Revista Catarinense da CIÊNCIA CONTÁBIL

ISSN 2237-7662, Florianópolis, SC, v. 20, 1-17, e3220, 2021

DOI: 10.16930/2237-7662202132202
Available at http://revista.crcsc.org.br

GENERAL DATA PROTECTION LAW: AN ANALYSIS OF THE DETERMINANTS AMONG ACCOUNTING PROFESSIONALS

CRISTIANE KRÜGER
Federal University of Santa Maria. ***Address:*** *Rua José Manhago, 154, apto 402 | Camobi | 97105-430 | Santa Maria/RS | Brazil.*
https://orcid.org/0000-0002-7774-2227
cristiane.kruger@ufsm.br

ADRIANA CRISTINA CASTANHO BALDASSARI
Federal University of Santa Maria. ***Address:*** *Rua Tuiuti, 250, apto 303 | Centro | 97050-420 | Santa Maria/RS | Brazil.*
https://orcid.org/0000-0002-5149-355X
adriccb@terra.com.br

LUIS FELIPE DIAS LOPES
Federal University of Santa Maria. ***Address:*** *Rua Dona Luiza, 216 | Rosário | 97010-160 | Santa Maria/RS | Brazil.*
https://orcid.org/0000-0002-2438-0226
lflopes67@gmail.com

LIZANA ILHA DA SILVA
Federal University of Santa Catarina. ***Address:*** *Avenida Liberdade, 214 Passo D'Areia | 97010-270 | Santa Maria/RS | Brazil.*
https://orcid.org/0000-0002-0448-9769
lizanailha@hotmail.com

ABSTRACT

Technological advances make it possible to quickly access and share personal data and information, which demands greater security and requires conscious attitudes from the different professionals who deal with these issues. Accounting professionals stand out in this universe for being responsible for customer, supplier, and employee data. The information insecurity scenario led to the creation of the General Data Protection Law (GDPL), a specific legislation for personal data handling. Driven by this context, this research aimed to analyze the GDPL compliance determinants among accounting professionals. In order to achieve this purpose, we conducted a quantitative, descriptive, survey study. For data collection, we developed and applied an *online* questionnaire addressed to accounting professionals. The final surveyed sample totaled 194 respondents. We performed the data analysis through Structural Equation Modeling. The validated model showed the dimensions of personal behaviors and attitudes and governance mechanisms as determinants, explaining 26.3% of GDPL compliance. This research contributes to the understanding of behavioral aspects of accounting professionals in face of the new legislation. It is an unprecedented approach and fills a gap in the accounting area, presenting useful contributions for educational institutions, class associations, and companies in the area.

Keywords: Accounting. Information security. Compliance. Structural Equation Modeling.

Edited in Portuguese and English. Original version in Portuguese.

Paper presented at the VI Management and Controllership Congress of Unochapecó (COGECONT), October 8th to 20th, 2021.

Received on 10/31/2021. **Reviewed on** 11/16/2021. **Accepted on** 11/23/2021 by Prof. Dr. Sérgio Murilo Petri (Editor-in-Chief) and Prof. Dr. Sandro Vieira Soares (Associate Editor). **Published on** 12/10/2021.

1 INTRODUCTION

Technological advancement has brought relevant issues regarding information security to light, and this is no different in accounting (Ribeiro, Krüger, Michelin & Raddatz, 2020). The access and use of personal data comprise one of the main business assets in contemporary society and, at the same time, mean privacy risks in the face of information technology (Miragem, 2019). These risks require conscious and proactive attitudes by managers and accountants regarding the security of corporate information, from their clients, employees, and suppliers (Moraes, 2019).

We realize that there is a dependence on technologies and interaction between the physical and digital aspects of individuals, so that people's identity considers not only the physical body but also the characteristics of their digital environment, which comprises the personal data set (natural or legal person) (Basan & Faleiros Jr, 2020). In this context, according to Celidonio, Neves, and Doná (2020), and Rosa (2021), data are vulnerable, since there were no regulations for their handling before, only general provisions present in the Civil and Consumer Defense Codes and in the Civil Rights Framework for the Internet, which generated a complex legal network.

This vulnerability concerning personal data, from the access and handling of data in general, such as accounting data, reflects on the economy and also affects social and political relations, given its interactions with issues such as the quality of public debate, freedom of demonstration, the protection privacy, among other fundamental issues for human development (Miragem, 2019). The (hyper)vulnerability of the individual in cyberspace and the protection of personal information in business relationships have come into focus (Siqueira, Contin, Barufi & Lehfeld, 2021). In order to reduce privacy risks and maintain the accomplishment of corporate goals, business leaders have envisioned less privacy-invasive methods with less risk to individuals (Willemsen, 2019). Thus, technological advances have enabled the rapid and continuous exchange of data between users, which has fostered the sharing of information and generated the need for specific legislation that could guide professionals, such as accountants (Schirmer & Thaines, 2021).

It is in this context that the General Data Protection Law (GDPL) was created, in order to establish rules and procedures for the use, storage, handling, and sharing of personal data, as well as sanctions to those who do not comply with the standards to ensure security, privacy, and transparency in the handling of users' personal information (Frazão, Oliva & Abilio, 2019). It is a new paradigm, as it changes the way organizations handle personal data in offline and online media, and it has the provision to protect the fundamental rights of freedom and privacy in any relationship involving such data (Falcon & Keller, 2021). Its purpose is to regulate the life cycle of users' personal data, as well as all handling related to it, which must be documented from initial collection to termination (Celidonio et al., 2020).

The GDPL provides that accounting professionals must follow principles listed in the law, such as purpose, adequacy, open access, data quality, transparency, prevention, non-discrimination, and accountability (Law No. 13,709, 2018). Moreover, they must be aware of the best practices required by the law to avoid leakage, dissemination, breaches, exposure, and unauthorized access of users' personal data (Law No. 13,709, 2018; Celidonio et al., 2020). In this regard, the law is clear as to the consequences of non-compliance and establishes sanctions that range from warnings or fines to partial or total prohibition of exercising activities related to data handling. The law also mandates the adoption of internal control mechanisms aimed at secure data handling, corrective measures, and governance policies (Mendes, 2019).

The law's implementation is complex, given the need for changes in mentality regarding best practices in data management, investments in information security, and training of professionals (Marques, 2020). It is possible to say that the aforementioned law also comes to guide the role of the accounting professional, as it presents as its main purpose to increase the protection of individuals' privacy (Law No. 13,709, 2018; Ribeiro et al., 2020). Given the above,

the question is: what are the determinants for the GDPL compliance among accounting professionals? In order to shed light on this issue, this study aims to analyze the GDPL compliance determinants among accounting professionals.

