets considering the LGPD requirements. In some cases, it may require the implementation of new technologies. However, opportunities to reduce IT costs should always be analyzed. This dimension can include the IT contract and supplier management process.

A sustainable data protection program requires effective interactions across People, Processes, and Technology [Tikkinen-Piri et al. 2018]. The LGPD framework will help provide a reference model to review and evaluate the current data protection practices and technologies and implement LGPD requirements in all technology dimensions. First, the organization must review and identify its current stage of adherence to the regulation (LGPD assessment). Then, it should identify gaps and risks and, subsequently, develop an implementation plan to solve the identified gaps.

5. Conclusions

The framework provides a standardized and comprehensive way to achieve sustainability and influence a long-term data protection strategy. Moreover, there is the benefit of being a flexible, scalable, and responsive model that different organizations can use. The LGPD framework is helpful because it aims to simplify understanding of the normative document (law), which sometimes requires legal knowledge, and presents how IT processes, roles, and responsibilities must be changed to meet LGPD requirements. It is a guideline, and each organization can decide how to implement it. Moreover, it brings together several best practices from internationally recognized frameworks and standards.

The LGPD regulation includes new obligation controllers, personal data processors, and penalties for non-compliance with LGPD principles, resulting in hefty fines. The LGPD emphasizes accountability, requires greater documentation and records, and applies to everyone's personal data in Brazil. The LGPD is not only about technology requirements. It also touches on all aspects of an organization, reaching across people, processes, and technology. The organization should determine which businesses and IT

processes are impacted. Maybe it could need to redesign its processes to incorporate steps that address key privacy requirements. In addition to that, the process implementation should have monitoring controls to provide transparency that consistently satisfies LGPD requirements.

Considering people changes, the organization should identify the relevant stakeholders across business units (who can contribute to compliance remediation planning and execution). They need to train all people involved and be responsible for handling personal data. Finally, organizations should understand their IT environment, data assets, and data processing applications to identify the impacts LGPD requirements present and develop a remediation plan to update the IT environment. The LGPD framework will help the organization to do that. The purpose was to create an LGPD model that was simple to understand and use. Furthermore, the framework should be consistent with the law and conceptual model theory. As a result, the LGPD framework should provide reliable, repeatable, and relevant results. Besides, it must also be flexible, up-to-date, and integrated with other IT models in the organization.

6. Future Works

There is no doubt that the LGPD will affect almost all organizations, generating implications and actions for technology areas. It will demand reviews into modeling, designing, IT architectures, tests, deploy, management operation, and monitoring, without mentioning the behavioral, cultural, and human values changes emerging with innovation systems' transformation and digital innovation. The LGPD will be present in this environment, too.

The complexity of the LGPD implementation cannot be underestimated. Many organizations still have several activities to be done to adjust the data processing of their employee, customer, and supplier information. The solution could be different for different organizations, but to comply with the LGPD is obligatory for all, independently of the organization size. Another critical topic is contracts that should be reviewed and adjusted according to personal data processing to comply with the new regulation. It brings more clarity to personal data privacy in Brazil, considerably reducing personal information leaks and improving the quality of their handling. Citizens will now be guaranteed the right to privacy and protection of their data. Discussing and sharing experiences and lessons learned about LGPD planning and implementation are always very useful. Indeed, the LGPD framework will accelerate the deployment process, protecting organizations from sanctions and, worst of all, undesirable leaks. Much is said about the regulation, but there is no pragmatic and demystified model of how the LGPD could be implemented in Brazil. No environment, tool, application, or service will be accepted by the market without adhering to this new law, meaning that everything in IT should understand, implement, and continuously comply with the LGPD.

