RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

The adequacy of small businesses to the General Data Protection Law and the limits of the simplified regime for small processing agents

Ricardo Mussi Pereira Paiva
Bachelor of Laws from the Pontifical Catholic University of Paraná (PUCPR). Specialist in Tax Law and Tax Procedural Law from PUCPR. Improvement in Civil Procedural Law from the Brazilian Institute of Legal Studies (IBEJ). Postgraduate student in Real Estate Law from PUCPR. Lawyer registered with the Brazilian Bar Association, Paraná Section.

ABSTRACT
This article analyzes the differentiated regime established by ANPD Resolution No. 2/2022 for smallscale processing agents and examines whether its flexibilities foster effective compliance of micro and small enterprises with the Brazilian General Data Protection Law or instead create a false perception that legal obligations have been waived. The research is qualitative, theoretical and exploratory, combining a literature review, a documentary analysis of Brazilian legislation and of the European Union General Data Protection Regulation, and a reading of secondary data from the survey Privacy and Personal Data Protection 2023, conducted by the Brazilian Network Information Center. The theoretical framework connects the conceptual path from privacy to data protection, risk-based regulation and the principle of accountability. The data show that the adoption of compliance measures by enterprises with 10 to 49 employees is roughly half, or less, of that observed in larger firms. The normative analysis shows that the simplified regime reduces formalities while preserving principles, legal bases and data subject rights, and excludes high-risk processing. The study concludes that simplification is legally sound but insufficient without support instruments such as templates, sector guidance and codes of conduct developed by representative associations.
Keywords: Personal data protection. LGPD. Small-scale processing agents. Risk-based regulation. Micro and small enterprises.

1 INTRODUCTION

Law No. 13,709/2018, known as the General Law for the Protection of Personal Data, applies to any personal data processing operation carried out by an individual or by a legal entity governed by public or private law in the cases provided for in its article 3, except for the exceptions of article 4, without any distinction of size (BRASIL, 2018). The breadth of the field of application is consistent with the nature of the protected right, elevated to the status of a fundamental right by Constitutional Amendment No. 115/2022, but creates a considerable challenge for micro and small companies, which process data from customers, suppliers, and employees in their routine and rarely have personnel specialized in privacy or information security. The legislator recognized this problem by attributing to the National Data Protection Authority the competence to issue simplified and differentiated rules for microenterprises, small businesses, and startups, a competence exercised through Resolution CD/ANPD No. 2/2022.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

The existence of a simplified regime raises, however, an issue that goes beyond the description of its rules. A poorly understood flexibility can be interpreted by small entrepreneurs as a general exemption from legal obligations, when, in fact, the resolution itself preserves the principles, legal bases and rights of the holders and excludes high-risk activities from the benefit. This possible distance between the normative text and its practical reception justifies an investigation that combines the examination of the norm with the theoretical literature on data protection and regulation, and with the available empirical data on the degree of adequacy of Brazilian companies.

The objective of this article is to assess whether the differentiated regime established by Resolution CD/ANPD No. 2/2022 contributes to the effective compliance of micro and small companies with the General Law for the Protection of Personal Data or if it creates a false perception of exemption. The working hypothesis is that simplification is legally adequate, as it is aligned with the logic of risk-based regulation, but that it is not enough, by itself, to overcome the material and cognitive limitations of these businesses. The text is organized into six development sections, which deal with the theoretical foundations of data protection, risk-based regulation, the simplified regime, the empirical portrait of adequacy, the limits of flexibility, and the European counterpoint, followed by the conclusions.

2 METHODOLOGY

The research adopts a qualitative approach, of a theoretical nature and exploratory and descriptive character. The problem investigated involves the interpretation of standards, the reconstruction of concepts and the evaluation of the coherence between the theoretical foundations of data protection and the regulatory choices made for smaller companies, which favors analytical and argumentative reasoning to the detriment of the statistical measurement itself. This does not prevent the use of secondary quantitative data, which were incorporated to illustrate the degree of adequacy of Brazilian companies and to test, albeit indirectly, the plausibility of the hypothesis.

The technical procedures combine literature review, document analysis, and secondary data reading. The literature review focused on reference works on privacy and data protection, such as Warren and Brandeis (1890), Westin (1967), Doneda (2006), Mendes (2014), Nissenbaum (2004), Solove (2013), and Bioni (2019), and on studies on regulation and compliance, such as Black and Baldwin (2010), Gellert (2020), Quelle (2018), Bamberger and Mulligan (2015), and Waldman (2020). The documentary analysis covered Law No. 13,709/2018 and its amendments, Constitutional Amendment

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

No. 115/2022, Resolutions CD/ANPD No. 2/2022, No. 4/2023 and No. 15/2024, the authority's guidance guide for small-sized agents, the authority's first sanctioning decision, Regulation (EU) 2016/679, the documents of the Article 29 Working Party and the reports and proposals of the European Commission.

