



General Data Protection Law: Observations and Analysis of the Compliance Level of Organizations

Matheus Lustosa de Souza Louzeiro*, Renato José da Silva Camões**, Vanessa Coelho Ribeiro***, Edna Dias Canedo****, Fábio Lúcio Lopes Mendonça*****, Rafael T. de Sousa Jr*****

* University Center Uniprojeção, Brasília, Brazil, matheuslustosa96@gmail.com

** University Center Uniprojeção, Brasília, Brazil, rjscamoes@gmail.com

*** University Center Uniprojeção, Brasília, Brazil, vanessa.ribeiro@redes.unb.br

**** Department of Computer Science, University of Brasília (UnB), Brasília-DF, Brazil, ednacanedo@unb.br, ***** National Science and Technology Institute on Cyber Security, Electrical Engineering Department (ENE), University of Brasília (UnB), Brasília-DF, Brazil, fabio.mendonca@redes.unb.br

***** National Science and Technology Institute on Cyber Security, Electrical Engineering Department (ENE), University of Brasília (UnB), Brasília-DF, Brazil, desousa@unb.br

Abstract: This article addresses the scenario of the impact of the Brazilian General Data Protection Law (LGPD) on organizations. For the research used a publication of the Federal Data Processing Service (SERPRO) in 2018, and the authors sent a survey with 14 questions related to the requirements established by the LGPD for companies. It was possible to interview, in 20 days, a total of 52 people who work both in the public service and in the private sector in organizations of different sizes. The study showed that the vast majority of companies have not yet fully adapted, even with the long period that lasted between the approval of the law and its entry into force, and that they need changes to meet the requirements proposed by the LGPD, whether in the area of security data, in the management of privacy, or in the processing of data of their holders, who may be natural or legal persons who in some way are also related to an individual.

Keywords: Brazilian General Data Protection Law, Compliance, Federal Data Processing Service

1. Introduction

The issue related to the protection of personal data began to be addressed in Brazil about 8 years ago, which established rules for the treatment of personal data of Brazilians, which public agencies and companies would have to follow. This bill, together with two others, were fundamental for the preparation of law, which was approved by the National Congress, was sanctioned by the Presidency of the Republic in 2018. With that, it is observed that, during the last decade, several

political and economic factors contributed to the emergence of a General Data Protection Law, among which we can mention the Brazilian Civil Rights Framework for the Internet, the Espionage CPI and the General Regulation European Union Data Protection Act (GDPR) which came into force in May 2018. Law No. 13,709 better known as LGPD was enacted in Brazil in August 2020.

Therefore, it is in this sense that the problems to be studied are found. This work addresses the aspects of the LGPD that impact organizations through a case study. For this purpose, a survey was carried out on how these organizations are prepared for this new scenario, through a questionnaire released by SERPRO and applied by researchers in companies, making it possible to carry out a subjective analysis of the organizations' adherence to the LGPD.

2. Research Results and Analysis

According to the chosen methodology, this section intends to analyze the collected data and present the results of the applied research through the questionnaire made available by SERPRO about the LGPD. The Questionnaire composed of 14 questions was created on the Google Forms platform, being available to be answered for a period of 20 days. In this period the link generated by the platform was shared through tools and applications such as e-mails, WhatsApp, LinkedIn and other social networks, which made it possible to select people who work in both the public and private sectors. Thus, it was possible to collect a total of 52 responses from the public and private sectors.

Of the 14 questions applied in the questionnaire, the analysis of the results of the six most relevant questions were selected for this poster, representing questions 3, 4, 11, 13 and 14. 34.6% of respondents work in the public sector, which represents a total of 18 responses. Regarding the private sector, the percentage is equal to 65.4%, which represents a total of 34 responses. Although the percentage of organizations interviewed in the public sector are smaller, the public sector has a larger number of employees, according to the observation in the results collected in question 2 of the questionnaire.