The LGPD framework is in the design phase, with the detailing of its domains and components. After that, the implementation phase will begin in an organization. The organization must ensure that personal data processing activities comply with good faith and principles. All of this has a greater purpose, to contribute to the right to freedom, privacy, and citizenship. Another concern is how data subjects know about privacy, LGPD, and their rights. In Europe, they are gaining awareness and knowledge about it [Presthus and Sørum 2018, Brodin 2019]. In Brazil, there is much to be done about

this perception. Future works will focus on detailing this LGPD framework and transforming it into a "chassis" that will help many organizations fulfill all requirements in less time. Equally important are the cultural and behavioral changes that involve people and processes and can make a good revolution in companies, depending on how they are managed.

7. Acknowledgements

The authors of this paper are very grateful to the Coordination for the Improvement of Higher Education Personnel (CAPES) for financial help and intellectual incentives.

References

Abrahams, M. Z. and Langerman, J. J. (2018). Compliance at velocity within a devops environment. In *Intl. Conf. on Digital Information Management*, pages 94–101. IEEE.

Audit, I. S. and Association, C. (2018). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

Axelos and Office, T. S. (2019). *ITIL Foundation, ITIL.* ITIL 4 Foundation Series. Stationery Office.

Barata, A. and Prado, E. (2015). Governança de dados em organizações brasileiras. In *Anais do XI Simpósio Brasileiro de Sistemas de Informação*, pages 267–274. SBC.

Brasil (2018). Lei geral de proteção de dados (lgpd) nº 13.709 (versão compilada). Acesso em 21 de Julho de 2020.

Brodin, M. (2019). A framework for gdpr compliance for small-and medium-sized enterprises. *European Journal for Security Research*, 4(2):243–264.

Calder, A. (2008). *ISO/IEC 38500: the IT governance standard.* IT Governance Ltd.

Canedo, E. D., Toffano Seidel Calazans, A., Cerqueira, A. J., Teixeira Costa, P. H., and Seidel Masson, E. T. (2021). Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 58–69.

Carturan, S. B. O. G. and Goya, D. H. (2019). A systems-of-systems security framework for requirements definition in cloud environment. In *Proceedings of the 13th European Conference on Software Architecture - Volume 2*, ECSA '19, page 235–240. ACM.

Carvalho, A. P. (2021). Proposta de um framework de compliance à lei geral de proteção a dados pessoais (lgpd): um estudo de caso para prevenção a fraude no contexto de big data. Master's thesis, UNB, Faculdade de Tecnologia, Dept. Engenharia Elétrica.

Cavoukian, A. (2020). Understanding how to implement privacy by design, one step at a time. *IEEE Consumer Electronics Magazine*, 9(2):78–82.

Checkland, P. and Holwell, S. (1998). Action research: its nature and validity. *Systemic practice and action research*, 11(1):9–21.

Dyck, A., Penners, R., and Lichter, H. (2015). Towards definitions for release engineering and devops. In *IEEE/ACM 3rd Intl. Workshop on Release Engineering*, pages 3–3.

Erich, F. M., Amrit, C., and Daneva, M. (2017). A qualitative study of devops usage in practice. *Journal of Software: Evolution and Process*, 29(6):e1885.

European-Parliament and Council (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). Acesso em 21 de Julho de 2020.

Fernandes, M. A. d. S., de Oliveira, F. G., Ferraz, F. S., da Silva, D. A., Canedo, E. D., and de Sousa Jr, R. T. (2021). Impactos da lei de proteção de dados (lgpd) brasileira no uso da computação em nuvem. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E42):374–385.

Graciano Neto, V., Oquendo, F., and Nakagawa, E. (2016). Systems-of-systems: Challenges for information systems research in the next 10 years.

Habl, A., Kipouridis, O., and Fottner, J. (2017). Deploying microservices for a cloud-based design of system-of-systems in intralogistics. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*, pages 861–866.

Hoyle, D. (2017). *ISO 9000 quality systems handbook: increasing the quality of an organization's outputs*. Routledge.

Huth, D. (2017). A pattern catalog for gdpr compliant data protection. In *10th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modelling*, PoEM 2017, page 34–40. CEUR-WS.

Janvrin, D. J., Payne, E. A., Byrnes, P., Schneider, G. P., and Curtis, M. B. (2012). The updated coso internal control—integrated framework: Recommendations and opportunities for future research. *Journal of Information Systems*, 26(2):189–213.