The empirical data were extracted from the publication Privacy and Protection of Personal Data 2023, by the Information and Coordination Center of Ponto BR, which presents indicators on actions to adapt to the law by company size (NIC.BR, 2024). Six indicators were selected from the group of actions for adequacy, chosen because they correspond to obligations or good practices directly related to the flexibilities of the resolution, such as the appointment of the person in charge, the service channel for data subjects, and the incident policy. The percentages were reproduced without any additional statistical treatment and organized in a graph in section 6.

The study recognizes three limitations. The first is that the survey by the Information and Coordination Center of Ponto BR covers companies with ten or more employed persons, so that microenterprises with fewer employees, which make up a significant portion of the universe of small agents, are not represented in the indicators. The second is that the cut by number of employed persons does not coincide with the criterion of gross revenue adopted by Complementary Law No. 123/2006 and by the resolution. The third stems from the regulatory dynamics, since the Brazilian authority and the European institutions frequently review their acts, which requires considering the versions in force at the time of writing.

3 FROM PRIVACY TO THE PROTECTION OF PERSONAL DATA

The legal construction of privacy is usually based on the essay by Warren and Brandeis (1890), published in the Harvard Law Review, which defended the existence of a right to be left alone in the face of the diffusion of instant photography and the sensationalist press. The formulation had an essentially negative and individualistic character, as it protected the intimate sphere against intrusions by others. Westin (1967) offered, almost eight decades later, a more adequate conception of the information society by defining privacy as the intention of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to third parties. The transition from an idea of recollection to an idea of control over the flow of information prepared the ground for the autonomous legal discipline of data protection. In Brazil, Doneda (2006) reconstructed this trajectory and demonstrated that the protection of personal data is

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

not to be confused with the traditional protection of intimacy and private life, because it deals with the processing of information in organized systems and the consequences of this treatment for the personality. Mendes (2014) deepened the argument by arguing that data protection constitutes a new fundamental right, whose structure is close to the informational self-determination recognized by the German Federal Constitutional Court in the 1983 census decision, and by examining its articulation with consumer protection. These works anticipated the normative recognition that would come later, in the general law itself and, later, in the constitutional text, and remain as references for the interpretation of the Brazilian system.

Recognition at the constitutional level occurred in two stages, one jurisprudential and the other legislative. In 2020, the Federal Supreme Court, when endorsing the precautionary measure in Direct Action of Unconstitutionality No. 6,387, suspended the effectiveness of a provisional measure that determined the sharing of data of telephone users with the Brazilian Institute of Geography and Statistics and recognized data protection as an autonomous fundamental right (BRASIL, 2020b). In 2022, Constitutional Amendment No. 115 included in article 5 of the Constitution item LXXIX, which ensures, under the terms of the law, the right to the protection of personal data, including in digital media, and attributed to the Federal Government the exclusive competence to legislate on the matter (BRASIL, 2022a). The consequence for companies of any size is clear, as the obligations of the general law now materialize a fundamental right, which limits the margin for flexibilities that empty protection.

Contemporary literature, however, warns that the model centered on individual control has limits. Solove (2013) demonstrated that the self-management of privacy, based on notices and consent, faces cognitive problems, because data subjects do not read or understand policies, and structural problems, because the number of agents and the aggregation of data make it impossible to make a rational assessment of each choice. Bioni (2019) examined the function and limits of consent in the Brazilian context, and his analysis helps to understand why the general law, by providing ten legal bases in article 7, did not make consent the only basis for processing and attributed to agents a relevant part of the responsibility for protection. Nissenbaum (2004), in turn, proposed understanding privacy as contextual integrity, according to which an information flow is adequate when it respects the norms of the context in which the data was originally shared.

These theoretical contributions have a direct consequence for the subject of this study. If protection cannot rest only on the control exercised by the data subject, it depends to a large extent on the conduct of those who process the data, which includes the small business that maintains customer records, the

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

office that keeps medical records, and the service provider that manages the payroll of its employees. The work coordinated by Tepedino, Frazão, and Oliva (2019) highlights the extent of the repercussions of the law on different branches of private law, which reinforces the perception that data protection is not a topic restricted to technology companies. The challenge, therefore, is to demand from small agents a level of care compatible with the fundamental right at stake without imposing structures that they are unable to maintain.

4 RISK-BASED REGULATION AND ACCOUNTABILITY

The institutional response to the limit of the individual control model was the strengthening of the obligations of processing agents, organized around two concepts, that of responsibility and accountability and that of risk-based approach. The Article 29 Working Party, a European advisory body that preceded the European Data Protection Committee, maintained in its Opinion 3/2010 that the principle of accountability requires the controller to adopt appropriate and effective measures to apply the principles of data protection and to be able to demonstrate this application when requested (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2010). Brazilian law incorporated this idea in article 6, item X, which deals with responsibility and accountability as a principle, and in article 50, which provides for rules of good practices and privacy governance programs (BRASIL, 2018).