In order to achieve the established objective, based on the theoretical basis analyzed, we developed a closed questionnaire consisting of 36 observed variables distributed into four constructs, namely: Workplace Behaviors and Attitudes, Education, and Organizational Governance Mechanisms as possible determinants of GDPL Compliance. We adopted a five-point Likert-type scale, and collected the data online. The survey included Brazilian accounting professionals and the stipulated minimum sample size was reached. After collecting the data, we analyzed it through Structural Equation Modeling, using SmartPLS®, following the criteria for evaluation of measurement and structural models of Lopes et al. (2020) and Ringle, Silva, and Bido (2014).

Different authors have pointed out the importance of studying the GDPL in accounting (Ribeiro & Moreira, 2021; Scherer Filho, 2020; Schirmer & Thaines, 2021). Thus, this study has its justification for contemplating recent legislation that impacts several activities, including accounting. Furthermore, the research is relevant because it seeks to provide greater understanding on the use of information security technologies, aiming to contribute to the promotion of a safe environment for the accounting professional's work, since information can be considered one of the main assets of a company (Pimenta & Quaresma, 2016).

Brazil is one of the leading countries in the world ranking of cyber attacks and this exposure generates concern for users and owners of accounting information (Ribeiro et al., 2020), which motivated this research among accounting professionals. Additionally, this professional is deficient in technology and information security skills, and makes little or no investment in this area, which makes him/her more vulnerable (Herath, 2011; Migliorini & Rocha, 2019; Ribeiro et al., 2020; Santos & Tabosa, 2020). It also justifies the execution of this research.

Also, it should be noted that the Accountant's Code of Professional Ethics, which aims to set the accountant's conduct in the exercise of his or her activities and in matters related to the class, classifies confidentiality as one of this professional's most important duties (NBC PG 01, 2019). As technologies advance, keeping data and information confidential has become a problem (Zanatta, 2015). According to the author, accounting professionals are responsible for the safekeeping of data and information used and generated in their services, and keeping them safe is becoming increasingly harder, in view of the growing commercialization of such data without authorization. Therefore, this paper aims to analyze GDPL compliance determinants among accounting professionals.

The research's main results include the construction and validation of an instrument to measure the determinants of compliance with the GDPL. Among the surveyed influencers, personal behaviors and attitudes in the workplace of accounting professionals and governance mechanisms were supported. It is noteworthy that the education construct, which corresponds to training and capacity building focused on the GDPL requirements, was not supported.

This work presents different contributory potentials. As for scientific contributions, we can mention the lack of research regarding information security in the accounting sector and the relationship between the accounting professional and the GDPL, given the recent nature of this legislation. Thus, the research may contribute as information regarding the GDPL, for the accounting area to understand, explore, and debate the subject, especially considering personal data security, and thereby promote advances in this theme's literature (Scherer Filho, 2020).

As far as practical contributions are concerned, it is significant that the accounting professional appropriates technologies as tools to carry out their functions, and that, moreover, they can ensure security and credibility in the information obtained and provided (Schirmer & Thaines, 2021). Information security management, like accounting, is an innovative topic of

interest to companies and the professionals who work in them (Marques, 2020). Therefore, the survey on this category's situation in light of the GDPL becomes an important contribution to the profession.

2 GENERAL DATA PROTECTION LAW

The motivation for the creation of regulatory frameworks for the protection of personal data comes from the fact that the digital economy has become more dependent on database flows, especially personal ones (Pinheiro, 2020). Personal data has come to be seen as the new oil, as it is considered an essential resource that develops the information economy, just as oil underpinned the industrial economy (Teves, 2019). The GDPL, Law No. 13,709 (2018), which must be observed by the Union, states, and municipalities and has been in effect since September 18, 2020 (Burkart, 2021), emerges in this scenario.

The law provides for the handling of personal data and aims to protect the citizen's fundamental rights, such as freedom and privacy, in addition to the free development of the natural person's personality (Law No. 13,709, 2018). The GDPL is based on respect for privacy, freedom of speech, information, communication, and opinion, inviolability of privacy, honor, and image, human rights, free development of personality, dignity, and the exercise of citizenship.

Data handling covers all personal data collected, stored, and processed by public and private organizations, and it has an international range, so data can be handled outside of Brazil, as long as the collection occurred in Brazilian territory (Carvalho, Oliveira, Cappelli & Majer, 2019). The GDPL was influenced by the European Union's General Data Protection Regulation (GDPR), which like the GDPR, the Brazilian law seeks means of control to balance relations and standardizes attributes for the protection of personal data, as well as generates not only economic, but also social and political effects (Pinheiro, 2020). For the author, the GDPL has the potential to become the law with the greatest impact on the Brazilian business community, affecting the most varied types of businesses and society as a whole. This law is an attempt to guarantee privacy to individuals and comes to facilitate the rights acquired by the holders (Burkart, 2021).

From the theoretical aspects reviewed, we present the research hypotheses that aim to analyze the GDPL compliance determinants among accounting professionals. The first hypothesis to be tested in the model sought to analyze whether behaviors and attitudes toward the security of personal data and information in the workplace refer to GDPL compliance. Therefore, attitudes determine the how, what, and why of behavior, while the latter concerns the actions externalized in their relationships in the social sphere, including the work context (Kanaane, 2017).

Thus, in addition to technical elements, in order to ensure the effectiveness of information and data security in companies, social aspects dictated by people, by their attitudes and their postures, are also necessary (Silva, 2011). As such, we expect that the attitudes taken and the behavior of professionals to ensure information security, from a number of actions, will influence GDPL compliance. That said, we present the first hypothesis, **H_1 Workplace Behaviors and Attitudes are significant and positive determinants of GDPL Compliance.**

The second hypothesis concerns the education of accounting professionals as a direct influencer for GDPL compliance. Ongoing training, courses, and conferences facilitate employee awareness on information security (Fontes, 2008). Therefore, companies must incorporate into their management educational activities for their employees regarding the new processes and policies aimed at protecting personal data (Lóssio & Santos, 2021). Pinheiro (2020) says that one level of investment for GDPL compliance is cultural, which includes training and awareness campaigns aimed at employees. Thus, education, consisting of courses, events, and internal capacity building through training, is expected to influence compliance with GDPL. In this regard, we propose hypothesis **H_2 Education significantly and positively determines GDPL Compliance.**

Finally, the third hypothesis investigates whether governance mechanisms for the protection of personal data and information are able to influence compliance with the law. Nascimento, Frogeri, and Prado (2019) state that to achieve information and data security, it is necessary to figure out the controls needed to decrease risks. Therefore, companies need to align best practice measures regarding information security (Buogo, Fachinelli & Giacomello, 2019). Hence, we expect that best practice and governance policies, conducted in the firms in which accounting professionals work, will make a difference for GDPL compliance. Thereafter, we arrive at hypothesis **H_3 Organizational Governance Mechanisms are significant and positive determinants of GDPL Compliance**. In light of this, the following is the research methodology.