Kunas, M. (2012). *Implementing service quality based on ISO/IEC 20000: A management guide*. IT Governance Publishing.

Leite, L., Rocha, C., Kon, F., Milojicic, D., and Meirelles, P. (2019). A survey of devops concepts and challenges. *ACM Computing Surveys (CSUR)*, 52(6):1–35.

Lwakatare, L. E., Kilamo, T., Karvonen, T., Sauvola, T., Heikkilä, V., Itkonen, J., Kuvaja, P., Mikkonen, T., Oivo, M., and Lassenius, C. (2019). Devops in practice: A multiple case study of five companies. *Information and Software Technology*, 114:217–230.

Marques, S., Lisboa, A., Érico Amaral, and Lampert, V. (2021). Pdagro: Uma proposta de protocolo para compliance à lgpd. In *Anais do XIII Congresso Brasileiro de Agroinformática*, pages 378–381, Porto Alegre, RS, Brasil. SBC.

McCarthy, M. A., Herger, L. M., Khan, S. M., and Belgodere, B. M. (2015). Composable devops: Automated ontology based devops maturity analysis. In *2015 IEEE International Conference on Services Computing*, pages 600–607.

Mendes, J. R. B., Cierco, A., and Santana, P. (2021). *Privacidade Ágil: implantação da LGPD de forma ágil*. Brasport.

Meriah, I. and Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, 160:85–92.

Oliveira, A. P. d., Zanetti, D., Lima, F. S., and Sampaio, T. O. (2019). A lei geral de proteção de dados brasileira na prática empresarial. *Revista Jurídica da Escola Superior de Advocacia da OAB-PR*. Acessado em: 15 de Janeiro de 2022.

Orlikowski, W. J. and Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems (TOIS)*, 12(2):174–207.

Perkins, K. (2013). Chapter 88 - data loss protection. In Vacca, J. R., editor, *Computer and Information Security Handbook (Third Edition)*, pages 1155–1172. Morgan Kaufmann, Boston, third edition edition.

Pitta, P. E. B., Costa, E., de Siqueira, J. P. L., and Lazarin, N. M. (2020). Lgpd compliance: A security persistence data layer. In *Anais da XVIII Escola Regional de Redes de Computadores*, pages 123–127, Porto Alegre, RS, Brasil. SBC.

Presthus, W. and Sørum, H. (2018). Are consumers concerned about privacy? an online survey emphasizing the general data protection regulation. *Procedia Computer Science*, 138:603–611.

Purdy, G. (2010). Iso 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, 30(6):881–886.

Rapôso, C. F. L., de Lima, H. M., de Oliveira Junior, W. F., Silva, P. A. F., and de Souza Barros, E. E. (2019). Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. *RACE-Revista de Administração do Cesmac*, 4:58–67.

Riungu-Kalliosaari, L., Mäkinen, S., Lwakatare, L. E., Tiihonen, J., and Männistö, T. (2016). Devops adoption benefits and challenges in practice: A case study. In *Intl. Conference on product-focused software process improvement*, pages 590–597. Springer.

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. volume 25 of *Advances in Experimental Social Psychology*, pages 1–65. Academic Press.

Sharma, D. H., Dhote, C. A., and Potey, M. M. (2016). Managed data loss prevention security service in cloud. In *3rd Intl. Conf. Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS 2016)*, pages 1–4.

Teixeira, G. A., Silva, M. M., and Pereira, R. (2019a). The critical success factors of gdpr implementation: a systematic literature review. *Emerald Publishing Limited*, 21 No. 4:402–418. Digital Policy, Regulation and Governance.

Teixeira, P. G., Lopes, V. H. L., Pereira dos Santos, R., Kassab, M., and Graciano Neto, V. V. (2019b). The status quo of systems-of-information systems. In *2019 IEEE/ACM SESoS/WDES*.

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153.

Venkatraman, N., Henderson, J. C., and Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal*, 11(2):139–149.