The risk-based approach is rooted in the theory of regulation. Black and Baldwin (2010) described risk-based regulation as a strategy that organizes the regulator's actions based on the assessment of the risks that regulated agents pose to the objectives of public policy, concentrating resources where the potential for damage is greatest. The same authors, in a previous work, proposed a more demanding version of responsive regulation, which considers not only the behavior of the regulator, but also its culture, the institutional context, the performance of the regime itself, and changes in the environment (BALDWIN; BLACK, 2008). Applied to data protection, this logic suggests that the intensity of obligations should vary according to the risk that each processing operation represents for the data subjects.

In the specific field of data protection, the Article 29 Working Party made an important warning in its 2014 statement about the role of the risk-based approach. The document stated that this approach cannot be used to disregard the rights of data subjects or fundamental principles, which must be respected regardless of the level of risk, and that it applies above all to the calibration of accountability

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

obligations, such as documentation, impact assessments and security measures (ARTICLE 29 DATA PROTECTION WORKING PARTY,
2014). Gellert (2020) examined this construction in depth and argued that data protection can be understood as a risk regulation regime, which requires specifying in what sense the notion of risk is used in each obligation of the regulation, to prevent it from being used as a generic justification to reduce protection.

Quelle (2018) pointed out the risk embedded in this architecture. According to the author, the risk-based approach can move data protection away from the logic of merely formal compliance and closer to the substantive protection of fundamental rights, but only if it is well applied by those responsible and control authorities, since it depends on those responsible themselves raising their compliance standards based on the evaluation of their activities. When this assessment is done poorly, the flexibility that should qualify protection can result in insufficient measures, which reinforces the importance of the authority's supervision and guidance. This point is particularly sensitive for small companies, which tend to be less able to interpret open concepts such as large scale, relevant risk, or adequate security measures.

The empirical research by Bamberger and Mulligan (2015) on privacy management in large companies in five countries helps to understand what is at stake. The authors found that countries with more open rules and active authorities, such as Germany and the United States, produced corporate privacy practices that were more integrated into the business than countries with more detailed rules, such as France and Spain, where a logic of formal compliance predominated. The result suggests that principle-based norms favor the internalization of protection when there are professionals capable of translating these principles into practices. In small companies, where these professionals rarely exist, the same openness can generate paralysis or improvisation, which makes support and guidance instruments even more necessary.

5 THE SIMPLIFIED REGIME OF RESOLUTION CD/ANPD NO. 2/2022

The legal basis of the differentiated regime is in article 55-J, item XVIII, of Law No. 13,709/2018, which assigns to the national authority the competence to issue simplified and differentiated rules, guidelines, and procedures, including deadlines, so that micro-enterprises, small businesses, and business initiatives of an incremental or disruptive nature that declare themselves startups or innovation companies can comply with the law. Article 41, paragraph 3, complements this provision

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

by authorizing the authority to establish hypotheses for exemption from the appointment of the person in charge according to the nature and size of the entity or the volume of processing operations (BRASIL, 2018). The National Data Protection Authority was created by Law No. 13,853/2019 (BRASIL, 2019), and the administrative sanctions of the law only began to be applied on August 1, 2021, by virtue of Law No. 14,010/2020 (BRASIL, 2020a).

Article 2 of Resolution CD/ANPD No. 2, of January 27, 2022, defines small-sized processing agents as micro-enterprises, small-sized businesses, startups, private legal entities, including non-profit entities, natural persons, and depersonalized private entities that process personal data as controllers or operators (BRASIL, 2022b). The classification of micro and small businesses follows the criteria of Complementary Law No. 123/2006, which sets the limits of annual gross revenue at BRL 360,000.00 and BRL 4,800,000.00, respectively, including individual microentrepreneurs (BRASIL, 2006). Startups follow the criteria of Complementary Law No. 182/2021 (BRASIL, 2021). Article 5 of the resolution determines that the agent must prove its classification within fifteen days when requested by the authority.

The exclusions are as relevant as the benefit itself. Under the terms of article 3, agents who carry out high-risk treatment, those who have gross revenue higher than the legal limits, and those who belong to an economic group in fact or in law whose global revenue exceeds these limits cannot use the differentiated regime. Article 4 defines high-risk treatment based on the cumulative presence of at least one general criterion and one specific criterion. The general criteria are large-scale processing and processing that may significantly affect the interests and fundamental rights of the data subjects. Specific criteria include the use of emerging or innovative technologies, surveillance or control of areas accessible to the public, decisions made solely based on automated processing, and the use of sensitive data or data of children, adolescents, and the elderly (BRASIL, 2022b).