3 METHODOLOGICAL PROCEDURES

The survey population was made up of accounting professionals working nationwide in Brazil. Therefore, the collection included accountants, accounting technicians, analysts, interns, *trainees*, auditors, experts, among others, as long as they had professional activities related to accounting services. Due to the survey's delimitation, we were unable to estimate the population in a conclusive way.

In order to calculate the minimum sample size, we used the criteria established by Hair Jr., Hult, Ringle, and Sarstedt (2017), which comprises the 5:1 ratio as the minimum ratio of observations per surveyed variables. Since the study includes 36 variables, we reached a minimum sample size of 180 responses. After data collection, we obtained a total of 198 responses, 194 of which considered valid, making up this study's examined sample, which exceeds the minimum desired sample size.

For data collection, the research relied on a questionnaire developed according to the theoretical framework discussed throughout the literature review, especially Law No. 13,709 (2018). The questionnaire was developed in the *Google Forms* platform, consisting of 36 questions separated into four blocks, as shown in Table 1.

Table 1
Research Assertives and Constructs

BLOCK I - Personal behaviors and attitudes for the security of personal data and information at the workplace (COMP)
01. I take effective measures to protect customer and employee personal data.
02. I explain what each of the personal data I request from customers and employees will be used for.
03. I request customer and employee authorization for the collection of personal data/information.
04. I use security mechanisms (antivirus, *antispyware*, etc.) to reduce and prevent possible incidents with third parties' personal data.
05. I do not exclude customer and employee personal data at the time of data handling because of characteristics such as racial or ethnic origin, religious conviction, political opinion, etc.
06. I request data and information strictly necessary to fulfill the intended purpose.
07. I update customer and employee information.
08. I inform the customer on what I do with his or her personal information, how the handling is done, and for how long.
09. The data I request for customers and employees is compatible with the purposes informed to the holder.
10. I inform my customers and co-workers with clear and simple language regarding the use, storage, and sharing of their personal data.
SECTION II - Education (EDU)
01. In the company I work for I provide training(s) and capacity building(s) on data protection and personal information, for example on the GDPL.
02. I invest, particularly, in courses and training on information systems, cybersecurity, data protection, and personal information.
03. I attend lectures and events related to the GDPL.

04. I find the GDPL application easy to understand for the accounting professional.
05. It is necessary for accounting professionals to have knowledge in the use of technologies in order to avoid risks in the storage, handling, and distribution of personal data.
06. Being up to date on the issues of information security and personal data protection is relevant for the accounting professional.
07. I feel sufficiently trained on the requirements and sanctions of the GDPL in my professional activity.
BLOCK III - Governance mechanisms for the protection of personal data and information at the company I work for (MGOV)
01. Regarding the handling of personal data/information, the company has established internal supervision and risk mitigation mechanisms.
02. There are security rules and standards for those involved in handling personal data in the company.
03. The company develops educational actions aimed at information security and personal data protection.
04. The company invests resources in protecting personal data/information.
05. A relationship of trust and transparency is always established with the holder of the personal data.
06. The organization applies appropriate policies and safeguards based on the privacy impact and risk assessment.
07. The care for personal privacy in the company is constantly updated.
08. There are internal processes and policies that ensure compliance with standards and best practices regarding the protection of personal data/information.
09. On personal data protection the company has incident response and remediation plans.
10. In the company there is a data controller/responsible for the handling of personal data.
11. The company's management is committed to information security and protection of personal data, whether of customers or employees.
BLOCK IV - GDPL Compliance
01. The GDPL establishes rules and procedures for the use, storage, and sharing of personal data.
02. Based on the GDPL the handling of each personal information/data must be done for specific purposes.
03. GDPL aims at the security and transparency of users' personal information.
04. Non-compliance with the GDPL does NOT provide for sanctions or penalties for violators.
05. The GDPL protects the citizen's fundamental rights, such as: freedom and privacy.
06. The handling of personal data in accounting may only be carried out upon provision of consent by the data holder.
07. The GDPL applies to all companies that collect, store, and process data, whether in physical or digital form, including those engaged in Accounting.
08. GDPL implementation can occur in the accounting area through data privacy programs with security policies, rules, code of conduct, and ongoing training.

Source: Authors

In order to measure and understand the investigated constructs (Table 1), we chose a 5-point Likert scale, relative to the frequency of occurrence for the assertions presented in blocks I and II, ranging from 1 (never) to 5 (always), and of agreement for blocks III and IV, ranging from 1 (strongly disagree) to 5 (strongly agree). After the assertions exposition in the four constructs formed, the questionnaire concludes with 7 questions related to the respondent's profile, as follows: gender, age, education, current or former course, position held in the organization, time as an accounting professional, and whether the individual had responsibilities regarding information security and protection of personal data in the professional activity performed.

In order to obtain the necessary data to develop the study, the survey instrument was widely publicized on social media (*Facebook, Whatsapp, LinkedIn*, and *Twitter*), and in discussion groups focused on accounting. In addition, we *e-mailed* the questionnaire to 26 Regional Accounting Councils (CRCs), with the CRC/RS publicizing the instrument on its *website* and the CRC/SC forwarding it to its registered members. Also, we sent *e-mails* to the largest accounting firms in the municipality of Santa Maria, after visiting them in person and sending the e-mails directly to known professionals. The survey instrument was available for responses between May 10 and June 11, 2021.

In the stipulated period, 198 questionnaires were answered. We reviewed all the questionnaires received for inconsistencies, such as duplicate *e-mails*, identical hours in the

responses, and identical answers for all questions. After checking, we excluded four participants from the sample, three of them because they had filled out all the questions with identical answers, and one because he or she answered half the questions and did not sign the Informed Consent Form. Thus, we obtained 194 valid responses, which we considered for the research analysis.

We tabulated the data obtained from the questionnaire responses in Microsoft Excel® software, creating a database, which was later imported into SmartPLS® version 3.3.3 software. After coding the indicators (Observed Variables - OVs) and their Constructs (Latent Variables - LVs) we carried out the analyses based on the constituted objective. First, we presented the surveyed professionals' profiles. Then, in order to ascertain the determinants for GDPL compliance in the accounting profession, and validate the theoretical model developed, we chose Structural Equation Modeling (SEM) (Hair Jr., Risher, Sarstedt, & Ringle, 2019). The SEM enables the use of multivariate techniques in a single method of analysis, allowing the evaluation of complex relationships, such as the relationship between independent variables, the magnitude of their influence on the dependent variable, and the relationship between variables outside the model and the independent variables (Hair Jr. et al., 2009).