Figure 11: Answers question 3 and 4 of the applied questionnaire

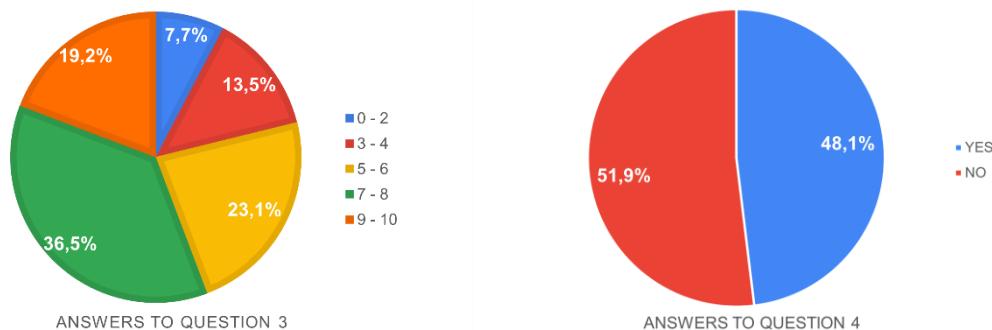


Figure 1, it can be seen from the responses collected that 59.6% of the interviewees assigned scores from 5 to 8, where most of them refer to companies in the private sector and in large part are companies that have a range of employees from 1000 to 5000 employees. It is noticed that these have

a reasonable score in relation to the LGPD implementation initiatives. Already 21.2% of the companies received relatively low marks, composing the ranges of 0 to 2, and 3 to 4. In these two ranges of grades ranging from 0 to 4 points, only 3 organizations are in the public sector, these being composed of between 500 and 5000 employees. In the private sector, 8 organizations also received grades from 0 to 4 points, these having between 50 and 5000 employees.

Question 4 sought to show the percentage of respondents who are involved in this process of adapting to the General Data Protection Law. According to the results obtained, it was possible to observe that 48.1% of the interviewees are involved or participate in some way in the implementation of technologies and innovations caused by the LGPD. Analyzing in parallel with the responses collected and presented in question 2, it was observed that 7 interviewees or 38.8% of the interviewees who work in the public sector are involved with the implementation of technologies due to LGPD, in the private sector the percentage is 52.9% of those involved.

Table 1: Notes from companies regarding LGPD implementation initiatives

Notes	Public	Private
	Quantity / %	Quantity / %
0 a 2	1 / 1.9%	3 / 5.8%
3 a 4	2 / 3.9%	5 / 9.6%
5 a 6	4 / 7.7%	8 / 15.4%
7 a 8	5 / 9.6%	14 / 26.9%
9 a 10	6 / 5.5%	4 / 3.7%

Table 1 shows the results obtained in relation to the marks given by the interviewees on the initiatives to implement the LGPD in the organizations in which they operate. In the same table, it can be said that the organizations that received scores from 0 to 4 have not yet been clearly revealed to the interviewees, that the organization is presenting initiatives to implement the LGPD. It can be deduced that the organizations that received scores from 5 to 8, in the view of the interviewees, have already started to give signs that they are looking to implement an LGPD compliance plan. The companies that received scores from 9 to 10 clearly express to the interviewees that the actions and measures to implement a data privacy program are already underway, seeking to meet the requirements demanded by the LGPD.

The question 11 sought to verify whether organizations have documentation and practices related to the management of information privacy, according to the data collected, it was possible to verify that 32.69% of the companies interviewed so far have not dealt with this issue with great concern, since the other 67.31% who answered the questionnaire, declared that they already have documentation and practices related to the management of information privacy, but that they need to update the documentation and practices to adapt them to the new law. As for 32% of respondents, they are late to start implementing the law in terms of knowing the data of the organization and its public.

According question 13, it is noticeable that 38.46% of the interviewed companies apply, in a certain way, actions regarding the privacy of users' data, and 61.5% still need to start training and guidance in addition to investing in the information structure. data security, which directly and indirectly impacts the performance of the professionals who process the company's data. In question 14 for the applied research, 69.23% of the interviewees declared that their companies have prevention and / or minimization management of security flaws that cause data leakage.

Most public sector organizations were at low risk, only 7.69% were at high risk, that is, they have good compliance with the LGPD, requiring only adjustments to meet the requirements of the General Data Protection Law. Therefore, 28.57% of the interviewed companies in the private sector showed low compliance with the LGPD, and it is necessary for these organizations to rethink their processes, technologies and cultures in order to adapt to the scenario that the General Data Protection Law proposes.

3. Conclusion

It was found in this research that most of the organizations interviewed, in a way know how to distinguish what is personal data and that some of them are subject to specific care such as sensitive data, and that these must be treated with the consent of the holder with the due legal justification.