The flexibilities themselves focus on documentation, governance, and deadline obligations. Article 9 allows for the simplified registration of processing operations, according to the model to be provided by the authority. Article 11 dispenses with the appointment of the person in charge, but requires the provision of a communication channel with the data subject, and considers voluntary indication a policy of good practices. Arts. 12 and 13 determine the adoption of essential administrative and technical security measures and allow for a simplified information security policy, which will be considered by the authority for the purposes of the principle of accountability and the dosimetry of sanctions. Article 14 grants a double period for the assistance of data subjects, for the communication of security incidents, except when there is potential compromise to the physical or moral integrity of

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

the data subjects or to national security, and for the presentation of information and documents requested by the authority, and article 15 allows the delivery of a simplified statement to the data subject within fifteen days (BRASIL, 2022b).

The resolution contains two clauses that function as safeguards for the system. Article 6 establishes that the flexibility does not exempt agents from complying with the other provisions of the general law, including the legal bases and principles, and article 16 authorizes the authority to require compliance with the obligations waived or relaxed when the nature, volume of the operations or the risks to the holders so recommend (BRASIL, 2022b). The authority also published, even before the resolution, an information security guideline aimed at these agents, with low-complexity administrative and technical measures and a checklist (AUTORIDADE NACIONAL DE PROTECÇÃO DE DADOS, 2021). The general design thus reveals a clear choice, which simplifies the form of compliance without changing the essential content of the protection.

6 THE EMPIRICAL PORTRAIT OF THE ADEQUACY OF SMALL BUSINESSES

The literature on small business management offers a key to reading the difficulties of adaptation. Welsh and White (1981) characterized the small business by the condition of poverty of resources, which involves limited capital, dependence on the owner's time and attention, and greater vulnerability to external changes, and concluded that the management practices of large organizations cannot be simply reduced in scale. Data protection exemplifies this problem well, because its obligations require legal knowledge, technical competence in information security, and documentation capacity, attributes that, in larger companies, are usually distributed among specialized departments and, in smaller ones, fall on the owner himself or on an employee with other attributions. Data from the Privacy and Protection of Personal Data 2023 survey allow us to observe this difference precisely. Among the companies that maintain data on individuals, only 28% of those with 10 to 49 employed persons declared that they had prepared a compliance or adequacy plan, against 53% of companies with 50 to 249 employed persons and 58% of those with 250 or more. The appointment of a person in charge was informed by 16% of the smallest, 35% of the medium, and 43% of the large ones, and the offer of a service channel to the holders by 17%, 38%, and 44%, respectively (NIC.BR, 2024). In another indicator of the same survey, 22% of the companies with 10 to 49 employed persons said they have a specific area or employees responsible for the topic, a proportion that reaches 56% among those with 250 or more.

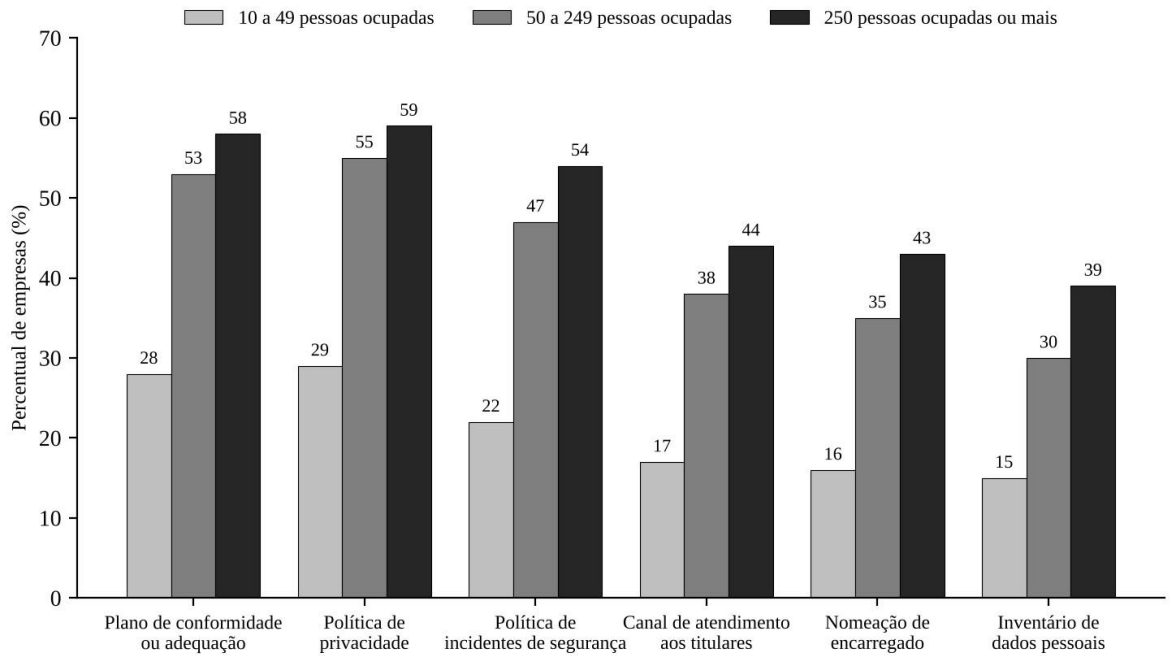
This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