The path diagram consists of two elements: the structural (or internal) model that shows the relationships (paths) between the constructs (endogenous or exogenous latent variables, represented by circles) and the measurement (or external) model that reports the relationships between the constructs and the indicator (or observed) variables, represented by rectangles (Hair Jr., Gabriel & Patel, 2014).

In this sense, in order to investigate the hypotheses built from the theory and the relationships among the constructs and the constructs with their variables, based on Lopes et al. (2020) and Ringle et al. (2014), we have taken the following steps: definition of the initial theoretical model with presentation of the constructs (exogenous and endogenous) and the indicator variables of each construct. Then, we adjusted the initial model. Afterwards, we determined the measurement model (confirmatory) with subsequent evaluation. Finally, we concluded the analysis with the definition of the final structural (path) model and its predictive evaluation. Table 2 shows the criteria used for the measurement model and structural model evaluation.

Table 2
Criteria for systematic evaluation of model results

Measurement Model Evaluation		
Test	**Criteria**	**Concept**
Internal Consistency		
Cronbach's alpha (α)	**0.7 < α < 0.95**	It is the estimation of reliability based on the intercorrelations of the observed variables (Hair Jr. et al., 2014).
Composite Reliability (ρ_c)	**0.7 < ρ_c < 0.95**	It is the verification of whether the LVs are "unbiased" (Hair Jr. et al., 2014).
Convergent Validity		
Average Variance Extracted - AVE	**AVE > 0.5**	It is the portion which the data is explained by LVs (Ringle et al., 2014).
Discriminant Validity		
Cross-Factor Loadings (CFL)	Original CFL > Other CFLs	It is the correlation of OVs with LVs (Ringle et al., 2014).
Fornell-Larcker Criterion	$\sqrt{AVE} > r_{i_J}$ for i≠j	It is the comparison of the square roots of the AVEs with Pearson's correlations (Fornell & Larcker, 1981).
Heterotrait-Monotrait Ratio Criterion (HTMT).	**HTMT < 0.9** $LS(HTMT)_{97.5\%} < 1.0$	It is a more efficient criterion than Fornell Larcker, it comes to be an estimate of the correlation between the LVs (Netemeyer, Bearder & Sharma, 2003).

Confirmed by the *Boostrapping* method		
Evaluation of the Structural Model		
Collinearity Assessment - *Variance Inflation Factor* (VIF)	**VIF < 5**	The existence of strong correlations between the LVs indicates collinearity problems (Hair Jr. et al., 2017).
Effect size (f^2); Confirmed by the *Boostrapping* method	$0.02 \leq f^2 \leq 0.075$ (small effect); $0.075 \leq f^2 \leq 0.225$ (medium effect); and $f^2 >$ 0.225 (large effect)	It assesses the usefulness of each endogenous LVs for model fitting (Cohen, 1988; Hair Jr. et al., 2014; Lopes et al., 2020).
Coefficient of Explanation (R^2) Confirmed by the *Boostrapping* method	$0.02 \leq R^2 \leq 0.075$ (weak effect); $0.075 < R^2 \leq 0.19$ (moderate effect); and $R^2 > 0.19$ (strong effect)	It assesses the variability portion of the predictor (endogenous) LVs (Cohen, 1988; Lopes et al., 2020).
Validity of the structural coefficient (β); Confirmed by the *Boostrapping* method	$H_1: \beta \neq 0$ $t_c \cdot > 1.96$ $(p < 0.05)$	It assesses the significance of the structural coefficient value (confirmation of the hypothesis or not) (Hair Jr. et al., 2017).
Predictive relevance (Q^2); Confirmed by the *Blindfolding method*	**$Q^2 > 0$** $0.01 \leq Q^2 \leq 0.075$ (weak degree); $0.075 < Q^2 \leq 0.25$ (moderate degree); and $Q^2 > 0.25$ (strong degree)	It assesses the final model's accuracy degree (Chin, 2010; Hair Jr. et al., 2017; Lopes et al., 2020).

Source: Prepared by Lopes et al. (2020), adapted from Ringle et al. (2014).

Table 2 presents the criteria for systematic evaluation of the measurement and structural models. Initially, we considered convergent validity based on AVE to evaluate the measurement model. Then, we observe the internal consistency by means of *Cronbach's Alpha* (α) and Composite Reliability (ρ_c). Thereafter, we analyze the discriminant validity by means of the cross-factor loadings (CFL), and the Fornell-Larcker and HTMT criteria. Next, we evaluate the structural model by assessing collinearity (VIF), effect size (f^2), coefficient of explanation (R^2), structural coefficient validity (β), and predictive relevance (Q^2).

4 RESULTS ANALYSIS AND DISCUSSION

4.1 Accounting Professionals Profile

In view of the responses obtained in the questionnaire, the seven profile questions sought to reveal the characteristics of the accounting professionals surveyed. The survey showed that of the 194 participants, the gender distribution was relatively balanced, with 52% female and 48% male. Regarding the professionals' age, 108 respondents, at the time of the survey, were concentrated in the 30 to 49 age bracket (56%), followed by 60 people (31%) who were between 19 and 29. The survey also showed that 25 individuals belong to the 50 to 59 age group, and there was one person who reported being 70 or older.

With regard to education, 45% (88 respondents) stated that they had completed their undergraduate studies, 20 professionals (10%) are in higher education, and 82 respondents have a graduate degree (42%). Among those who have attended or are attending higher education, 93% (181 respondents) have studied/are studying Accounting Sciences, and 3% have completed or are in the process of completing an accounting technician degree. When asked about the position held in the company, there is a preponderance of professional accountants (22%), followed by analysts, auxiliaries, and assistants, these making up 37% of the sample. Also, 8% of the respondents are partner-owners.

As for the time as an accounting professional, most of those surveyed said they have been in the market for more than 10 years; in this time range there are 82 people (42%). In addition,

24% of the sample has been working between 6 and 10 years, which shows the experience of the professionals surveyed in the function performed. Regarding responsibility for information, 171 individuals (88% of the sample) stated that they have responsibility for customer data.

In general, the surveyed sample is made up of women, over 30 and under 50 years old, who attended or are attending an undergraduate program in Accounting Sciences, and have attended or are attending a graduate program. The study also highlights that those surveyed are experienced in their positions, having been in the profession for more than 10 years. Furthermore, they have demonstrated that they are responsible with the data and information they handle.

4.2 Determinants for GDPL compliance in the accounting profession

In order to validate the hypotheses of the theoretical model developed, we used Structural Equation Modeling. For the definition of the initial theoretical model, we considered as exogenous constructs behaviors and attitudes, education, and organizational governance mechanisms for data security, and as an endogenous construct we considered GDPL compliance. After inserting the data into the SmartPLS® program, we conducted the first calculations and began the evaluation of the measurement model based on the criteria of convergent validity, internal consistency, and discriminant validity (Hair Jr. et al., 2014).