In view of the aspects mentioned, it is concluded that through this research it was possible to observe that most of the organizations interviewed are already taking actions, measures and reviewing their processes to reach the level of adequacy sufficient to comply with the LGPD, however, there are still a large number of companies that fall short of compliance with the LGPD, which may be more likely to leak data and incorrect treatment of user information, which can have bad consequences for organizations and holders of data. data, since there was a long period from the approval of the LGPD in 2018 until the beginning of its 2020 term, enough time to implement a data privacy plan.

References

- Bernardes, M. B., de Andrade, F. P., and Novais, P.(2020). Data protection in public sector: Normative analysis of portuguese and brazilian legalorders. InWorld Conference on Information Systemsand Technologies, pages 807–817. Springer.
- Carauta Ribeiro, R. and Dias Canedo, E. (2020). Us-ing mcda for selecting criteria of lgpd compliantpersonal data security. InThe 21st Annual Interna-tional Conference on Digital Government Research,dg.o '20, page 175–184, New York, NY, USA.Association for Computing Machinery.
- G., G.: Informações valiosas: o que podemos levar para outras empresas? administradores. OM2018(2020), <https://administradores.com.br/noticias/informacoes-valiosas-o-que-podemos-levar-para-outras-empresas>.Heeks, R. (2006). Implementing and Managing eGovernment. London: Sage Publications.
- Ramiro, A.. Proteção de dados pessoais no Brasil e no Chile: uma análise comparativa sob a perspectiva da decisão de adequação da Comissão Europeia, 2020.
- SERPRO: Preparada para a lgpd? <https://www.serpro.gov.br/lgpd/empresa/esta-preparada-para-lgpd21>.

SERPRO: Dados públicos, segundo a lgpd (2018), <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-publicos-lgpd22>.

About the Authors

Matheus Lustosa de Souza Louzeiro

Graduated in Information Systems from UniProjeção University Center, Brazil, in 2020. He is currently an Educational Management Technician - Technical Support. His current research interests include cloud computing, LGPD and information security.

Renato José da Silva Camões

He holds a master's degree in ICT Management from the Catholic University of Brasília in 2010. Graduated in Computer Science from Faculdade Integrada do Planalto Central, Brazil, in 2001. He is currently a Professor at the School of Technology at UniProjeção University Center. His current research interests include computer history, cloud computing, hyperconvergence, information security and artificial intelligence.

Vanessa Coelho Ribeiro

Graduated in Computer Science from the Catholic University of Brasília(2000), master's in Information Science from the University of Brasília (2007), coordinator of IT courses at the UniProjeção University Center, Professor of Information Technology and researcher in a cooperation project between the Latitude Laboratory - UnB and Administrative Council for Economic Defense - CADE.

Edna Dias Canedo

Received the master's degree in software systems from the Federal University of Campina Grande (UFCG), in 2002, and the Ph.D. degree in electrical engineering from the University of Brasília (UnB), Brazil, in 2012. She is currently an Assistant Professor (tenure track) with the Computer Science Department, UnB. Her current research interests include software engineering, cloud computing, informatics in education, and software systems.

Fábio Lúcio Lopes Mendonça

Doctorate in Electrical Engineering and Telecommunications from the University of Brasília (2019), Master's in Electrical Engineering and Telecommunications from the University of Brasília (2008), postgraduate in Project Management from the Estácio Brasília University Center (2018), graduated in Data Processing from the Catholic University of Brasília (2004). He is an Adjunct Professor at the Department of Electrical Engineering, Faculty of Technology, University of Brasília - UnB, University Professor at Centro Universitário Projeção and Project Manager at the Decision Making Technology Laboratory - LATITUDE.

Rafael Timóteo de Sousa Jr.

Graduated in electrical engineering from the Federal University of Paraíba (UFPB), Campina Grande, Brazil, in 1984, and received the Ph.D. degree in telecommunications from the University of Rennes, France, in 1988. He is currently a Network Engineering Professor with the Electrical Engineering Department, University of Brasília (UnB), Brazil. He is the Coordinator of the Professional Postgraduate Program on Electrical Engineering (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE), UnB. He has developed research in information and network security, intrusion, and fraud detection.