Figure 1 brings together six of these indicators and shows a consistent pattern. In all the selected actions, the proportion observed in companies with 10 to 49 employed persons corresponds to about half of that recorded in companies with 50 to 249 employed persons and to something between 37% and 49% of that verified in companies with 250 or more, and the most pronounced difference appears between the smaller group and the intermediate group, and not between the latter and large companies. This result suggests the existence of an organizational threshold, from which the company has sufficient structure to incorporate data protection routines. It is important to remember, as recorded in the methodology, that the survey does not reach companies with less than ten employed persons, which allows us to suppose that the real picture of microenterprises is even less favorable.

Figure 1 – Companies that maintain data on individuals, by type of action to adapt to the LGPD and size (%)



Source: prepared by the author based on NIC.br (2024), XP12 indicator, data from TIC Empresas 2023. Base: companies with 10 or more employed persons that maintain data on individuals.

The international literature encountered similar difficulties after the entry into force of the European regulation. Sirur, Nurse, and Webb (2018) conducted semi-structured interviews with twelve heads of security, governance, technology, and policies of organizations of different sizes, including six small and medium-sized companies, and found that large organizations and small companies with a

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

focus on security considered compliance reasonable and achievable, while small companies without this specialization had difficulty in making a satisfactory attempt at compliance. Among the obstacles reported were the breadth of the regulation, the translation of qualitative requirements into concrete actions, the mapping of data flows, budget and personnel constraints, and exposure to unreliable consultants. The similarity with the Brazilian data indicates that the problem stems less from national particularities and more from the structure of small organizations.

The European Commission reached a compatible conclusion in its evaluation report of two years of application of the regulation. The document recognized that the application of the rules can be particularly difficult for small and medium-sized enterprises, especially due to the proportionally higher costs, and suggested practical instruments, such as models for recording processing activities, models of contracts with operators, seminars, service channels, and codes of conduct adapted to this audience (EUROPEAN UNION, 2020). The same report warned, however, that the risk-based approach does not justify exemptions based only on the size of the company, because size, by itself, does not indicate the level of risk that a processing represents for data subjects. This warning will be taken up again in the analysis of the limits of the Brazilian regime.

7 SIMPLIFIED DOES NOT MEAN DISMISSED

The distance between the flexibility of the resolution and the perception of total dismissal can be explained, in part, by the way regulation is received in organizations. Waldman (2020), supported by Edelman's (2016) theory of legal endogeneity, argues that the effectiveness of privacy laws is often compromised when organizations themselves start to define what it means to comply with the law, converting substantive obligations into formal procedures and façade documentation. In large companies, this phenomenon is manifested by the proliferation of compliance policies and tools. In small companies, the risk is the opposite and consists of interpreting the absence of formal requirements, such as the dismissal of the person in charge or the simplification of registration, as the absence of substantive obligations.

The first sanction applied by the Brazilian authority to a private agent illustrates this point. In a decision published in the Federal Official Gazette in July 2023, the General Coordination of Inspection applied to Telekall Infoservice, a microenterprise in the telemarketing sector, a warning for violation of article 41 of the law, which deals with the person in charge, and two simple fines of BRL 7,200.00 each, one for the violation of article 7, which regulates the legal bases of the processing,

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

and another for the violation of article 5 of the Inspection Regulation, regarding the duty to comply with the authority's requests (BRASIL, 2023b). The case shows that the size does not prevent sanctioning and the warning regarding the person in charge applied to a microenterprise suggests that the classification in the differentiated regime is not automatic, and must be verified in light of the hypotheses of exclusion and the nature of the treatment.

The law's sanctions system reinforces this reading. Article 52 provides for a warning, a simple fine of up to 2% of the legal entity's revenue in Brazil in its last fiscal year, limited to R$50,000,000.00 per infraction, publicity of the infraction, blocking and deletion of data, among other penalties. Its paragraph 1 determines that dosimetry considers, among other criteria, the economic condition of the offender, the repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage, and the adoption of a policy of good practices and governance (BRASIL, 2018). The Dosimetry Regulation, approved by Resolution CD/ANPD No. 4/2023, detailed the application of these criteria (BRASIL, 2023a), and the simplified security policy provided for in article 13 of the resolution on small agents was expressly linked to them.

The subsequent regulation confirms that simplification operates on deadlines and forms, and not on the existence of obligations. The Security Incident Communication Regulation, approved by Resolution CD/ANPD No. 15/2024, set a general deadline of three business days for reporting incidents that may entail relevant risk or damage to the authority and to the holders, except for the double deadline provided for small agents (BRASIL, 2024). In other words, the microenterprise that suffers a relevant leak continues to be obliged to report it, only with a longer deadline, and even loses this benefit when the incident may compromise the physical or moral integrity of the holders (BRASIL, 2022b). Likewise, the dismissal of the person in charge does not eliminate the duty to comply with the requests of the holders, who continue to require some effective communication channel.