Convergent validity is based on AVE, which shows how positively variables correlate with their respective constructs (Ringle et al., 2014). According to the authors, the accepted values of the AVE should be greater than 0.5. After the first calculation, we found the need for adjustments in the initial model, since the constructs COMP (0.431), EDU (0.412), and GDPL (0.448) obtained AVE values below the mentioned criteria. MGOV was the only one with an adequate value, 0.612.

Therefore, to refine the model, we excluded, one by one, the variables EDU_05 (0.538) and EDU_06 (0.431) from the education construct, COMP_05 (0.220) and COMP_04 (0.493) from the personal behaviors and attitudes construct, and the variable LGPD_04 (-0.045) from the compliance with GDPL construct. These assertions presented low factor loadings and compromised the model. It should be noted that LGPD_04 was a negative assertion, used to test respondents' attention, and was reversed for the analyses. Figure 1 presents the measurement model after the reported exclusions.

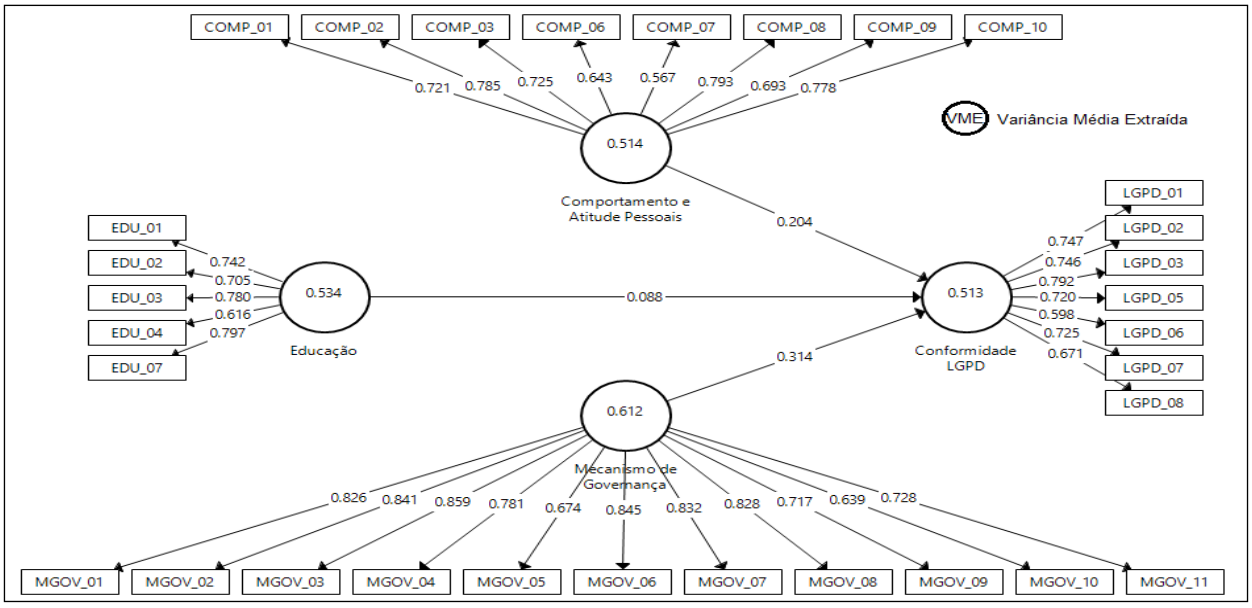

Figure 1. Measurement model
Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle, Wende & Becker, 2015).

Figure 1 shows that after the exclusions, the AVE values increased to 0.514 in COMP, 0.534 in EDU, 0.612 in MGOV, and 0.513 in GDPL. Therefore, the AVEs were within the classification proposed by Ringle et al. (2014). This shows convergent validity and reflects the portion of variance of the indicators explained by the constructs. In addition, we analyzed *Cronbach's Alpha* and Composite Reliability (ρ_c) values, which are part of the measurement of model reliability and validity (Table 3).

Table 3
Internal consistency and convergent validity of the measurement model

Constructs	Cronbach's alpha	Composite Reliability	AVE
COMP	0.863	0.893	0.514
GDPL	0.843	0.880	0.513
EDU	0.781	0.851	0.534
MGOV	0.936	0.945	0.612

Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

From the information in Table 3, it can be seen that the internal consistency values are appropriate as they have Cronbach's Alpha between 0.7 and 0.95 (Hair Jr. et al., 2014). It is also noted that the Composite Reliability values are adequate ($0.7 < \rho_c < 0.95$), evidencing that the sample is free of bias (Hair Jr. et al., 2014). For the discriminant validity evaluation, we initially consider the CFL values, as already highlighted in Figure 1. After that, we verified that there is discriminant validity, because the variables obtained higher factor loadings next to the original constructs (Ringle et al., 2019).

Then, following the assumptions for evaluating the measurement model, we present the indicators of discriminant validity based on the Fornell-Larker and HTMT criteria (Table 4).

Table 4
Discriminant validity by Fornell-Larcker and HTMT criteria

Constructs	$\sqrt{AVE}$	Fornell-Larker			
		COMP	GDPL	EDU	MGOV
COMP	0.717	1			
GDPL	0.716	0.400	1		
EDU	0.731	0.476	0.387	1	
MGOV	0.782	0.490	0.470	0.642	1
		UL(HTMT)$_{97.5\%}$			
GDPL		0.605			
EDU		0.687	0.587		
MGOV		0.674	0.606	0.842	

Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

Table 4 shows the square root values of the average extracted variance and the values of the correlations between the constructs. For discriminant validity, using the Fornell-Larker test, the square roots of the AVEs should be greater than the correlations between the constructs (Fornell & Larcker, 1981). As it turns out, this criterion has been met. Complementarily, for HTMT, confirmed by the *bootstrapping* method for 5,000 subsamples, the stipulated criterion was met (Netemeyer et al., 2003).

Therefore, after the specification and evaluation of the measurement model, we evaluate the structural model. Initially, we evaluated the collinearity (VIF) for the observed variables (OV), as shown in Table 5.