The most delicate point of the regime is on the border of high risk. As the specific criteria include the processing of sensitive data and data of children, adolescents, and the elderly, many small businesses may be outside the regime without realizing it. Clinics, offices, laboratories, gyms, language schools, and establishments aimed at children or the elderly routinely process data of this nature, and the presence of a general criterion, such as the possibility of significantly affecting the rights of data subjects, completes the classification as high risk (BRASIL, 2022b). Quelle (2018) had already warned that the risk-based approach depends on the agents themselves correctly evaluating their

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

activities, and this warning applies especially strongly to companies that do not have specialized advice to interpret open criteria.

8 THE EUROPEAN COUNTERPOINT AND THE PATHS TO PROPORTIONAL GOVERNANCE

Regulation (EU) 2016/679 adopted a different strategy from the Brazilian one. Instead of creating a specific statute for small companies, the regulation maintained the same obligations for all those responsible and introduced specific adjustments. Recital 13 encourages the institutions and bodies of the Union, as well as the Member States and their control authorities, to take into account the specific needs of micro, small and medium-sized enterprises, and arts. 40 and 42 provide that codes of conduct and certification mechanisms consider these needs. The obligation to appoint a person in charge, provided for in article 37, does not depend on the size, but on the nature of the person in charge and the activities, and is required of public authorities and bodies and, in the private sector, when the main activities involve regular and systematic large-scale monitoring or large-scale processing of special categories of data (EUROPEAN UNION, 2016).

The only derogation expressly linked to carrying is that of article 30, paragraph 5, which exempts organizations with less than 250 employees from the registration of processing activities, except when the processing is likely to entail a risk to the rights and freedoms of the data subjects, is not occasional or covers special categories of data or data relating to criminal convictions (EUROPEAN UNION, 2016). In practice, as almost every business processes data on a non-occasional basis, the derogation had limited scope. In May 2025, the European Commission presented a proposal to amend the regulation that extends this exemption to organizations with less than 750 employees and conditions it only to the absence of high risk (EUROPEAN UNION, 2025), and its legislative outcome has yet to be monitored. The proposal reveals that even the European model, which is more resistant to exemptions for carrying, has come to admit the need to alleviate documentary burdens. The comparison between the two systems shows advantages and risks in each choice. The Brazilian model offers greater security to small entrepreneurs, who find in a single standard the

set of applicable flexibilities, but uses size as the main criterion for access to the benefit, which is far from the European Commission's warning that size does not indicate risk. The Brazilian resolution partially compensates for this weakness by excluding high-risk activities and allowing the authority to require the obligations waived. The European model is more consistent with the logic of risk, but

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

less accessible to those who do not have advice, since it requires the small responsible person to interpret open concepts such as large scale and occasional treatment.

The literature suggests that the solution lies not only in the design of obligations, but in the instruments that translate principles into practices. Bamberger and Mulligan (2015) showed that open standards produce good results when there are professionals and networks capable of building shared understandings of what the law requires. For small companies, which do not have these professionals, the same function can be performed by representative entities. Resolution CD/ANPD No. 2/2022, in its article 8, allows small agents to organize themselves through representative entities to negotiate, mediate, and reconcile claims from data subjects (BRASIL, 2022b), and article 50 of the general law allows the formulation of rules of good practices by associations (BRASIL, 2018).

These provisions pave the way for proportional governance, built collectively and sectorally. Trade associations, employers' unions, and entities that support entrepreneurship can develop registration models, privacy and security policies adapted to each segment, offer shared service channels, and promote periodic training, reducing costs that would be prohibitive for each company alone. The European Commission has recommended a similar path when defending codes of conduct adapted to small and medium-sized enterprises (EUROPEAN UNION, 2020). A strategy of this type is compatible with the responsive regulation proposed by Baldwin and Black (2008), as it combines guidance, cooperation, and supervision, and reserves the sanction for cases in which compliance is not sought in good faith.

9 CONCLUSION

The study was based on the hypothesis that the differentiated regime established by Resolution CD/ANPD No. 2/2022 is legally adequate, but insufficient to ensure the effective compliance of micro and small companies with the General Law for the Protection of Personal Data. Theoretical, normative, and empirical analysis confirmed this hypothesis. The resolution coherently simplifies formal obligations, but Brazilian and international experience shows that the difficulty for small companies lies less in the number of formal requirements and more in the ability to understand and apply substantive requirements.

The conceptual trajectory from privacy to data protection, reconstructed from Warren and Brandeis, Westin, Doneda and Mendes, demonstrates that the current discipline protects an autonomous fundamental right, today expressly provided for in article 5, item LXXIX, of the Constitution. Solove

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

and Bioni's criticisms of the consent-centered model, added to Nissenbaum's proposal of contextual integrity, reinforce that protection depends above all on the conduct of the processing agents, the which includes small businesses and limits the scope for flexibilities that reduce the content of protection.

Risk-based regulation and the principle of accountability offer the appropriate theoretical basis for grading obligations according to the potential for damage of each activity. The warning of the Article 29 Working Party that principles and rights of data subjects cannot be set aside by risk is reflected in article 6 of the Brazilian resolution, which preserves the legal bases and principles. The analyses of Gellert and Quelle show, however, that the notion of risk needs to be carefully delimited and that its effectiveness depends on the assessment made by the agents themselves, which makes the guidance of the authority indispensable.

The examination of Resolution CD/ANPD No. 2/2022 revealed a careful normative design, which defines the beneficiaries, excludes high-risk activities and economic groups with higher revenues, concentrates flexibilities on documentation, person in charge, security, and deadlines, and reserves to the authority the power to demand the obligations waived. The simplification falls on the form of compliance, and not on the existence of the duty to protect the personal data processed by the company. This choice is compatible with the logic of risk-based regulation, as long as the boundary between common processing and high-risk processing is understood by the agents themselves.

Data from the Privacy and Personal Data Protection 2023 survey showed that companies with 10 to 49 employed persons adopt adequacy measures in a proportion equivalent to about half, or less, of that observed in larger companies, in all actions analyzed, and that the biggest jump occurs in the group of 50 to 249 employed persons. As the survey does not cover companies with less than ten employed persons, it is reasonable to assume that the picture of microenterprises is even more fragile, which confirms the relevance of the problem investigated.

The analysis of the limits of the regime indicated that the main threat to effectiveness is the mistaken perception that simplified means waived. The first sanction of the Brazilian authority, applied to a microenterprise, and the maintenance of the duty to report incidents within only double the period demonstrate that the essential obligations remain. The high-risk frontier, which reaches any business that deals with sensitive data or data of children and the elderly with the potential to significantly affect the holders, requires special attention from sectors such as health, education, and services to the vulnerable public.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

The European counterpoint showed that the European Union regulation avoided broad exemptions based on size and preferred specific adjustments, consistent with the logic of risk, but less accessible to small parents. The 2025 proposal to expand the exemption from registration indicates, on the other hand, that the pressure for documentary relief also exists in that system. The two models converge on the need for practical support instruments, such as adapted models, guides, and codes of conduct, and on the perception that the simple reduction of requirements is not enough for small organizations to achieve an adequate level of protection.

As a contribution, the study proposes that the effectiveness of the Brazilian regime depends on three complementary fronts, which are the continuous production of models and sectoral guides by the authority, the performance of representative entities in the elaboration of rules of good practices, under the terms of article 50 of the law and article 8 of the resolution, and the training of small entrepreneurs to recognize when their activities constitute high risk. As a research agenda, it is recommended the inclusion of companies with less than ten employed persons in the national surveys and the monitoring of the authority's inspection of small agents.

REFERENCES

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 3/2010 on the principle of accountability**. WP 173. Brussels, 13 July 2010.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Statement on the role of a risk-based approach in data protection legal frameworks**. WP 218. Brussels, 30 May 2014.

NATIONAL DATA PROTECTION AUTHORITY (Brazil). **Guideline**: information security for small processing agents. Brasília, DF: ANPD, 2021.

BALDWIN, Robert; BLACK, Julia. Really responsive regulation. **The Modern Law Review**, Oxford, v. 71, n. 1, p. 59-94, 2008.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. **Privacy on the ground**: driving corporate behavior in the United States and Europe. Cambridge, MA: MIT Press, 2015.

BIONI, Bruno Ricardo. **Personal data protection**: the function and limits of consent. Rio de Janeiro: Forense, 2019.

BLACK, Julia; BALDWIN, Robert. Really responsive risk-based regulation. **Law & Policy**, Oxford, v. 32, n. 2, p. 181-213, 2010.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

BRAZIL. Complementary Law No. 123, of December 14, 2006. Establishes the National Statute of Micro and Small Enterprises. **Federal Official Gazette**: section 1, Brasília, DF, Dec. 15. 2006.

BRAZIL. Law No. 13,709, of August 14, 2018. General Law for the Protection of Personal Data (LGPD). **Federal Official Gazette**: section 1, Brasília, DF, 15 Aug. 2018.

BRAZIL. Law No. 13,853, of July 8, 2019. Amends Law No. 13,709, of August 14, 2018, to provide for the protection of personal data and to create the National Data Protection Authority. **Federal Official Gazette**: section 1, Brasília, DF, July 9, 2019. 2019.