Table 5
VIF evaluation for the observed variables

OV	VIF	OV	VIF	OV	VIF	OV	VIF	OV	VIF
COMP_01	1,726	COMP_09	1,736	EDU_07	1,579	GDPL_07	2,376	MGOV_05	1,730
COMP_02	2,700	COMP_10	2,054	GDPL_01	1,796	GDPL_08	2,108	MGOV_06	3,126
COMP_03	1,751	EDU_01	1,587	GDPL_02	1,988	MGOV_01	3,429	MGOV_07	3,722
COMP_06	1,467	EDU_02	1,770	GDPL_03	2,110	MGOV_02	3,337	MGOV_08	3,277
COMP_07	1,329	EDU_03	2,138	GDPL_05	1,574	MGOV_03	3,888	MGOV_09	2,089
COMP_08	2,591	EDU_04	1,246	GDPL_06	1,360	MGOV_04	2,688	MGOV_10	1,883
								MGOV_11	2,187

Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

From Table 5 it is clear that the values obtained for the variables did not present collinearity problems (Hair Jr. et al., 2017). That said, Table 6 presents the results for collinearity (VIF), effect size (f^2), and coefficient of explanation (R^2) for the researched constructs.

Table 6
VIF evaluation and effect size (f^2) for the GDPL for the constructs

Exogenous Constructs	VIF	f^2
COMP	1.398	0.058 (0.357)
EDU	1.806	0.006 (0.682)
MGOV	1.838	0.073 (0.122)
R^2	0.263 (0.000)	

Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

According to information in Table 6, the VIF values were between 1.398 and 1.838, demonstrating that there are no collinearity problems (Hair Jr. et al., 2017). Regarding effect size (f^2), this is an evaluation item that considers how useful the predictive construct is for model adjustment (Cohen, 1988; Hair Jr. et al., 2014; Lopes et al., 2020). Thus, only the COMP and MGOV constructs had an effect on model adjustments, which was considered small, with values of 0.058 and 0.073, respectively.

Regarding the coefficient of determination R^2, this shows how much the variation in the predictor variable (GDPL compliance) is explained by the variation in the exogenous variables. GDPL compliance obtained a value of $R^2 = 0.263$, which according to Cohen (1988) and Lopes et al. (2020) indicates strong explanatory power. This means that personal behaviors and attitudes, and governance mechanisms are able to explain the variation corresponding to approximately 26.3% of GDPL compliance.

Table 7 presents the values of the structural coefficient betas (β's) and shows the significance of their value for confirming the hypotheses (p-value). The strength of the relationship between the constructs is indicated by the (t) statistic, calculated in the analysis of the statistical significance of structural relationships (Hair Jr. et al., 2014).

Table 7
Evaluation of structural coefficients

Hyp.	Structural Relationship	(β's)	S. Deviation (sd)	T-statistic ($\|\beta/sd\|$)	p-value	Situation
H_1	COMP → GDPL	0.204	0.093	2.203	0.028	Supported
H_2	EDU → GDPL	0.088	0.086	1.024	0.306	Not supported
H_3	MGOV → GDPL	0.314	0.091	3.440	0.001	Supported

Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

Based on the information in Table 7, it follows that the supported hypotheses (H_1 and H_3) demonstrate positive structural coefficients and with significance level ($p < 0.05$) and $t_{calc.} > 1.96$. However, this does not occur in the second hypothesis, which showed $p > 0.05$ and was not considered statistically significant, since $t_{calc.} < 1.96$. Thus, we can infer that the variables personal behaviors and attitudes and governance mechanisms for the security of personal data and information are positive and significant predictors for GDPL compliance among accounting professionals.

Figure 2 demonstrates the final structural model.

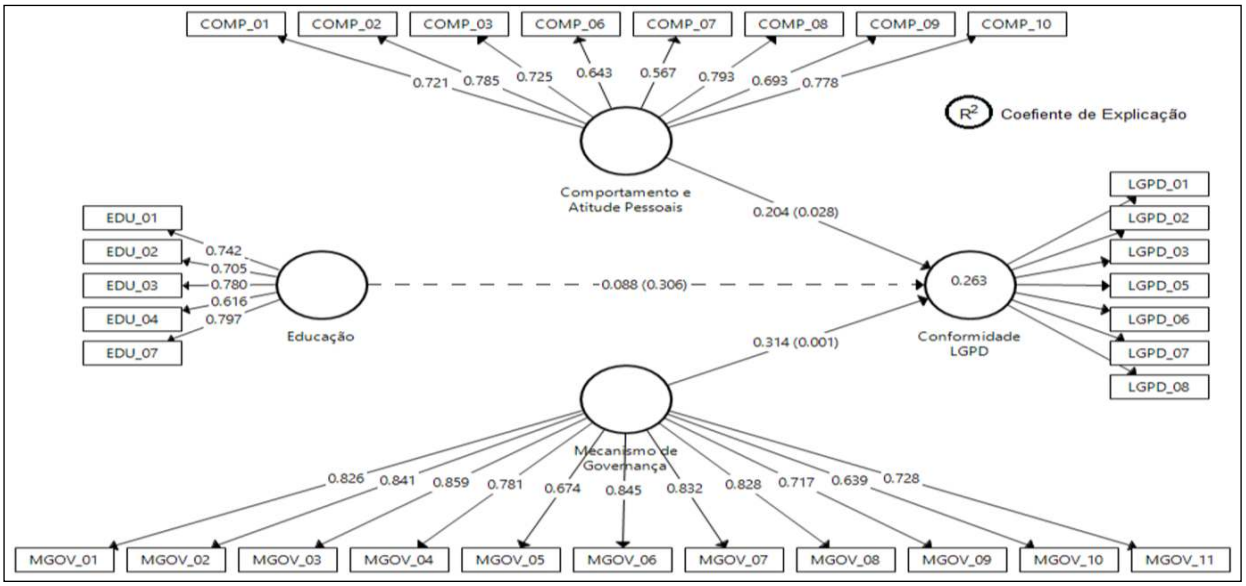

Figure 2. Final structural model
Source: Prepared by the authors in SmartPLS® software, v. 3.3.3 (Ringle et al., 2015).

The final structural path model (Figure 2 and Equation 1) shows the positive and significant relationships ($p < 0.05$ and $t_{calc.} > 1.96$) among the constructs:

$$GDPL = 0.204\ COMP + 0.314\ (MGOV) + \varepsilon_{GDPL} \quad (1)$$

Given this, the first hypothesis that personal behaviors and attitudes in the workplace are positive determinants of GDPL compliance was supported. The results pointed out that Accounting professionals are aware of the GDPL and act in favor of data security. This result is supported by Silva (2011) who points out that social factors dictated by people, such as their attitudes and behaviors, are key to ensuring a culture of security and protection of data and information in organizations.

Whereas, the second hypothesis, focusing on education as a positive determinant for GDPL compliance, was not supported. On education, these results diverge from Schirmer and Thaines (2021) who point to training and capacity building as necessary for accounting organizations to meet the GDPL requirements. In addition, according to Kohls, Dutra, and Welter (2021) and Pinheiro (2020), following the GDPL determinations requires investment to adapt to this reality, which reflects in the education of employees who deal with personal data, through training and even hiring consultants. Therefore, aspects related to education (capacity building and training) deserve attention and leave room for development by the entities.

While the third hypothesis, which considers governance mechanisms for data security and personal information as positive determinants for GDPL compliance, was supported. It is thus clear that the organizations in which these professionals work are concerned and have adopted

mechanisms to comply with the GDPL's provisions. Buogo, et al. (2019) and Kohls et al. (2021) describe that GDPL in organizations reflects the need to implement governance focused on data and information security, which corroborates to the present finding.

Thus, relationships between the constructs behaviors and attitudes and governance mechanisms for data security demonstrated significance and strength for GDPL compliance. On the other hand, the education dimension did not prove to be a determining factor for GDPL compliance in the present model, represented by a dotted arrow. External factor loadings can be observed on the variables of each construct surveyed. In addition, COMP and MGOV explain approximately 26.3% of GDPL compliance (Figure 2).

Afterwards, we verified the accuracy and predictive relevance of the structural model, by means of Q^2, confirmed by the Blindfolding method. The calculated Q^2 values represent a measure of how well the path model can predict the originally observed values (Chin, 2010; Hair Jr. et al., 2017; Lopes et al., 2020). We found $Q^2 = 0.117$, which for Chin (2010), Hair Jr. et al. (2017), and Lopes et al. (2020), corresponds to a moderate degree of model accuracy, so the model can be considered relevant.

At the end of the results systematic evaluation we can state that the structural model of pathways to reach GDPL compliance has been validated. Hence, according to the assessments of the indicators used, we can infer that the relationships between the constructs personal behaviors and attitudes and governance mechanisms for personal information security with the construct GDPL compliance are supported. Therefore, we present below the research conclusion, which recalls the research problem, the general objective, and presents contributions, limitations, and suggestions for future studies.

5 FINAL CONSIDERATIONS

The technological evolution of the last decades has made available the fast and continuous access and sharing of data and information, which are considered valuable resources for organizations. The flow in the exchange of information and personal data has demanded greater security in their handling, and has come to require conscientious attitudes from the professionals who deal with these issues on a daily basis. This is the case for the accounting professional, who is responsible for customer, supplier, and employee data. Given this scenario, this research asked: what are the determinants for GDPL compliance among accounting professionals?

In order to answer the research problem raised, we initially described the profile of the accounting professionals surveyed. Overall, the surveyed sample is made up of women, over 30 and under 50 years old, who majored in Accounting, and have completed or are currently undergoing a graduate program. The study also highlights that the respondents are experienced in their positions, have been working in the accounting area for more than 10 years, and have, in their function, responsibility for data and information.

In order to assess the determinants of GDPL compliance among accounting professionals, we performed structural equation modeling. In the multivariate analysis, the personal behaviors and attitudes construct revealed significant and positive influence for GDPL compliance, demonstrating that it is a determinant and validating the first hypothesis. When analyzing the construct of governance mechanisms for data security, the results were significant and the third hypothesis was also accepted. Thus, governance mechanisms exert a positive influence for GDPL compliance with accounting professionals.

As for the education dimension, the results were not significant, not supporting the second research hypothesis. Hence, the data on this construct confirmed the descriptive statistics and showed that this is still a factor to be developed by accounting organizations. These entities, despite

trying to comply with the law, do little to encourage training and capacity building, and the professionals also do not try to do it themselves.

Therefore, we found that the constructs of personal behaviors and attitudes, for the security of data and information in the workplace, and governance mechanisms, for the security of personal data and information, are determinants of GDPL compliance. In light of this, the overall objective of analyzing the determinants for GDPL compliance among accounting professionals was achieved. It is worth noting that in the validated model, personal behaviors and attitudes and governance mechanisms showed 26% explanatory power for GDPL compliance among accounting professionals.

This research presents practical and scientific contributions, since it is an unprecedented approach and fills a gap in the accounting area, helping in the understanding of the accounting professional's behavior in face of a new legal basis. It also opens up discussions on the subject and encourages the accounting professional to improve and seek knowledge regarding the security of data and personal information. Furthermore, we see potential contributions for educational institutions, class associations, and entities in the sector, since the survey on this category's situation in light of the GDPL becomes a relevant contribution.

The limitations of this research include the scarcity of studies on the subject, especially for the accounting area, precisely because it is a recent law, which made it difficult to discuss the results. It also corresponds to a limiting factor the variables and constructs developed, since there may be other influencers for GDPL compliance that we may not have considered. In addition, it is difficult to estimate the size of the population of professionals in the accounting area in a conclusive way. It is worth mentioning that the research was limited to a cross-section and that the collection was restricted to Brazilian accounting professionals. Finally, the survey's lack of control over the size of the companies in which the surveyed professionals work may have some bearing on the lack of significance of the education construct.

Therefore, for future research, we suggest replicating this study to compare the results found here. Moreover, we encourage the application of this validated instrument with professionals in specific areas of accounting, such as auditing, and in other contexts, which aims to stimulate the scientific development of research focused on the protection of personal data and information. Also, we encourage the inclusion of other influencers for GDPL compliance. Furthermore, we suggest repeating the research in a longitudinal manner and replicating the validated instrument in other populations. In addition, one should consider the size of the companies in which the professionals work as a research variable, especially for the education construct.

REFERENCES

Basan, A. P., & Faleiros Jr., J. L. de M. (2020). A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo. *Civilistica.com: Revista Eletrônica de Direito Civil, 9*(3), 1-27.

Buogo, M., Fachinelli, A. C., & Giacomello, C. P. (2019). Gestão do conhecimento e segurança da informação. *Revista AtoZ, 8*(2), 39-59.

Burkart, D. V. V. (2021). *Proteção de dados e o estudo da LGPD.* Dissertação (Pós-graduação em Mídia e Tecnologia), Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, SP.

Carvalho, L. P, Oliveira, J., Cappelli, C., & Majer, V. (2019). Desafios da transparência pela Lei Geral de Proteção de Dados Pessoais. *Anais do Workshop de Transparência em Sistemas,* Porto Alegre: Sociedade Brasileira de Computação, 21-30, 7. Recuperado de https://sol.sbc.org.br/index.php/wtrans/ article/view/6438/6334

Celidonio, C., Neves, P. S., & Doná, C. M. (2020). Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - um estudo de caso. *Brazilian Journals of Business, 2*(4), 3626-3648.

Chin, W. W. (2010). *How to Write Up and Report PLS Analyses.* In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.). *Handbook of Partial Least Squares: Concepts, Methods and Applications.* Springer: Heidelberg, Dordrecht, London, New York, 655-690.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2a ed.). New York: Psychology Press.

Falcão, C. M. R., & Keller, E. Z. (2021) Terceirização do tratamento de dados – a relação entre controlador e operador. In A. P. M. C. Lima, M. Crespo, P. P. Pinheiro. (coord.). *LGPD aplicada.* São Paulo: Atlas.