BRAZIL. Law No. 14,010, of June 10, 2020. Provides for the Emergency and Transitional Legal Regime of Private Law Legal Relations (RJET) in the period of the coronavirus pandemic (Covid-19). **Federal Official Gazette**: section 1, Brasília, DF, June 12, 2020a.

BRAZIL. Federal Supreme Court (Full Court). **Referendum on the Precautionary Measure in Direct Action of Unconstitutionality 6.387/DF.** Rapporteur: Justice Rosa Weber, May 7, 2020b.

BRAZIL. Complementary Law No. 182, of June 1, 2021. Establishes the legal framework for startups and innovative entrepreneurship. **Federal Official Gazette**: section 1, Brasília, DF, June 2, 2021.

BRAZIL. Constitutional Amendment No. 115, of February 10, 2022. Amends the Federal Constitution to include the protection of personal data among the fundamental rights and guarantees and to establish the exclusive competence of the Union to legislate on the protection and processing of personal data. **Federal Official Gazette**: section 1, Brasília, DF, 11 Feb. 2022a.

BRAZIL. National Data Protection Authority. Resolution CD/ANPD No. 2, of January 27, 2022. Approves the Regulation for the application of Law No. 13,709, of August 14, 2018, General Law for the Protection of Personal Data (LGPD), for small processing agents. **Federal Official Gazette**: section 1, Brasília, DF, p. 6, 28 Jan. 2022b.

BRAZIL. National Data Protection Authority. Resolution CD/ANPD No. 4, of February 24, 2023. Approves the Regulation on Dosimetry and Application of Administrative Sanctions. **Federal Official Gazette**: section 1, Brasília, DF, 2023a.

BRAZIL. National Data Protection Authority. General Coordination of Inspection. **Administrative sanctioning proceeding No. 00261.000489/2022-62**. Fine: Telekall Infoservice. Decision published in the Official Gazette of the Union, Brasília, DF, July 6. 2023b.

BRAZIL. National Data Protection Authority. Resolution CD/ANPD No. 15, of April 24, 2024. Approves the Security Incident Communication Regulation. **Federal Official Gazette**: section 1, Brasília, DF, April 26, 2024.

DONEDA, Danilo. **From privacy to the protection of personal data**. Rio de Janeiro: Renovar, 2006.

EDELMAN, Lauren B. **Working law**: courts, corporations, and symbolic civil rights. Chicago: University of Chicago Press, 2016.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

GELLERT, Raphaël. **The risk-based approach to data protection**. Oxford: Oxford University Press, 2020.

MENDES, Laura Schertel. **Privacy, data protection and consumer protection**: general lines of a new fundamental right. São Paulo: Saraiva, 2014.

NIC.BR. **Privacy and personal data protection 2023**: perspectives of individuals, companies and public organizations in Brazil. São Paulo: Internet Steering Committee in Brazil, 2024.

NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review**, Seattle, v. 79, n. 1, p. 119-157, 2004.

QUELLE, Claudia. Enhancing compliance under the General Data Protection Regulation: the risky upshot of the accountability- and risk-based approach. **European Journal of Risk Regulation**, Cambridge, v. 9, n. 3, p. 502-526, 2018.

SIRUR, Sean; NURSE, Jason R. C.; WEBB, Helena. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *In*: INTERNATIONAL WORKSHOP ON MULTIMEDIA PRIVACY AND SECURITY, 2., 2018, Toronto. **Proceedings** [...]. New York: ACM, 2018. p. 88-95.

SOLOVE, Daniel J. Privacy self-management and the consent dilemma. **Harvard Law Review**, Cambridge, MA, v. 126, n. 7, p. 1880-1903, 2013.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **General Law for the Protection of Personal Data and its repercussions on Brazilian law**. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN UNION. 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). **Official Journal of the European Union**, Luxembourg, L 119, pp. 1-88, 4 May 2016.

UNIÃO EUROPEIA. Comissão Europeia. **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition**: two years of application of the General Data Protection Regulation. COM(2020) 264 final. Brussels, 24 June 2020.

UNIÃO EUROPEIA. Comissão Europeia. **Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures**. COM(2025) 501 final. Brussels, 21 May 2025.

WALDMAN, Ari Ezra. Privacy law's false promise. **Washington University Law Review**, St. Louis, v. 97, n. 3, p. 773-834, 2020.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.

RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 09/02/2026 | Accepted: 10/07/2026 | Published: 11/12/2026

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Cambridge, MA, v. 4, n. 5, p. 193-220, 1890.

WELSH, John A.; WHITE, Jerry F. A small business is not a little big business. **Harvard Business Review**, Boston, v. 59, n. 4, p. 18-32, jul./ago. 1981.

WESTIN, Alan F. **Privacy and freedom**. New York: Atheneum, 1967.

This is an article published in open access under the CreativeCommons Attribution license, which allows use, distribution and reproduction in any medium, without restriction as long as the original work is correctly cited.