Fontes, E. (2008). *Praticando a segurança da informação* (1a ed.). Rio de Janeiro: Brasport.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Frazão, A., Oliva, M. D., & Abilio, V. S. (2019). *Compliance* de dados pessoais. In G. Tepedino, A. Frazão, & M. S. Oliva (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Thomson Reuters.

Hair Jr, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Análise multivariada de dados* (6a ed.). Porto Alegre: Bookman.

Hair Jr., J. F., Gabriel, M. L. S. S., & Patel, V. K. (2014). Modelagem de Equações Estruturais Baseada em Covariância (CB-SEM) com o AMOS: Orientações sobre a sua aplicação como uma Ferramenta de Pesquisa de Marketing. *Revista Brasileira de Marketing, 13*(2), 44-55.

Hair Jr., J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM).* Los Angeles: Sage publications.

Hair Jr., J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2-24.

Herath, H. S. B. (2011). Cybersecurity: An Emerging Area for Collaborative Post-Modern Management Accounting Research. *Journal of Cost Management, 25*, 14-27.

Kanaane, R. (2017). *Comportamento humano nas organizações: o desafio dos líderes no relacionamento intergeracional* (3a ed.). São Paulo: Atlas.

Kohls, C., Dutra, L. H., & Welter, S. (2021). *LGPD: da teoria a implementação nas empresas*. SP: Rideel.

Lei n. 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

Lopes, L. F. D., Chaves, B. M., Fabricio, A., Almeida, D. M., Obregon, S. L., Lima, M. P., Silva, W. V., Camargo, M. E., Veiga, C. P., Moura, G. L., Silva, L. S. C. V., & Costa, V. M. F. (2020). Analysis of Well-Being and Anxiety among University Students. *Int. J. Environ. Res. Public Health, 17*(3874), 1-23.

Lóssio, C. J. B., & Santos, C. A. A. C. (2021). A confidencialidade e a Lei Geral de Proteção de Dados. In A. P. M. C. Lima, M. Crespo, & P. P. Pinheiro (coord.). *LGPD aplicada*. São Paulo: Atlas, Cap. 1, 17-23.

Moraes, M. C. B. (2019). LGPD: um novo regime de responsabilização civil dito proativo. *Civilistica.com: Revista Eletrônica de Direito Civil*, *8*(3), 1-6.

Marques, L. N. (2020). *O mapeamento do modelo data management maturity (dmm) à Lei Geral de Proteção de Dados (LGPD).* Trabalho de Conclusão de Curso, Pontifícia Universidade Católica de Goiás, Goiás, Goiânia, GO, Brasil.

Mendes, L. S. (2019). Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Revista Panorama Setorial da Internet*, *11*(2), 1-20.

Migliorini, I. B., & Rocha, E. (2019). Estudo de viabilidade sobre a utilização do blockchain na Contabilidade. *CAFI: Revista Contabilidade, Atuária, Finanças & Informação*, *2*(1), 99-111.

Miragem, B. (2019). A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais Online, 1009*, 1-35.

Nascimento, T. F. do, Frogeri, R. F., & Prado, L. A. (2019). Gestão de Segurança da Informação no Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo Brasileiro. *Revista de Sistemas e Computação, 9*(1), 189-210.

NBC PG 01: código de ética profissional do contador (2019). Recuperado de https://cfc.org.br/tecnica/normas-brasileiras-de-contabilidade/nbc-pg-geral/.

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: issues and applications*. Thousand Oaks: Sage.

Pimenta, A. M. S., & Quaresma, R. F. C. (2016). A segurança dos sistemas de informação e o comportamento dos usuários. *Journal of Information Systems and Technology Management*, *13*(3), 533-552.

Pinheiro, P. P. (2020). *Proteção de dados pessoais: comentários à Lei n. 13.709/2018* (2a ed.). São Paulo: Saraiva Educação.

Ribeiro, R., Krüger, C., Michelin, C. de F., & Raddatz, J. C. (2020). Cibersegurança e segurança da informação contábil: uma análise da percepção do profissional contábil. *RAGC: Revista de Auditoria, Governança e Contabilidade, 8*(32), 71-85.

Ribeiro, F. R. P., & Moreira, C. (2021). A percepção dos profissionais da área contábil e dos gestores sobre os impactos da implementação da LGPD. *RAGC: Revista de Auditoria, Governança e Contabilidade*, Monte Carmelo, *9*(39), 119-134.

Ringle, C. M., Silva, D., & Bido, D. S. (2014). Modelagem de equações estruturais com utilização do SmartPLS. *REMark - Revista Brasileira de Marketing, 13*(2), 56-73.

Ringle, C. M., Wende, S., & Becker, J.M. (2015). *SmartPLS 3*. Boenningstedt: SmartPLS GmbH. Recuperado de http://www.smartpls.com.

Rosa, J. C. (2021). *Abusividade contratual na era digital sob a ótica do código de defesa do consumidor: aspectos teóricos, práticos e reflexos da LGPD* (1a ed.). Dialética.

Teves, D. M. (2019). *A proteção de dados pessoais: o novo paradigma jurídico*. Dissertação (Mestrado em Ciências Econômicas e Empresariais), Universidade dos Açores, Ponta Delgada.

Santos, L. T. F., & Tabosa, M. C. O. (2020). O mercado contábil e os novos rumos da contabilidade: uma análise da percepção dos alunos concluintes. *Revista Campo do Saber, 6*(2), 80-95.

Scherer Filho, J. L. (2020). *Tratamento de dados em sistemas de informações contábeis a partir da lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais): um estudo multicaso*. Trabalho de Conclusão de Curso em Ciências Contábeis, Universidade de Caxias do Sul, Caxias do Sul.

Schirmer, D. L., & Thaines, A. H. (2021). A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos contabilistas do Vale do Paranhana/RS. *Revista Eletrônica de Ciências Contábeis, 10*(1), 31-56.

Silva, W. L. (2011). *Segurança da informação: um estudo sobre a percepção do usuário da informação contábil*. Dissertação (Mestrado em Ciências Contábeis), Universidade Presbiteriana Mackenzie, SP.

Siqueira, O. N., Contin, A. C., Barufi, R. B., & Lehfeld, L. S. (2021). A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. *Revista Eletrônica Pesquiseduca, 13*(29), 236-255.

Willemsen, B. (2019). *Gartner IT Symposium*/Xpo 2019™. *Simpósio,* São Paulo, SP. Recuperado de http://www.gartner.com/br/symposium

Zanatta, R. A. F. (2015). A proteção de dados entre leis, códigos e programação: os limites do marco civil da internet. In N. de Lucca, A. Simão Filho, C. R. Pereira de Lima (coord.). *Direito & Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, 447-470.